



O. V. Karpenko

Kyiv National Economic University named after Vadym Hetman, Kyiv

MECHANIZMY PRZECIWDZIAŁANIA DEZINFORMACJI W WARUNKACH WOJENNYCH

Zidentyfikowano manipulacyjne narzędzia oddziaływania dezinformacji na świadomość masową, które kształtują zniekształcone wyobrażenia o procesach politycznych, społecznych i gospodarczych, stwarzając zagrożenie dla bezpieczeństwa narodowego w warunkach zbrojnej agresji przeciwko Ukrainie. Stwierdzono, że media społecznościowe są głównym obiektem infiltracji fałszywych narracji, co zwiększa podatność przestrzeni informacyjnej. Podkreślono priorytetowy charakter zagrożeń informacyjnych, które pojawiają się podczas stosowania wojskowych i niewojskowych komponentów łączonych metod prowadzenia wojen hybrydowych. Udoskonalono klasyfikację przestrzeni sieciowej (według popularności treści generowanych przez użytkowników poprzez wyodrębnienie czterech podstawowych segmentów: "wiedza społecznościowa", "handel społecznościowy", "media społecznościowe", "sieci społecznościowe") oraz klasyfikację prowadzenia wojen informacyjnych (według sposobu oddziaływania na świadomość masową: "miękkie", "twarde", "inteligentne"). Przeanalizowano praktyczne podejścia do przeciwdziałania infiltracji dezinformacyjnej w krajach UE, które koncentrują się na zwalczaniu nielegalnych treści i cyberprzestępczości. Uzasadniono konieczność ukształtowania na Ukrainie kompleksowego systemu mechanizmów organizacyjno-prawnych, społeczno-ekonomicznych, informacyjno-komunikacyjnych (ideologicznych, aksjologicznych, znaczeniowych) oraz technologicznych przeciwdziałania infiltracji dezinformacyjnej. Wykazano, że w celu zwalczania sfabrykowanych narracji i dekontekstualizacji ich treści konieczne jest stosowanie cyfrowych narzędzi przeciwdziałania infiltracji, które będą minimalizować tempo i skalę rozpowszechniania dezinformacji w przestrzeni informacyjnej. Zaproponowano wdrożenie obowiązkowych filtrów blokujących, algorytmów monitoringu, wzmocnienie regulacji działalności platform medialnych, rozwój społeczności fact-checkerów, wprowadzenie sankcji wobec podmiotów rozpowszechniających niebezpieczne materiały oraz stworzenie warunków sprzyjających zwiększeniu odporności informacyjnej społeczeństwa.

Słowa kluczowe: dezinformacja, infiltracja dezinformacyjna, wojny informacyjne, środowisko informacyjne, treści manipulacyjne, dekontekstualizacja treści.

Wstęp

Opis problemu. W warunkach wojennych wykorzystanie technologii manipulacyjnych jest skutecznym środkiem oddziaływania w sferze informacji. Propaganda pozwala wpłynąć na masową świadomość i zachowania ludzi. Dzięki manipulacji świadomością zbiorową możliwe jest wywarcie wpływu na psychikę każdego człowieka. Polityka informacyjna państwa kształtuje opinię publiczną, co nie pozostaje bez związku z kierunkami rozwoju wydarzeń mających miejsce w państwie. Szczególnie niebezpieczne są treści złośliwie szkodliwe, skierowane przeciwko interesom państwa i społeczeństwa demokratycznego. Do takich treści należy zaliczyć dezinformację, która:

- jest skierowana przeciwko interesom narodowym i integralności terytorialnej kraju;
- celowo zniekształca obraz procesów społeczno-politycznych i fakty historyczne;
- zmienia znaczenie pojęć i tworzy mity;
- promuje wrogie narracje i wartości (tradycje) kraju agresora (dla Ukrainy jest to Federacja Rosyjska);
- dzięki populizmowi i manipulacji kształtuje negatywne stereotypy polityczne wobec przywódców narodu.

