Історико-політичні проблеми сучасного світу: Збірник наукових статей. – Чернівці: Чернівецький національний університет, 2020. – Т. 42. – С. 160-172
DOI: 10.31861/mhpi2020.42.160-172

Modern Historical and Political Issues: Journal in Historical & Political Sciences. – Chernivtsi: Chernivtsi National University, 2020. – Volume. 42. – pp. 160-172
DOI: 10.31861/mhpi2020.42.160-172

УДК 327.88:316.772.23(438)

© Оксана Звоздецька [1]

Протидія дезінформаційним впливам у національному просторі Республіки Польща

В статті авторка досліджує неетичне використання інформаційного простору для маніпулятивного впливу на особистість, і посилення такої діяльності під час виборчих кампаній. В цьому контексті наводяться статистичні дані досліджень, які проводилися в Польщі та в ЄС щодо загроз маніпулювання та дезінформування в інформаційному просторі, результати опитування поляків про те, хто повинен боротися з явищем фальшивих новин, а також дані опитування з проблеми розрізнення факту від думки, некритичністю підходу до вмісту, опублікованого в Інтернеті.

Дослідниця підкреслює, що як наслідок, у Польщі все більше засобів масової комунікації запускають послуги, що здійснюють перевірку фактів. Також в останні роки в Польщі спостерігається посилення реагування з боку державних структур на загрози дезінформації та маніпуляції: інтенсивна співпраця та координація діяльності ключових інститутів інформаційної безпеки держави.

Ключові слова: дезінформація, пропаганда, Республіка Польща, ЄС, боротьба з дезінформацією, фактчетинг.

Countering Disinformation Influences in the National Space of the Republic of Poland

The body of the article goes on to disclose the problem of the impact of digital technologies and media on democracy, its grounds and values. The author addresses the problem of the broad using of cutting-edge technology in Poland by those in power, serving their goals and posing a clear threat to democratic outcomes, in particular during the election campaigns.

Furthermore, the author states that through advanced technological capacity and the use of highly targeted behavior modification techniques, different governmental institutions have been applying new and more-sophisticated forms of propaganda and disinformation enabling deepfakes, trolls, bots – artificial intelligence technology and other malicious software so that to refine and shape public opinion with an easy reach and power.

In this context, the findings of the research, conducted in Poland and the EU, on the threats of hostile social manipulation and disinformation in the information space are significant, whereas the poll results testify to the Poles' concerns about who is supposed to be in control of efficient debunking 'fake news' as well as their aspirations to be internet-literate in terms of deepfakes. The author concludes by arguing that well-informed societies are more resistant to being encroached and manipulated, and a quick and effective joint reply to potential threats requires strategic mass communication.

The researcher emphasizes that recently in Poland Mass Communication have launched fact-checking services, in particular several Polish fact-checking projects set up designing websites that provide fact-checking. Regrettably, so far none of the Polish platforms has been involved in closer international cooperation in the framework of the European initiatives.

Several landmark studies observed that Poland has also failed to create a common front in countering disinformation even during the elections. Each organization works according to its own vision of solving the problem. However, in recent years in Poland there has been a tendency of developing the

[1] Кандидат історичних наук, доцент кафедри міжнародної інформації Чернівецького національного університету імені Юрія Федьковича, Україна. E-mail: o.zvozdecka.chnu.edu.ua; http://orcid.org/0000-0003-2623-7615.

government agencies' capacity to strengthen their response to the threats of disinformation and manipulation: namely, the state key institutions for cyber security successfully implemented their cooperation and coordination initiatives.

Key words: disinformation, propaganda, Republic of Poland, EU, debunking 'fake news', fact-checking outlets.

«Критичний розум є ключовим інструментом у всі часи,
але особливо важливий у період масової дезінформації»[2]

Постановка проблеми. Становлення та розвиток глобальних інформаційних потоків, в контексті останніх інформаційних революцій, значно збільшили можливість комунікаційної присутності однієї держави на території іншої. Інформаційний простір європейських країн все більше наповнюється змістом, який не є характерним для духовних, ціннісних, моральних орієнтирів її внутрішніх комунікаторів. Відповідно до цього, виникають інформаційні загрози, сформовані деструктивними інформаційними потоками, створення яких відбувалось за межами власного інформаційного простору.

Деструктивні інформаційні впливи (пропаганда, маніпуляція, дезінформація, фейки, цензура) є гібридними загрозами, які є формою ворожих дій, що здійснюється нижче порогу відкритої війни. Основна їх мета – викликати дестабілізацію, а також породжувати нові конфлікти або посилювати існуючі. Боротьба, яка ведеться в сфері інформації, може бути спрямована як на заклик до соціальних заворушень так і дестабілізацію політичної, соціальної, фінансової чи економічної системи. Державна боротьба з деструктивними інформаційними впливами пов'язана з небезпеками, які спрямовані на уряд та суспільство; телекомунікації, критичні інфраструктури та несанкціонований доступ до таємної інформації.

Особливої актуальності дана проблематика набуває в межах відкритого національного інформаційного простору, оскільки це дозволяє зарубіжним суб'єктам не тільки поширювати деструктивну інформацію, а й впливати на загальну можливість її функціонування. Коли руйнується простір для демократичного, публічного дискурсу, суспільство стає розпорошеним і ним легше маніпулювати за допомогою політики поділу та перемоги. Також, ситуація погіршується і завдяки інформаційному впливу Росії, яка намагається посилити існуючі протиріччя в польському суспільстві за допомогою поширення дезінформації. «Жорсткі» інформаційні впливи, що спрямовані на підрив супротивника на сьогодні, не є новиною; але «набір інструментів» для дезорінтації об'єкту впливу, який включає численні, часто латентні, та явні інструменти, продовжує зростати, особливо гостро це на собі відчула Україна в умова ведення гібридної війни на Сході.

Забезпечення національної безпеки держави вимагає постійного моніторингу існуючих загроз, реалізації відповідних механізмів захисту, впровадження інструментів протидії та здійснення превентивних заходів щодо їх попередження. Тому проблема боротьби з дезінформацією, пропагандою, фейками, інформаційним маніпулюванням є на сьогодні надзвичайно актуальним як для Польщі так і для всього Європейського Союзу.

Аналіз останніх досліджень та публікацій. Торкнемося лише окремих аспектів, що висвітлені в роботах польських дослідників. Зокрема в статті фахівця з питань комунікацій та сучасних технологій Науково-академічної комп'ютерній мережі (NASK) Рафала Бабрая (Rafał Babraj) проаналізовано причини поширення дезінформаційних операцій, зародження та розвиток фактчетингу, як методу боротьби з дезінформацією в світі та Польщі[3].

Не можна оминути, на нашу думку, також дослідження відомого польського політолога, перекладача, експерта з питань безпеки на пострадянському просторі Центру східних досліджень у Варшаві Йоланти Дарчевської (Jolanta Darczewska), котра у своїй статті акцентує увагу на тому, що дезінформуючи та маніпулюючи реальністю, Москва проводить довгострокову діяльність з дестабілізації, розпалюючи конфлікти між окремими країнами НАТО та ЄС, підриваючи

[2] Akademia Fact-Checking, 2020. Dostępny: <https://akademia.demagog.org.pl/> [Data przeglądu 10 czerwca 2020].

[3] Babraj, Rafał, 2019. «Czym jest fact-checking? – Zarys inicjatyw na świecie i w Polsce». NASK CyberPPOLICY. 14 października. Dostępny: <https://cyberpolicy.nask.pl/czym-jest-fact-checking-zarys-inicjatyw-na-swiecie-i-w-polsce/> [Data przeglądu 10 czerwca 2020].

