МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

VII МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ (PCSITS)

26 квітня 2024 року

Збірник матеріалів доповідей та тез

Київ – 2024

УДК 621.39:351.861(06)
ББК 32.88:67.401.212.431
П 78

П78 Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 26 квітня 2024 року; Київський національний університет імені Тараса Шевченка / Редкол.: *В.В. Ільченко, д.ф-м.н., проф., (голова);* та ін. – К.: ВПЦ "Київський університет", 2024. – 171 с.

Тексти виступів і тез опубліковано в авторській редакції однією з робочих мов конференції: українською або англійською.

УДК 621.39:351.861(06)
ББК 32.88:67.401.212.431

ВСТУП

Завдяки інтеграції передових досягнень у сфері інформаційних і комунікаційних технологій та швидкому прогресу у розвитку інформаційних систем, виникли нові глобальні структури, такі як інформаційне суспільство, інформаційний та кібернетичний простори. Ці структури відкрили величезний потенціал і стали важливими чинниками у соціальному та економічному розвитку на глобальному рівні, сприяючи обміну інформацією та знаннями між країнами і культурами.

Проте, із розвитком інформаційного суспільства зросла кількість викликів, особливо у сфері безпеки. Загрози для інформаційних та комунікаційних систем стають все більш серйозними, включаючи ризики несанкціонованого доступу, витоку даних та інших форм втручання. Захист цих систем стає критичним аспектом національної безпеки і потребує постійного вдосконалення захисних механізмів та методів.

На відповідь цим викликам направлені численні наукові дослідження та розробки. Центральним елементом захисту інформаційних ресурсів є розробка новітніх технологій, що охоплюють як фізичний, так і кібернетичний захист. Важливість створення надійних захисних систем вимагає впровадження складних математичних моделей та алгоритмів, які б могли ефективно протидіяти сучасним загрозам.

У рамках VII міжнародної науково-практичної конференції, яка проходила під егідою Київського національного університету імені Тараса Шевченка, було представлено значну кількість доповідей та тез, що висвітлювали як теоретичні, так і практичні аспекти розвитку інформаційної безпеки.

Серед присутніх учасників конференції були: іноземні гості, представники Міністерства освіти та науки України, різних державних установ і відомств, а також провідних вищих навчальних закладів міст України, науковці, науково-педагогічні працівники, аспіранти, докторанти, студенти, представники підприємств, установ та організацій різних форм власності, основним профілем наукової та практичної діяльності яких є саме напрям кібербезпека.

Учасники конференції обговорили сучасні методи та системи захисту інформації, стратегії їх ефективного впровадження. Обговорення зосереджувалось на необхідності розробки нових, більш досконалих систем безпеки, здатних забезпечити надійний захист від різноманітних загроз в інформаційному просторі в умовах сучасного стану.

СЕКЦІЯ 2
«МЕТОДИ, ЗАСОБИ ТА ЗАХОДИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Державна інформаційна політика України щодо протидії інформаційно-психологічному впливу в кіберпросторі під час повномасштабної воєнної агресії рф проти України

Артем Плужник[1],
Володимир Наконечний[2]
Микола Мордвинцев[3]

1. Кафедра кібербезпеки та захисту інформації,
Київський національний університет імені Т. Шевченка,
УКРАЇНА, м. Київ, вул. Б. Гаврилишина, 24,
e-mail: pluzhnyk.artem@gmail.com
2. Кафедра кібербезпеки та захисту інформації,
Київський національний університет імені Т. Шевченка,
УКРАЇНА, м. Київ, вул. Б. Гаврилишина, 24,
e-mail: nvc2006@i.ua
3. Харківський національний університет внутрішніх справ
УКРАЇНА, м. Харків, пр. Льва Ландау, 27.

The article analyzes the state information policy of Ukraine in the context of countering information and psychological influence in cyberspace during the full-scale military aggression of the russian federation against Ukraine. Focusing on the key aspects of the policy and its effectiveness, the article considers the importance of these measures for preserving national security and sovereignty in the context of a military conflict with russia.

Ключові слова: державна інформаційна політика, кіберпростір, національна безпека, ефективність політики, психологічний вплив.

Вступ

У кіберпросторі, який є важливою ареною для боротьби за вплив та геополітичну перевагу, інформація стає основним інструментом формування суспільних думок, маніпулювання громадською думкою та впливу на події.

У зв'язку з цим протидія інформаційно-психологічному впливу набуває вирішального значення для забезпечення національної безпеки та суверенітету країни.

Особливо загострюється ця проблематика в контексті повномасштабної воєнної агресії, яку російська федерація веде проти України, де кожен аспект державної інформаційної політики стає не лише актуальним, але й стратегічно важливим завданням для збереження та захисту національних інтересів.

