УДК 327. 004.056:355.02(477)
DOI https://doi.org/10.32782/2663-6170/2023.35.10

СУЧАСНІ ВИКЛИКИ ТА СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ РОСІЙСЬКОЇ АГРЕСІЇ: ПЕРСПЕКТИВИ ТА ЗАВДАННЯ

CURRENT CHALLENGES AND STRATEGIES OF ENSURING INFORMATION SECURITY IN UKRAINE IN THE CONDITIONS OF RUSSIAN AGGRESSION: PROSPECTS AND TASKS

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

Дана стаття розглядає сучасні виклики та стратегії забезпечення інформаційної безпеки України в умовах російської агресії. Аналізуються кібератаки, гібридна війна та дезінформація. Розглядаються стратегії кіберзахисту, міжнародне співробітництво та важливість освіти у галузі безпеки. Стаття висвітлює потребу в інноваційних рішеннях, законодавчих змінах та співпраці з приватним сектором для створення стійкої системи в умовах постійної загрози.

Стаття аналізує складні сценарії та виклики, з якими стикається Україна через російську агресію в інформаційному просторі. Обговорюється необхідність ефективних стратегій відповіді на кіберзагрози, враховуючи міжнародне співробітництво та важливість освіти для підготовки кадрів. Стаття також розглядає високотехнологічні рішення та інновації як критичні елементи в області забезпечення інформаційної безпеки. Приділено окрему увагу, стратегіям забезпечення інформаційної безпеки, названо та висвітлено основні підходи та рішення у контексті сучасних викликів, створених російською агресією. Здійснено обговорення перспектив розвитку та визначення завдань, які важливо вирішити в майбутньому, задля забезпечення ефективної інформаційної безпеки України в умовах постійних викликів.

Стаття завершується визначенням конкретних шляхів вдосконалення стратегій та систем інформаційної безпеки. Запропоновано практичні кроки, спрямовані на підвищення ефективності заходів з кіберзахисту та розвитку кіберспроможностей. У висновку статті відзначається необхідність спільних зусиль національних та міжнародних гравців у сфері інформаційної безпеки. Зазначається, що лише шляхом об'єднання зусиль можна ефективно протистояти складним викликам російської агресії та забезпечити стійкість інформаційного простору України.

Отже, стаття ставить за мету не лише аналіз сучасних викликів інформаційній безпеці, але і надає конкретні практичні рекомендації та стратегії для подолання цих викликів у контексті російської агресії.

Ключові слова: інформаційна безпека, інформаційний простір, інформаційна загроза, стратегії інформаційної безпеки, інформаційна загроза, кіберзагрози, гібридна війна, російська агресія.

This article examines modern challenges and strategies for ensuring information security of Ukraine in the conditions of Russian aggression. Cyber attacks, hybrid warfare and disinformation are analyzed. Cyber defense strategies, international cooperation and the importance of security education are discussed. The article highlights the need for innovative solutions, legislative changes and cooperation with the private sector to create a sustainable system in the face of constant threat.

The article analyzes the complex scenarios and challenges that Ukraine faces due to Russian aggression in the information space. The need for effective strategies to respond to cyber threats is discussed, taking into account international cooperation and the importance of education for training personnel. The article also considers high-tech solutions and innovations as critical elements in the field of ensuring information security. Particular attention is paid to strategies for ensuring information security, the main approaches and solutions in the context of modern challenges created by Russian aggression are named and highlighted. A discussion of development prospects and identification of tasks that are important to solve in the future in order to ensure effective information security of Ukraine in conditions of constant challenges was carried out.

The article concludes with the determination of specific ways of improving information security strategies and systems. Practical steps aimed at increasing the effectiveness of cyber defense measures and developing cyber capabilities are proposed. The conclusion of the article notes the need for joint efforts of national and international players in the field of information security. It is noted that only through joint efforts can one effectively resist the complex challenges of Russian aggression and ensure the stability of Ukraine's information space.

Therefore, the article aims not only to analyze modern challenges to information security, but also to provide specific practical recommendations and strategies for overcoming these challenges in the context of Russian aggression.

Key words: information security, information space, information threat, information security strategies, information threat, cyber threats, hybrid war, Russian aggression.