демократичний виборчий процес та європейську систему цінностей, послаблюючи інтеграційний проект ЄС та трансатлантичне співробітництво, виправдовуючи своє право побудувати власну сферу впливу в Європі[4]. Все більше і більше країн відчувають наслідки цих дій для національної безпеки, спонукає країни НАТО та ЄС розробити попереджувальні механізми для виявлення та протидії загрозі.

Серед вітчизняних дослідників можна виокремити статті Р. Черниша («Правовий досвід країн Європейського Союзу у сфері протидії поширенню фейкової інформації», DOI: 10.32849/2663-5313/2019.10.21), котрий констатує, що в країнах ЄС розпочали активно розроблятися саме правові механізми протидії поширенню фейкової інформації, та М.Н. Алексеева («Протидія кібернетичним загрозам у Польщі: досвід для України», DOI: 10.33099/2304-2745/2018-3-64/49-53), в якій автор аналізує кроки збройних сил Республіки Польща щодо формування захисту кіберпростору та ставлення керівництва Міністерства національної оборони Польщі до цієї проблеми.

Метою дослідження є висвітлення існуючих механізмів протидії деструктивним інформаційним впливам на рівні державних та громадських установ Польщі. Для досягнення поставленої мети у роботі було визначено *наступні завдання*: проаналізувати існуючі загрози в польському інформаційному просторі, зокрема, поширення дезінформації, пропаганди, фейку; простежити рівень поінформованості громадян Польщі та ЄС щодо розуміння наявних загроз та охарактеризувати боротьбу з дезінформацією з боку державних. громадських структур.

Виклад основного матеріалу. Точність інформації є важливим фактором для якості наших знань про навколишній світ, явища та процеси, що в ньому відбуваються. Створюючи повідомлення на основі суміші істини та вигадки, ми впливаємо на здатність сприймати об'єктивну реальність. Процес глобалізації та доступу до ЗМІ впливають на залежність одержувача від засобів передачі інформації, даних, що надаються численними інформаційними центрами. Ці центри формують думки, погляди на світ та цінності суспільства. Джерелом влади є не тільки доступ до інформації, але й можливість її інтерпретації чи маніпуляції[5].

Цифрова революція, що триває, тобто розвиток Інтернету та швидке поширення соціальних медіа спричинили те, що традиційні ЗМІ втратили своє значення. Тепер інформацію може публікувати кожен: громадянин-журналіст, блогер чи впливовий користувач, використовуючи соціальні ЗМІ. В той же час, не всі ці люди повинні мати відповідні компетенції або професійну етику. У сучасному потоці інформації час публікації часто важливіший, ніж надійність повідомлення. Більше того, сам процес публікації часто не має елементу двоступеневої перевірки, що було одним із стандартів, що діють у традиційних ЗМІ.

Роль користувачів Інтернету трансформувалась як і нові засоби масової інформації. Вони вже не є лише одержувачами повідомлень, але мають безпосередній вплив на їх поширення. Ділячись або коментуючи вибраний вміст – збільшують їх охоплення, а це певним чином впливає на прибуток, отриманий від реклами. Як результат, пріоритетом часто є доставка «клікального» вмісту, тобто контенту, який дозволить досягти максимально можливого прибутку.

Виявилося, що нове інформаційне середовище може бути використане для того, щоб чинити набагато серйозніший вплив, ніж ми очікували. Інтернет та соціальні медіа все частіше використовуються неетично, і посилення такої діяльності було особливо помітним під час виборчих кампаній. Постійне оцифрування та прогресивна мережа інформаційного середовища робить Інтернет основним полем дезінформаційної діяльності. Технічні можливості, що збільшують лавину неправдивої інформації, дозволяють ефективно використовувати мережу за допомогою, наприклад, тролів, ботів – зомбі-мереж та інших видів зловмисного програмного забезпечення, що використовуються для ведення активної діяльності в інформаційному середовищі. На думку польського дослідника Бабрая Рафала, «збільшення цього «віртуального» потенціалу дезінформування є результатом глобалізації, що прогресує (широкий доступ до мережі та пов'язане з

[4] Darczewska, Jolanta, 2017. «Dezinformacja – rosyjska broń strategiczna– Ośrodek Studiów Wschodnich». Biuletyn analityczny Rządowe Centrum Bezpieczeństwa, Numer 19, pp. 6-8. Dostępny: <https://rcb.gov.pl/wp-content/uploads/BIULETYN-ANALITYCZNY-nr-19.pdf> [Data przeglądu 18 czerwca 2020].

[5] Araźna, Marzena, 2015. «Conflicts of the 21st century based on multidimensional warfare– «hybrid warfare», disinformation and manipulation». Security and Defence Quarterly, issue 8 (3), p. 124. Available at: <doi: https://doi.org/10.5604/23008741.1189421> [Accessed 25 April 2020].

цим явище так званого астротурфінгу[6]), низькі експлуатаційні витрати та високий прибуток, анонімність користувачів (кожен має право коментувати та висловлювати свої погляди), недостатня компетентність користувачів у сфері медіаосвіти, нещільна правова система, що залишає багато сфер мережевої діяльності поза законом (darknet), що суттєво перешкоджає ефективному, швидкому та законному запобіганню дезінформації в Інтернеті»[7].

За оцінкою аналітика з питань технології та демократії у Freedom House Еллі Функ (Allie Funk) та наукового директора з питань технологій та демократії у Freedom House Адріана Шахбаза (Adrian Shahbaz), свобода Інтернету все більше знижується в останні роки, завдяки перетворенню платформ соціальних медіа на інструменти політичного впливу та суспільного контролю. Крім того, вражаюча кількість урядів застосовує передові інструменти для ідентифікації та моніторингу користувачів у величезному масштабі. Те, що колись було технологією свободи, стало каналом для спостереження та маніпуляцій під час виборів. «Соціальні медіа дозволяють звичайним людям, громадським групам та журналістам за будь-яку ціну охоплювати широку аудиторію, й і одночасно вони також надають недорогу платформу для операцій із деструктивним впливам як іноземних, так і вітчизняних акторів. Політичні лідери наймають людей, щоб вони штучно формували думки в Інтернеті в 38 з 65 країн, що досліджуються в цьому звіті – новий максимум» – відзначають автори дослідження[8].

Окрім сприяння поширенню пропаганди та дезінформації в періоди виборів, платформи соціальних медіа дали змогу збирати та аналізувати велику кількість даних про цілі групи населення. Складний масовий нагляд, який колись був можливий лише для провідних світових спецслужб, тепер доступний для більш широкого кола держав. Навіть у демократичних країнах такий масовий моніторинг поширюється на урядові установи та використовується для нових цілей без належних гарантій. Результатом цього є різке глобальне зростання зловживань громадянськими свободами та скорочення в Інтернеті простору громадянської активності. З 65 країн, оцінених у цьому звіті, у рекордних 47 представлені арешти користувачів за політичну, соціальну чи релігійну активність[9]. Польський соціолог, радник президента Республіки Польща Анджея Дуди Анджей Зібертович (Andrzej Zybertowicz) відзначив, що «соціальні медіа, нажаль, сьогодні працюють інакше, ніж очікувалося. Існує переконання, що вони є інструментами дезінформації, а не пояснення світу. Соціальні медіа більше вносять розбрат між людьми, ніж допомагають їм спілкуватися»[10].