Znaczenie badań. Informacje przekazywane za pośrednictwem portali społecznościowych (Facebook, Telegram, X, TikTok, Instagram) mają charakter zarówno psychologiczny, jak i nakierowujący na określone postawy. Zaufanie obywateli do środków masowego przekazu może prowadzić do usprawiedliwienia konfliktu militarnego. Zniekształcenie informacji może prowadzić do podważania instytucji i wartości demokratycznego społeczeństwa.

W takich warunkach poszczególne jednostki (osoby) samodzielnie tworzą informację lub dezinformację, wykorzystując powszechnie dostępne cyfrowe środki rozpowszechniania informacji.

Dzięki temu każda osoba rozpowszechniająca informację zajmuje swoje miejsce w przestrzeni informacyjnej i otrzymuje nowe możliwości samorealizacji. Od tych osób będzie zależało, czy taka przestrzeń informacyjna stanie się ekosystemem, czy środowiskiem toksycznym.

Cel badań i główne zadania dla jego osiągnięcia. Określenie organizacyjnych i prawnych mechanizmów przeciwdziałania dezinformacji w warunkach wojennych.

Przedmiot badań. Mechanizmy przeciwdziałania dezinformacji w warunkach wojennych.

Інформація про авторів:

Карпенко Олександр Валентинович, д-р наук з державного управління, професор. Email: dr.karpenko@kneu.edu.ua;

<https://orcid.org/0000-0002-9301-7973>

Цитування за ДСТУ: Карпенко О. В. Механізми протидії дезінформації в умовах воєнного стану. *Ефективність державного управління* : зб. наук. пр. Вип. 3/4(84/85). Львів: НЛТУ України, 2025. С. 48–58.

Citation APA: Karpenko, O. V. (2025). Mechanizmy przeciwdziałania dezinformacji w warunkach wojennych. *Efficiency of public administration*, 3/4(84/85), 48–52. <https://doi.org/10.36930/508407>

Metody badawcze i baza informacyjna

Metoda analizy i syntezy – pozwoliła na usystematyzowanie dostępnych danych dotyczących natury dezinformacji, technologii jej rozpowszechniania oraz konsekwencji społeczno-politycznych wynikających z jej oddziaływania. Analiza obejmowała zarówno źródła naukowe, dokumenty regulacyjne, jak i materiały publicystyczne. Metoda porównawcza – służyła do zestawienia praktyk i ram prawnych stosowanych w poszczególnych państwach Unii Europejskiej (m.in. w Niemczech, Francji, Szwecji, Litwie) oraz w Ukrainie w zakresie przeciwdziałania dezinformacji. Umożliwiła identyfikację różnic, podobieństw i luk regulacyjnych. Metoda systemowa – zastosowana w celu rozpatrywania zjawiska dezinformacji jako elementu szerszego systemu zagrożeń informacyjnych, obejmującego zarówno narzędzia technologiczne, jak i mechanizmy psychologiczne oddziaływania na świadomość zbiorową. Metoda analizy treści (content analysis) – wykorzystana do oceny sposobów rozpowszechniania manipulacyjnych narracji w mediach społecznościowych (Facebook, X, Telegram) oraz w tradycyjnych środkach masowego przekazu. Analiza treści objęła komunikaty propagandowe, fake newsy oraz materiały tworzone przez użytkowników. Metoda instytucjonalno-prawna – użyta do zbadania mechanizmów regulacyjnych dotyczących przeciwdziałania dezinformacji na poziomie krajowym (Ukraina) i międzynarodowym (UE, Rada Europy). Uwzględniono obowiązujące ustawy, rozporządzenia, rezolucje oraz praktyki instytucji odpowiedzialnych za bezpieczeństwo informacyjne. Metoda prognostyczna – zastosowana w celu przewidywania potencjalnych skutków braku skutecznego systemu przeciwdziałania dezinformacji w warunkach agresji.

Analiza najnowszych badań i publikacji

Problematyka przeciwdziałania dezinformacji nabrała aktualności w literaturze naukowej oraz w raportach instytucji międzynarodowych, szczególnie w kontekście konfliktów zbrojnych. Badania wskazują, że współczesna państwowa polityka informacyjna wymaga integracji mechanizmów prawnych, organizacyjnych i technologicznych.

