УДК 342.1
DOI https://doi.org/10.24144/2788-6018.2023.05.57

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ АТАКИ ЯК ЗАГРОЗА ДЕРЖАВНІЙ БЕЗПЕЦІ

Дерюгін І.К.,
студент групи ПВПР-23
Національний університет «Львівська політехніка»,
Навчально-науковий інститут права та психології

Батько І.І.,
асистент кафедри адміністративного та інформаційного права
Національний університет «Львівська політехніка»,
Навчально-науковий інститут права та психології

Дерюгін І.К., Батько І.І Інформаційно-психологічні атаки як загроза державній безпеці.

У статті розглянуто актуальну проблему в сучасному світі — використання інформаційно-психологічних методів для здійснення атак на національну безпеку. Було акцентовано увагу на дослідженні впливу таких атак на суспільство та національну безпеку загалом. Докладно проаналізовано природу інформаційно-психологічних атак, їхні основні види та ефективність. Наголошено на тому, що інформаційно-психологічні атаки можуть мати значний вплив на національну безпеку, оскільки вони можуть призвести до дезінформації, маніпулювання суспільними настроями. Розглянуто також законодавчу базу щодо боротьби з інформаційно-психологічними атаками. Зауважено, що законодавство повинно відповідати вимогам сучасної дійсності та забезпечувати ефективний захист держави від інформаційно-психологічних загроз. Також наведено рекомендації щодо того, як захистити себе від інформаційно-психологічних атак, враховуючи пошук надійних джерел інформації, критичне мислення та розуміння того, як працюють інформаційно-психологічні атаки.

Також було зроблено висновок, що інформаційно-психологічні атаки можуть істотно впливати на національну безпеку, відтак наголошено на необхідності розвитку комплексних заходів для захисту від таких загроз. Актуальність пропонованої статті є беззаперечною з огляду на важливість розуміння проблем, пов'язаних з інформаційно-психологічними атаками на національну безпеку. Відзначається, що боротьба з інформаційно-психологічними атаками потребує взаємодії державних та приватних структур, які повинні працювати разом для забезпечення національної безпеки. Загалом, стаття є важливим внеском у розуміння проблем, пов'язаних з інформаційно-психологічними атаками як загрозою національній безпеці. Буде корисною для широкої аудиторії, враховуючи державні структури, приватний сектор та громадськість.

Ключові слова: інформаційно-психологічні атаки, національна безпека, законодавчі заходи, співпраця державних та приватних структур, захист від інформаційно-психологічних атак, надійні джерела інформації, критичне мислення.

Deryugin I., Batko I. Information-psychological attacks as a threat to national security.

The article "Information-Psychological Attacks as a Threat to National Security" discusses the pressing issue of using information-psychological methods to carry out attacks on national security in the modern world. The article focuses on the study of the impact of such attacks on society and national security as a whole.

The article thoroughly analyzes the nature of information-psychological attacks, their main types, and effectiveness. It emphasizes that information-psychological attacks can have a serious impact on national security as they can lead to disinformation, manipulation of public sentiments, and influence on citizens' thoughts.

The article also discusses the legislative framework for combating information-psychological attacks. Attention is drawn to the fact that legislation should meet the requirements of modern reality and ensure effective protection of the state from information-psychological threats.

In summary, the article concludes that information-psychological attacks can have a serious impact on national security and emphasizes the need for the development of comprehensive measures to protect against such threats. As this problem becomes increasingly relevant in the modern world, the article is relevant and important for understanding the issues related to information-psychological attacks on national security. It is emphasized that combating information-

psychological attacks requires the interaction of state and private structures, which must work together to ensure national security.

The article also provides readers with recommendations on how to protect themselves from information-psychological attacks, including seeking reliable sources of information, critical thinking, and understanding how information-psychological attacks work.

Overall, the article is an important contribution to understanding the issues related to information-psychological attacks as a threat to national security. It provides readers with information on the nature and effectiveness of such attacks, legislative frameworks for their prevention, and recommendations on how to protect oneself from them. This article is useful for a wide audience, including government structures, the private sector, and the public.

Key words: information-psychological attacks, national security, legislative measures, cooperation between governmental and private structures, protection from information-psychological attacks, reliable sources of information, critical thinking.

