

<https://doi.org/10.26565/2220-8089-2022-42-08>

УДК 32.019.51

**Людмила Іванівна Мазуренко**

кандидат політичних наук, доцент кафедри соціально-гуманітарних та фундаментальних дисциплін Інституту Військово-Морських Сил Національного університету «Одеська морська академія» вулиця Дідріхсона, 8, 65029, м. Одеса  
[ruzam11@ukr.net](mailto:ruzam11@ukr.net), <https://orcid.org/0000-0003-3189-8215>

## ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ: ВИКЛИКИ ТА ЗАГРОЗИ

Обґрунтовано необхідність створення ефективного механізму забезпечення державної інформаційної безпеки. Зазначено, що блокування правдивої інформації про роль Збройних Сил України, дій керівництва та владних структур не сприяє здобуттю перемоги у війні, розв'язаній Росією проти України.

Визначено такі головні шляхи поширення недостовірної інформації в умовах війни є: соціальні мережі; підроблені акаунти відомих людей, політиків, телерадіомовні канали; особисті повідомлення чи групи Viber, WhatsApp, Telegram та інших месенджерів.

Вказано, що в аспекті забезпечення інформаційної безпеки значне місце займають проблеми поширення чуток, пліток, фейків. Виділено такі види фейків: фейк-реклама, фейк-псевдоексперт, фейк-конспірологія, фейк-клікбейт. Для просування фейкових новин у мережах діють ботоферми, «фабрики Інтернет-тролів» та практикується пранкінг. До того ж, фейки в умовах російської агресії є ще й битвою нарративів і культур.

Виділено такі складові інформаційної безпеки, як інформаційно-технічний та інформаційно-психологічний захист.

Розкрито основні механізми протидії неправдивій інформації в умовах війни, а саме: формування медіаграмотності населення; висвітлення об'єктивної інформації через урядові Інтернет-видання, ЗМІ, електронне врядування; встановлення відповідальності за поширення фейкових новин серед населення; контроль фейкових акаунтів; нейтралізація фейків спецпідрозділами в кіберполіції.

Визначено та охарактеризовано головні напрями підвищення інформаційної безпеки як компонента державної безпеки України.

**Ключові слова:** інформаційна безпека, фейк, фейкові новини, чулки, медіаграмотність населення, війна, військові дії, військові конфлікти.

**Як цитувати:** Мазуренко, Л.І. 2022. Інформаційна безпека в умовах російсько-української війни: виклики та загрози. *Вісник Харківського національного університету імені В.Н. Каразіна, серія «Питання політології»* 42: 50-57. <https://doi.org/10.26565/2220-8089-2022-42-08>

**In cites:** Mazurenko, Lyudmila. 2022. Information Security in the Terms: The Russian-Ukrainian War: Challenges and Threats. *The journal of V. N. Karazin Kharkiv National University. Series «Issues of Political Science»* 42: 50-57. <https://doi.org/10.26565/2220-8089-2022-42-08> (in Ukrainian)

День 24 лютого 2022 р. назавжди залишиться в історії чорним днем військового вторгнення Росії в Україну (Залевська, Удренас 2022: 21). Він розділив життя і українців, і взагалі всього світу на «до» і «після». Держава-агресор проводить також дезінформаційні атаки на українців,

намагаючись за допомогою поширення фейків змусити українців боятися та панікувати, зруйнувати політичну та соціально-економічну стабільність в Україні. Вдираючись у наш інформпростір, ворог посягає на громадянську ідентичність українців. Актуальність статті полягає у необхідності аналізу основних механізмів забезпечення інформаційної безпеки в умовах війни.

Науковці В. Горовий, Б. Кормич, О. Онищенко, О. Панченко, Я. Гмир та ін. досліджували сутність поняття «інформаційна безпека», аналізували основні загрози інформаційній безпеці, характеризували стадії підвищення цієї безпеки, законодавче підґрунтя інформаційної безпеки держави, визначали механізми протидії дезінформації тощо.

Існують поодинокі дослідження шляхів поширення та протидії дезінформації. Так, Б. Миколайчук виокремлює критерії оцінки дезінформації, основні шляхи протидії дезінформації. Ю. Мазур, В. Крижановський наводять найпоширеніші ознаки фейкових новин. Однак на сьогодні відсутні системні дослідження проблем забезпечення інформаційної безпеки в умовах війни, характеристика основних механізмів протидії дезінформації в умовах військових дій.