Постановка проблеми. Україна, як сучасна країна в умовах глобалізації та інформаційного розвитку, стає свідком та полем надзвичайно активної російської агресії, яка простягається не лише як у фізичний, але і не менш важливо – у віртуальний простір. Ця ситуація породжує величезні виклики для національної інформаційної безпеки, ризикуючи не лише технологічною стійкістю, але

й соціокультурним зламом. Російська агресія, яка виявляється окрім фізичного повномасштабного вторгнення, проявляється також і через кібератаки, дезінформацію та гібридну війну, створює складну, що у свою чергу створює складну інформаційну обстановку. Ця ситуація не лише піддає сумніву надійність джерел інформації, але й загрожує безпеці особистих даних, функціонуванню критичних інфраструктур та загрожує соціокультурній єдності країни.

В умовах сучасних технологічних досягнень, роль кіберзагроз у веденні агресивних дій збільшується. Російські хакерські групи ведуть не тільки кібершпигунство, але й вдаються до руйнівних кібератак на українські інфраструктури. Це порушує не тільки стійкість державних інформаційних систем, але й ставить під загрозу економіку та національну безпеку. Російська гібридна війна включає елементи дезінформації та психологічної війни, спрямовані на дестабілізацію суспільства та порушення довіри до владних структур. Систематичне поширення фейків та маніпуляція інформацією створюють серйозні перешкоди для формування об'єктивного світогляду громадян та національної єдності. У цьому контексті, варто відзначити важливість даної проблематики та розглянути детальніше, які саме виклика стоять перед нами сьогодні та, як нам з цим боротися на полі інформаційної арени.

Аналіз останніх досліджень і публікацій. Вчені з України та інших країн активно приносять величезний внесок у розробку та реалізацію стратегій забезпечення інформаційної безпеки України в умовах російської агресії. Їхні дослідження охоплюють широкий спектр аспектів, від розробки технологій кіберзахисту та виявлення кіберзагроз до вивчення впливу дезінформації та психологічних аспектів інформаційної безпеки. Серед дослідження наукового доробку сучасного інформаційно-безпекового простору варто відзначити таких вітчизняних вчених як: Дергачов О. (Інститут Кібербезпеки НАНУ – розробляє технології виявлення та захисту від кіберзагроз), Лисенко М. (кібершкола KNU – активно залучена до освітніх програм у галузі кібербезпеки), Гайдамака С. (Інститут Інформаційних Технологій та Засобів Навчання НАПН України – вчений спеціалізується на розробці систем безпеки інформаційних технологій), Кащук Ю. (Київський Політехнічний Інститут – веде дослідження з інтеграції кіберзахисту в інфраструктуру критичних об'єктів України) та ін. Ці вчені та дослідники відіграють ключову роль у розвитку інформаційної безпеки в Україні через свій внесок у дослідження, розробку технологій та навчання нового покоління фахівців у цій області, особливо в у військовий період. Щодо зарубіжного досвіду, слід відзначити, що в світі щороку дедалі більше вчених намагається зрозуміти проблеми та виклики інформаційної безпеки в Україні з міжнародної перспективи та висвітлити проблеми та стратегії кібербезпеки в контексті російської агресії для широко загалу. Так, американська дослідниця Доктор Кімберлі Мартіно у працях: "Кіберстійкість України: Поворотний момент в історії", "Протидія інформаційній війні: уроки з України" – досліджує кіберстійкість України та її ключового значення в історії, а також аналіз методів протистояння інформаційній війні; Т. Рід: "Атрибуція кібератак", Активні заходи: Історія дезінформації та політичної війни" – вивчає історію дезінформації та політичної війни на прикладах сучасних конфліктів та воєн; Я. Каленський: "Стійкість до дезінформації в Центральній та Східній Європі", "Боротьба України з інформаційною війною: Тріумф рішучості" – фокусування на дослідженні стійкості до дезінформації в Центральній та Східній Європі, а також аналіз інформаційної війни та заходів України для її подолання.

Ці та багато інших вчених допомагають розуміти виклики інформаційної безпеки в Україні з міжнародної перспективи та висвітлюють проблеми та стратегії кібербезпеки в контексті російської агресії.

