РОЗДІЛ 1
АКТУАЛЬНІ ПИТАННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

УДК 351.862.4(477)«364»
DOI https://doi.org/10.32782/2786-9385/2024-4-1

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ПОВНОМАСШТАБНОГО ВТОРГНЕННЯ

Владімірова Карина Павлівна,
здобувач кафедри національної безпеки
Волинського національного університету імені Лесі Українки
ORCID ID: 0009-0004-7745-7452

Стрелков Владислав Володимирович,
Ph. D., старший викладач кафедри національної безпеки
Волинського національного університету імені Лесі Українки
ORCID ID: 0000-0001-8436-3260

Статтю присвячено дослідженню проблем забезпечення інформаційної безпеки України в умовах повномасштабного вторгнення російської федерації на її територію. Автори не оминули увагою й ключові події та інцидент що передували цьому вторгненню, однак мали небезпечний характер та несли відповідні ризики та загрози для національних інтересів України, готували відповідний ґрунт для вторгнення, були своєрідними «пробами пера» в контексті загострення та поглиблення гібридної агресії російської федерації проти України. Дослідити такі гібридні акції впливу інформаційного характеру вдалося завдяки використанню методу "case-study", який передбачає виокремлення та вивчення окремих випадків та прецедентів. Також автори застосували метод структурно-функціонального аналізу для дослідження структур що забезпечують захист інформаційного простору України від ворожих впливів. Окрему увагу приділено дослідженню стратегічних документів в галузі, які було розглянуто із застосуванням методу контент-аналізу. Серед тенденцій що спостерігаються в інформаційному просторі України в контексті протистояння збройній агресії автори виділяють урізноманітнення та збільшення кількості загроз. Оперативне реагування на ці загрози значно ускладнене через брак кваліфікованих спеціалістів у галузі та недостатнє фінансування в умовах коли значний фінансовий ресурс з об'єктивних причин скеровано на забезпечення відсічі загрозам воєнного характеру. Автори встановили, що Україна досягла значного прогресу в питаннях забезпечення інформаційної безпеки, однак швидкість з якою рухається розвиток та вдосконалення сучасних технологій в галузі вимагає від українського уряду нової якості управлінських рішень задля захисту інформаційного простору держави.

Ключові слова: *інформаційна безпека, повномасштабне вторгнення, національна безпека, кібербезпека, інформаційно-психологічні операції.*

Vladimirova Karyna, Strelkov Vladyslav. Information Security of Ukraine during a full-scale invasion

The article is devoted to the study of the problems of ensuring information security of Ukraine in the conditions of a full-scale invasion of the Russian Federation on its territory. The authors did not ignore the key events and incidents that preceded this invasion, however, they were of a dangerous nature and carried corresponding risks and threats to the national interests of Ukraine, prepared the appropriate ground for the invasion, were a kind of "pen tests" in the context of the exacerbation and deepening of the hybrid aggression of the Russian Federation against Ukraine. It was possible to investigate such hybrid actions of the influence of an information nature thanks to the use of the "case-study" method, which involves the selection and study of individual cases and precedents. The authors also used the method of structural and functional analysis to study the structures that ensure the protection of the information space of Ukraine from hostile influences. Particular attention is paid to the study of strategic documents in the industry,

which were considered using the method of content analysis. Among the trends observed in the information space of Ukraine in the context of resistance to armed aggression, the authors highlight the diversification and increase in the number of threats. Prompt response to these threats is significantly complicated by the lack of qualified specialists in the field and insufficient funding in conditions where a significant financial resource is directed for objective reasons to countering threats of a military nature. The authors established that Ukraine has made significant progress in ensuring information security, but the speed with which the development and improvement of modern technologies in the field is moving requires the Ukrainian government to make new quality management decisions to protect the information space of the state.