Метою статті є аналіз викликів і загроз інформаційній безпеці України під час війни, визначення механізмів протидії фейковій інформації в умовах воєнного стану.

Досягнення визначеної мети передбачає вирішення низки таких завдань:

- означення сутності поняття «інформаційна безпека»;
- вказати принципи, на яких базується здійснення інформаційної безпеки;
- зазначити основні шляхи поширення недостовірної інформації;
- виділити складові інформаційної безпеки;
- охарактеризувати основні механізми протидії неправдивій інформації в умовах військових дій;
- розкрити можливі напрями вдосконалення забезпечення інформаційної безпеки.

XXI століття в науковій літературі неадаремно називають інформаційним, оскільки інформація стає рушійною продуктивною силою суспільства. В умовах глобалізації та інтеграції країн, створення належних умов подолання кризових явищ в їхньому політичному та соціально-економічному розвитку є забезпечення інформаційної безпеки. О.С. Бодрук зазначає, що існує три основні підходи до визначення сутності поняття «інформаційна безпека» (Бодрук 2001) – компонент державної безпеки; захищеність інформаційного середовища та державних інтересів від гіпотетичних загроз; стан системи, що може гарантувати дотримання бажаних безпекових параметрів.

У ст. 17 Конституції України вказано, що охорона суверенітету та цілісності України, економічної та інформаційної

безпеки є найголовнішими функціями Української держави (Конституція України).

Доктрина інформаційної безпеки України визначає інформаційну безпеку як важливу самостійну сферу забезпечення національної безпеки (Про Доктрину інформаційної безпеки України 2017). Указом Президента України № 685/2021 від 15.10.2021 р. було схвалено Стратегію інформаційної безпеки (Про рішення Ради національної безпеки і оборони України 2021). Її метою є регулювання інформаційної безпеки на нормативно-правому рівні, посилення можливостей щодо забезпечення інформаційної безпеки України, інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, охорони суверенітету та цілісності України, демократії, прав та свобод людини і громадянина. Таким чином закладалися основи національної та інформаційної безпеки в інформаційній сфері. Вітчизняні науковці звертали свою увагу на важливість для безпеки країни цього питання до рішення його на державному рівні. Так, В.С. Цимбалюк вважає, що інформаційна безпека України – це стан захищеності державних інтересів у сфері інформації (Цимбалюк 2014: 24). На думку Л.О. Кочубей, інформаційна безпека характеризує стан захищеності життєво важливих інтересів, інформаційну озброєність держави, суспільства, особистості (Кочубей 2015: 222).

О. Гончаренко, Р. Джангужин, Е. Лисицин виділяють такі принципи, на яких базується здійснення інформаційної безпеки: системність; міцність; багаторівневий захист; безперервність; розсудливість (Гончаренко, Джангужин, Лисицин 2003: 40).

Можна стверджувати, що інформаційна безпека сьогодні виходить на перший план. Повномасштабне вторгнення РФ на територію України, знищення міст, сіл подається російськими ЗМІ як нібито «військова операція», виправдовуючи тим самим свої дії, та вказуючи при цьому на постійну небезпеку, яка йде від України. Тому блокування правдивої інформації про роль Збройних Сил України, керівництва держави, дій владних структур має негативний вплив на здобуття перемоги Україною у цій війні.

На наш погляд, інформаційна безпека включає достатній рівень інформаційної культури особистості; спроможність держави створити умови для нормального розвитку й задоволення потреб людини в інфор-

мації, уникаючи при цьому інформаційних загроз; гарантії розвитку та використання інформаційного середовища в інтересах кожної особистості; захищеність від загроз.

Останніми роками відбувається насичення соціальних мереж інформаційними потоками. На сьогодні практично немає наукового емпіричного та соціально-управлінського досвіду реагування на такі хвилі інформації.

Інформаційна безпека є дуже важливою під час військових дій, адже неправильно подана чи помилкова інформація може змусити населення панікувати, впливати на перебіг подій, прискорювати внутрішню міграцію населення, погіршувати імідж вищого військово-політичного керівництва, розпалювати недовіру до політиків, їхніх заяв і звернень, що може негативно позначитись на веденні бойових дій, крім того, може завдати непоправної шкоди для очікуваного результату військового конфлікту. Таким чином, боротьба з поширенням шкідливої інформації під час війни має істотне значення для перебігу воєнного конфлікту.

