МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНИХ КОНФЕРЕНЦІЙ ЧОРНОМОРСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ПЕТРА МОГИЛИ
MATERIALS OF THE SCIENTIFIC AND PRACTICAL CONFERENCE OF PETRO MOGYLA BLACK
Серія «Публічне управління та адміністрування»

ISSN 3083-6417 (online)
ISSN 3083-6409 (print)
№ 1(1) 2025
Series «Public management and administration»

DOI 10.34132/mspc2025.01.13.17

Станіслав Ларін

СУЧАСНІ ВИКЛИКИ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Інформаційна безпека стала однією з найважливіших складових національної безпеки України, особливо в умовах триваючої російсько-української війни. В сучасних умовах агресії з боку Російської Федерації інформаційний простір України зазнає безпрецедентного тиску з боку ворога, який застосовує різноманітні інструменти дезінформації, пропаганди, кібертерору та маніпуляцій громадською думкою. З огляду на це, комплексне вивчення і аналіз сучасних викликів інформаційній безпеці України набуває особливої актуальності, оскільки успішне протистояння інформаційній агресії безпосередньо впливає на обороноздатність держави, стабільність суспільства і демократичний розвиток. В офіційному документі – Стратегії інформаційної безпеки України, прийнятому у 2021 році, виклики, що постали перед інформаційним простором, класифікуються на глобальні та національні. Це дозволяє чітко розмежувати зовнішні загрози, які мають транснаціональний характер, від внутрішніх, пов'язаних з особливостями функціонування інформаційної сфери в Україні.

***Ключові слова**: інформаційний простір, інформаційна сфера, інформаційна безпека, транснаціональний характер викликів, глобальні та національні виклики*

Інформаційна безпека стала однією з ключових і найважливіших складових системи національної безпеки України, особливо в умовах повномасштабної військової агресії з боку Російської Федерації. Сучасна війна ведеться не лише на полі бою, а й у віртуальному просторі, де інформаційна зброя дедалі частіше використовується для досягнення політичних, військових і психологічних цілей. Росія активно використовує широкий арсенал інформаційних впливів – від дезінформації, фейкових новин і пропаганди до кібертерору, атак на інформаційну інфраструктуру, зламів державних ресурсів, зливів персональних даних та спроб дестабілізувати інформаційний простір України.

Окрім зовнішнього тиску, інформаційна сфера України стикається з низкою внутрішніх викликів: недостатній рівень медіаграмотності населення, недосконале законодавче регулювання інформаційної діяльності, обмеженість ресурсів у сфері кіберзахисту, а також повільна модернізація інформаційних систем державного управління. Усі ці фактори підвищують вразливість країни до зовнішніх і внутрішніх загроз в інформаційному середовищі.

В умовах гібридної війни, яку веде Росія проти України, інформаційна безпека виступає не лише інструментом захисту, але й важливим чинником стійкості держави, її політичної, соціальної й економічної стабільності. Протистояння інформаційній агресії є складовою національного спротиву, який охоплює не тільки силові структури, а й громадянське суспільство, журналістську спільноту, науковців, освітян і всіх, хто долучається до збереження інформаційного суверенітету держави.

Таким чином, комплексне вивчення сучасних загроз в інформаційній сфері та аналіз ефективності існуючих механізмів протидії цим загрозам набуває особливої актуальності. Успішне протистояння інформаційній агресії напряму впливає на обороноздатність України, консолідацію українського суспільства, формування національної ідентичності, розвиток демократії та інтеграцію в європейський і євроатлантичний безпековий простір [1].

Глобальні виклики охоплюють такі напрямки:

1) Збільшення кількості та інтенсивності глобальних дезінформаційних кампаній. Світова цифрова комунікація стрімко розвивається, що значно полегшує поширення фейкових новин, маніпулятивної інформації і пропаганди на масовому рівні. Росія як держава-агресор активно використовує такі кампанії для дискредитації України, розколу суспільства, підриву міжнародної підтримки та дестабілізації суспільних інститутів. Дезінформація поширюється через соцмережі, месенджери, інтернет-ЗМІ, а також

ISSN 3083-6417 (online)
ISSN 3083-6409 (print)
№ 1(1) 2025
Series «Public management and administration»

через підконтрольні проросійські ресурси, що створюють штучний інформаційний шум і ускладнюють формування об'єктивної картини подій.

2) Інформаційна політика Росії, спрямована на агресію проти України. Російський інформаційний вплив є цілеспрямованим і системним. Він передбачає не лише пропаганду власних політичних інтересів, а й створення альтернативних наративів, які спотворюють історичні факти, дискредитують українську владу та збройні сили, а також культивують недовіру до західних партнерів України.
3) Недостатній рівень медіаграмотності та інформаційної культури в суспільстві. У сучасному цифровому світі, коли обсяг інформації збільшується експоненційно, вміння критично оцінювати джерела, аналізувати зміст і виявляти фейки стає життєво необхідним. В Україні значна частина населення не володіє необхідним рівнем медіаграмотності, що підвищує вразливість перед інформаційними маніпуляціями та підриває здатність громадян приймати усвідомлені рішення.