Постановка проблеми. Інформаційно-психологічні атаки (далі – ІПА) – це один з видів інформаційної війни. Їх метою є вплив на масову свідомість задля зміни уявлень про певну проблему або подію. ІПА можуть бути спрямовані на різні цільові аудиторії: громадськість, політиків, військових та ін.

Одним з основних засобів реалізації ІПА є використання інформаційних технологій та соціальних мереж. Наприклад, штучний інтелект може створювати фейкові новини, які дуже складно відрізнити від реальних. Зазвичай використовують психологічні методи впливу, зокрема підриви авторитету, поширення страху та непевності, створення ілюзії загрози тощо.

Автори ставлять собі за **мету** розглянути актуальну проблему в сучасному світі – використання інформаційно-психологічних методів для здійснення атак на національну безпеку.

Слід відзначити, що **окремі питання досліджуваної тематики** було розглянуто в працях Бондаренко В., Литвиненко О., Горбаня Ю., Гусарова В., Кормича Б. та ряду інших вітчизняних та зарубіжних вчених.

Виклад матеріалу дослідження. ІПА можуть мати серйозні наслідки для державної безпеки. Наприклад, вони можуть впливати на результати виборів, як це було в США 2016 року. Також ІПА можуть сприяти поширенню тероризму та екстремізму, дестабілізувати ситуацію в країні, спровокувати міжнаціональні та міжрелігійні конфлікти. Можливі й економічні наслідки ІПА, такі як втрата довіри до фінансових інститутів, втрата ринків та репутації [1–3].

Ще однією проблемою є те, що ІПА можуть бути спрямовані не тільки на зовнішніх ворогів, але й на внутрішніх. Наприклад, російська влада, щоб зберегти владу та контроль над населенням, використовувала ІПА для підриву довіри до власного опозиційного руху та засобів масової інформації.

Протидіяти ІПА – складне завдання. Насамперед потрібно розвивати медійну грамотність населення та підвищувати рівень інформаційної грамотності, щоб люди могли розрізняти правдиву інформацію від фейкової. Наприклад, у Європейському Союзі було запроваджено спеціальну програму «Європа для громадян», яка спрямована на підвищення інформаційної грамотності [4; 5, с. 218–221; 6]. Також треба розвивати технології виявлення фейкової інформації. Наприклад, компанія «Facebook» використовує спеціальні алгоритми для виявлення фейкових новин, а також співпрацює з фактчекерськими організаціями [7, с. 74–77; 8; 9].

Для боротьби з ІПА необхідно і розвивати законодавство та правові механізми. До прикладу, у США було запроваджено закон «Протидія іноземним втручанням у вибори», який передбачає введення санкцій для протидії зовнішнім особам та організаціям, що намагаються втручатися у виборчий процес у США.

Окрім того, важливо підвищувати рівень кібербезпеки. У сучасному світі багато інформації зберігається в електронному вигляді, яку кіберзлочинці можуть використовувати для здійснення ІПА. Тому варто розвивати технології кіберзахисту і створювати ефективні системи виявлення кібератак та запобігання їм.

Важливо й те, щоб держави співпрацювали в боротьбі з ІПА. Для цього необхідно створювати міжнародні механізми та організації, які виявлятимуть і запобігатимуть ІПА, дбатимуть про розвиток інформаційної грамотності. Скажімо, у Європейському Союзі було створено спеціальну групу експертів з питань протидії дезінформації, яка має забезпечувати краще розуміння проблеми ІПА та працювати над розробкою спільної стратегії протидії їй.

Інформаційно-психологічні атаки є серйозною загрозою для державної безпеки. Вони можуть мати різні цілі: підірвання довіри до влади, збереження влади, вплив на громадську думку тощо. А відтак ІПА можуть мати різноманітні наслідки, зокрема економічні та соціальні.

Отже, протидія ІПА вимагає розвитку інформаційної та медійної грамотності населення, розвитку технологій виявлення фейкової інформації, підвищення рівня кібербезпеки і створення міжнародних механізмів та організацій для виявлення і запобігання ІПА.