Key words: *information security, full-scale invasion, national security, cyber security, information and psychological operations.*

Вступ. Актуальність дослідження проблематики забезпечення інформаційної безпеки України в умовах повномасштабного вторгнення є надзвичайно високою з огляду на сучасний геополітичний контекст та вплив інформаційної безпеки на національну безпеку загалом. З початком повномасштабного вторгнення РФ в Україну, питання інформаційної безпеки стало критично важливим для захисту суверенітету, територіальної цілісності та демократичних інститутів держави.

Вторгнення РФ в Україну супроводжується масштабними кібератаками на урядові та приватні установи, що включає спроби зламів, розповсюдження шкідливого програмного забезпечення, а також спроби виведення з ладу важливих сервісів і систем. Успішні атаки можуть призвести до значних економічних втрат, збоїв у роботі критичної інфраструктури та поширення паніки серед населення. Також агресор ставить за мету зломити опір цивільного населення, переконати громадян в тому що спротив окупанту не має сенсу та перспектив, за допомогою проведення інформаційно-психологічних спеціальних операцій в українському інформаційному просторі.

Інформаційна безпека охоплює захист від кібератак, поширення пропаганди та дезінформації, забезпечення безпеки критичної інформаційної інфраструктури, а також захист інших національних інтересів в інформаційному просторі. У сучасних умовах воєнного конфлікту інформаційні атаки стають невід'ємною частиною агресії, що ведеться як на полі бою, так і в інформаційній площині. Відповідно, забезпечення стійкості до таких загроз є життєво необхідним для підтримки морального духу населення, функціонування державних структур і захисту стратегічних об'єктів. Дослідження проблематики інформаційної безпеки як складової компоненти національної безпеки дозволить ефективно протидіяти агресії, підтримувати стабільність всередині країни та забезпечувати надійну роботу ключових державних та приватних структур.

Матеріали та метод. У цьому дослідженні автори ставлять перед собою за мету висвітлити стан захищеності інформаційного простору в Україні в умовах повномасштабного простора, оцінити ефективність заходів, які наша держава застосовує для захисту власного інформаційного середовища, виявити проблеми у цій галузі, які потребують невідкладного вирішення. Дослідження ґрунтується на публікаціях засобів масової інформації, звітах міжнародних організацій, аналізі керівних документів довгострокового планування у сфері національної безпеки. Серед методів, що використовувалися авторами, слід відзначити такі: структурно-функціональний, контент-аналізу та "case-study".

Результати. Відповідно до усталеного визначення, «інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення» [4, с. 55].

Інформаційна безпека держави характеризується ступенем захище-

ності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості та ін.) та її здатністю протистояти небезпечним впливам (дестабілізаційним, деструктивним тощо), в тому числі інформаційного характеру. Державні структури та служби повинні бути здатні та готові як до вилучення контенту що містить загрози та небезпеки, так і до впровадження контрзаходів в інформаційному просторі.

В Україні забезпечення інформаційної безпеки здійснюється через низку органів, структур та служб, усі вони виконують свої специфічні завдання:

– Рада національної безпеки і оборони України (РНБО). Розробляє і координує виконання стратегій і політик у сфері інформаційної безпеки. Центр протидії дезінформації при РНБО займається виявленням і протидією дезінформації, пропаганді та іншими деструктивними інформаційними впливами [6];

– Центр стратегічних комунікацій та інформаційної безпеки. Розробляє контрнаративи, проводить інформаційні кампанії і працює над підвищенням медіаграмотності населення. Взаємодіє з громадянським суспільством і міжнародними партнерами для посилення стійкості до гібридних загроз [8];

– Міністерство оборони України. Відповідає за інформаційну безпеку у військовій сфері, включаючи протидію дезінформації в умовах військових конфліктів [5].

– Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ). Забезпечує кібербезпеку та захист державних інформаційних ресурсів [2].

– Державний комітет телебачення і радіомовлення України. Контролює медійний простір і захист національного інформаційного суверенітету [3].

Крім вищезазначених суб'єктів, в Україні діє Стратегія інформаційної безпеки до 2025 р., яка є документом довгострокового планування та визначає основні цілі, напрями і принципи державної політики у цій сфері. Основна мета запровадження та втілення цієї стратегії – захист інформаційного суверенітету і забезпечення національних інтересів України [7].