Дезінформація на сьогодні є дуже популярною темою. Зростаюча обізнаність ЗМК, а отже, і одержувачів сприяє дискусіям на цю тему. Для оцінки небезпеки дезінформування суспільства, необхідно чітко дати визначення цьому феномену. Дезінформація – одна з гібридних загроз, яка є формою ворожих дій, що здійснюється нижче порогу відкритої війни. Основна його мета – викликати дестабілізацію, а також породжувати нові конфлікти або посилювати існуючі. Боротьба, яка ведеться в сфері інформації, може бути спрямована на: заклик до соціальних заворушень та дестабілізацію політичної, соціальної, фінансової чи економічної системи. Державна боротьба з дезінформацією пов'язана з небезпеками, які спрямовані на уряд та суспільство; телекомунікаційні пристрої, мережі та несанкціонований доступ до секретної інформації[11].

---

[6] Астротурфінг (англ. astroturfing) – це створення штучної громадської думки за допомогою гласних чи негласних заходів, форм та методів впливу зацікавленими іноземними спеціальними службами, окремими організаціями, групами та особами, що використовують програмне забезпечення або наймають представників засобів масової інформації, блогерів, інтернет-коментаторів, спеціалістів з метою витіснення думки реальних людей і створення враження, наче велика кількість людей вимагає чогось конкретного або виступає проти чого-небудь.

[7] Babraj, Rafał, 2019. Op. cit.

[8] Shahbaz, Adrian and Funk, Allie, 2019. «The Crisis of Social Media» Freedom on the Net, p. 1. Available at: <https: //www.freedomonthenet.org/report/freedom-on-the-net/2019/the-crisis-of-social-media> [Accessed 25 April 2020].

[9] Ibid.

[10] Zybertowicz, Andrzej, 2017. «Internet to narzędzie dezinformacji». PolskieRadio24.pl2017. Dostępny: <https://www.polskieradio24.pl/130/6409/Artykul/1962714,Andrzej-Zybertowicz-Internet-to-narzedzie-dezinformacji> [Data przeglądu 02 czerwca 2020].

[11] Araźna, Marzena, 2015. «Conflicts of the 21st century based on multidimensional warfare– «hybrid warfare», disinformation and manipulation». Security and Defence Quarterly, issue 8 (3), p. 122. Available at: <doi: https://doi.org/10.5604/23008741.1189421> [Accessed 25 April 2020].

У міждисциплінарному дослідженні «Феномен дезінформації в епоху цифрової революції. Держава. Суспільство. Політика. Бізнес», поняття «дезінформації» в інформаційному середовищі (здійснена іншим державним чи недержавним актором) визначається: «як навмисно шкідливе і неетичне досягненням цілей, використовуючи всі інструменти, включаючи протизаконні. Це може стосуватися будь-якої сфери діяльності держави, яка є об'єктом дезінформації, з особливим акцентом на безпеку (оборона, внутрішня безпека), економіку (включаючи енергетичну безпеку та постачання стратегічної сировини), позицію на міжнародній арені (включаючи довіру та позицію на переговорах), відносини держави з громадянами (включаючи основні демократичні цінності, такі як виборчі механізми та прозорість діяльності державних структур) використання інформаційного середовища (одержувачів контенту) як вирішального інструменту для тиску на органи управління»[12].

«Дезінформація» – відрізняється від традиційної форми пропаганди. Її мета – не переконувати а підривати. Польська дослідниця Йоланта Дарчевська (Darczewska, Jolanta) у своїй роботі відзначає, що «дезінформація трактується в Росії як зброя в інформаційному протистоянні із Заходом та інструмент впливу, індоктринації та дестабілізації суспільств противника. Це безперервний процес, що складається із системної інтегрованої державної діяльності на багатьох фронтах, що ведеться через різні канали (дипломатичний, політичний, економічний, військовий, соціальний, ЗМК), відповідно до цілей та принципів стратегічного планування»[13].

У звіті американського Центру аналізу європейської політики[14] (The Center for European Policy Analysis CEPA) «Перемога в інформаційній війні» 2017 р. відзначалося, що російська інформаційна війна становить серйозну загрозу для Сполучених Штатів та їх європейських союзників, передусім таких держав як Польща, країни Балтії, Чехія, Словаччина та Україна. Як і у Польщі, так і у Чехії та Словаччині, Росія поширює «токсичні меми», які не створюють нових повідомлень, але націлені посилити існуючу напруженість і розбіжності в польському суспільстві. Коли руйнується простір для демократичного, публічного дискурсу, суспільство стає розпорошеним і ним легше маніпулювати за допомогою політики поділу та перемоги. Зрештою, Кремль намагається підірвати віру в демократію, посилити ксенофобію і змусити поляків відчути, що вони не схожі на західноєвропейців. Як не парадоксально, кремлівські наративи також прагнуть просувати крайній польський націоналізм – навіть антиросійський націоналізм – з метою зробити Польщу ненадійною та «істеричною» для своїх західних союзників[15].

Крім цього викликають занепокоєння результати опитування поляків про їх думку та спостереження щодо поширення дезінформації в мережі, що було проведене Лабораторією соціальних досліджень Науково-академічної комп'ютерної мережі (Pracownię Badań Społecznych Naukowa i Akademicka Sieć Komputerowa NASK) в березні-квітні 2019 р. за методом CAWI (Computer Assisted Web Interviews) – інтерв'ю (зазвичай у формі анкет), що проводиться через Інтернет. Завдяки спеціалізованому програмному забезпеченню експорт даних після експертизи відбувається дуже швидко, а отже, час очікування звіту короткий. У дослідженні взяли участь 1000 осіб старше 15 років. Керівник Лабораторії Рафал Ланге (Rafał Lange) зазначив, що «відповіді респондентів, отримані в ньому, показують, що велика частина

[12] Wydział Strategii Komunikacyjnej w Centrum Operacyjnym MON, 2019. «Dezinformacja a bezpieczeństwo informacyjne państwa». W Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes, redaktor Wrzosek, Magdalena. S. 12. Warszawa, NASK Państwowy Instytut Badawczy. Dostępny: <https://cyberpolicy.nask.pl/wp-content/uploads/2019/09/Raport_CP_Dezinformacja_ONLINE_s.pdf> [Data przeglądu 02 czerwca 2020].

[13] Darczewska, Jolanta, 2017. «Dezinformacja – rosyjska broń strategiczna– Ośrodek Studiów Wschodnich». Biuletyn analityczny Rządowe Centrum Bezpieczeństwa, Numer 19, p. 6. Dostępny: <https://rcb.gov.pl/wp-content/uploads/BIULETYN-ANALITYCZNY-nr-19.pdf> [Data przeglądu 18 czerwca 2020].

[14] Центр аналізу європейської політики (CEPA) - некомерційний, безпартійний, науково-дослідний інститут державної політики, провідний науково-дослідний інститут, присвячений вивченню країн Центральної та Східної Європи та Росії. Місія Центру – сприяти розвитку економічно живої, стратегічно безпечної та політично вільної Європи з тісними та стійкими зв'язками зі Сполученими Штатами.

[15] Lucas, Edward, 2017. Winning the Information War Redux. Techniques and Counterstrategies to Russian Propaganda in Central and Eastern Europe. Extended and Revised Editio April. Center for European Policy Analysis (CEPA). P. 23. Available at: <https://cepa.ecms.pl/files/?id_plik=4803> [Accessed 25 April 2020].

польських користувачів Інтернету має серйозні проблеми з розмежуванням думок від фактів»[16]. Лише 4,5% респондентів могли правильно відрізнити факт від думки у всіх 7 тестових запитаннях[17].