Виділення невирішених раніше частин загальної проблеми. Досліджуючи стратегії забезпечення інформаційної безпеки, варто зупинитись на таких основних викликах та аспектах, як: кіберзагрози та гібридна війна (із зростанням технологічних можливостей російської сторони, важливо розглядати нові форми кіберзагроз та гібридної війни, які можуть виникати в контексті інформаційної безпеки), захист критичної інфраструктури (питання захисту критичної інфраструктури залишається невирішеним, особливо в умовах можливих кібератак на енергетичні, транспортні та інші системи), інформаційна гігієна громадян (залучення громадян до збереження власної інформаційної безпеки та підвищення рівня інформаційної гігієни залишається актуальною проблемою), міжнародна підтримка (Невирішеною залишається проблема підвищення рівня міжнародної співпраці в області кібербезпеки для вирішення глобальних викликів та обміну інформацією). Ці невирішені аспекти формують основу для подальших досліджень та розробки стратегій забезпечення інформаційної безпеки в Україні в умовах сучасної геополітичної ситуації.

Формулювання цілей статті (постановка завдання). Мета статі полягає у ретельному аналізі інформаційної безпеки, висвітленні актуальних викликів та розробці стратегій для справжнього захисту в умовах постійної загрози кібератак та гібридної війни. Основні цілі статті:

− Проаналізувати сучасні виклики для інформаційної безпеки України: ретельний розгляд та ідентифікація конкретних викликів, що виника-

ють в контексті російської агресії та їхній вплив на інформаційну безпеку України.

− Визначити стратегії захисту: розробка конкретних стратегій та заходів для забезпечення ефективного захисту інформаційних ресурсів та інфраструктури України.

− Оцінка перспектив розвитку: визначення можливих напрямків розвитку інформаційної безпеки в Україні та визначення стратегій для ефективного впорядкування із сучасними та майбутніми викликами.

− Формулювання рекомендацій: надання конкретних рекомендацій для удосконалення інформаційної безпеки на різних рівнях, від індивідуального користувача до державних структур.

− Висвітлення заходів для активного захисту: підкреслення важливості активних заходів, включаючи освіту, технічні інновації та міжнародне співробітництво, для забезпечення повноцінного захисту інформаційного простору.

Дані завдання спрямовані на створення інформативної, стратегічної та практичної основи для подальшого розвитку та зміцнення інформаційної безпеки України в умовах російської агресії.

Виклад основного матеріалу дослідження. У сучасному світі, де технологічний розвиток прискорюється, інформаційна безпека стає фундаментальним аспектом національної безпеки, особливо для країн, які зазнають впливу геополітичних конфліктів та воєн. Російська агресія в Україні виявилася не лише військовою загрозою, але й систематичними атаками на інформаційний простір, спрямованими на дестабілізацію внутрішнього порядку та порушення національної безпеки. Сутність проблеми полягає в тому, що інформаційний простір України став полем бою, де кіберзагрози стають ефективним інструментом гібридної війни. Російські кібератаки націлені на враження не лише на військові об'єкти, а й на господарську інфраструктуру та суспільство загалом, переплітаючи фізичний та кібернетичний фронти. Розгортання російської агресії та її вплив на інформаційну безпеку ставить перед Україною нагальні завдання в області кіберзахисту, вивчення новітніх методів кібератак та розробки стратегій для протидії цим загрозам [4, с. 89].

Актуальність цієї теми полягає в необхідності розуміння та вирішення системних проблем інформаційної безпеки для забезпечення стабільності та безпеки країни в умовах геополітичних турбуленцій. Сучасні виклики інформаційної безпеки в Україні невдовзі стали не лише технічним завданням, а й складною мозаєкою гібридних загроз, в основі яких лежать різні форми кібератак та дезінформації. Розглядаючи сучасні виклики інформаційної безпеки в Україні, ми виявляємо два ключові аспекти: кібератаки та дезінформацію, які стали необхідними компонентами гібридної війни, що веде Росія. У контексті російської агресії, кібератаки відіграють ключову роль у веденні гібридної війни. Російська сторона активно використовує технічні засоби для порушення інформаційної безпеки України. Це включає в себе напади на критичну інфраструктуру, великі корпоративні системи та спроби отримання конфіденційної інформації [5, с. 20-23]. Адже, гібридна війна, яку Росія веде проти України, не обмежується лише військовими операціями. Вона включає в себе широкий спектр інструментів, таких як економічний тиск, дипломатичні впливи та особливо ефективну інформаційну складову. Аналізуючи цей аспект, можна визначити, як Росія використовує гібридну війну для досягнення своїх політичних та стратегічних цілей. Сюди відносимо: дезінформаційні кампанії (російські дезінформаційні кампанії не лише створюють хаос та непевність, але й спрямовані на вплив на громадську думку) [3, с. 4-5].