У цьому контексті важливо аналізувати та вдосконалювати інформаційну політику країни, використовуючи сучасні технології та міжнародний досвід, щоб ефективно протистояти впливові інформаційних атак і зміцнити внутрішню стійкість суспільства до маніпуляцій та дезінформації.

Основна частина

Сьогодні Україна стикається з серйозними викликами і загрозами у кіберпросторі через повномасштабну воєнну агресію російської федерації. Інформаційно-психологічний вплив росії має на меті дезорієнтацію суспільства, дестабілізацію ситуації в Україні та підрив довіри до уряду. Запровадження та розвиток ефективних стратегій протидії цим впливам у кіберпросторі стає критично важливим завданням для збереження національної безпеки та суверенітету України. Однією з найважливіших складових вирішення цієї проблеми є розвиток та впровадження ефективної державної інформаційної політики, спрямованої на протидію інформаційному впливу рф та зміцнення інформаційної безпеки України.

Розробка та впровадження ефективної державної інформаційної політики також має важливе стратегічне значення для зміцнення міжнародного образу України та її статусу в глобальній спільноті. В умовах кіберпростору інформаційні кампанії мають потенціал впливати не лише на внутрішні справи країни, але й на міжнародну дипломатію та економіку.

Правильно спланована та реалізована інформаційна політика може допомогти позитивно вплинути на сприйняття України як сучасної, демократичної та надійної держави, що дотримується міжнародних норм та стандартів. Це, в свою чергу, може сприяти залученню міжнародної підтримки, інвестицій та розвитку співробітництва з іншими країнами, що є важливим для зміцнення геополітичної позиції України та забезпечення стабільності в регіоні.

У рамках державної інформаційної політики необхідно встановити основи для вирішення ряду завдань, що включають формування єдиного інформаційного простору країни та її інтеграцію в світовий інформаційний простір, забезпечення інформаційної безпеки громадян, суспільства та держави, а також формування демократично налаштованої масової свідомості. Державна інформаційна політика повинна стати інструментом укріплення зв'язку між Центром та регіонами, сприяючи проведенню єдиної політики на всій території країни. Для вирішення цих завдань необхідне ефективне управління всіма типами інформаційних ресурсів, складовими інформаційно-телекомунікаційної інфраструктури, а також державною підтримкою вітчизняного інформаційного виробництва і розвитку ринку інформаційних технологій [7].

Швидкі дії в реакції на дезінформаційні кампанії російської федерації відображаються у створенні Центру протидії дезінформації при РНБО (ЦПД) та Центру стратегічних комунікацій та інформаційної безпеки Міністерства культури та інформаційної політики України (ЦСКІБ). Ці організації забезпечують моніторинг та аналіз інформаційних загроз національній безпеці України. Наприклад, з лютого 2022 року ЦПД активно проводив перевірку фактів і розвінчання неправдивої інформації на платформах Telegram і Twitter. Цей центр є офіційним

експертним інструментом для уряду України у боротьбі з російськими дезінформаційними кампаніями [3]. Крім того, за ініціативою Міністерства культури та інформаційної політики України та за підтримки посольства Швеції у липні 2022 року розпочалася реалізація проєкту «Школа протидії дезінформації» для працівників державної служби. Цей захід спрямований на підвищення рівня інформаційної стійкості та медіаграмотності серед працівників державного сектору і управління комунікаціями [4].

Подібні заходи можуть сприяти покращенню комунікації щодо розповсюдження інформації, наприклад, про «Батальйон Монако» (українських політиків та державних службовців, які виїхали за межі держави під час воєнного стану). Свобода доступу до інформації та свобода слова надзвичайно важливі для демократії. Однак, саме такі новини російська федерація швидко використовує для проведення інформаційно-психологічних операцій, які сприяють загостренню внутрішніх конфліктів в Україні, розбурхуючи ворожнечу між громадянами та підриваючи довіру до уряду.

Це досягається легко, оскільки російська сторона, здійснюючи ракетні удари, намагається посіяти хаос серед українського населення, використовуючи при цьому психологічні маніпуляції та наративи, такі як «зрада серед своїх» або «зрадники на Банковій». Вона також створює діпфейки, розповсюджуючи інформацію про те, що Президент та інші державні службовці давно виїхали з країни та перебувають за кордоном.

Ідея «Інформаційного Рамштайну» є предметом активних обговорень і визначається як ініціатива та новий формат міжнародного співробітництва, спрямований на протидію російській дезінформації та пропаганді. За словами Міністра культури та інформаційної політики Олександра Ткаченка, «Інформаційний Рамштайн» може стати ефективним інструментом для забезпечення інформаційної безпеки України та сприяти зміцненню співпраці з партнерськими країнами.