Перелічені структури, на підставі та в рамках визначеної нормативно-правової бази, формують комплексну систему забезпечення інформаційної безпеки, спрямовану на захист від внутрішніх і зовнішніх загроз, розвиток національного інформаційного простору та підвищення стійкості до дезінформації та пропаганди.

Сучасний стан інформаційної безпеки України є «надзвичайно складним та динамічним, зумовленим постійними загрозами, що виникають в умовах повномасштабного військового вторгнення Росії. Основні виклики включають кібератаки, дезінформаційні кампанії та пропаганду, спрямовані на підрив національної безпеки, дестабілізацію суспільства та дискредитацію української влади» [7].

Разом із повномасштабним воєнним вторгненням росія значно активізувала застосування невоєнних методів, які вона використовує для досягнення стратегічних воєнних цілей, До них відносяться й інформаційні атаки, які є елементом гібридної війни проти України та спрямовані як на державні установи, так і на приватний сектор. Кібератаки стали масштабнішими і складнішими, націленими на критичну інфраструктуру, включаючи енергетичні системи, телекомунікаційні мережі та фінансові установи. Відповіддю нашої держави на ці загрози стало зміцнення кібербезпеки, посилення захисту інформаційних систем та розробку нових стратегій протидії кібератакам.

Дезінформаційні кампанії та пропаганда й нині залишаються потужними інструментами у гібридній війні. Російські медіа та соціальні мережі використовуються для поширення фейкових новин, маніпуляції громадською думкою та поширення панічних настроїв. Україна активно працює над протидією цим загрозам шляхом підвищення медіаграмотності населення, розробки

механізмів виявлення та спростування фейкової інформації, а також співпраці з міжнародними організаціями та партнерами [7].

Законодавча та нормативно-правова база України у сфері інформаційної безпеки постійно вдосконалюється. Було прийнято ряд законів та постанов, спрямованих на посилення інформаційної безпеки, включаючи закони про кібербезпеку та інформаційну політику. Водночас, державні органи та спецслужби активізували свою діяльність у сфері кіберзахисту, що включає як превентивні заходи, так і швидке реагування на інциденти.

Незважаючи на значні досягнення, існують і певні проблеми. Недостатнє фінансування та брак фахівців у сфері кібербезпеки залишаються серйозними викликами. Крім того, необхідно постійно вдосконалювати технічну базу та методи протидії новим загрозам. Проблемні моменти щодо захисту кіберпростору викристалізувалися у відповідних «кейсах», про які піде мова далі.

У грудні 2015 р. відбувся один із найвідоміших випадків кібератаки на українські об'єкти критичної енергетичної інфраструктури, коли російські хакери зламали інформаційні системи кількох енергетичних компаній і відключили електропостачання в частині західних регіонів України. Це призвело до масштабних перебоїв у постачанні електроенергії, що торкнулося сотень тисяч громадян. Ця атака показала вразливість критичної інфраструктури та необхідність посилення кіберзахисту [1].

Ще одним значущим випадком стала атака вірусом "NotPetya" у червні 2017 р. Цей вірус, замаскований під програму для бухгалтерського обліку, швидко поширився по мережах українських компаній та урядових установ, спричинивши значні фінансові збитки та порушення роботи багатьох систем. Хоча вірус поширився і на інші країни, Україна постраждала найбільше. Наслідки цієї атаки були настільки серйозними, що дехто назвав її наймасштабнішою кібератакою в історії.

Іншим прикладом є атака на українські державні веб-сайти в січні 2022 р., коли на головних сторінках урядових сайтів з'явилися повідомлення з погрозами та дезінформацією. Ці атаки мали на меті створити хаос і продемонструвати вразливість українських інформаційних ресурсів напередодні вторгнення.