Autorzy raportu CSIS Commission on Smart Power [1] podkreślają znaczenie łączenia "twardej" i "miękkiej" siły w ramach "smart power" w celu osiągnięcia maksymalnej skuteczności działań informacyjnych. Taka strategia przewiduje zarówno wykorzystanie technologii do ochrony przed zagrożeniami informacyjnymi, jak i budowanie zaufania do państwa poprzez tworzenie pozytywnych narracji. Podobne podejście opisuje S. Nossel [2], który również wskazuje na konieczność synergii "miękkiej" i "twardej" polityki informacyjnej dla skutecznego oddziaływania na opinię publiczną.

Według C. Wardle i H. Derakhshan [3] zjawisko określane jako "information disorder" obejmuje stosowanie dezinformacji, fałszywych wiadomości oraz manipulacyjnych narracji. M. Wenzel i K. Stasiuk-Krajewska [4], analizując wykorzystanie dezinformacji w kontekście wojny w Ukrainie, wskazują na priorytetowe znaczenie mediów społecznościowych jako głównego kanału manipulacji opinią publiczną. Autorzy pokazują, że zarówno materiały propagandowe, jak i fałszywe wiadomości są rozpowszechniane z dużą skutecznością, wpływając na decyzje zarządcze i polityczne.

J. Lipińska [5] podkreśla wzrost znaczenia dezinformacji w procesie komunikacji online. K. Kopecka-Piech,

D. Dyksik i M. Sobiech [6] analizują specyfikę fałszywych wiadomości związanych z wojną rosyjsko-ukraińską w mediach społecznościowych, ujawniając mechanizmy ich powstawania i rozprzestrzeniania. Z kolei K. Chałubińska-Jentkiewicz, U. Soler i A. Makuch [7] badają tendencje oraz kanały rozpowszechniania dezinformacji, podkreślając znaczenie edukacji medialnej w ograniczaniu wpływu fałszywych materiałów. Podobnie M. Jas-Koziarkiewicz i J. Dobrowolska [8] wskazują główne wyzwania związane z działalnością faktcheckerów w Polsce i rekomendują wdrażanie systemowych mechanizmów przeciwdziałania dezinformacji.

Wpływ rosyjskiej propagandy na polityczną kulturę społeczeństwa polskiego został szczegółowo przedstawiony w badaniach P. Pawlaka, który pokazuje, że systematyczne rozpowszechnianie dezinformacji może osłabiać zaufanie obywateli do instytucji demokratycznych oraz destabilizować procesy polityczne.

Podsumowując, literatura i raporty analizowane w ramach badań wskazują na konieczność stosowania kompleksowych mechanizmów przeciwdziałania dezinformacji, obejmujących środki technologiczne, regulacje prawne oraz działania edukacyjne. Połączenie podejścia teoretycznego i empirycznego umożliwia opracowanie skutecznych strategii ochrony społeczeństwa przed materiałami manipulacyjnymi w warunkach wojennych.

Wyizolowanie dotychczas nierozwiązanych części większego problemu. Naukowo-teoretyczne uzasadnienie mechanizmów przeciwdziałania dezinformacji oraz opracowanie praktycznych rekomendacji dotyczących ich stosowania w warunkach wojennych.

Przedstawienie głównego materiału badawczego z uzasadnieniem uzyskanych wyników

Ze względu na popularność treści tworzonych przez użytkowników Internet można podzielić na cztery główne segmenty:

- "wiedza społecznościowa";
- "handel społecznościowy";
- "media społecznościowe";
- "sieci społecznościowe".

Media społecznościowe i sieci społecznościowe tworzą platformy dzielenia się oraz "udostępniania" komunikacji interpersonalnej i sprzyjają rozprzestrzenianiu się dezinformacji.

Dezinformacja to fałszywa informacja, która została stworzona celowo z zamiarem wyrządzenia szkody jednostce, grupie społecznej, organizacji lub krajowi. Dezinformacja jest skuteczną bronią w wojnie informacyjnej.

