УДК 327. 004.056.5:351.861(477)
DOI https://doi.org/10.32782/2663-6170/2023.34.13

БЕЗПЕКА ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ В УМОВАХ РОСІЙСЬКОЇ АГРЕСІЇ НА СУЧАСНОМУ ЕТАПІ: ОСНОВНІ ЗАВДАННЯ ТА ВИКЛИКИ

SECURITY OF UKRAINE'S INFORMATION SPACE IN THE CONDITIONS OF RUSSIAN AGGRESSION AT THE PRESENT STAGE: MAIN TASKS AND CHALLENGES

Галіпчак В.Д.,
аспірант кафедри політичних інститутів та процесів
Прикарпатського національного університету імені Василя Стефаника

Дана стаття присвячена аналізу основних викликів та завдань, пов'язаних із забезпеченням безпеки інформаційного простору України в умовах російської агресії на сучасному етапі. У центрі уваги – методи російської дезінформації та пропаганди, основні типи та стратегії кібератак, вплив нових технологій на інформаційну безпеку. Визначається ряд ключових завдань для України, що включають розробку та впровадження ефективних стратегій протидії кібератакам, боротьбу з дезінформацією та пропагандою, а також необхідність адаптації сучасних міжнародних підходів до забезпечення кібербезпеки.

В статті досліджено проблематику безпеки інформаційного простору України в контексті російської агресії: проаналізовано вплив дезінформаційних кампаній, розповсюдження фейкових новин та кібератак на стабільність інформаційного простору України. У статті визначаються основні виклики та завдання, що стоять перед українською державою в сфері інформаційної безпеки. Висвітлюється роль та вплив сучасних технологій на процеси в інформаційному просторі. Наголошується на важливості розробки ефективних механізмів протидії кібератакам та стратегій боротьби з дезінформацією та пропагандою.

Розглянуто важливість таких основних складових держави як: інформаційні інститути – західні партнери – громадянське суспільство, які разом складають об'єднуючу ланку для боротьби в кібер та інформаційному просторі фронті війни. Окрему увагу приділено аналізу підходів, прийнятих Україною та іншими країнами для протистояння російській агресії в інформаційному просторі. Подається візія того, як ці підходи та стратегії можуть бути адаптовані та використані в Україні.

Дослідження можуть бути використані для поглибленого розуміння викликів, пов'язаних з безпекою інформаційного простору України в умовах російської агресії. Результати дослідження можуть бути корисними для вчених, експертів у сфері безпеки, військових та політичних діячів, що працюють над проблемами безпеки інформаційного простору України.

Ключові слова: інформаційний простір, інформаційна безпека, кібератаки, дезінформація, маніпуляція.

This article is devoted to the analysis of the main challenges and tasks related to ensuring the security of the information space of Ukraine in the conditions of Russian aggression at the current stage. The focus is on the methods of Russian disinformation and propaganda, the main types and strategies of cyberattacks, the impact of new technologies on information security. A number of key tasks for Ukraine are identified, including the development and implementation of effective strategies for countering cyberattacks, the fight against disinformation and propaganda, as well as the need to adapt modern international approaches to ensuring cyber security.

The article examines the security issues of Ukraine's information space in the context of Russian aggression: the impact of disinformation campaigns, the spread of fake news, and cyber attacks on the stability of Ukraine's information space is analyzed. The article identifies the main challenges and tasks facing the Ukrainian state in the field of information security. The role and influence of modern technologies on processes in the information space is highlighted. The importance of developing effective mechanisms to counter cyberattacks and strategies to combat disinformation and propaganda is emphasized.

The importance of such main components of the state as: information institutes – Western partners – civil society, which together form a unifying link for fighting in the cyber and information space on the war front, is considered. Particular attention is paid to the analysis of approaches adopted by Ukraine and other countries to resist Russian aggression in the information space. A vision of how these approaches and strategies can be adapted and used in Ukraine is provided.

The research can be used for a deeper understanding of the challenges related to the security of the information space of Ukraine in the conditions of Russian aggression. The results of the study can be useful for scientists, experts in the field of security, military and political figures working on the security problems of the information space of Ukraine.

Key words: information space, information security, cyber attacks, disinformation, manipulation.