У поляків є не тільки проблема з розрізненням факту від думки, але й з некритичністю підходу до вмісту, опублікованого в Інтернеті (56% респондентів). Так, 7,9% поляків протягом останніх півроку пересилали інформацію, яка була фальшивою новиною, 11,8% зробили це ненавмисно. Лише 41,6% респондентів за останні 6 місяців перевіряли надійність змісту інформації, розміщеної в Інтернеті. 37,1% визнали, що цього не робили. Майже 25% перевіряє джерело повідомлення, для 24% достатнім доказом є достовірність профілю в соціальних мережах або людини, яка ним керує. Лише 12% респондентів перевіряють обліковий запис електронної пошти, з якого надсилалася інформація[18].

Про загрози маніпулювання та дезінформування в європейському інформаційному просторі повідомляється і у звіті 2019 р. Європейської комісії, яка давно намагається боротися з дезінформацією, що поширюється в ЗМІ та в соціальних мережах. У документі описано масштаб проблеми, яка полягала в поширенні помилкових, оманливих звітів та неправдивих повідомлень перед виборами в Європі. За словами представників Європейської комісії, Польська Республіка була однією з країн, які опинилися на перехресті російської дезінформації перед виборами в Європарламент. Зокрема, єврокомісар з питань безпеки Джуліан Кінг (Julian King) зазначив, що «прокремлівський Sputnik поширював неправдиву інформацію про те, що Польща з часів вступу до ЄС стала більш збіднілою, ніж у епоху комунізму»[19]. Серед розповсюдженої інформації, що піддається маніпулюванню, серед інших, було і твердження, що сам Європейський Союз був побудований на нацистських коренях[20].

Присутність солдатів США та НАТО в даній країні є частим об'єктом дезінформаційних кампаній. Неправдиві повідомлення з цього приводу викликають масу емоцій, завдяки чому можуть охопити широку аудиторію. У 2018 та 2019 рр. у Польщі спостерігали щонайменше такі випадки використання цього сценарію для поширення дезінформації:

- вбивство польського солдата громадянином США під час сварки;
- навчання, під час яких військова поліція та війська, що дислокуються у Польщі, мали евакуювати жителів[21];
- помилкові інтерв'ю та маніпульовані цитати із заяв ключових командирів;
- створення на основі неіснуючих джерел (або не без вказівки на них та анонімних джерел) негативного зображення можливостей Збройних сил Польщі та вигаданих розповідей, що дискредитує фактичну діяльність міністерства, підрозділу, командира;
- висловлювання вигаданих експертів та організацій третього сектору щодо діяльності у сфері оборони[22].

[16] NASK Raport, 2019. Dezinformacja w sieci jest powszechna. Ale weryfikacja jest możliwa. 08.05.2019. Dostępny: <https://www.tvp.info/42533173/raport-nask-dezinformacja-w-sieci-jest-powszechna-ale-weryfikacja-jest-mozliwa> [Data przeglądu 20 lipca 2020].

[17] NASK PBS Raport, 2019. Bezpieczne wybory Badanie opinii o (dez)informacji w sieci. Redakcja: Marcin Bochenek, dr Rafał Lange. Warszawa: NASK Państwowy Instytut Badawczy. Dostępny: <https://www.nask.pl/pl/raporty/raporty/2592,Bezpieczne-wybory-raport-na-temat-dezinformacji-w-internecie.html> [Data przeglądu 25 lipca 2020].

[18] Ibid.

[19] TVP.INFO, 14.06.2019. «Polska na celowniku rosyjskiej dezinformacji – wynika z raportu KE». Dostępny: <https://www.tvp.info/43081474/polska-na-celowniku-rosyjskiej-dezinformacji-wynika-z-raportu-ke>[Data przeglądu 02 czerwca 2020].

[20] Kobla, Michalina, 2019. «Komisja Europejska: Polska była zagrożona prorosyjską dezinformacją przed wyborami do Parlamentu Europejskiego». ANTYFAKE. 15 Czerwca 2019. Dostępny: https://www.antyfake.pl/dezinformacja-wybory-do-pe\> [Data przeglądu 02 czerwca 2020].

[21] InteriaBiznes, 2019. «Reaguj na dezinformację w sieci». 20 maja 2019. Dostępny: <https://biznes.interia.pl/gospodarka/news-reaguj-na-dezinformacje-w-sieci,nId,4195815> [Data przeglądu 10 czerwca 2020].

[22] Wydział Strategii Komunikacyjnej w Centrum Operacyjnym MON, 2019. «Dezinformacja a bezpieczeństwo informacyjne państwa». W Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes, redaktor Wrzosek, Magdalena, s. 14. Warszawa, NASK Państwowy Instytut Badawczy. Dostępny: <https://cyberpolicy.nask.pl/wp-content/uploads/2019/09/Raport_CP_Dezinformacja_ONLINE_s.pdf> [Data przeglądu 02 czerwca 2020].

Низька вартість та потенційний ефект, який може принести дезінформація, демонструє його як один з найефективніших інструментів дестабілізації держави. Ще загрозливішим є той факт що, – це інструмент, проти якого важко захищатись – діяльність в Інтернеті не має кордонів, і закон не є ідеальним у сфері протидії дезінформації. Адже у польському законодавстві немає положень, які безпосередньо регулювали б явище дезінформації в Інтернеті, є статті, що містяться у різних правових актах, які висвітлюють питання доступу до інформації, можливості її розповсюдження та її правдивість[23].

Тому в інформаційному просторі з'являється все більше організацій, які займаються перевіркою фактів. Опитування, проведене Інститутом Пойнтера серед членів Міжнародної мережі фактчекінгу (IFCN), демонструє, що більшість ініціатив такого роду були нещодавно розпочаті, зокрема у 2015-2017 рр. Результатом цієї діяльності є наявність 187 організацій, що перевіряє факти, які працюють у 60 країнах[24].

Все це означає, що нинішня роль ЗМК повинна змінитися. Перевірка інформації, опублікованої в Інтернеті, тобто перевірка фактів, стала новим і надзвичайно важливим завданням журналістів. Користувачі Інтернету також мають такі очікування щодо представників ЗМІ. В опитуванні Євробарометра за 2018 р. 49% користувачі польської мережі вказали, що саме з явищем фальшивих новин повинні боротися журналісти, тоді як 20% зазначили, що керівництво преси та телерадіомовлення несе цю відповідальність. Національні організації (40%) згадуються частіше, ніж установи ЄС (18%), або неурядові організації (22%). Третина (34%) вважає, що громадяни самі повинні діяти, щоб зупинити поширення фальшивих новин, а п'ята частина (18%) вважає, що соціальні мережі в Інтернеті повинні нести цю відповідальність[25].

У Польщі все більше ЗМІ запускають платформи, які займаються верифікацією інформації. Асоціація Demagog – перша організація, що займається фактчетингом у Польщі з квітня 2014 р. Основна мета платформи – покращити якість публічних дебатів, надаючи громадянам об'єктивну та достовірну інформацію. Команда фахівців перевіряє заяви та передвиборчі обіцянки політиків на веб-сайті demagog.org.pl. Вони також поширюють ідею перевірки фактів у Польщі. У рамках боротьби з фальшивими новинами також проводять семінари та реалізовують освітні проекти, орієнтовані на молодих людей, наприклад, Академія перевірки фактів (Akademia Fact-Checkingu). Також, цей інформаційний ресурс є першою факчетинговою організацією, яка з травня 2019 р. є членом Міжнародної мережі перевірки фактів (IFCN), що була заснована Інститутом Пойнтера у вересні 2015 р., яка займається підготовкою журналістів, а також перевіркою фактів[26].