Wojny informacyjne dzielą się na:

- "miękkie" (soft power) – nie są związane z bezpośrednim wykorzystaniem fałszywych informacji, polegają na manipulowaniu świadomością zbiorową; "miękkie" kształtowanie opinii publicznej działa skutecznie w krajach o rozwiniętych systemach demokratycznych;
- "twarde" (hard power) – świadome zastępowanie prawdy kłamstwem i jego rozpowszechnianie jest typowe dla krajów totalitarnych (Rosja, Korea Północna, Chiny, Kuba);
- "inteligentne" (smart power) – łączenie zasobów twardej i miękkiej siły oddziaływania na świadomość masową, w ramach którego polityka informacyjna jest postrzegana jako manipulacyjne narzędzie budowania zaufania, legitymacji i atrakcyjności dla społeczeństwa (USA, Indie, Chiny).

Oprócz propagandy wrogości, terroryzmu, narkotyków i pornografii dziecięcej, dla społeczeństwa szczególnie niebezpieczne jest celowe rozpowszechnianie treści fałszywych, szkodliwych i manipulacyjnych, skierowanych przeciwko konkretnej osobie lub określonym grupom społecznym (wyróżnionym ze względu na język, wiek, religię, płeć).

Regularna i metodycznie prowadzona dezinformacja może skutkować nie tylko samobójstwami poszczególnych jednostek, ale także wywoływaniem paniki w społeczeństwie. Obecnie rozpowszechnianie dezinformacji jest realizowane na poziomie innowacyjnych kampanii cyfrowych, które celowo zanieczyszczają i zaburzają ekosystem globalnej przestrzeni informacyjnej poprzez manipulowanie opinią publiczną w celu wywoływania konfliktów narodowościowych i wojen.

Przykładowo, konsekwencje nieskutecznej walki z infodemią (czyli dezinformacją o pandemii COVID-19) nie tylko przyczyniły się do dynamicznego rozwoju populistycznych kampanii "antyszczepionkowych", ale także doprowadziły do śmierci ludzi na całym świecie z powodu manipulacyjnego wpływu na postrzeganie informacji poprzez zaszczepienie paniki w społeczeństwie.

Systematyczna i konsekwentna (na przestrzeni ostatnich dwudziestu lat) dezinformacja skierowana wobec obywateli Federacji Rosyjskiej przez propagandystów prokremłowskich środków masowego przekazu doprowadziła do miażdżącego poparcia mieszkańców kraju dla agresji zbrojnej, w wyniku której dochodzi do ludobójstwa narodu ukraińskiego.

Do walki ze sfabrykowanymi treściami konieczne jest stosowanie różnych (w tym cyfrowych) środków zaradczych, które minimalizują tempo i rozmiary rozprzestrzeniania się dezinformacji w środowisku informacyjnym.

Zjawisko infiltracji dezinformacji należy rozumieć nie tylko jako przenikanie do środowiska informacyjnego treści fałszywych, szkodliwych, sfabrykowanych i manipulacyjnych, ale także jako ich wpływ na świadomość zbiorową członków społeczeństwa, będących konsumentami i użytkownikami tego środowiska informacyjnego.

Niezwłocznego uregulowania prawnego, a zwłaszcza wprowadzenia sankcji administracyjnych i odpowiedzialności karnej za niestosowanie się do technologicznych warunków zwalczania rozprzestrzeniania się niebezpiecznych treści w cyberprzestrzeni Ukrainy, wymaga:

- założenie przez dostawców usług internetowych filtrów blokujących, bez możliwości ich włączania lub wyłączania przez użytkowników;
- zastosowanie algorytmów monitorowania i filtrowania ruchu sieciowego poprzez wykorzystanie sztucznej inteligencji w celu identyfikacji lub blokowania dostępu do nielegalnych materiałów i kanałów ich dystrybucji;
- umieszczanie na stronach internetowych specjalnej usługi powiadamiania świadomych społecznie użytkowników o wykryciu treści szkodliwych, nielegalnych i niebezpiecznych;
- przymusowe blokowanie stron internetowych, które mogą stanowić zagrożenie dla życia, czci, godności, dobrego imienia i zdrowia, a także sprzyjać wojnie, konfliktom narodowościowym i religijnym, nielegalnej zmianie ustroju konstytucyjnego lub naruszeniu integralności terytorialnej i niezależności kraju;
- umożliwienie rejestracji lub aktywacji mobilnych kart SIM wyłącznie za pomocą dokumentu potwierdzającego

tożsamość (dowodu osobistego, paszportu), tak jak ma to miejsce obecnie w Polsce i innych krajach Unii Europejskiej;