Головними шляхами поширення недостовірної інформації в умовах війни є соціальні мережі; підроблені акаунти відомих людей, політиків, телерадіомовні канали; особисті повідомлення або в групах Viber, WhatsApp, Telegram та інших месенджерах.

У сфері забезпечення інформаційної безпеки важливе місце посідає проблема чуток – недостовірних повідомлень, що мають різноманітну комунікативну форму. Чутки є найпершою формою суспільної комунікації, і незважаючи на технічний прогрес, появу Інтернету та інших телекомунікаційних технологій, не тільки не зменшили свого впливу, більше того, чутки стали «віртуальними» (Пархоменко-Куцевіл 2022: 179).

Варто відзначити, що миттєва швидкість передачі повідомлень у мережі, максимальна анонімність інтернет-спілкування стали гарним живильним середовищем для поширення чуток. Порівняно зі звичайними чутками, інтернет-чутки передаються миттєво та швидко охоплюють гігантську аудиторію, впливаючи на свідомість та поведінку громадян. Науково-технічний прогрес не лише не витіснив цю найдавнішу форму комунікації, а навпаки, своєрідно оновив її та надав їй оновлену форму.

Нині чутки не втратили свого значення і, на противагу традиційним ЗМІ, після

появи Інтернету пристосовуються до нових умов та інтегруються в глобальну мережу, набуваючи нові властивості та руйнівну силу. До прикладу, істотно збільшилася швидкість їхня поширеність та масштаби охоплення аудиторії. Коли в мирних умовах плітки могли знищити чиюсь кар'єру чи особисте життя, то у воєнних умовах – драматично вплинути на долі сотень тисяч людей.

Так звані «колишні», гвардія новітніх «експертів» є старими генераторами з видумування чуток, поширення пліток і погослосок. Посилаючись на авторитетне американське видання, вони стверджують, що гуманітарна допомога, яка надходить в Україну від європейських країн розбазарюється, розкрадається; що зброя, яку Захід постачає нам, не доходить до фронту; що Україна – ненадійний партнер. Вони, синхронно з російським ворогом стараються протиставляти команду Президента та ЗСУ, шукають особистий конфлікт між Зеленським і Залужним. База інформації «колишніх» – це грузьке болото чуток та особистих фантазій, тому що вони насправді не мають ніякої достовірної інформації ні про переговори, ні про тактичні чи стратегічні плани української влади і командування, тому що вони не бувають там, де приймаються серйозні рішення.

Окремо стоїть проблема поширення фейків. Фейк являє собою навмисно сфабриковану інформацію, яка не має ніяких підстав. Ця інформація завжди комусь вигідна: якщо на сайті з'являється «жовта» новина, то вона приносить більше трафіку; «зраду» та «перемогу» часто використовують як техніки політичної пропаганди, плітки під виглядом фактів використовують, щоб зіпсувати репутацію конкуренту (Писаренко 2022: 860). Фейки ґрунтуються на брехні, маніпуляціях та перекручуваннях фактів. Нині фейки та інша дезінформація поширюється через Інтернет. Найчастіше для цього використовуються месенджери (Whatsapp, Viber, Telegram), соцмережі (Facebook, Twitter, Instagram), онлайн-платформи (Reddit, 4chan).

Можна виділити такі види фейків:

- *фейк-реклама* характеризується тим, що просуває певний продукт (перевірити інформацію можна на офіційних сайтах);

- *фейк-псевдоексперт* має особливістю вказувати форму особи, ім'я, які не можна зауглити, не вказуються імена і посилання на офіційні ресурси (в таких випадках

необхідно наводити справжні дослідження на схожу тематику);

- *фейк-конспірологія* заснований на теорії змови, абсурду (в таких випадках у соцмережах слід відразу писати коментар);

- *фейк-кликбейт* відрізняється від інших «сенсацією», «шоком», заголовок не відповідає тексту повідомлення.

З ціллю максимального просування фейків працюють ботоферми та «фабрики Інтернет-тролів». Широко практикується пранкінг, інші новітні форми дезінформування, просування особистостей, теорій, ідей, проєктів, партій – заради створення у свідомості людей якогось бажаного образу (позитивного чи негативного).

Під час російсько-української війни фейки використовуються ще й у битві наративів та культур. Найчастіше РФ застосовує такі наративи: «Україна – фашистська держава», «українці – бандерівці», «звільнення українців від націоналістів» тощо.