Постановка проблеми. В умовах російської агресії, інформаційний простір України перебуває під постійною загрозою. Інформаційна дестабілізація українського суспільства почалась ще задовго о повномасштабного російського втручання, проте зараз проблема набуває особливого гострого характеру, своєчасне реагування на яку, та вдала протидія гарантує збереження української державності та здійснює відсіч ворогу на всіх фронтах боротьби, зокрема і на інформаційному. Маніпуляції інформацією, цілеспрямована дезінформація, фальсифікація фактів, розпалювання ворожнечі, а також кібератаки на стратегічно важливі об'єкти – все це становить серйозну

проблему для національної безпеки країни. Така ситуація вимагає негайного і комплексного реагування, оскільки від стабільності інформаційного простору залежить не тільки безпека держави, але й сприйняття ситуації міжнародною спільнотою. Проблема посилюється ще й тим, що існуючі механізми захисту не завжди ефективно протистоять новим методам кібератак, а також тому, що дезінформація впливає на суспільне свідомість і може підривати стабільність в країні. Проте, незважаючи на актуальність та важливість цієї проблеми, вона поки що не отримала належної уваги в наукових дослідженнях. Це вказує на необхідність подальшого вивчення і аналізу ситуації, визначення основних викликів та розробки ефективних механізмів захисту інформаційного простору України в умовах російської агресії.

Аналіз останніх досліджень і публікацій. Багато останніх досліджень і публікацій на тему безпеки інформаційного простору України були присвячені вивченню способів протидії дезінформації та кібератакам. Зокрема дослідження інформаційного простору України в безпекові сфері було здійснено як низкою вітчизняних так і зарубіжних західних науковців. Можна відзначити таких вчених як Харченко Л.С., Ліпкан В.А., Логінов О.В., Камінська Н.В. та ін. Серед основних обговорень їхніх праць, варто відзначити основні тезиси: «Інформаційна безпека України в умовах гібридної війни»: це дослідження розглядає стратегії та тактики, використані в процесі гібридної війни, і їх вплив на інформаційну безпеку України; «Соціальні медіа як інструмент дезінформації в умовах російської агресії»: це дослідження аналізує способи, якими соціальні медіа використовуються для проведення кампаній дезінформації, і пропонує стратегії протидії цим тактикам; «Роль освіти в протидії дезінформації». Багато напрацювань західних вчених по даній тематиці були присвячені дослідженням ролі громадяньского суспільства (“Media Influence on Public Perception of the Conflict in Ukraine” – досліджує вплив медіа на формування громадської думки про конфлікт в Україні; “Countering Hybrid Threats in the Cyber Domain” – зосереджується на гібридних загрозах в кіберпросторі і способах їх протидії). Ці та інші дослідження підкреслюють важливість комплексного підходу до забезпечення безпеки інформаційного простору, який би включав технічні заходи, громадську освіту та міжнародне співробітництво. Незважаючи на велику кількість досліджень, присвячених проблемам кібербезпеки та боротьбі з дезінформацією, питання безпеки інформаційного простору України в умовах російської агресії потребує додаткового аналізу

Виділення невирішених раніше частин загальної проблеми. Дослідження інформаційного безпекового простору України, дає підстави зупинитися на таких основних проблемах дослідження, як: недостатній рівень громадської обізнаності (незважаючи на численні інформаційні кампанії та навчальні програми, рівень обізнаності громадян щодо дезінформації та кібербезпеки залишається недостатнім. Це є важливою частиною проблеми, яка потребує подальшої уваги), недостатній рівень міжнародного співробітництва, технологічні виклики (технології швидко розвивається, і хоча Україна робить значні зусилля для залишання в ногу з найновішими тенденціями у галузі кібербезпеки, є ще багато областей, які потребують подальших досліджень та розробок. Особливо це стосується захисту від кібератак нового покоління та штучного інтелекту), законодавча база (питання законодавчого регулювання в області інформаційної безпеки потребує подальшої уваги. Українське законодавство повинне бути адаптоване до нових викликів та загроз, що постають в результаті технологічного прогресу та змін у тактиці ведення інформаційної війни). Враховуючи швидкість розвитку технологій та постійне змінювання ситуації, потрібно постійно переглядати і оновлювати стратегії забезпечення інформаційної безпеки.