Національні виклики в інформаційній безпеці сформульовані з урахуванням специфіки внутрішньої ситуації та особливостей гібридної війни:

1) Інформаційний вплив Росії на населення України. Це не лише зовнішні кампанії дезінформації, а й проникнення проросійських ідей у різні соціальні групи, що створює додаткову загрозу внутрішньому консолідованому суспільству. Ворожі наративи спрямовані на розпалювання міжетнічних, соціальних та політичних конфліктів.
2) Інформаційне домінування Росії на тимчасово окупованих територіях України. В умовах контролю інформаційного простору на окупованих територіях Росія фактично монополізувала канали комунікації, заборонивши незалежні ЗМІ та нав'язуючи свої пропагандистські меседжі, що значно ускладнює роботу державних органів України з інформування населення та протидії агресії.
3) Обмежені можливості реагування на дезінформаційні кампанії. Українська держава поки що не має достатньо розвинених механізмів стратегічних комунікацій для системної протидії ворожим інформаційним атакам, що обмежує оперативність і ефективність заходів із захисту інформаційного простору.
4) Несформованість системи стратегічних комунікацій. Відсутність узгодженої, комплексної політики у сфері інформаційної безпеки призводить до розпорошеності зусиль, дублікації функцій та недостатньої координації між державними, громадськими і приватними акторами.
5) Недосконалість законодавчого регулювання інформаційної діяльності та захисту професійної діяльності журналістів. Це створює ризики для свободи слова та безпеки журналістів, що ускладнює формування незалежного інформаційного поля та забезпечення прозорості влади.
6) Спроби маніпуляції свідомістю громадян щодо європейської та євроатлантичної інтеграції України. Інформаційні атаки спрямовані на посів сумнівів щодо доцільності курсу на євроінтеграцію, що може призвести до політичної дестабілізації.
7) Обмежений доступ до об'єктивної інформації на місцевому рівні. Це особливо актуально для сільських і малих громад, де інформаційний вакуум сприяє поширенню неперевірених чуток та дезінформації.
8) Недостатній рівень інформаційної культури й медіаграмотності в суспільстві для протидії маніпулятивним і інформаційним впливам.
9) Відсутність системного підходу до навчання та просвітництва в цих сферах підсилює вразливість населення до гібридних загроз [2].

Дослідження Т. Слінько виявляє низку специфічних загроз інформаційній безпеці в умовах активної військової агресії [3]:

- поширення дезінформації як основний засіб психологічної війни, що впливає на моральний стан військових і цивільних, дестабілізує внутрішню ситуацію і створює хаос у системі прийняття рішень;
- кібератаки на державні об'єкти та критичну інфраструктуру, які ставлять під загрозу функціонування ключових систем життєзабезпечення, енергетики, комунікацій;
- шпигунство і витік інформації, що призводить до втрати стратегічних переваг і підвищує ризик провалів на фронті;
- дезорганізація комунікацій із фронту, що погіршує координацію дій сил оборони та знижує ефективність управління;
- кібершпигунство та підрив кібербезпеки, що включає використання сучасних технологій для зломів і кібервійни;
- зростання застосування штучного інтелекту й складних алгоритмів у кібератаках, що робить загрози більш масштабними і складними для протидії;

ISSN 3083-6417 (online)
ISSN 3083-6409 (print)
№ 1(1) 2025
Series «Public management and administration»

– ризики і можливості для зловживання у сфері захисту персональних даних і конфіденційної інформації, що стосуються перш за все військовослужбовців і ветеранів;
– розвиток кібервійськових здібностей, які стають невід'ємною складовою сучасних воєнних конфліктів.

Дослідження інформаційної безпеки вітчизняних банків, проведене Ю. Худолієм та Т. Андрієцем, виділяє три основні категорії викликів, які суттєво впливають на здатність фінансових установ ефективно захищати свої інформаційні ресурси [4]. По-перше, технологічні виклики пов'язані із застарілою інфраструктурою, яка не відповідає сучасним вимогам кібербезпеки. Відсутність інноваційних систем захисту, використання вразливих і застарілих програмних продуктів і обладнання створюють значні ризики для роботи банківських установ, особливо в умовах активної кіберагресії з боку ворожих державних і неурядових структур. По-друге, соціальні виклики відображаються у важливості людського фактора як слабкої ланки у системі безпеки. Люди, які працюють у банках, стають жертвами фішингових атак, соціальної інженерії та інших маніпулятивних технологій, що значно знижує рівень загальної кіберстійкості. По-третє, організаційні виклики включають у себе труднощі інтеграції сучасних технологічних рішень у вже існуючі бізнес-процеси, а також недостатнє фінансування заходів, спрямованих на підвищення рівня інформаційної безпеки.

Варто наголосити, що ці виклики, характерні для фінансової сфери, одночасно резонують із ширшою картиною загроз, з якими стикається Україна в інформаційному просторі в умовах триваючої російсько-української війни. Сучасні виклики інформаційній безпеці країни охоплюють як глобальні загрози, такі як поширення масованих дезінформаційних кампаній і активне втручання держави-агресора в інформаційне поле України, так і специфічні національні проблеми, зокрема обмеженість можливостей для оперативного реагування на інформаційні атаки, відсутність розвиненої системи стратегічних комунікацій, недосконалість нормативно-правового регулювання в інформаційній сфері та недостатній рівень медіаграмотності громадян.