Фейки дають можливість дистанційно управляти противником без насилля та кровопролиття. В контексті гібридної війни інформацією намагаються погіршити стосунки між людьми, схилити їх до порушень норм поведінки, традиції, права, підірвати довіру до влади, формувати панічні настрої тощо. Для боротьби з фейками, на нашу думку, необхідно відкинути емоції, перевірити джерела інформації, дані про авторів інформації, достовірність фактів, дати публікації матеріалів.

Виділимо такі компоненти інформаційної безпеки, як: інформаційно-технічна – додержання законності та правопорядку в кіберпросторі (захист від незаконного доступу, хакерських проникнень до комп'ютерних мереж та сайтів, комп'ютерних вірусів, незаконного використання телерадіомовних частот, радіоелектронних атак та ін.); інформаційно-психологічний захист психічного стану суспільства та держави від деструктивного інформаційного впливу. Це гостро відчувається у воєнний час, бо тоді емоції заважають критично оцінювати та аналізувати ситуацію і ту інформацію, що поширюється в соціальних мережах. Інформація під час воєнних конфліктів стає ще одним видом зброї ворога, враховуючи інформаційно-психологічний аспект інформаційної безпеки.

Механізмами захисту від психологічних наслідків інформаційних загроз мають бути такі: свобода слова; незалежність ЗМІ та свобода друку; ЗМІ мають здійснювати свою діяльність на благо держави; органи

державної влади мають звертати увагу ЗМІ та населення на відповідальність за подання свідомо неправдивих даних.

Ще одним важливим аспектом інформаційно-психологічної безпеки є блокування прихованого шкідливого інформаційного впливу, що особливо важливо для жителів фронтних та прифронтних територій. Науковці виокремлюють два головні методи прихованого інформаційного впливу: ін'єкція інформації в неусвідомлювані сфери області пам'яті людини шляхом навіювання, пояснення, навчання в дисоційованому стані; створення прямого доступу до пам'яті через зміни стану свідомості або її відключення. Під час бойових дій виникає безліч фейкових новин про події в регіонах, рішення влади, думки та офіційні заяви, які можуть істотно вплинути на підсумок військового конфлікту. Так, з'явилися засновані на технології штучного інтелекту генератори синтезованого медіа-контенту – фейкових новин, «глибоких фейків» (Deep Fake), що дозволило робити реалістичні фото-, аудіо- та відео-підробки (створені навіть на основі лише голосу людини). Науковці Технологічного університету Наньянга (Сінгапур) та китайські розробники в галузі штучного інтелекту із Sense Time розробили метод створення дідфейків на основі звукозапису: штучний інтелект використовує голос однієї людини, що поєднує з фото або відео іншої людини – і синтезує цілком реалістичне відео того, як людина промовляє слова із джерела звуку; в такому разі людина на відео стає маріонеткою для оригінального голосу (Cole Samantha 2020). У глядача при перегляді дідфейкового відео створиться враження, що він дивиться справжнє відео. Можемо згадати дідфейкові відео про капітуляцію Президента Зеленського. Хоча відразу було зрозуміло, що це фейк, але ж легко уявити, наскільки руйнівним це може бути, коли технологію дідфейків стане важче виявити. Коли розкрити подібні відео стане неможливим, то сфабриковані медіа різко збільшать ризик дідфейкових новин і можуть розпалити недовіру до головних ЗМІ, адже підроблені відео та зображення може створювати будь-хто за допомогою безкоштовних програм, таких як Wombo та FaceApp.

Головними механізмами протистояння брехливій, перекрученій, неперевірній інформації в умовах війни є такі. Насамперед, це підвищення медіа грамотності населення, що дозволяє йому захищатися від дезінформаційних впливів та допомагати

підтримувати інформаційну безпеку держави. Медіаграмотність містить такі компоненти, як критичне мислення, орієнтування в медіа, споживання медіа та дизайн медіа. Медіа-маніпуляція суспільною свідомістю або думками здійснюється за допомогою впливів на сприйняття людини через зір (медіадизайн); можливість орієнтуватися в інформаційному просторі, який є просто гігантським, а часу на повноцінне його вивчення бракує; через значні обсяги контенту, а також через неможливість критично сприймати інформацію через прихильність тільки конкретним ЗМІ.