Формулювання цілей статті (постановка завдання). Основна мета цієї статті – дослідити стан безпеки інформаційного простору України в умовах російської агресії на сучасному етапі, визначити основні виклики, завдання та шляхи їх розв'язання. До основних цілей статті можна віднести: Дослідити сучасний стан інформаційного простору України, особливо з урахуванням викликів, пов'язаних з російською агресією.

− Визначити ключові виклики: Визначити основні виклики та загрози, з якими стикається Україна в контексті забезпечення безпеки свого інформаційного простору.

− Вивчення наявних стратегій: Оцінити ефективність наявних стратегій і практик, які використовуються для забезпечення безпеки інформаційного простору України.

− Порівняння та кореляція з міжнародними практиками: порівняльний аналіз з міжнародними практиками та стратегіями в галузі інформаційної безпеки.

− Розробити пропозиції: На основі отриманих результатів сформулювати конкретні рекомендації щодо вдосконалення політики в галузі інформаційної безпеки в Україні.

Виклад основного матеріалу дослідження. Сучасний світ характеризується все більшою взаємозалежністю та взаємовпливом країн, що обумовлено розвитком глобальних інформаційних мереж. Інформаційний простір, що створюється за допомогою цих мереж, відіграє ключову роль в суспільному, політичному та економічному житті кожної держави. Проте розвиток технологій призводить до появи нових викликів і загроз, особливо в умо-

вах міжнародних конфліктів. Ситуація з безпекою інформаційного простору України в умовах російської агресії є яскравим прикладом такого контексту. Сучасний інформаційний простір характеризується невід'ємними зв'язками між технологічними, соціальними та політичними аспектами життя суспільства. Він створює безліч можливостей для комунікації, освіти, комерції та розваг, але водночас відкриває нові вектори для потенційних загроз. Найбільш небезпечні з них стосуються кібербезпеки та інформаційної війни, особливо в контексті державних конфліктів [7, с. 17–23].

Починаючи з 2014 року, коли Росія почала свою агресію проти України, кібератаки та інформаційна війна стали важливими інструментами її воєнної стратегії. Метою цих дій є підрив довіри до українських інститутів, дестабілізація ситуації в країні, а також вплив на міжнародну спільноту в цілому.Росія використовує цілий спектр методів, включаючи кібератаки на критичну інфраструктуру, поширення дезінформації та фальсифікації, використання тролів та ботів для маніпуляції суспільною думкою в соціальних медіа, а також підтримку антиукраїнських елементів всередині країни. Від часу початку російської агресії, методи та стратегії кібератак зазнали значних змін. Вони стали більш розрахованими, тонкими та багатоаспектними. Раніше використовувалися прямі атаки на конкретні цілі, тоді як сьогодні дедалі більше використовуються методи соціальної інженерії, такі як фішинг або спроби обману людей для отримання доступу до конфіденційної інформації.

Однією з ключових тенденцій стала зміна фокусу з простих перебоїв роботи систем до витоку чутливої інформації, що може використовуватися для політичного чи військового пресингу. Також зростає важливість тактик, які включають в себе довготривалі кампанії з ціллю дестабілізації або руйнування віддалених мереж, використовуючи віруси та шпигунські програми [4, с. 220–224].

Україна зіткнулася з серйозними викликами в галузі інформаційної безпеки. Основними серед них є кібератаки, що цілять на критичну інфраструктуру та державні інституції, а також масова кампанія дезінформації та пропаганди, що має на меті підривати довіру до українських інститутів та суспільства в цілому. Основні типи кібератак, з якими зішлася Україна, включають:

− Атаки на фізичну інфраструктуру: Такі атаки мають на меті порушити нормальну роботу важливих інфраструктурних об'єктів, таких як енергетичні системи, транспорт або системи связі.

− Атаки на державні органи: Метою цих атак є збір конфіденційної інформації та підрив довіри до державних структур.

− Атаки на приватні особи або організації: В цьому випадку, метою може бути збір персональних даних, шантаж, або просто саботаж.