- identyfikacja urządzeń cyfrowych użytkowników na podstawie adresu IP, adresu MAC oraz kodu IMEI;
- kontrola hotspotów – publicznych punktów dostępu do Internetu (Wi-Fi);
- zobowiązanie dostawców usług internetowych do przechowywania przez określony czas metadanych ruchu internetowego użytkowników oraz adresów IP (w tym zmiennych adresów IP) przypisanych do poszczególnych urządzeń;
- zobowiązanie właścicieli zasobów internetowych do przechowywania komentarzy pozostawionych przez użytkowników (z określeniem czasu ich przechowywania, w szczególności na serwerach fizycznie zlokalizowanych na terytorium Ukrainy).

Ustawodawstwo ukraińskie jest przestarzałe i nie zawiera mechanizmów prawnych pozwalających na przeciwdziałanie rozpowszechnianiu dezinformacji. Obecnie obowiązujące regulacje nie przewidują odpowiedzialności za rozpowszechnianie fałszywych informacji. Pozwala to uniknąć odpowiedzialności osobom, które celowo przyczyniają się do rozpowszechniania fałszywych treści w środkach masowego przekazu i mediach społecznościowych.

Obecnie w Ukrainie konieczne jest stworzenie skutecznego systemu przeciwdziałania infiltracji dezinformacji oraz zapewnienia ochrony interesów każdego człowieka, społeczeństwa i państwa. Jest to możliwe pod warunkiem wykorzystania nie tylko technologicznych narzędzi informacyjno-komunikacyjnych, ale także spójnego zespołu mechanizmów organizacyjno-prawnych o charakterze prewencyjnym, bieżącym i systemowym, takich jak:

- normatywne określenie kryteriów kwalifikacji i oceny infiltracji dezinformacji w środkach masowego przekazu i mediach społecznościowych;
- ustalenie warunków i zasad funkcjonowania w cyberprzestrzeni środków masowego przekazu i platform medialnych (obowiązkowe ujawnienie informacji o właścicielach i założycielach oraz źródłach finansowania i hostingu);
- stosowanie przez państwo surowych środków prawnych wobec dystrybutorów treści sfabrykowanych, szkodliwych, niebezpiecznych i manipulacyjnych (usuwanie i blokowanie treści zgodnie z obowiązującym prawem);
- utworzenie niezależnej społeczności fact-checkerów – aktywistów społecznych i niezależnych dziennikarzy, kontrolujących i weryfikujących prawdziwość faktów wykorzystywanych w różnego rodzaju tekstach, przemówieniach i "postach" rozpowszechnianych w środkach masowego przekazu;
- regulacja i kontrola reklam udostępnianych na portalach informacyjnych, w szczególności zapewnienie weryfikacji prawdziwości sponsorowanych treści politycznych oraz ograniczenie możliwości targetowania w celu zminimalizowania dochodów podmiotów rozpowszechniających dezinformację;
- stworzenie warunków do wprowadzenia specjalistycznych programów edukacji medialnej dla społeczeństwa w celu opanowania podstaw higieny cyfrowej;
- wykorzystanie wartościująco-semantycznych środków obrony informacyjnej, w szczególności prowadzenie kampanii informacyjnych i komunikacyjnych w celu rozpowszechniania pozytywnych narracji o Ukrainie przez

"liderów opinii" (np. "Ukraińcy to naród, który nigdy się nie poddaje");

- kształtowanie trwałej komunikacji strategicznej państwa w dziedzinie polityki zagranicznej i wewnętrznej w celu zapobiegania fałszerstwom i zniekształcaniu informacji o rzeczywistych wydarzeniach w Ukrainie;
- zapewnienie wygodnego, szybkiego i niezawodnego dostępu do dokumentów urzędowych określonych w Konwencji Rady Europy o dostępie do dokumentów urzędowych.