Нині стало зрозумілим, що інформаційна війна є елементом повномасштабної війни, що медіаосвіта, медіаграмотність, вироблення стійкості до впливу дезінформації є питаннями національної безпеки. Ми бачимо, як Росія докладає всіх зусиль, аби очорнити українців в очах світу та розбити єдність українців. Кремлівські пропагандисти прикладають надзусилля для поширення проросійської ідеології та відповідних наративів. Свідомість українців атакують з метою виявити слабкі місця, які відкрила війна, та вдарити по них. А тому, щоб оминати пастки проросійських ресурсів й не поширювати дезінформацію, необхідно по-перше, застосовувати критичне мислення, а саме чітко бачити для чого використовується в певному медіа той чи інший контент як інструмент пропаганди чи маніпуляції, яке завдання ставить перед собою і зміст недійсного матеріалу і сам цей медіа, в чому виявляється їхня шкода.

По-друге, потрібно щоденне об'єктивне висвітлення новин та іншої інформації через державні інтернет-видання, ЗМІ, звернення до народу. Регулярне надання інформації про основні події, тим більше під час війни допоможе розвіяти чутки та викрити фейки. Зокрема, з початку повномасштабної агресії на всіх українських телеканалах почала йти телепрограма «Інформаційний телемарафон «Єдині новини», яка не лише розповідала про російське вторгнення, військові події, переміщення техніки окупантів, успіхи та невдачі ЗСУ, а й трансливала думки та коментарі представників влади, включаючи Президента України, прем'єр-міністр та міністрів, висновки яких склалися з під час особистого перебування на різних ділянках лінії фронту. Ці дії дають змогу боротися з фейками, чутками, маніпуляціями, перекручуваннями та іншою дезінформацією щодо бойових дій, а також зміцнюють ставлення звичайних українців до влади, знижують

рівень паніки серед народу, поліпшують морально-психологічний стан населення, яке проживає у прифронтовій зоні.

По-третє, слід запровадити юридичну відповідальність за створення та поширення фейків. Важливим компонентом забезпечення інформаційної безпеки суспільства є встановити кримінальну відповідальність за надання свідомо невірної, неперевіреної, перекрученої інформації, особливо коли дезінформація поширюється під час війни.

По-четверте, встановити жорсткий контроль підrobлених акаунтів, що свідомо розсилають дезінформацію у вигляді фейків. Наприклад, контроль за поширенням фейкової інформації зараз втілюють найпопулярніші месенджери. WhatsApp особливим символом маркує повідомлення, які пересілалися дуже багато разів, що є важливою ознакою фейку.

По-п'яте, повномасштабне вторгнення російських військ на територію нашої країни супроводжується потужною агресією в кіберпросторі. Для захисту інформаційного простору в умовах воєнних дій працює Ситуаційний центр забезпечення кібербезпеки при СБУ. Там діє система керування інформаційними подіями, яка відслідковує такі події в реальному часі та допомагає аналізувати стан інформаційної безпеки держави, що дає змогу швидко виявляти, реагувати та упереджувати загрози для українського кіберпростору.

Виявленням фейків, дїпфейків та їх нейтралізацією займатимуться сформовані спеціальні підрозділи в кіберполіції. Нині діє громадський рух кіберопору ворогові, що називається «КіберАрмія». Звичайні люди, разом із професійними айтїшниками, атакують ворога в кіберпросторі, завдають йому збитків та зривають плани.

Крім того, під час війни, надзвичайно важливим стає нейтралізація численних інформаційних загроз, для чого необхідно проведення низки організаційно-правових заходів. Вважаємо, що основними напрямками поліпшення системи забезпечення інформаційної безпеки держави мають стати:

- стратегічне стримування та припинення бойових дій та військових конфліктів, що можуть виникнути після зумисного застосування дезінформаційних технологій;
- поліпшення системи забезпечення інформаційної безпеки ЗСУ, інших військових формувань, включно з силами та засобами інформаційної протидії;

• прогнозування, виявлення та оцінка загроз, включаючи загрози для ЗСУ в сфері інформації.

У зв'язку з цим, зазначені напрями мають бути головними складовими діяльності органів, які формують інформаційну безпеку країни. Нині інформація як зброя є доволі серйозним засобом ведення війни оскільки її технологічна інноваційність, потужність є небезпечними. Відповідно, інформаційна безпека України має базуватися на синхронізованих діях структур держави та громадянського суспільства. Під час війни суттєво зросла роль інформаційної культури як чинника підсилення опору дезінформаційній зброї громадянами та збереження державного суверенітету України.