Це, однак, не вичерпує перелік організацій, які з'явилися в Польщі за останні роки:

OKO.press – працює з червня 2016 р. Це найбільш впізнаваний портал, який перевіряє факти та проводить журналістські розслідування. У Facebook у нього понад 250 000 шанувальників, у Twitter 34,3 тис послідовників. Серед платформ, що діють у Польщі, він, найбільше займається аналізом політики[27].

Konkret24.pl – проект, започаткований у жовтні 2018 р. групою TVN. Журналісти не лише перевіряють заяви політиків, вони також перевіряють інформацію у семи категоріях – Польща, Світ, Політика, Наука, Здоров'я, Розваги та Міфи. Користувачі Інтернету можуть також повідомляти про підроблені новини. Проект отримав фінансування в рамках інноваційної програми Google DNI, яка підтримує розвиток якісної журналістики в Інтернеті.

Demaskator24.pl – проект, розпочатий у листопаді 2018 р. інформаційним агентством AIP24 (Polska Press Group). Журналісти та редактори перевіряють суперечливі новини та заяви

[23] Zakrzewski, Patryk, 2018. «Monitoring w obszarze wprowadzania uregulowań prawnych jako metody walki z fałszywymi informacjami w Internecie». Raport, grudzień 2018. Dostępny: <http://obserwatoriumdemokracji.pl/wp-content/uploads/2019/01/Raport-aktualizacja-grudzie%C5%84.pdf> [Data przeglądu 02 czerwca 2020].

[24] Babraj, Rafał, 2019. Op. cit.

[25] Flash Eurobarometer 464. Report, 2018. Fake news and disinformation online Fieldwork. February Publication April 2018. Available at: <https://bezpiecznewybory.pl/raporty/fake-newsy-oraz-dezinformacja-w-sieci> [Accessed 12 April 2020].

[26] Bezpieczne Wybory. Fact Checking, 2 maja 2019. Dostępny: <https://bezpiecznewybory.pl/baza-wiedzy/fact-checking > [Data przeglądu 06 lipca 2020].

[27] Babraj, Rafał, 2019. Op. cit.

політиків. Читачі також мають можливість повідомляти про фальшиві новини. В рамках проекту працює Академія Демаскаторів, яка навчає, як перевірити різні види матеріалів в Інтернеті.

Antyfake – портал перевірки фактів, який веде HGA Media. Створення веб-сайту є опосередкованим результатом журналістського розслідування, яке виявило, що портали HGA Media публікували та поширювали неправдиву інформацію. У той час власник оголосив про запуск платформи для перевірки фактів. Antifake працює з квітня 2019 р. Незважаючи на короткий час роботи, він нараховує понад 12 000 шанувальників у Facebook, при цьому у Twitter – лише 82 особи, котрі підписані на цю платформу[28].

Отже, у Польщі все більше засобів масової інформації запускають свої послуги, що здійснюють перевірку фактів. На жаль, поки що жодна з польських платформ не брала участь у тіснішому міжнародному співробітництві в рамках європейських ініціатив. У Польщі також не вдалося створити спільний фронт у боротьбі з дезінформацією, навіть під час виборів. Кожна організація працює згідно з власним баченням вирішення проблеми. Однак, подальший руйнівний вплив дезінформаційних кампаній та нових загроз, таких як глибинні фейки (DeepFake – підроблені відео), які найбільш небезпечні, може змусити до об'єднання сил усіх організацій, які борються проти фальшивих новин у польському суспільстві.

5 грудня 2018 р. Державний секретар Міністерство дигіталізації (Ministerstwo Cyfryzacji) Кароль Оконьський (Karol Okoński), під час засідання Комітету з питань цифризації, інновації та сучасних технологій (Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii) в своїй доповіді надав роз'яснення щодо розуміння основних понять заявивши, що «під дезінформацією ми розуміємо свідому оперативну діяльність, яка здійснює конкретний вплив. Отже, ми маємо на увазі організовану діяльність, в якій використовуються фейкові новини, але не тільки. Fake news – це також підмножина або одна з методик, що використовуються в дезінформації». Розв'язання даної проблеми, Міністерство дигіталізації вбачає не у прийнятті нових нормативно-правових актів, а в так званих м'яких методах: медіаосвіта, підвищення прозорості в аспекті походження джерел фінансування, підтримка діяльності саморегулювання, що здійснюють інтернет-платформи, а також підтримка журналістів, що пропагують надійні та якісні джерела інформації, введення заходів для виявлення та закриття помилкових облікових записів та боротьби з ботами[29].

Окрім вищезазначених аспектів, боротьба з дезінформацією вимагає всебічного та дуже швидкого реагування з боку державних структур. В останні роки спостерігається інтенсивна співпраця та координація діяльності ключових інститутів інформаційної безпеки держави: Бюро національної безпеки, Міністерства закордонних справ, Міністерства національної оборони, Міністерство внутрішніх справ та управління, Міністерства дигіталізації та Державного центру безпеки. Наступний кроком повинно бути створення стратегічної системи комунікацій на рівні уряду[30].

Першим кроком Польщі у боротьбі з дезінформацією на загальному рівні, тобто користувачами Інтернету, зроблено Міністерством дигіталізації та Науково-академічною комп'ютерною мережею (Naukowa i Akademicka Sieć Komputerowa NASK), яка є державним науково-дослідним інститутом, яким керує Міністерство дигіталізації. Ключовим напрямком діяльності NASK є діяльність, пов'язана із забезпеченням безпеки в Інтернеті. Діяльність цієї структури розпочалася ще в 1991 р., коли у Варшавському університеті було сформовано координуючу команду для розвитку академічних комп'ютерних мереж (Академія комп'ютерної мережі університету Варшави). В 1992 р. на Академію було покладено завдання обробляти імена в домені .pl., а вже в 1993 р. NASK відокремився від Варшавського університету і почав діяти як

[28] Babraj, Rafał, 2019. Op. cit.

[29] Zakrzewski, Patryk, 2018. «Monitoring w obszarze wprowadzania uregulowań prawnych jako metody walki z fałszywymi informacjami w Internecie». Raport, grudzień 2018, s.15. Dostępny: <http://obserwatorium demokracji.pl/wp-content/uploads/2019/01/Raport-aktualizacja-grudzie%C5%84.pdf> [Data przeglądu 02 czerwca 2020].

[30]Wydział Strategii Komunikacyjnej w Centrum Operacyjnym MON, 2019. «Dezinformacja a bezpieczeństwo informacyjne państwa». W Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes, redaktor Wrzosek, Magdalena, s.14. Warszawa, NASK Państwowy Instytut Badawczy. Dostępny: <https://cyberpolicy.nask.pl/wp-content/uploads/2019/09/Raport_CP_Dezinformacja_ONLINE_s.pdf> [Data przeglądu 02 czerwca 2020].

незалежний підрозділ досліджень та розробок. Головною метою діяльності було забезпечення доступу наукових та академічних установ до Інтернету, проведення досліджень щодо використання нових технологій, безпеки мережі та міжнародної співпраці.

1996 р. в рамках NASK в Польщі була створена перша CERT Polska (Комп'ютерна команда реагування на надзвичайні ситуації), яка співпрацювала з міжнародною спільнотою аналітиків з кібербезпеки. CERT Polska визначає, аналізує та допомагає усунути наслідки інцидентів кібербезпеки, а також блокує домени, створені виключно з метою поширення дезінформації[31].