У межах цього міжнародного партнерства планується розробити комплекс спільних заходів та проєктів, встановити стратегічні цілі для боротьби з інформаційно-психологічними операціями російської федерації, налагодити зв'язки та комунікації, засновані на умовах спільного фінансування [6].

Розглядаючи цей проєкт як чинник впливу на систему протидії інформаційно-психологічному впливу з боку росії, можна зазначити, що він має найбільший позитивний ефект, оскільки сприяє розвитку розширеної співпраці з міжнародними ЗМІ, розвиває кіноіндустрію України та стимулює громадську активність українського населення.

За словами О. Ткаченка, «Інформаційний Рамштайн» розглядається у контексті трьох основних напрямів дій:

1. Зміцнення геополітичної позиції України та її міжнародного статусу як суверенної держави.

2. Приведення стратегій у відповідність до наявних ресурсів та можливостей учасників, а також узгодження зусиль державного та приватного секторів.

3. Розгортання глобальних ініціатив з метою зміцнення стійкості перед пропагандою та дезінформацією [6].

Створення так званої матеріальної бази є значним кроком у протидії інформаційно-психологічним операціям російської федерації на державному рівні. Ця база складається з сучасних технологій, які автоматично виконують фактчекінг (перевірку інформації), фільтрують та блокують її. Компанії з кібербезпеки, супутникові зображення (дистанційне зондування землі або Remote sensing), технологія Open source intelligence (OSINT) і штучний інтелект (ШІ) є критично важливими складовими цієї системи протидії інформаційно-психологічним операціям російської федерації [1, с. 595–597].

До стратегій державної інформаційної політики відноситься метод дистанційного зондування Землі (ДЗЗ), що дозволяє виявляти та відстежувати фізичні особливості місцевості та поверхні Землі з космосу або повітря. Цей інструмент вважається необхідною складовою тактики у військовій справі, використовуючи його для проведення бойової розвідки та моніторингу військових злочинів, зокрема в інформаційному оточенні [2, с. 119].

З початку повномасштабного вторгнення, цей процес включав у себе створення супутникових знімків та документування злочинів російської федерації. Інформацію про ці злочини почали активно висвітлювати міжнародні ЗМІ, журналісти New York Times, аналітичні центри та інші. Це не лише допомогло спростувати маніпулятивні «вкиди» з боку рф, що Україна якось сама провокувала обстріли міст, таких як Буча, Ірпінь, Маріуполь, Миколаїв, Запоріжжя тощо, але також сприяло визнанню росії державою-спонсором тероризму [1, с. 595–598].

Багато звичайних громадян не мають усвідомлення про розширені можливості пошуку, наданих Google, таких як пошук за зображенням, окремих файлів та документів у мережі Інтернет та соціальних мережах. Проте ці інструменти доступні для загального використання, і завдяки технології аналізу відкритих джерел інформації (OSINT) аналітики та журналісти на державному рівні сьогодні можуть розкривати фейкову інформацію та виявляти канали та джерела поширення інформаційно-психологічних операцій рф. Під час холодної війни Центральне розвідувальне управління та Комітет державної безпеки СРСР використовували аналіз відкритих джерел інформації для впливу на тенденції військових дій на свою користь, збираючи дані про військові, політичні та економічні можливості свого ворога [1, с. 595–598].

Технології OSINT і дистанційного зондування Землі (ДЗЗ) активно поєднуються, утворюючи своєрідну розвідку з відкритим кодом, що часто супроводжується конспірологічним мисленням. Наприклад, перед війною комерційні супутникові

знімки та відеоматеріали, опубліковані жителями російської федерації у соціальних мережах, зокрема на TikTok, дозволили журналістам і дослідникам підтвердити твердження Заходу про готовність росії до вторгнення. Крім того, з часом з'явилися докази того, що рф використовує зброю, заборонену згідно з усіма правилами та принципами справедливого ведення війни, в таких населених пунктах, як Нікополь, Марганець, Маріуполь, Мелітополь та інші [1, с. 595-600]. Саме ці підтверджені факти стали каталізатором об'єднання з міжнародною спільнотою у боротьбі проти рф не лише на полі бою, а й на інформаційному фронті.

Ще одним важливим інструментом у протидії інформаційно-психологічному впливу російської федерації є штучний інтелект, який дозволяє автоматизувати процес фільтрації інформації, включаючи джерела та емоційний контекст, який не завжди може помітити людське око. Проте існує чимало обурення щодо того, що штучний інтелект може збільшувати обсяг дезінформації в Інтернеті, автоматизуючи процес створення фейкових матеріалів. Виникли значні ризики з появою чат-ботів, які використовують великі мовні моделі, такі як ChatGPT OpenAI, які можуть створювати текст, що звучить природно, з одного натискання кнопки, в суті автоматизуючи виробництво дезінформації.