Методи, що використовуються для проведення цих атак, включають віруси, троянські коні, шпигунські програми, а також методи соціальної інженерії, такі як фішинг. Вплив дезінформації та пропаганди на суспільство та інформаційний простір Дезінформація та пропаганда стали потужними інструментами в руках агресора. Вони використовуються для маніпулювання громадською думкою, підриву довіри до уряду, та створення суспільної напруженості та поділів. Соціальні медіа є основним полем для цих атак, але вони також відбуваються через традиційні медіа та інші канали комунікації. Сучасні технології, такі як штучний інтелект, машинне навчання, та блокчейн, відкривають нові можливості для кібератак. Водночас, вони також надають нові інструменти для захисту. Наприклад, машинне навчання може бути використано для виявлення аномалій та автоматизованого виявлення атак. Блокчейн може допомогти в створенні захищених систем, які важко взламати. Однак, є велика потреба в постійному навчанні та оновленні знань та навичок, щоб забезпечити ефективний захист від постійно розвиваючихся загроз [6, с. 176].

Для запезпечення надійного функціонування інформаційного простору України, потрібно дотримуватись алгоритму злагоджених дій як в інститутах держави так і в приватному секторі та громадському секторі. Надалі наводимо розроблений короткий алгортим кроків для ефективного запезпечення інформаційного простору держави на наш погляд:

1. Розробка та впровадження стратегії кібербезпеки: Ця стратегія повинна охоплювати різні аспекти, включаючи захист критичної інфраструктури, державних інституцій та приватних осіб. Вона повинна бути гнучкою, щоб адаптуватися до змінюваних тактик ворога.

2. Навчання і освіта: Оскільки технології постійно розвиваються, постійне навчання та освіта є важливими для забезпечення інформаційної безпеки. Це означає, що слід проводити навчання для працівників усіх рівнів, включаючи керівників, інженерів, а також звичайних користувачів.

3. Посилення міжнародної співпраці: Україна може скористатися підтримкою міжнародних партнерів у боротьбі проти кібератак. Це може включати обмін інформацією про загрози, співпрацю в розслідуваннях та підтримку у впровадженні кращих практик з кібербезпеки.

4. Боротьба з дезінформацією та пропагандою: Це може включати розробку та впровадження стратегій для ідентифікації та контролю дезінформації, а також освітні програми для населення про те, як виявляти та обробляти дезінформацію.

Інвестиції в інновації та технології: Нові технології можуть допомогти в захисті від кібератак, але потребують інвестицій для розробки та впро-

вадження. Україна повинна стимулювати інновації в цій області через державне фінансування, партнерства з приватним сектором, а також міжнародну співпрацю [1, с. 29–32].

До основних методів боротьби з російською пропагадою та дезінорфмацією в Україні потрібно перш за все відносити комплексний підхід, адже тільки в сукупності та злагоджених діях результат буде на високо-якісному рівні. Проте для простого населення варто виділити, ряд ознак, які допомодуть боротися з дезінформацією та манупіляційми з сторони російської федерації:

• Виховання критичного мислення: Однією з найефективніших стратегій протидії дезінформації є виховання критичного мислення.

• Фактчекінг: спеціалізовані організації та волонтерські групи можуть систематично перевіряти інформацію, що поширюється, на правдивість та надавати відповіді на неправдиві твердження.

• Підвищення прозорості в соціальних медіа: Платформи соціальних медіа мають важливу роль у поширенні дезінформації. Вони можуть вживати кроків, щоб зробити більш прозорими процеси, які визначають, яка інформація доходить до користувачів.

• Регуляція і санкції: держава може приймати закони та регуляції, що встановлюють відповідальність за поширення дезінформації.

• Підвищення громадської обізнаності: загальнодоступні кампанії з інформування можуть допомогти громадськості краще розуміти, як і чому поширюється дезінформація.

Співпраця з міжнародними партнерами: Спільна робота з міжнародними партнерами для боротьби з дезінформацією на глобальному рівні, обміну кращими практиками та координації дій [2, с. 137].