Obecnie w prawodawstwie Unii Europejskiej nie istnieją jeszcze mechanizmy sankcyjne stosowane w celu przeciwdziałania infiltracji dezinformacji. Jedynym państwem Unii Europejskiej, w którego ustawodawstwie zdefiniowano pojęcie dezinformacji, jest Litwa – zgodnie z prawem litewskim dezinformacja to "fałszywa informacja ujawniona publicznie w sposób celowy" (O informowaniu społeczeństwa, 1996). Chociaż dezinformacja może powodować nieufność społeczeństwa wobec rządów i wartości demokratycznych, co stanowi poważne zagrożenie i wyrządza znaczne szkody społeczne, nie jest ona nielegalna w krajach Unii Europejskiej.

Regulacja prawna działalności mediów społecznościowych i środków masowego przekazu wciąż nie obejmuje zakazu dezinformacji. Osoby tworzące i rozpowszechniające fake newsy nie ponoszą odpowiedzialności karnej za swoją działalność, a ponadto są one chronione demokratycznym prawem do wolności słowa i wolności wypowiedzi. Unia Europejska nie zwalcza dezinformacji jako takiej, lecz koncentruje się na cyberprzestępczości oraz rozpowszechnianiu nielegalnych treści związanych z ekstremizmem, nienawiścią rasową, mową nienawiści, przemocą, nietolerancją płciową lub religijną, pornografią dziecięcą, handlem narkotykami oraz handlem bronią.

W roku 2015, w celu zwalczania dezinformacji zewnętrznej w Unii Europejskiej, pod auspicjami Europejskiej Służby Działań Zewnętrznych utworzono grupę zadaniową East StratCom (ESCTF), a dwadzieścia siódmego kwietnia dwa tysiące szesnastego roku przyjęto rozporządzenie Parlamentu Europejskiego i Rady 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz w sprawie swobodnego przepływu takich danych na obszarze Unii Europejskiej i Europejskiego Obszaru Gospodarczego.

Rada Europy przyjęła szereg rekomendacji w celu zwalczania rozprzestrzeniania się dezinformacji. Są to przede wszystkim rezolucje Zgromadzenia Parlamentarnego:

- numer 2217 (2018) "Wyzwania prawne związane z wojną hybrydową i zobowiązaniami w zakresie praw człowieka";
- numer 2314 (2019) "Edukacja medialna w nowym środowisku medialnym";
- numer 2281 (2019) "Sieci społecznościowe: strumienie społecznościowe czy zagrożenia dla praw człowieka?";
- numer 2255 (2019) "Media państwowe w kontekście dezinformacji i propagandy";
- numer 2326 (2020) "Zhakowana demokracja? Jak odpowiedzieć?".

W dokumentach tych wskazuje się, że w dzisiejszych czasach państwa coraz częściej stykają się ze zjawiskiem "wojny hybrydowej", która tworzy nowy rodzaj zagrożenia, polegający na połączeniu metod wojskowych i niemojskowych, takich jak cyberataki oraz masowe kampanie dezinformacyjne, w tym z wykorzystaniem fake newsów, w

szczegółności za pośrednictwem mediów społecznościowych.

Zgromadzenie Parlamentarne zauważa, że cyfryzacja, mobilność i komunikacja internetowa przyniosły niezaprzeczalne korzyści społeczeństwu, które uzyskało szeroką gamę źródeł informacji oraz dostęp do informacji kulturalnych, historycznych, politycznych, ekonomicznych i technicznych. Otwarty charakter platform cyfrowych promuje inkluzywną, przejrzystą i skuteczną demokrację. Jednocześnie w erze cyfrowej nasilają się zagrożenia dla praw podstawowych, demokracji i praworządności. Znaczna część społeczeństwa, zwłaszcza młodzież, traktuje sieci społecznościowe jako podstawowe źródło informacji.

Dezinformacja i propaganda mogą wpływać nie tylko na wyniki wyborów i referendów, ale także na życie codzienne; oddziałują na preferencje polityczne obywateli oraz ich zaufanie do mediów tradycyjnych. Aby rozwiązać problemy związane z dezinformacją, rządy państw członkowskich Rady Europy powinny realizować zalecenia z 2018 roku dotyczące ról i obowiązków pośredników internetowych oraz z 2020 roku w sprawie wpływu systemów algorytmicznych na prawa człowieka, a także inne wytyczne.