Згідно з дослідженнями, інформаційно-психологічні атаки набувають дедалі більшого поши-

рення в сучасному світі. Це може бути пов'язано зі зростанням впливу інформації та медіа на суспільство. Тому важливо забезпечити захист від ІПА на рівні і окремих осіб, і держав [10, с. 181–189; 11, с. 362–367; 12, с. 259–264].

У боротьбі з ІПА важливо не тільки розробляти технології та системи захисту, але й вдосконалювати законодавство та регуляторну базу. Держави повинні напрацьовувати закони і політику, які забезпечували б ефективну протидію ІПА, враховуючи запобігання їх поширенню та відшкодування збитків від їхніх наслідків.

Вагоме значення має й розвиток міжнародної співпраці у боротьбі з ІПА. Це може бути забезпечено шляхом створення спеціальних міжнародних організацій та механізмів, які займатимуться виявленням та запобіганням ІПА, а також співпрацею між державами у сфері кібербезпеки та інформаційної безпеки.

Україна потерпає від інформаційно-психологічних впливів, війни та загрози інформаційної безпеки. Український інформаційний простір наразі вразливий до зовнішніх негативних пропагандистсько-маніпулятивних впливів і стає об'єктом інформаційної експансії. Немає українського національного інформаційного продукту, який поширював би об'єктивну, неупереджену та актуальну інформацію про події в Україні, тому світова громадськість відчуває брак інформації або отримує її з інших джерел, які часом дезінформують [13, с. 7–11; 14, с. 293–295].

До того ж потужний медіаресурс активно застосовується проти України, здійснюється експансія іноземних суб'єктів на ринку інформаційних послуг, активізуються негативні інформаційні впливи, які спрямовані на викривлення реальності та заниження міжнародного іміджу держави.

Крім того, недостатньою є діяльність вітчизняних ЗМІ щодо систематичного й об'єктивного висвітлення фактів, подій та явищ, інформаційно-комунікативна політика України у сфері національної безпеки потребує невідкладного перегляду та удосконалення. Стратегія національної безпеки України визначає агресивні дії Росії як такі, що підривають суспільно-політичну стабільність з метою знищення держави України й захоплення її території.

Отож інформаційна безпека України наразі є у критичному стані, оскільки країна є об'єктом негативного впливу з боку інших країн і суб'єктів, що здійснюють активну пропаганду та маніпуляції через медіаресурси.

Зовнішні впливи спрямовані на викривлення інформаційної картини України у світі, а також на підрив національної свідомості і маніпуляцію суспільством задля досягнення своїх цілей.

Недостатня робота вітчизняних ЗМІ з об'єктивного висвітлення подій і фактів, а також відсутність національного інформаційного продукту у світі призводить до браку об'єктивної і надійної інформації про Україну для світової громадськості.

У зв'язку із цим потрібно вжити невідкладних заходів для захисту національної інформаційної безпеки, зокрема шляхом розвитку вітчизняних медіа та національного інформаційного продукту у світі, а також ефективного контролю за інформаційним простором країни.

Варто зазначити, що у Стратегії національної безпеки України розрізнено прояви інформаційної та психологічної агресії (п. 3.1), небезпеки кібербезпеки та безпеки інформаційних ресурсів (п. 3.7) від загроз суто інформаційній безпеці [15, с. 218–221].

Заходи, що мають на меті боротьбу з масштабними негативними впливами на психологічний стан населення, операціями та війнами, повинні бути пріоритетними напрямами державної інформаційної політики в Україні. Серед них можна виділити:

1) приєднання України до світового та регіонального європейського інформаційного просторів;

2) участь у міжнародних інформаційних та інформаційно-телекомунікаційних системах та організаціях;

3) створення власної національної моделі інформаційного простору та розвиток інформаційного суспільства;

4) поліпшення всієї системи інформаційної безпеки держави та формування і реалізація ефективної інформаційної стратегії;

5) покращення законодавства щодо інформаційної безпеки, гармонізація національного законодавства з міжнародними стандартами та ефективне регулювання інформаційних процесів;

6) розгорнутий розвиток національної інформаційної інфраструктури, враховуючи її інтеграцію з міжнародними стандартами та забезпеченням її безпеки;

7) підвищення конкурентоспроможності вітчизняної інформаційної продукції та послуг через запровадження ефективних механізмів її підтримки і стимулювання її розвитку;

8) впровадження передових інформаційно-комунікаційних технологій у процеси державного управління задля підвищення їхньої ефективності та якості;

9) ефективне співробітництво між органами державної влади та громадськими організаціями під час формування, реалізації та коригування державної політики в інформаційній сфері для забезпечення її ефективності та прозорості [15, с. 241–244; 16, с. 427–432].