Боротьба на так званій «другій лінії форнту», інфомраційному фронті не повинна бути недооціненою чи недостатньою. Слід сказати, що сучасні підходи прийняті УкраїноЮ у сфері протистояння кібератакам багато чим послуговуються західним практикам та тим не менше знайшли і свою універсальність. В Україні та інших країнах активно працюють над стратегіями протидії кібератакам з боку Росії. Ці стратегії включають в себе декілька основних напрямків: розробка та впровадження національних стратегій кібербезпеки: Україна, наприклад, в 2020 році прийняла нову стратегію кібербезпеки, що містить в себе ряд ключових напрямків розвитку в цій сфері. Інші країни, такі як США, Великобританія, Німеччина та Франція, також розробили свої національні стратегії кібербезпеки; підвищення кібероборони: Україна, як і інші країни, активно працює над покращенням своєї кібероборони. Це включає в себе розробку та впровадження нових технологій, зміцнення кіберінфраструктури та підготовку кадрів у сфері кібербезпеки; міжнародна співпраця: протидія кіберзагрозам вимагає міжнародної співпраці. Україна активно співпрацює з країнами НАТО та ЄС у цьому напрямку, а також з іншими країнами, які стикаються з аналогічними викликами. Спільні зусилля включають в себе обмін інформацією, координацію дій та спільні навчання. Законодавчі реформи: щоб ефективно протистояти кібератакам, потрібне відповідне законодавство. Україна та інші країни активно працюють над законодавчими змінами, що дозволяють краще виявляти, розслідувати та протидіяти кібератакам. Ці підходи, прийняті Україною та іншими країнами, створюють ефективну систему протидії кібератакам та іншим безпековим загрозам, що несе Російська Федерація [5, с. 20–27].

Отже, слід зазначити, що адаптація цих стратегій щодо здійснення безпекової політики інформаційного простору України на сучасному потребує постійного вивчення, актуалізації та вдосконалення. Після 2014 та 2022 р. з початком повномашстабного російського вторгнення концеція безпеки українського простору залежить в своєму вимірі як і від дій інформаційних інститутів держави так і всебічній підтримці кібер та онлайн спеціалістів та громадського населення в мережі інтернет (зокрема телеграм канали, фейсбук та інстаграм мережі, ЗМІ та інші інформаційні ресурси), які спільно працюють на збереження та зміцнення українського суверенітету та державності.

Висновки. Україна, в умовах російської агресії та війни, зіткнулася з необхідністю захистити свій інформаційний простір. Сучасний військовий конфлікт, що набув особливої гостроти, та перейшому у повномасштабні військові дії та агресію з російської сторони має не тільки «гарячі» точки на лінії фронту, але й цифрове поле битви, де розігрується не менш важлива війна за контроль над інформацією та громадською думкою. Російська агресія в інформаційному просторі націлена на створення хаосу, посів дезінформації, знецінення фактів та розкол суспільства. Відбувається реалізація цілеспрямованих кібератак на критичні інфраструктури та розповсюдження пропагандистських повідомлень з метою дестабілізації ситуації в країні та за її межами з метою викревлення фактів дійсності.

Саме тому, безпека інформаційного простору в умовах російсько-української війни є одним з ключових завдань для України. Ефективна протидія кібератакам, боротьба з пропагандою та дезінформацією, а також співпраця на міжнародному рівні є важливими інструментами в цій боротьбі.

Адже, тільки спільною працею всіх сторін як і громадського простору та держави й збройних сил можлива ефективна протидія загрозам, які існують на сьогоднішній день в інформаційному й не тільки полі української держави та за її межами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Боднар І.Р. Державна політика та інформаційна безпека України: післякризові виклики. Актуальні проблеми післякризового відновлення економіки України: зб. матер. наук.-практ. конф. Львів. 2013. С. 29-32.
2. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. Вісн. Нац. акад. держ. упр. при Президентові України. 2015. № 1. С. 136-141. Бібліогр.: 17 назв. – укр.
3. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. URL: https://cutt.ly/aaXrdtE (Last access: 27.04.2020).
4. Кочубей Л.О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно комунікаційних технологій у сучасному Донбасі. Наукові записки Інституту політичних і етнонаціональних досліджень імені І. Ф. Кураса. 2015. Вип. 3. С. 220-237.
5. Малик Я. Забезпечення інформаційної безпеки України у контексті світового досвіду. Збірник наукових праць: «Ефективність державного управління». Випуск 32. 2012. С. 20-27.
6. Махній М. Мережеве суспільство: кіберпсихологічний путівник. Київ: Academia.edu, 2018. 176 с.
7. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17-23.
8. Brandon Valeriano, Benjamin Jensen, Ryan C. Maness. (2018). "Cyber Strategy: The Evolving Character of Power and Coercion".
9. Hybrid Warfare (2019). URL: http://www.gao.gov/assets/100/97053.pdf
10. Lucas Kello (2017). The Virtual Weapon and International Order".