Дослідження механізмів дезінформації дозволить виявити вразливі точки та слабкі місця. Розгляд інноваційних стратегій для протидії впливу дезінформації та підвищення інформаційної грамотності суспільства стане основою для розробки ефективних методів контрдії. Тому, стає очевидним, що кібератаки та дезінформаційні кампанії, які здійснює Росія в контексті агресії проти України, стали не тільки загрозою технічної безпеки, але й складною гібридною стратегією впливу. Кібератаки виявляються ключовим інструментом для порушення інформаційної стійкості, водночас дезінформаційні кампанії викликають глибокий соціокультурний вплив.

В умовах постійної російської агресії та неперерваної кіберзагрози, стратегії забезпечення інформаційної безпеки для України стають ключовим фактором у збереженні національної безпеки та суверенітету. В цьому контексті розглядаємо ключові аспекти стратегічного планування та реалізації заходів, спрямованих на забезпечення інформаційної безпеки країни:

1. Кіберзахист та Заходи Кібербезпеки: розробка та впровадження передових систем, таких як системи виявлення вторгнень та протишпигунства, для ефективної оборони від кібератак, проведення освітніх кампаній щодо безпечного користування інтернетом та протидії соціальному інженерингу.

2. Розвиток військових кіберпідрозділів для ефективного опору кіберагресії та захисту критично важливої інфраструктури.

3. Фінансування та підтримка інновацій у галузі кібербезпеки та власних технологічних розробок.

4. Моніторинг та виявлення вторгнень: встановлення систем для постійного моніторингу та виявлення вторгнень у інформаційний простір.

5. Медійна грамотність: розвиток медійної грамотності для ефективного визначення та протидії дезінформації [2, с. 136-141].

Спільна мета даних стратегій – створення комплексного та взаємодіючого підходу до забезпечення інформаційної безпеки України в умовах російської агресії. Проте, забезпечення інформаційної безпеки не може бути вирішеним національними зусиллями однієї країни. Міжнародна співпраця грає ключову роль у формуванні відповідальності та ефективної реакції на кіберзагрози. Саме міжнародна кооперація та співпраця є стратегічно важливим елементом у забезпеченні інформаційної безпеки України та в реагуванні на виклики російської агресії в кіберпросторі. Виділимо основні сфери та стратегії співпраці України з іншими країнами та міжнародними організаціями:

1. Участь у Міжнародних Організаціях: активна участь у міжнародних організаціях, таких як Інтерпол, ООН та Європейський Союз, для обміну інформацією та розробки спільних стратегій.

2. Укладання двосторонніх угод: встановлення партнерств та угод із стратегічними країнами для обміну інформацією та спільної боротьби з кіберзагрозами.

3. Спільні технічні проєкти: участь у спільних технічних проєктах та дослідженнях з іншими країнами для розробки нових засобів та стратегій кібербезпеки.

4. Спільна кібернавігація: об'єднання зусиль для створення міжнародної системи моніторингу та виявлення кіберзагроз.

5. Взаємодія у сфері захисту прав людини [1, с. 43-44].

Наводячи, приклади спільних ініціатив України та країн західних партнерів в сфері запезпечення інформаійного простору України та Європи загалом, слід зазначити про проведення спільних інформаційних кампаній (для виявлення та розкриття дезінформації, яка надходить з боку російських джерел. Розробка спільних повідомлень та матеріалів, щоб розкрити маніпуляції і введення в оману); участь в міжнародних кіберкоаліціях, які об'єднують сили для взаємодії та реагування на кіберзагрози з боку Росії; спільні технічні операції з захоплення інфраструктури, використованої для здійснення кібератак, для зменшення їхньої ефективності; створення міжнародних експертних груп для спільного аналізу та розслідування кіберінцидентів, пов'язаних із російською агресією. Ці приклади вказують на важливість співпраці України з міжнародними партнерами у сфері інформаційної безпеки для ефективного протидії кіберзагрозам з боку Росії.