Росія також активно використовує дезінформаційні кампанії в рамках проведення інформаційно психологічних операцій. Під час повномасштабного вторгнення в 2022 р. російські пропагандистські ЗМІ та соціальні мережі масово поширювали фейкові новини та маніпулятивні повідомлення. Наприклад, було запущено кілька кампаній, що стверджували про капітуляцію українських військових частин або про вигадані «злочини» української армії проти мирного населення. Метою таких дій було деморалізація українського суспільства та підрив довіри до української влади та збройних сил. Ці дезінформаційні атаки створювали паніку, плутанину серед громадян та поширювали недовіру до представників та органів державної влади [2].

Наслідки цих атак включають не лише матеріальні збитки та перебої в роботі критичних систем, але й значний психологічний вплив на населення. Вони підривають довіру до урядових структур та створюють атмосферу невизначеності та страху. Ці події підкреслюють важливість зміцнення кібербезпеки, розробки ефективних стратегій протидії дезінформації та пропаганді, а також постійного вдосконалення захисту критичної інфраструктури. Можемо говорити про те, що сучасний стан інформаційної безпеки України характеризується постійною боротьбою з численними та різноманітними загрозами. За таких умов, активна та результативна робота щодо зміцнення кібербезпеки, підвищення медіаграмотності громадян та міжнародної співпраці, може створити передумови для ефективної протидії інформаційним атакам. Однак підкреслимо, що робота в цьому напрямку потребує подальшого розвитку та вдосконалення.

Оцінка ефективності заходів, вжитих Україною для захисту інформаційної безпеки, показує значний прогрес, хоча й існують певні виклики та недоліки. Україна здійснила ряд кроків, мова про них піде нижче, для зміцнення своєї кібербезпеки та протидії дезінформації, що включає оновлення законодавчої бази, покращення технічних засобів захисту та міжнародну співпрацю.

Український уряд прийняв низку законів і постанов, спрямованих на посилення кібербезпеки та боротьбу з інформаційними загрозами. Зокрема, було затверджено національні стратегії з кібербезпеки та інформаційної безпеки, які визначають основні напрями діяльності та заходи для захисту інформаційного простору країни. Це дозволило створити більш структуровану і цілеспрямовану систему реагування на інформаційні атаки.

Реалізація технічних заходів включає впровадження сучасних систем кіберзахисту та моніторингу, що дозволяють виявляти і нейтралізувати загрози на ранніх етапах. Українські державні органи та великі приватні компанії поступово переходять на використання більш захищених програмних продуктів і протоколів зв'язку, що значно підвищує рівень кібербезпеки. Також створено спеціальні кіберпідрозділи в структурах Міністерства оборони та Служби безпеки України, які займаються виключно питаннями кіберзахисту.

Міжнародна співпраця відіграє важливу роль у зміцненні інформаційної безпеки України. Співпраця з НАТО, Європейським Союзом, США та іншими міжнародними партнерами дозволяє Україні отримувати необхідну технічну та експертну підтримку, обмінюватися інформацією про кіберзагрози та впроваджувати передові практики захисту. Крім того, міжнародні санкції проти росії, введені за її агресивні дії, також мають стримуючий ефект.

Однак, попри досягнення, існують і певні проблеми. Однією з головних є недостатнє фінансування та брак висококваліфікованих фахівців у сфері кібербезпеки. Це ускладнює швидке реагування на нові загрози та впровадження новітніх технологій. Також, в умовах війни, ресурси часто перенаправляються на нагальні військові потреби, що може послаблювати увагу до інформаційної безпеки.

Крім того, боротьба з дезінформацією та пропагандою вимагає постійного вдосконалення методів виявлення та нейтралізації фейкових новин. Хоча Україна досягла значного прогресу в цьому напрямі, все ще існує потреба в підвищенні медіаграмотності населення та покращенні співпраці з соціальними мережами та медіаплатформами для швидшого видалення шкідливого контенту.

Висновки. Події повномасштабного вторгнення РФ в Україну засвідчили, що забезпечення інформаційної безпеки має критичне значення для національної безпеки країни. З початком вторгнення росії в Україну, інформаційна безпека набула особливого значення, ставши одним з ключових елементів захисту держави. Україна зіткнулася з потужними кібератаками, дезінформаційними кампаніями та пропагандою, спрямованими на підрив стабільності, морального духу населення та функціонування критичної інфраструктури.