Нинішня війна добре демонструє, що інформація використовується і в якості зброї масового ураження. У зв'язку з цим потрібно побудувати ефективний механізм, котрий би гарантував інформаційну безпеку України, в основу якого, на нашу думку, важливо покласти такі складові: технічну – створити належну технічну базу функціонування інформаційної безпеки; політичну – державна політика повинна бути направлена на забезпечення інформаційної безпеки; правову – оформлення всіх заходів інформаційної безпеки якісними нормативно-правовими актами. Аналіз проблеми забезпечення інформаційної безпеки громадянина та держави під час бойових дій та конфліктів дозволяє дійти висновку, що інформаційна безпека відіграє надзвичайно важливу роль особливо під час війни. Адже дезінформація може викликати панічні настрої серед населення, негативно вплинути на перебіг подій, прискорювати внутрішню міграцію населення, що може негативно позначитись на даєдатності Збройних Сил України, а також на фізичному й психічному стані громадян.

Ефективно протидіяти інформаційній агресії видається, на нашу думку, можливим за рахунок залучення до цього процесу міжнародних організацій, інституцій та міжнародної спільноти загалом. Практика показує – кордонів для ведення інформаційної війни не існує. Начасі захищати відкритий інформаційний простір країни від ворожих впливів та навіювань.

Перспективами подальших досліджень є проведення аналізу зарубіжного досвіду протидії поширенню фейків в умовах інформаційних війн та висвітлення воєнних подій.

Стаття надійшла до редакції 3.11.2022.

Стаття рекомендована до друку 30.11.2022

## СПИСОК ЛІТЕРАТУРИ

1. Залєвська, І.І., Удренас, Г.І. 2022. Інформаційна безпека України в умовах російської військової агресії, *Південно-український правничий часопис* 1-2: 20–26.
2. Бодрук, О.С. 2001. *Структури воєнної безпеки: національний та міжнародний аспекти: Монографія*. Київ: НІПМБ.
3. *Конституція України*. 2019. URL: <https://zakon.rada.gov.ua/laws/show/27-20#n2>
4. *Про Доктрину інформаційної безпеки України: Указ Президента України №47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»*. URL: <https://www.president.gov.ua/documents/472017-21374>
5. *Про рішення Ради національної безпеки і оборони України 2021: Указ Президента України № 685/2021 від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»*. URL: <https://www.president.gov.ua/documents/6852021-41069>
6. Цимбалюк, В.С. 2014. Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики, *Адміністративне право і процес* 2(8): 22–30.
7. Кочубей, Л.О. 2015. 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* 3: 220-237.
8. Гончаренко, О., Джангужин Р., Лисицин Е. 2003. Громадянський контроль і система національної безпеки, *Національна безпека України* 1: 39-46.
9. Пархоменко-Куцевіл, О. І. 2022. Забезпечення інформаційної безпеки під час здійснення військових операцій та бойових дій. *Публічне управління та адміністрування в умовах війни і в поствоєнний період в Україні: м-ли Всеукр. наук.-практ. конф. у 3х т. Київ: ДЗВО «Університет менеджменту освіти» НАПН України* 1 : 39-43.
10. Писаренко, Л.М. 2022. Фейки як інструменти інформаційної війни. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття*: у 2 т.: м-ли Міжнар. наук.-практ. конф. Одеса: *Видавничий дім «Гельветика»*. 1: 859-861.
11. Cole, Samantha. 2020. New Deepfake Method Can Put Words In Anyone's Mouth. *Tech by VICE* 24.01.2020. URL: [https://www.vice.com/en\\_us/article/g5xvk7/researchers-created-a-way-to-makerealistic-deepfakesfrom-audio-clips](https://www.vice.com/en_us/article/g5xvk7/researchers-created-a-way-to-makerealistic-deepfakesfrom-audio-clips)

## Lyudmila Mazurenko

candidate of political sciences, associate professor of the department of socio-humanitarian and fundamental disciplines of the Institute of Military and Naval Forces of the National University "Odesa Maritime Academy"  
Didrichson Street, 8, 65029, Odessa

[ruzam11@ukr.net](mailto:ruzam11@ukr.net), <https://orcid.org/0000-0003-3189-8215>

## INFORMATION SECURITY IN THE TERMS THE RUSSIAN-UKRAINIAN WAR: CHALLENGES AND THREATS

The need to create an effective mechanism for ensuring state information security is substantiated. It is noted that the blocking of true information about the role of the Armed Forces of Ukraine, actions of the leadership and power structures does not contribute to victory in the war waged by Russia against Ukraine.