Зокрема, щоб виробити комплекс заходів для власного сталого інформаційного розвитку в

умовах жорсткої конкуренції з урахуванням чинників інформаційної безпеки, потрібно консолідувати діяльність органів державної влади та ЗМІ у сфері політичного інформування суспільства для нейтралізації негативного психологічного впливу в умовах криз та конфліктів.

Національній безпеці можуть загрожувати, серед іншого, обмеження свободи слова та доступу до інформації, спотворення інформації, несанкціоноване поширення, дезінформація, інформаційна експансія з боку інших країн, культуралізація насильства та жорстокості, повільний вхід у світовий інформаційний простір, невиважена державна інформаційна політика, відсутність необхідної інфраструктури в інформаційній сфері, розміщення дезінформації в інтернеті.

Загрози національній безпеці в інформаційній сфері можуть виникати через дії інших держав, а також через внутрішні проблеми, спричинені відсутністю адекватної інформаційної політики та інфраструктури в країні. Такі загрози можуть мати негативний вплив на демократію, економіку, соціальну стабільність та національну безпеку загалом. Щоб запобігти таким загрозам, треба розвивати ефективні механізми захисту національної безпеки в інформаційній сфері, зокрема розробляти і впроваджувати адекватну державну інформаційну політику та створювати необхідну інфраструктуру в цій сфері [10, с. 185–189; 17, с. 183–185].

І саме загроза інформаційно-психологічних атак на державну безпеку вимагає залучення багатьох галузей діяльності, таких як наука, технології, мас-медіа, законодавство та політика, для розв'язання цієї проблеми. Застосування новітніх технологій для виявлення та боротьби з дезінформацією є дуже важливим, проте воно не повинно перетворитися на цензуру чи обмеження свободи слова, а має забезпечувати підвищення критичного мислення та медійної грамотності серед населення.

Держава повинна розвивати політику захисту від інформаційно-психологічних атак, зокрема шляхом встановлення механізмів моніторингу, аналізу та реагування на поширення дезінформації. Крім того, важливо проводити освітні кампанії: навчати населення відрізняти правдиву інформацію від брехні, навчати ефективних стратегій протидії маніпулятивним технологіям [18, с. 70–73].

Інформаційно-психологічні атаки не є проблемою однієї країни чи регіону, але набувають дедалі більшого поширення на світовому рівні. Тому треба встановити міжнародний діалог та співпрацю в боротьбі з дезінформацією. Це можна зробити шляхом створення спільних міжнародних проєктів, обміну досвідом та розробки спільних стратегій протидії інформаційно-психологічним атакам.

У сучасному світі, де інформація стала головним ресурсом, важливо забезпечити державну безпеку шляхом запобігання інформаційно-психологічним атакам. Це можливо тільки за умови взаємодії державних і недержавних структур, наукових і дослідницьких організацій, спільних зусиль для виявлення та боротьби з дезінформацією і фейками.

Тому за умови сучасної конфронтації інформації про експансіоністську політику Російської Федерації національний інформаційний простір України недостатньо захищений від зовнішньої інформації про негативну рекламу та психологічні наслідки й загрози. Отже, захист інформаційного суверенітету, створюючи потужну та ефективну систему інформаційної безпеки в Україні, як розробка ефективних стратегій та стратегій реакцій медіа, має бути пріоритетним завданням для державних органів і неурядових агентств.

Звідси випливає, що ІПА є серйозною загрозою для державної безпеки, і їхній вплив може бути дуже шкідливим для суспільства. Протидія ІПА потребує комплексного підходу та співпраці на рівні окремих осіб, держав та міжнародних організацій. Забезпечення ефективної протидії ІПА є важливим завданням для забезпечення національної безпеки і стабільності в сучасному світі.