Зусилля України щодо зміцнення інформаційної безпеки включають оновлення законодавчої бази, впровадження сучасних технологій кіберзахисту та активну міжнародну співпрацю. Прийняття національних стратегій з кібербезпеки та інформаційної безпеки стало важливим кроком у структуризації зусиль держави в цьому напрямі. Технічні заходи, такі як створення кіберпідрозділів та впровадження передових систем захисту, підвищують здатність України протидіяти кіберзагрозам.

Однак, існують і певні проблеми. Недостатнє фінансування та брак висококваліфікованих фахівців у сфері кібербезпеки залишаються серйозними викликами. Боротися з дезінформацією та пропагандою теж є складним завданням, яке потребує постійного вдосконалення методів виявлення спеціальних інформаційно-психологічних впливів,

локалізації та нейтралізації їх наслідків, а також підвищення медіаграмотності суспільства.

Вжиті Україною заходи для захисту національних інтересів в інформаційній сфері демонструють ефективність і поступовий прогрес, хоча й потребують подальшого вдосконалення та більшої підтримки для повної реалізації потенціалу захисних механізмів.

ЛІТЕРАТУРА:

1. Аудит інформаційної безпеки : підручник / В. А. Ромака та ін. Львів : Сполом, 2015. 363 с.

2. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua (дата звернення 02.05.2024).

3. Державний комітет телебачення і радіомовлення України. URL: https://comin.gov.ua/ (дата звернення 03.05.2024).

4. Кормич Б. А. Інформаційне право : підручник. Харків : Бурун і К, 2011. 333 с.

5. Міністерство оборони України. URL: https://www.mil.gov.ua/ (дата звернення 05.05.2024).

6. Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/ (дата звернення 09.05.2024).

7. Стратегія інформаційної безпеки до 2025 р. URL: https://ips.ligazakon.net/document/JG3TH00A (дата звернення 09.05.2024).

8. Центр стратегічних комунікацій та інформаційної безпеки. URL: https://spravdi.gov.ua/ (дата звернення 12.05.2024).

9. Цимбалюк В. С. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Київ : НТУУ «КПІ», 2001. № 4.

REFERENCES:

1. Romaka V. A. (2015). Audyt informatsiinoi bezpeky : pidruchnyk [Information security audit: textbook]. Lviv : Spolom. 363 s. [in Ukrainian]

2. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy (2024). Official site [Official site]. Retrieved from: https://cip.gov.ua/ua [in Ukrainian]

3. Derzhavnyi komitet telebachennia i radiomovlennia Ukrainy (2024). Official site [Official site]. Retrieved from: https://comin.gov.ua/ [in Ukrainian]

4. Kormych B. A. (2011). Informatsiine pravo : pidruchnyk [Information law: textbook]. Kharkiv : Burun i K. 333 s. [in Ukrainian]

5. Ministerstvo oborony Ukrainy (2024). Official site [Official site]. Retrieved from: https://www.mil.gov.ua/ [in Ukrainian]

6. Rada natsionalnoi bezpeky i oborony Ukrainy (2024). Official site [Official site]. Retrieved from: https://www.rnbo.gov.ua/ [in Ukrainian]

7. Stratehiia informatsiinoi bezpeky do 2025 r. (2014). Retrieved from: https://ips.ligazakon.net/document/JG3TH00A [in Ukrainian]

8. Tsentr stratehichnykh komunikatsii ta informatsiinoi bezpeky (2024). Retrieved from: https://spravdi.gov.ua/ [in Ukrainian]

9. Tsymbaliuk B. C. (2001). Problemy derzhavnoi informatsiinoi polityky: harmonizatsiia mizhnarodnoho i natsionalnoho informatsiinoho prava [Problems of state information policy: harmonization of international and national information law]. *Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini.* Kyiv : NTUU "KPI". № 4. [in Ukrainian]