2005 р. NASK став партнером польського Центру безпечного Інтернету (Polskiego Centrum Programu Safer Internet). Програма була ініційована Європейською Комісією з метою навчання дітей та молоді щодо небезпеки доступу до Інтернету та сприяння безпечному та цінному використанню нових технологій. Того ж року NASK розпочав роботу з контактним пунктом для реагування на незаконний та шкідливий вміст в Інтернеті, який зараз працює під назвою Dyżurnet.pl, незалежно від того, чи в Польщі відбуваються вибори, чи вже відбулися[32]. У 2017 р. NASK отримав статус Національного науково-дослідного інституту.

1 серпня 2018 р. Президент Республіки Польща підписав закон «Про національну систему кібербезпеки»[33], імплементуючи до польської правової системи директиву Європейського парламенту та Ради (ЄС) ««Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» 2016 р[34]. (Network and Information Security Directive 2016/1148), або так звана Директива NIS. Цей закон санкціонував діяльність трьох структур на національному рівні, які мають здійснювати реагування на комп'ютерні інциденти та управління ними. Відповідно до термінології, прийнятої в Директиві 2016/1148, вони позначаються як CSIRT (Група реагування на інциденти, пов'язані з комп'ютерною безпекою). У Польщі це відповідно до закону (ст. 26), команда CSIRT Агентства внутрішньої безпеки (Agencja Bezpieczeństwa Wewnętrznego CSIRT GOV), CSIRT NASK – Команда Національного науково-дослідного інституту NASK, та CSIRT MON – Група реагування на інциденти, пов'язані з комп'ютерною безпекою, яка працює на національному рівні, на чолі з Міністром національної оборони (Ministr Obrony Narodowej)[35]. Ці три команди на національному рівні працюватимуть разом для забезпечення послідовної та системної роботи з управління ризиками у сфері кібербезпеки держави та для вирішення повідомлених інцидентів, зокрема серйозних та критичних інцидентів з погляду держави.

CSIRT GOV, тобто урядова команда реагування на комп’ютерні інциденти на чолі з Головою Агенції внутрішньої безпеки, до складу завдань якої входить розгляд або координація протидії інцидентам, про які повідомляють підрозділи сектору державних фінансів, найбільш важливі для роботи державних структур, підрозділи, які підзвітні та під наглядом Прем'єр-міністра, Національного банку Польщі та юридичні особи, на які поширюється дія Закону «Про управління кризовими ситуаціями»[36], тобто суб'єкти, системи ІКТ або ІКТ-мережі, включені до єдиного переліку об'єктів, пристроїв та послуг, що входять до критичної інфраструктури.

---

[31] Rządowe Centrum Bezpieczeństwa, 2019. «Działania Rządowego Centrum Bezpieczeństwa w zakresie przeciwdziałania dezinformacji». W Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes, redaktor Wrzosek, Magdalena, s. 16. Warszawa, NASK Państwowy Instytut Badawczy. Dostępny: https://cyberpolicy.nask.pl/wp-content/uploads/2019/09/Raport_CP_Dezinformacja_ONLINE_s.pdf> [Data przeglądu 02 czerwca 2020].

[32] InteriaBiznes, 2019. «Reaguj na dezinformację w sieci». 20 maja 2019. Dostępny: <https://biznes.interia.pl/gospodarka/news-reaguj-na-dezinformacje-w-sieci,nId,4195815> [Data przeglądu 10 czerwca 2020].

[33] Sejm Rzeczypospolitej Polskiej, 2018. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dziennik Ustaw. 2018 poz. 1560. Dostępny: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf> [Data przeglądu 10 czerwca 2020].

[34] EU. Directive, 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Available at: <https://eur-lex.europa.eu/eli/dir/2016/1148/oj> [Accessed 12 April 2020].

[35] CSIRT NASK, 2020. Dostępny: <https://www.nask.pl/pl/dzialalnosc/csirt-nask/3424,CSIRT-NASK.html> [Data przeglądu 10 czerwca 2020].

[36] Sejm Rzeczypospolitej Polskiej, 2007. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Dziennik Ustaw. 2007, nr 89, poz. 590. Dostępny: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20070890590/T/D20070590L.pdf> [Data przeglądu 25 lipca 2020].

CSIRT MON – це система реагування на комп'ютерні інциденти Міністерства національної оборони. Вона координує розгляд повідомлених інцидентів суб'єктами, які підпорядковуються міністру національної оборони або контролюються ними, та підприємцями, що мають особливе економічне та оборонне значення.

NASK CSIRT курується Науково-академічною комп'ютерною мережею. Реагує на кібератаки у науково-дослідних інститутах, Польському агентстві аеронавігаційних служб або фізичних осіб[37].

Напередодні до місцевих виборів восени 2019 р. за ініціативою Міністерства та NASK було запущено портал *bezpiecznewybory.pl,* що містить інформацію не тільки про те, що таке дезінформація, але і про те, як підтвердити надійність вмісту чи джерела та де повідомляти про інциденти. А також веб-сайт – *MamPrawoWiedziec.pl,* який надає інформацію про досвід, погляди та діяльність осіб, що виконують громадські функції, в т.ч депутати, які представляють Польщу в Європарламенті.

Навмисна дезінформація, розповсюджена ворогом і адресована різним адресатам для дестабілізації внутрішньої ситуації, може призвести до кризи. Ось чому її контролює та аналізує *Державний центр безпеки* (Rządowe Centrum bezpieczeństwa RCB), який є ключовою інституцією системи управління кризовими ситуаціями, створеної для координації запобігання загрозам. У той же час RCB не входить до складу військової системи. Здійснює щомісячний моніторинг безпеки для східного кордону Республіки Польща – зовнішнього кордону ЄС. Матеріал адресований державним керівникам та міністрам та керівникам служб. Він підсумовує ситуацію на державному кордоні з Російською Федерацією, Білорусією та Україною, а також у прикордонних районах. Аналізуються найважливіші дезінформаційні заходи щодо Польщі, спрямовані на формування негативного іміджу Республіки Польща зовні, а також на вплив громадської думки та суспільно-політичних процесів у країні[38].

Фахівці Центру у своєму дослідженні визначають та описують як окремі інциденти, так і дезінформаційні кампанії, що послідовно проводяться зарубіжними центрами на Сході. При цьому вони враховують особливості висловлювань основних учасників таких кампаній (у тому числі провідних політиків), канали розповсюдження неправдивої чи маніпульованої інформації, режим роботи, методи впливу та ступінь організованості дезінформаційних дій[39].

Ще однією державною установою, що працює в цьому напрямку є *Урядова команда з питань врегулювання кризових ситуацій* (Zespół roboczy Rządowego Zespołu Zarządzania Kryzysowego RZZK) – дорадчий та консультативний орган, створений при Раді Міністрів. До свого завдання включають ініціювання та координацію діяльності з управління кризовими ситуаціями. Для ефективного виконання завдань RZZK його голова може створити робочі групи. Дезінформація є одним із предметів роботи робочої групи щодо раннього виявлення гібридних загроз та підтримки координації діяльності в цій галузі. Команда була створена у вересні 2018 р., і до її завдань входять:

- моніторинг гібридних загроз;
- оцінка ризику надзвичайних ситуацій внаслідок гібридної діяльності;
- підготовка пропозицій щодо реагування на гібридні загрози;
- координація державної адміністрації та державних установ та послуги[40].

Окрім державних структур протидією дезінформації в польському інформаційному просторі займаються і неурядові установи, такою організацією в є *Центр аналізу пропаганди та дезінформації* (Centrum Analiz Propagandy i Dezinformacji), що заснований у 2017 р. На веб-сайті фонду зазначається, що він «є першою неурядовою організацією в Польщі, орієнтованою на системний та аналітичний підхід до викликів, пов'язаних із сферою інформаційної та психо-

[37] Sejm Rzeczypospolitej Polskiej, 2018. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dziennik Ustaw. 2018 poz. 1560. Dostępny: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf> [Data przeglądu 10 czerwca 2020].