Komisja Europejska przyjmuje wyłącznie zalecenia w celu przeciwdziałania infiltracji dezinformacji. Dlatego w praktyce zakres konkretnych działań jest określany samodzielnie przez każde z państw Unii Europejskiej. W większości krajów Unii Europejskiej podstawową taktyką walki z rozprzestrzenianiem się dezinformacji jest podnoszenie poziomu umiejętności korzystania z mediów, kształtowanie krytycznego myślenia oraz świadomości społecznej w zakresie ataków informacyjnych i zagrożeń związanych z ich wpływem na procesy społeczne. Uważa się, że niski poziom kompetencji cyfrowych i umiejętności korzystania z mediów przez internautów stanowi jedną z przyczyn wzrostu skali działalności hakerów, cyberprzestępców i cyberterrorystów.

Wnioski i perspektywy dalszych badań

Atak na Ukrainę pokazał, że w rzeczywistości społeczeństwo europejskie okazało się nieprzygotowane na wojnę, której jednym z narzędzi są rosyjskie ataki informacyjne, a umiejętność korzystania z mediów nie rozwiązuje problemu przeciwdziałania dezinformacji.

W przypadku Ukrainy polityka inna niż stosowanie sankcji jest nieskuteczna, gdyż znaczna część terytorium Ukrainy jest już zajęta przez Rosję, a ludność jest celem nie tylko ataków rakietowych i artyleryjskich, ale przede wszystkim ataków informacyjnych kremlowskiej propagandy.

Ci, którzy dziś tworzą i rozpowszechniają dezinformację w Ukrainie, stają się, bez przesady, zdrajcami ideałów demokracji. Dlatego, aby skutecznie przeciwdziałać ukrytym kampaniom dezinformacyjnym wymierzonym w państwo (których cele, zadania i konsekwencje są znane), konieczne jest:

- najpierw – przeprowadzenie analizy środowiska informacyjnego oraz kręgu adresatów informacji;
- opracowanie strategii i taktyki przeciwdziałania dezinformacji (kontrpropagandy) przez władze publiczne;
- określenie wykonawców, zasobów oraz możliwego ryzyka (zagrożeń), z uwzględnieniem wyników wcześniejszych interwencji dezinformacyjnych przeciwko Ukrainie.

References

1. CSIS Commission on Smart Power. (2007). A Smarter, More Secure America. Washington, DC: Center for Strategic and International Studies. 35 p. URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/071106_csis-smartpower-report.pdf
2. Nossel, S. (2004). Smart Power. *Foreign Affairs*, 83(2), 131-142.
3. Wardle, C., & Derakshan, H. (2017). Information disorder: toward an interdisciplinary framework for research and policy making. Strasbourg: Council of Europe. URL: <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c>
4. Wenzel, M., & Stasiuk-Krajewska, K. (2023). Dezinformacja związana z wojną w Ukrainie: media społecznościowe kluczowym kanałem manipulacji. *Mediatization Studies*, 6, 23-38. <https://doi.org/10.17951/ms.2022.6.23-38>
5. Lipińska, J. (2023). Disinformation content in Polish cyberspace. *Humanities and Social Sciences*, 30(2). URL: <https://doi.org/10.7862/rz.2023.hss.14>
6. Kopecka-Piech, K., Dyksik, D., & Sobiech, M. (2023). The construction of fake war news: Specificities of disinformation in social media during the first six months of the Russia-Ukraine war (March-September 2022). *Rocznik Instytutu Europy Środkowo-Wschodniej*, 21(2), 155-173. URL: <https://doi.org/10.36874/RIESW.2023.2.8>
7. Chalubińska-Jentkiewicz, K., Soler, U., & Makuch, A. (2023). Disinformation in Polish society in 2021 – trends, topics, channels of transmission. *Polish Political Science Yearbook*, 52(1), 93-107. URL: <https://doi.org/10.15804/ppsy202309>
8. Jas-Koziarkiewicz, M., & Dobrowolska, J. (2024). Challenges, assessment and recommendations of the fact-checkers regarding Polish policy of combating and counteracting disinformation. *Polish Political Science Yearbook*, 29(2). URL: <https://doi.org/10.14746/pp.2024.29.2.8>
9. Pawlak, P. (2022). The influence of Russian propaganda and disinformation on Poland's political culture in virtual space. *Studia nad Bezpieczeństwem*, 7. URL: https://doi.org/10.34858/SNB_7_2022_006