The following main ways of disseminating unreliable information in the conditions of war have been identified. social networks; fake accounts of famous people, politicians, TV and radio channels; personal messages or in shared groups of Viber, Telegram, WhatsApp and other messengers.

It is indicated that in the aspect of ensuring information security, a significant place is occupied by the problems of spreading rumors, gossip, and fakes. The following types of fakes are highlighted. fake advertising, fake pseudo-expert, fake conspiracy, fake clickbait. To promote fake news, there are bot farms, «Internet troll factories», and pranking is practiced. In addition, fakes in the conditions of Russian aggression are also a battle of narratives and cultures.

Such components of information security as information-technical and information-psychological protection are highlighted.

The main mechanisms of combating false information in the conditions of war are disclosed, namely. formation of media literacy of the population; coverage of objective information through government Internet publications, mass media, e-government; establishment of responsibility for spreading fake news among the population; control of fake accounts; neutralization of fakes by special units in the cyber police.

The main directions of improving information security as a component of the state security of Ukraine have been identified and characterized.

Keywords: *information security, fake, fake news, rumors, media literacy of the population, war, military operations, military conflicts.*

## REFERENCES

1. Zaljevsjka, I., Udrenas, Gh.. 2022. Information security of Ukraine in the conditions of Russian military aggression, *South Ukrainian legal journal*. 1-2: 20–26 (in Ukrainian).
2. Bodruk, O. 2001. *Structures of military security: national and international aspects*: Monograph. Kyiv: NIPMB (in Ukrainian)..
3. *Constitution of Ukraine*. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80> (in Ukrainian).
4. *On the Doctrine of Information Security of Ukraine: Decree of the President of Ukraine No. 47/2017 «On the Decision of the National Security and Defense Council of Ukraine dated December 29, 2016 «On the Doctrine of Information Security of Ukraine»*. URL: <https://www.president.gov.ua/documents/472017-21374> (in Ukrainian).
5. *About the decision of the National Security and Defense Council of Ukraine 2021: Decree of the President of Ukraine No. 685/2021 dated October 15, 2021 «On Information Security Strategy»*. URL: <https://www.president.gov.ua/documents/6852021-41069> (in Ukrainian).
6. Cymbaljuk, V. 2014. Legal regulation of information security in Ukraine: problems of theory and practice, *Administrative law and process* 2(8): 22-30 (in Ukrainian).
7. Kochubej, L. 2015. State information security. tools for the protection of the Ukrainian information field (on the example of the features of information and communication technologies in modern Donbas), *Scientific notes of the Institute of Political and Ethnonational Studies named after I.F. Kurasa*. 3: 220-237 (in Ukrainian).
8. Ghoncharenko, O., Dzhanghuzhyn, R., Lysycyn, E. 2003. Civil control and the system of national security, *National security of Ukraine*. 1: 39–46 (in Ukrainian)..
9. Parkhomenko-Kucevil, O. 2022. Ensuring information security during military operations and hostilities. *Public management and administration in the conditions of war and in the post-war period in Ukraine: materials of Vseukr. science and practice conf. in three volumes*. Kyiv: DZVO «University of

Education Management» National Academy of Sciences of Ukraine 1: 39-43 (in Ukrainian).

10. Pysarenko, L. 2022. Fakes as tools of information warfare, *The European choice of Ukraine, the development of science and national security in the realities of large-scale military aggression and global challenges of the 21st century*: in 2 volumes: materials of International Sciences.- practice conf. Ukraine,

Odesa: «Helvetika» publishing house 1: 859–861 (in Ukrainian).

11. Cole, Samantha. 2020, *New Deepfake Method Can Put Words In Anyone's Mouth*, Tech by VICE 24.01.2020. URL:

[https://www.vice.com/en\\_us/article/g5xvk7/researchers-created-a-way-to-make-realistic-deepfakes-from-audio-clips](https://www.vice.com/en_us/article/g5xvk7/researchers-created-a-way-to-make-realistic-deepfakes-from-audio-clips)

The article was received by the editors 1.11.2022.

The article is recommended for printing 30.11.2022