[38] Rządowe Centrum Bezpieczeństwa (RCB), 2020. Dostępny: <https://rcb.gov.pl/> [Data przeglądu 02 czerwca 2020].

[39] Ibid.

[40] Rządowe Centrum Bezpieczeństwa, 2019. Op. cit.

логічної війни»[41]. Основне завдання Центру полягає в проведенні освітніх, дослідницьких та аналітичних ініціатив, пов'язаних із безпекою інформаційного простору та у сфері протидії пропаганді, дезінформації та інших гібридних загроз. В останніх публікаціях цього центру подається аналіз та протидія хибним наративам про Польщу та поляків у російському інформаційному просторі, аналіз польської системи стратегічної комунікації та кампанії з нагоди 20-ї річниці вступу Польщі в НАТО, інформаційні загрози для Польщі під час виборів у Європарламент.

Ще дві польські неурядові організації, зосереджені на відносинах з Росією та її політиці: *Центр східних досліджень* (Ośrodek Studiów Wschodnich OSW) та *Фонд INFO OPS*, що базуються у Варшаві. OSW створений у 1990 р. та зосередженений на аналізі ключових процесів та подій, що відбуваються в міжнародному середовищі та Польщі. ЇЇ портфель включає Росію, Кавказ та Центральну Азію, Центральну та Східну Європу, країни Балтійського моря (Німеччина, Скандинавія та країни Балтії), а також Китай, Туреччину та Ізраїль. Завданням Центру є моніторинг політичних, соціальних та економічних процесів, пропонування як сучасних, так і поглиблених аналізів для уряду, а також участь у дискусіях в експертних та академічних громадах у Польщі та за кордоном. Для виконання цього завдання працює понад сорок аналітиків[42].

Фонд INFO OPS, заснований у 2015 р. (з 2017 року у складі Фонду з кібербезпеки) фахівцем з безпеки інформаційного середовища, директором цього фонду Камілем Басаєм (Kamil Basaj). INFO OPS здійснює моніторинг соціальних мереж, аналіз інформаційно-психологічних операцій, дезінформації, пропаганди в інформаційному просторі Польщі[43]. Проблематика дослідження Фонду зосереджена на дослідженні радянської та російської дезінформації, невійськових засобах у гібридній війні, інформаційних операціях[44].

Висновки. Отже, варто наголосити на тому, що сьогодні Інтернет став місцем розповсюдження дезінформаційних кампаній, активно використовуються для маніпулятивного впливу на особистість, і посилення такої діяльності особливо є помітним під час виборчих кампаній. Окрім сприяння поширенню пропаганди та дезінформації в періоди виборів, платформи соціальних медіа дали змогу збирати та аналізувати велику кількість даних про цілі групи населення. Результатом цього є різке глобальне зростання зловживань громадянськими свободами та скорочення в Інтернеті простору громадянської активності. Дезінформація може дестабілізувати ситуацію в державі, здійснити руйнівний вплив на її адміністративні структури та структури, що приймають рішення, а також підірвати соціальні, економічні та культурні основи. Особливо коли Російська Федерація намагається посилити існуючі протиріччя в польському суспільстві за допомогою поширення дезінформації.

З метою протидії цим деструктивним впливам в інформаційному просторі Польщі з'являється все більше організацій, які займаються перевіркою фактів. Асоціація Demagog – перша організація, що займається фактчетингом у Польщі, також верифікацією даних займаються ще такі організації як OKO.press, Demaskator24.pl, Antyfake та інші. На жаль, поки що жодна з польських платформ не брала участь у тіснішому міжнародному співробітництві в рамках європейських ініціатив. У Польщі також не вдалося створити спільний фронт у боротьбі з дезінформацією, навіть під час виборів. Кожна організація працює згідно з власним баченням вирішення проблеми.

Окрім вищезазначених аспектів, боротьба з дезінформацією вимагає всебічного та дуже швидкого реагування з боку державних структур. В останні роки спостерігається інтенсивна співпраця та координація діяльності ключових інститутів інформаційної безпеки держави: Бюро національної безпеки, Міністерства закордонних справ, Міністерства національної оборони,

[41] Centrum Analiz Propagandy i Dezinformacji, 2020. Dostępny: <https://capd.pl/pl/>[Data przeglądu 10 czerwca 2020].

[42] Ośrodek Studiów Wschodnich (OSW), 2020. Dostępny: <https://www.osw.waw.pl/en/o-nas> [Data przeglądu 02 czerwca 2020].

[43] Fundacja Bezpieczna Cyberprzestrzeń, 2017. «InfoOps – Projekt badań nad zjawiskiem manipulowania polskim środowiskiem informacyjnym». Lut 22, 2017. Dostępny: <https://www.cybsecurity.org/pl/infoops-projekt-badan-nad-zjawiskiem-manipulowania-polskim-srodowiskiem-informacyjnym/> [Data przeglądu 10 czerwca 2020]

[44] Ibid.

Міністерство внутрішніх справ та управління, Міністерства Оцифрування та Державного центру безпеки. Наступний кроком повинно бути створення стратегічної системи комунікацій на рівні уряду.