Зважаючи на те, що ІПА можуть мати серйозні наслідки для державної безпеки та соціальної стабільності, важливо розглядати їх як глобальну проблему, яка потребує спільних зусиль усіх держав. Для цього необхідно забезпечити належну організацію та координацію дій на рівні окремих країн, а також у міжнародному форматі. Така співпраця може виявитися дуже ефективною у протидії ІПА, особливо якщо вона ґрунтується на принципах відкритості, довіри та взаємної підтримки.

Висновки. Отже, ІПА є серйозною загрозою для державної безпеки, яка вимагає відповідного захисту та протидії. Це можливо тільки за умови комплексного підходу, який охоплює розробку новітніх технологій та систем захисту, вдосконалення законодавства та регуляторної бази, розвиток міжнародної співпраці й усвідомлення громадянами небезпек, що випливають з ІПА. Тільки в такий спосіб можна забезпечити ефективний захист від ІПА та зберегти державну безпеку в умовах постійно зростаючої кількості цих загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бондаренко В.О., Литвиненко О. В. Інформаційна безпека сучасної держави: концептуальні роздуми. *Стратегічна панорама*. 1999. № 1-2. С. 127–133. URL: http://www.crime-research.iatp.org.ua/library/strateg.htm (дата звернення: 28.03.2023).
2. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення. *Вісник НАДУ*.

2015. Вип. 1. С. 136–141. URL: http://www.visnyk.academy.gov.ua/wpcontent/uploads/2015/04/20.pdf (дата звернення: 28.03.2023).

3. Гусаров В. Кремль розпочав нову інформаційну операцію проти України. *Детектор медіа*. 2014. 4 верес. URL: http://www.osvita.mediasapiens.ua/material/34281 (дата звернення: 29.03.2023).
4. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: дис. д-ра юрид. наук: 12.00.07. Харків: НУВС, 2004. URL: http://www.mego.info/матеріал/23-захист-інформаційної-безпеки-як-функція-держави (дата звернення: 01.04.2023).
5. Інформаційна безпека держави у контексті протидії інформаційним війнам: навч. посіб. Київ: НАОУ, 2004. 315 с.
6. Концепція національної безпеки України. URL: http://www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1.
7. Качинський А.Б. Індикатори національної безпеки: визначення та застосування їх граничних значень. Київ: НІСД, 2013. 104 с.
8. Литвин М.М. Умови та фактори внутрішньої загрози національній безпеці України. URL: plesetsk-info.ru/uchebnoe-posobie/umovi-ta-faktorivnutrshno-zagrozi-natconalni-bez.
9. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. *Бизнес и безопасность*. 2014. № 1. С. 46–50. URL: http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.
10. Berenger J. & Johnson J. The fake news challenge: exploring boundary conditions for "satirical" criticism. Journal of Social and Political Psychology. 2018. № 6(2). P. 177–198.
11. Світлична В.Ю. Інформаційна безпека: багатогранність сутності, види загроз та шляхи забезпечення. *Науково-технічний збірник*. Харків: ХНАМГ, 2013. № 109. С. 360–369.
12. Боднар І.Р. Сучасні реалії інформаційного суспільства: проблеми становлення та перспективи розвитку: монографія. Львів: Вид-во Львівської комерційної академії, 2013. 320 с.
13. Bossetta M. & Rieder B. Political communication in the digital age: mapping the field and assessing its implications for democratic theory. *Journal of Information Technology & Politics*. 2018. № 15(1). С. 1–19.
14. Боднар, І.Р. Роль держави у формуванні інформаційної політики. *Вісник ЛКА*. 2011. № 34. С. 291–296.
15. Почепцов Г. Інформаційна політика: навч. посіб. Київ: Знання, 2006. 663 с.
16. Hameleers M., Bos L. & De Vreese C. It's not fake news, it's misinformation: how to define and characterize misleading information in contemporary media landscapes. *American Behavioral Scientist*. 2020. № 64(3). P. 422–436.
17. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право*. 2017. № 10. С. 182–186.
18. Боднар І.Р. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки*. 2014. № 1. С. 68–75.