На жаль, країни, такі як росія та Китай, фінансують свої власні чат-боти. Проте штучний інтелект також має значний потенціал для зменшення шкоди, завданої фейковою інформацією [5].

Наприклад, Україна активно розвиває різноманітні проекти з фактчекінгу та використання блокчейну, де поєднуються зусилля фахівців та штучного інтелекту.

Один з таких проєктів – Texty, який використовує передові технології для швидкого аналізу тисяч каналів Telegram, де росія активно розповсюджує інформаційно-психологічні операції. Крім того, Detector Media застосовує машинне навчання та штучний інтелект для аналізу великих обсягів даних з метою розуміння та прогнозування майбутніх інформаційних кампаній кремля. Не менш важливою є співпраця з LetsData, українською приватною компанією, яка спеціалізується на штучному інтелекті та машинному навчанні. Спільно з LetsData, Detector Media здійснює моніторинг дискурсу та документує хроніки дезінформації кремля в реальному часі у понад 30 країнах. [1, с. 597–600].

Висновок

Виходячи з цього, для забезпечення інформаційної безпеки України надзвичайно важливо розробляти власні інструменти на основі штучного інтелекту з метою автоматизації та прискорення процесу пошуку дезінформації та її спростування. По-перше, необхідно забезпечити оперативне та швидке поширення інформації про інформаційно-психологічні операції, які проводить РФ, через заяви офіційних осіб та впливових особистостей. Далі, важливо комплексно удосконалювати правову базу інформаційної безпеки.

Окрім цього, необхідно розробити власні технології аналізу даних для виявлення інформаційно-психологічних операцій, поєднуючи їх з розвитком власних інструментів дистанційного зондування Землі, штучного інтелекту, нейромереж та супутникової навігаційної системи для отримання незалежної інформації.

Також необхідно налагодити надійну та своєчасну систему комунікації між урядом та громадянами. Важливим аспектом є розробка механізмів взаємодії між державними органами, науково-дослідними установами та приватним сектором з метою обміну інформацією та спільного реагування на загрози інформаційної безпеки. Співпраця між цими суб'єктами може значно підвищити ефективність заходів з протидії дезінформації та забезпечити більш швидкий реагування на виникаючі загрози.

При цьому важливим є розробка комплексної Національної OSINT-стратегії, яка визначатиме підхід уряду до збору, аналізу та розповсюдження розвід та інформаційних даних з відкритих джерел.

Крім того, необхідно інвестувати в розробку освітніх програм для підготовки наступного покоління висококваліфікованих фахівців, які будуть забезпечувати ефективну протидію інформаційно-психологічним операціям рф.

Література

[1] Hutchinson B. Information Warfare: Using the Viable System Model as a framework to attack organizations / B. Hutchinson, M. Warren. // Australasian Journal of Information Systems. 2012. Vol 9. № 2.

[2] Johnson L. S. Toward a Functional Model of Information Warfare / L. S. Johnson // Center for the Study of Intelligence. CIA.

[3] Грищук Р. В. Технологічні аспекти інформаційного протиборства на сучасному етапі / Р.В. Грищук, І.О. Канкін, В.В. Охрімчук // Захист інформації. 2015. Том 17. № 1 С. 80–86.

[4] Історія інформаційно-психологічного протиборства : підруч. / [Я.М. Жарков, Л.Ф. Компанцева, В.В. Остроухов В.М. Петрик, М.М. Присяжнюк, Є.Д. Скулиш]; за заг. Ред. д.ю.н., проф., засл. юриста України Є.Д. Скулиша. Київ : Наук.-вид. відділ НА СБ України, 2012. 212 с.

[5] Рачкевич М. Вийти з-під культурної тіні Росії: як Україна просуває культурну дипломатію // Радіо Свобода. URL: https://www.radiosvoboda.org/a/kulturna-dyplomatiya-ukrainskii-instytut/31117518.html.

[6] Ростислав Хотин Чому Україна визнала Чечню окупованою Росією і чи означає це визнання незалежності Ічкерії? // Радіо Свобода. URL: https://www.radiosvoboda.org/a/ukrayina-rosia-chechnya-nezalezhnist-ichkeria/32091704.html

[7] Чукут С.А., Джига Т.В. Інформаційна політика в Україні: навчальний посібник. Київ. 94 с.

ЗМІСТ

СЕКЦІЯ 1

«НАУКОВО-ТЕХНІЧНІ ТА ПРАКТИЧНІ АСПЕКТИ КІРБЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»

СЕКЦІЯ 2

«МЕТОДИ, ЗАСОБИ ТА ЗАХОДИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»