O. V. Karpenko

Київський національний економічний університет імені Вадима Гетьмана (Україна)

МЕХАНІЗМИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ

Визначено маніпулятивні інструменти впливу дезінформації на масову свідомість, які формують викривлені уявлення про політичні, соціальні та економічні процеси, що створює загрозу національній безпеці в умовах збройної агресії проти України. Констатовано, що соціальні мережі є головним об'єктом інфільтрації фейкових наративів, що посилює вразливість інформаційного простору. Наголошено на пріоритетності інформаційних загроз, які виникають під час застосування військових та невійськових складових комбінованих методів ведення гібридних воєн. Удосконалено класифікації мережевого простору (за популярністю користувацького контенту шляхом виділення чотирьох основних сегментів: "соціальні знання", "соціальна комерція", "соціальні медіа" і "соціальні мережі") та ведення інформаційних воєн (за способом впливу на масову свідомість: "м'яка сила", "жорстка сила", "розумна сила"). Проаналізовано практичні підходи до протидії дезінформаційній інфільтрації у країнах ЄС, які зосереджуються на боротьбі з незаконним контентом і кіберзлочинністю. Обґрунтовано необхідність формування в Україні комплексної системи організаційно-правових, соціально-економічних, інформаційно-комунікативних (ідеологічних, ціннісних, смислових) та технологічних механізмів протидії дезінформаційній інфільтрації. Доведено, що для боротьби зі сфабрикованими наративами й деконтекстуалізацією їх змістів потрібно використовувати цифрові інструменти протидії інфільтрації, які мінімізуватимуть темпи й обсяги поширення дезінформації в інформаційному просторі. Запропоновано впровадження обов'язкових фільтрів блокування, алгоритмів моніторингу, посилення регуляції діяльності медіаплатформ, розвитку спільнот фактчекерів, запровадження санкцій щодо поширювачів небезпечних матеріалів і створення умов для підвищення інформаційної стійкості населення.

Ключові слова: дезінформація; дезінформаційна інфільтрація; інформаційні війни; інформаційне середовище; маніпулятивний контент; деконтекстуалізація змісту.

O. V. Karpenko

Kyiv National Economic University named after Vadym Hetman, Kyiv

MECHANISMS FOR COUNTERING DISINFORMATION UNDER MARTIAL LAW

Manipulative instruments of disinformation influencing mass consciousness have been identified, which shape distorted perceptions of political, social, and economic processes, thereby posing a threat to national security in the context of armed aggression against Ukraine. It is stated that social networks are the primary targets for the infiltration of fake narratives, which increases the vulnerability of the information space. Emphasis is placed on the priority of information threats that arise during the application of military and non-military components within combined methods of hybrid warfare. The classifications of the networked space have been refined (based on the popularity of user-generated content, distinguishing four main segments: "social knowledge", "social commerce", "social media" and "social networks"), as well as the classification of information warfare (based on modes of influence on mass consciousness: "soft power", "hard power" and "smart power"). Practical approaches to countering disinformation infiltration in EU countries, which focus on combating illegal content and cybercrime, are analyzed. The necessity of establishing in Ukraine a comprehensive system of organizational-legal, socio-economic, information and communication (ideological, value-based, and semantic), and technological mechanisms for countering disinformation infiltration is substantiated. It is demonstrated that, in order to combat fabricated narratives and the decontextualization of their content, it is necessary to employ digital counter-infiltration tools that minimize the speed and scale of disinformation dissemination in the information space. The implementation of mandatory blocking filters, monitoring algorithms, strengthened regulation of media platforms, the development of fact-checking communities, the introduction of sanctions against disseminators of harmful materials, and the creation of conditions to enhance public information resilience are proposed.

Keywords: disinformation, disinformation infiltration, information warfare, information environment, manipulative content, content decontextualization.