References

1. Akademia Fact-Checkingu Raport, 2018. Praw(n)y sierpowy w starciu z fake newsem. Monitoring w obszarze wprowadzania uregulowań prawnych jako metody walki z fałszywymi informacjami w Internecie. grudzień 2018. redaktor Zakrzewski. Dostępny: <http://obserwatoriumdemokracji.pl/wp-content/uploads/2019/01/Raport-aktualizacja-grudzie%C5%84.pdf> [Data przeglądu 06 lipca 2020].
2. Akademia Fact-Checking, 2020. Dostępny: <https://akademia.demagog.org.pl/> [Data przeglądu 10 czerwca 2020].
3. Analysis: EC intervention over Polish presidential election likely, 13.04.2020. Available at: <https://polandin.com/47550324/analysis-ec-intervention-over-polish-presidential-election-likely> [Accessed 12 April 2020].
4. Analysis: EU Commission's challenge to Polish election is partisan, 24.04.2020. Available at: <https://polandin.com/47726239/analysis-eu-commissions-challenge-to-polish-election-is-partisan> [Accessed 25 April 2020].
5. Araźna, Marzena, 2015. «Conflicts of the 21st century based on multidimensional warfare– «hybrid warfare», disinformation and manipulation». Security and Defence Quarterly, issue 8 (3), pp. 103–129. Available at: <doi: https://doi.org/10.5604/23008741.1189421> [Accessed 25 April 2020].
6. Babraj, Rafał, 2019. «Czym jest fact-checking? – Zarys inicjatyw na świecie i w Polsce». NASK CyberPpolicy. 14 października. Dostępny: <https://cyberpolicy.nask.pl/czym-jest-fact-checking-zarys-inicjatyw-na-swiecie-i-w-polsce/> [Data przeglądu 10 czerwca 2020].
7. Bezpieczne Wybory. Fact Checking, 2 maja 2019. Dostępny: <https://bezpiecznewybory.pl/baza-wiedzy/fact-checking> [Data przeglądu 06 lipca 2020].
8. Centrum Analiz Propagandy i Dezinformacji, 2020. Dostępny: <https://capd.pl/pl/>[Data przeglądu 10 czerwca 2020].
9. CSIRT NASK, 2020. Dostępny: <https://www.nask.pl/pl/dzialalnosc/csirt-nask/3424,CSIRT-NASK.html> [Data przeglądu 10 czerwca 2020].
10. Darczewska, Jolanta, 2017. «Dezinformacja – rosyjska broń strategiczna– Ośrodek Studiów Wschodnich». Biuletyn analityczny Rządowe Centrum Bezpieczeństwa, Numer 19, pp. 6-8. Dostępny: <https://rcb.gov.pl/wp-content/uploads/BIULETYN-ANALITYCZNY-nr-19.pdf> [Data przeglądu 18 czerwca 2020].
11. EU. Directive, 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Available at: <https://eur-lex.europa.eu/eli/dir/2016/1148/oj> [Accessed 12 April 2020].
12. Flash Eurobarometer 464. Report, 2018. Fake news and disinformation online Fieldwork. February Publication April 2018. Available at: <https://bezpiecznewybory.pl/raporty/fake-newsy-oraz-dezinformacja-w-sieci> [Accessed 12 April 2020].
13. Freedom House Report, 2020. Freedom in the World 2020. A Leaderless Struggle for Democracy. Democracy and pluralism are under assault. Available at: <https://freedomhouse.org/report/freedom-world/2020/leaderless-struggle-democracy/> [Accessed 12 April 2020].
14. Fundacja Bezpieczna Cyberprzestrzeń, 2017. «InfoOps – Projekt badań nad zjawiskiem manipulowania polskim środowiskiem informacyjnym». Lut 22, 2017. Dostępny: <https://www.cybsecurity.org/pl/infoops-projekt-badan-nad-zjawiskiem-manipulowania-polskim-srodowiskiem-informacyjnym/> [Data przeglądu 10 czerwca 2020].
15. InteriaBiznes, 2019. «Reaguj na dezinformację w sieci». 20 maja 2019. Dostępny: <https://biznes.interia.pl/gospodarka/news-reaguj-na-dezinformacje-w-sieci,nId,4195815> [Data przeglądu 10 czerwca 2020].
16. Kobla, Michalina, 2019. «Komisja Europejska: Polska była zagrożona prorosyjską dezinformacją przed wyborami do Parlamentu Europejskiego». Antyfake. 15 Czerwca 2019. Dostępny: https://www.antyfake.pl/dezinformacja-wybory-do-pe\> [Data przeglądu 02 czerwca 2020].
17. Lucas, Edward, 2017. Winning the Information War Redux. Techniques and Counterstrategies to Russian Propaganda in Central and Eastern Europe. Extended and Revised Editio April. Center for

European Policy Analysis (CEPA). Available at: <https://cepa.ecms.pl/files/?id_plik=4803> [Accessed 25 April 2020].

18. «Most Poles want presidential elections by end of June: poll», 01.06.2020. Available at: <https://polandin.com/48323248/most-poles-want-presidential-elections-by-end-of-june-poll> [Accessed 25 April 2020].

19. Naukowa i Akademicka Sieć Komputerowa (NASK). Raport, 2019. Dezinformacja w sieci jest powszechna. Ale weryfikacja jest możliwa. 08.05.2019. Dostępny: <https://www.tvp.info/42533173/raport-nask-dezinformacja-w-sieci-jest-powszechna-ale-weryfikacja-jest-mozliwa> [Data przeglądu 20 lipca 2020].

20. Naukowa i Akademicka Sieć Komputerowa (NASK).PBS Raport, 2019. Bezpieczne wybory Badanie opinii o (dez)informacji w sieci. Redakcja: Marcin Bochenek, dr Rafał Lange. Warszawa: NASK Państwowy Instytut Badawczy. Dostępny: https://www.nask.pl/pl/raporty/raporty/2592,Bezpieczne-wybory-raport-na-temat-dezinformacji-w-internecie.html> [Data przeglądu 25 lipca 2020].

21. Ośrodek Studiów Wschodnich (OSW), 2020. Dostępny: <https://www.osw.waw.pl/en/o-nas> [Data przeglądu 02 czerwca 2020].

22. Rządowe Centrum Bezpieczeństwa (RCB), 2020. Dostępny: <https://rcb.gov.pl/> [Data przeglądu 02 czerwca 2020].

23. Rządowe Centrum Bezpieczeństwa, 2019. «Działania Rządowego Centrum Bezpieczeństwa w zakresie przeciwdziałania dezinformacji». W Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes, redaktor Wrzosek, Magdalena. Warszawa, NASK Państwowy Instytut Badawczy. Dostępny: <https://cyberpolicy.nask.pl/wp-content/uploads/2019/09/Raport_CP_Dezinformacja_ONLINE_s.pdf> [Data przeglądu 02 czerwca 2020].

24. Sejm Rzeczypospolitej Polskiej, 2007. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Dziennik Ustaw. 2007, nr 89, poz. 590. Dostępny: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20070890590/T/D20070590L.pdf> [Data przeglądu 25 lipca 2020].

25. Sejm Rzeczypospolitej Polskiej, 2018. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dziennik Ustaw. 2018 poz. 1560. Dostępny: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf> [Data przeglądu 10 czerwca 2020].

26. Shahbaz, Adrian and Funk, Allie , 2019. «The Crisis of Social Media» Freedom on the Net, pp. 1-11. Available at: <https://www.freedomonthenet.org/report/freedom-on-the-net/2019/the-crisis-of-social-media> [Accessed 25 April 2020].

27. TVP.INFO, 14.06.2019. «Polska na celowniku rosyjskiej dezinformacji – wynika z raportu KE». Dostępny: <https://www.tvp.info/43081474/polska-na-celowniku-rosyjskiej-dezinformacji-wynika-z-raportu-ke>[Data przeglądu 02 czerwca 2020].

28. «Wybory prezydenckie 2020 w Polsce: kiedy będą? [data, termin, kandydaci, sondaże]», 21.05.2020. Dostępny: <https://www.radiozet.pl/Co-gdzie-kiedy-jak/Wybory-prezydenckie-2020-w-Polsce-kiedy-beda-DATA-TERMIN-KANDYDACI-SONDAZE>[Data przeglądu 02 czerwca 2020].

29. Wydział Strategii Komunikacyjnej w Centrum Operacyjnym MON, 2019. «Dezinformacja a bezpieczeństwo informacyjne państwa». W Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes, redaktor Wrzosek, Magdalena. Warszawa, NASK Państwowy Instytut Badawczy. Dostępny: <https://cyberpolicy.nask.pl/wp-content/uploads/2019/09/Raport_CP_Dezinformacja_ONLINE_s.pdf> [Data przeglądu 02 czerwca 2020].

30. Zakrzewski, Patryk, 2018. «Monitoring w obszarze wprowadzania uregulowań prawnych jako metody walki z fałszywymi informacjami w Internecie». Raport, grudzień 2018. Dostępny: <http://obserwatoriumdemokracji.pl/wp-content/uploads/2019/01/Raport-aktualizacja-grudzie%C5%84.pdf> [Data przeglądu 02 czerwca 2020].

31. Zerka, Pawel, and Buras, Piotr, 7.05.2020. «Poland's presidential election: Political chaos and divides on Europe». Available at: <https://www.ecfr.eu/article/commentary_polands_presidential_election_political_chaos_and_divides_on_eur> [Accessed 25 April 2020].

32. Zybertowicz, Andrzej, 2017. «Internet to narzędzie dezinformacji». PolskieRadio24.pl2017. Dostępny: <https://www.polskieradio24.pl/130/6409/Artykul/1962714,Andrzej-Zybertowicz-Internet-to-narzedzie-dezinformacji>[Data przeglądu 02 czerwca 2020].