Освіта в галузі інформаційної безпеки є ще однією стратегічною ланкою та ключовим чинником для забезпечення стійкості суспільства в умовах російської агресії. Адже, інформаційна безпека визначається не лише технічними заходами, але й глибоким розумінням інформаційних ризиків, етичних аспектів та здатністю ефективно реагувати на змінюючіться ситуації. Освічені та підготовлені кадри є основною ланкою в боротьбі з кіберзагрозами та дезінформацією. Основні завдання, які ставить перед собою едукаційна стратегія:

− Розширення освітніх програм (розробка та впровадження більш широкого спектру освітніх програм у галузі інформаційної безпеки, охоплюючи аспекти кіберзахисту, кібербезпеки та боротьби з дезінформацією).

− Підвищення рівня технічних навичок: (спрямування зусиль на підготовку фахівців з високим рівнем технічних знань, які здатні ефективно виявляти та протидіяти кіберзагрозам).

− Створення інноваційних навчальних центрів (розробка та підтримка іноваційних навчальних центрів, що сприяють практичній підготовці та використанню сучасних технологій) [7, с. 125-127].

Ефективна підготовка кадрів у галузі інформаційної безпеки є стратегічно важливою для забезпечення стійкості суспільства в умовах російської агресії. Освіта створює основу для розвитку кваліфікованих фахівців, здатних адаптуватися до постійно змінного інформаційного середовища та ефективно протидіяти сучасним безпековим викликам.

Таким чином, у контексті постійно зростаючої загрози російської агресії після 2014 року та її впливу на інформаційну безпеку України особливо з початку 2022 року, визначення майбутніх викликів стає надзвичайно важливим завданням. Прогноз показує, що кіберзагрози та методи гібридної війни будуть продовжувати еволюцію, створюючи нові виклики та перспективи для країни, що у свою чергу потребує комплексного використання вище розглянутих стратегій, для збереження суверенітету держави та її комплексної відбудови.

Висновки. У світлі постійних загроз російської агресії інформаційна безпека України вимагає не лише уважності, а й стратегічного та інноваційного підходу. Стаття розкрила низку викликів, які постають перед країною в цьому контексті, вказуючи на необхідність негайних заходів. Огляд сучасних стратегій та викликів забезпечення інформаційної безпеки дозволив сформулювати ключові напрями розвитку. Від технологічності та розробки інноваційних рішень до зміцнення кадрового потенціалу та міжнародного співробітництва – кожен аспект має важливу роль у створенні надійного щита перед загрозами. Спільна відповідь українського уряду, впровадження законодавчих змін, удоскона-

лення правового поля щодо питання кібербезпеки, роль приватного сектору та міжнародних партнерів є вирішальною для забезпечення інформаційної безпеки. Саме розуміння прогнозованих викликів та наполегливе вдосконалення стратегій дозволять Україні зберегти контроль над своєю інформаційною сферою та забезпечити стійкість у вирішальні моменти. Адже, наше основне завдання на майбутнє – це постійно вдосконалювати стратегії інформаційного захисту, бути гнучкими в адаптації до нових загроз і навчатися від кожного етапу відповідаючи на агресію. Лише таким чином Україна може побудувати надійний фундамент для своєї інформаційної безпеки та захистити себе від сучасних та еволюціонуючих загроз на сучасній геополітичній арені.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бондаренко В. О., Литвиненко О. В. (2013). Інформаційна безпека сучасної держави: концептуальні роздуми URL: http://www.crime-research.iatp.org.ua/library/strateg.html (Дата звернення 28.11.2023)
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.
3. Гусаров В. (2014). Кремль розпочав нову інформаційну операцію проти України URL: http://www.osvita.mediasapiens.ua/material/34281.
4. Довгань О.Д., Ткачук Т.Ю. Система інформаційної безпеки України: онтологічні виміри. Інформація і право. № 1(24)/2018. С. 89-103.
5. Залєвська І.І., Удренас Г.І. Інформаційна безпека України в умовах російської військової агресії. Південноукраїнський правничий часопис. 2022. № 1-2. С. 20-26.
6. Кузьмінська Р.В. Забезпечення інформаційної безпеки України в умоваї російсько-української війни. Київ, 2023. С. 38-42.
7. Турчак А.В. Основні засади державної політики забезпечення інформаційної безпеки в Україні. Інвестиції: практика та досвід. 2019. №11. С.123-127.
8. Jakub Kalenský (2018). "Ukraine's Struggle with Information Warfare: A Triumph of Resolve".
9. Hybrid Warfare (2019). URL: http://www.gao.gov/assets/100/97053.pdf.
10. Kimberly Martineau (2022). "Ukraine's Cyber Resilience: A Pivotal Point in History".