Серед ключових проблем, що загрожують інформаційній безпеці України, варто виділити поширення дезінформації, особливо на тимчасово окупованих територіях, де Росія проводить систематичні інформаційні операції для легітимізації своєї агресії та послаблення єдності українського суспільства. Значну загрозу становлять також кібератаки на критично важливі державні об'єкти, зокрема енергетичну інфраструктуру, органи влади та оборонні установи, що ставить під загрозу стабільність функціонування держави. Окрім того, існує постійний ризик шпигунства, витоку конфіденційної інформації, а також маніпуляцій громадською свідомістю, спрямованих на дискредитацію євроінтеграційних прагнень України.

Для подолання цих комплексних загроз вкрай важливо впроваджувати багаторівневі заходи, які включають не лише технічні рішення, а й розвиток людського потенціалу через підвищення рівня медіаграмотності, вдосконалення нормативно-правової бази, а також налагодження ефективної координації між державними органами, приватним сектором і суспільством. Такий системний підхід дозволить забезпечити гнучкість і стійкість інформаційної безпеки України у складних умовах гібридної війни та сприятиме захисту суверенітету, територіальної цілісності і національних інтересів держави.

References

1. Larin, S. (2025). Analiz suchasnykh vyklykiv informatsiinii bezpetsi Ukrainy v umovakh rosiisko-ukrainskoi viiny [Analysis of modern challenges to information security of Ukraine in the conditions of the Russian-Ukrainian war]. Proceedings from SSPACS '25: Vseukrainska naukovo-praktychna konferentsiia studentiv, aspirantiv ta molodykh vchenykh «Shevchenkivska vesna – 2025: publichne upravlinnia ta derzhavna sluzhba» – All-Ukrainian scientific and practical conference of students, postgraduates and young scientists «Shevchenko Spring – 2025: public administration and civil service». (pp. 163-164). L.H. Komakha, T.P. Palamarchuk (Eds.). Kyiv: NNI PUDS KNU [in Ukrainian].
2. Ukaz Prezydenta Ukrainy Stratehiia informatsiinoi bezpeky vid 28.12.21 r. No. 685/2021 [Decree of the President of Ukraine Information security strategy dated 12/28/21 No. 685/2021]. *www.president.gov.ua.* Retrieved from: https://www.president.gov.ua/documents/6852021-41069 [in Ukrainian].
3. Slinko, T. Suchasni vyklyky informatsiinii bezpetsi v realiiakh viiskovoi ahresii [Modern challenges to information security in the realities of military aggression]. (n.d.). *dspace.nlu.edu.ua.* Retrieved from: https://dspace.nlu.edu.ua/bitstream/123456789/19775/1/Slinko_143-148.pdf [in Ukrainian].
4. Khudolii, Yu., & Andriiets, T. Informatsiina bezpeka vitchyznianykh bankiv: vyklyky ta maibutni rishennia [Information security of domestic banks: challenges and future solutions]. (n.d.). *reposit.nupp.edu.ua.* Retrieved from: https://surl.lu/csoyay [in Ukrainian].

ISSN 3083-6417 (online)
ISSN 3083-6409 (print)
№ 1(1) 2025
Series «Public management and administration»

DOI 10.34132/mspc2025.01.13.17

Stanislav Larin

CURRENT CHALLENGES IN THE FIELD OF INFORMATION SECURITY OF UKRAINE IN THE CONTEXT OF THE RUSSIAN-UKRAINIAN WAR

Information security has become one of the most important components of Ukraine's national security, especially in the context of the ongoing Russian-Ukrainian war. Under the current conditions of aggression by the Russian Federation, Ukraine's information space is under unprecedented pressure from the enemy, which uses various tools of disinformation, propaganda, cyber terror and manipulation of public opinion. In view of this, a comprehensive study and analysis of current challenges to Ukraine's information security is of particular relevance, as successful countering information aggression directly affects the state's defence capability, social stability and democratic development. The official document, the Information Security Strategy of Ukraine, adopted in 2021, classifies the challenges facing the information space as global and national. This allows for a clear distinction between external threats that are transnational in nature and internal threats related to the specifics of the information sphere in Ukraine.

Keywords: *information space, information security, information sphere, global and national challenges, transformational nature of threats.*

Відомості про автора / Information about the Author

Станіслав Ларін, к. н. держ. упр., доцент кафедри державного управління, Навчально-наукового інституту державного управління та державної служби Київського національного університету імені Тараса Шевченка, м. Київ, Україна. E-mail: larin.stan@gmail.com, orcid: https//orcid.org/0000-0001-8544-7714.

Stanislav Larin, Candidate of Sciences in Public Administration, Associate Professor, Department of Public Administration, Educational and Scientific Institute of Public Administration and Civil Service, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine. E-mail: larin.stan@gmail.com, orcid: https//orcid.org/0000-0001-8544-7714.

Стаття отримана редакцією 04.06.2025.