

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
Національний університет оборони України
Інститут стратегічних комунікацій

**Науково-дослідний відділ проблем розвитку
та впровадження стратегічних комунікацій**



VI МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ
СТРАТЕГІЧНІ КОМУНІКАЦІЇ У СФЕРІ ЗАБЕЗПЕЧЕННЯ
НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНИ:
ПРОБЛЕМИ, ДОСВІД, ПЕРСПЕКТИВИ

29 жовтня 2025 року

ТЕЗИ ДОПОВІДЕЙ

Видання університету
2025

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
Національний університет оборони України

Інститут стратегічних комунікацій

**СТРАТЕГІЧНІ КОМУНІКАЦІЇ
У СФЕРІ ЗАБЕЗПЕЧЕННЯ
НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНИ:
ПРОБЛЕМИ, ДОСВІД, ПЕРСПЕКТИВИ**

VI Міжнародна науково-практична конференція
29 жовтня 2025 року

ТЕЗИ ДОПОВІДЕЙ

Видання університету
2025

УДК: 355.451

Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи : VI міжнар. наук.-практ. конф., 29 жовтня 2025 р.: тези доповідей / Міністерство оборони України, НУОУ. К.: НУОУ, 2025. 237 с.

До збірника увійшли тези доповідей, що містять теоретичні та практичні результати наукових досліджень і розробок учасників міжнародної науково-практичної конференції, присвячені проблемам інформаційної безпеки та розбудови стратегічних комунікацій.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Голова організаційного комітету:

ВОЙТКО О.В., доктор військових наук, доцент, лауреат Національної премії України імені Бориса Патона;

Заступник голови організаційного комітету:

РАХІМОВ В.В., доктор філософії;

Члени організаційного комітету:

ФЕДОРІЄНКО В.А., кандидат технічних наук (головний модератор конференції);

БАЗАРНИЙ С.В., доктор філософії (модератор);

Секретар:

ЗУБКО Р.В.;

ЯНКОВИЙ Я.М.

Технічне супроводження:

ЛАШИН Я.О.;

ТЕРНОВИЙ С.В.

Затверджено протоколом та схвалено до друку на засіданні інституту стратегічних комунікацій Національного університету оборони України (протокол №3 від 13 листопада 2025 року).

За достовірність наданого матеріалу, фактів, цитат та інших відомостей відповідальність несуть автори.

© Національний університет оборони України, 2025

ВСТУПНЕ СЛОВО	10
<i>СЕКЦІЯ 1: СОЦІАЛЬНА КОМУНІКАЦІЯ ТА ПУБЛІЧНА ДИПЛОМАТІЯ</i>	
LEMBERSKYI OLESANDR, CHERNIAVSKYI OLEGH "Public diplomacy as a technology of Ukrainian foreign policy"	13
Olga PONOMARENKO, "Military-Diplomatic Discourse as an Instrument for Shaping International Support: the Experience of Italy, Spain, France, and Argentina"	16
ГОРЧАНЮК ОЛЕНА "Публічна комунікація як елемент міжнародної співпраці"	20
ГУСЬКОВА ЕЛЕОНОРА "Публічна дипломатія України в умовах збройного конфлікту"	21
МЕЛЬНИЧУК НАТАЛІЯ "Сучасні виклики стратегічних комунікацій"	25
ФІСАНОВ ВОЛОДИМИР, ОСАДЦА ІВАН "Стратегічні комунікації як інструмент формування суспільної довіри в умовах довготривалої війни"	26
РАХІМОВ ВОЛОДИМИР, ЯНКОВИЙ ЯРОСЛАВ "Аналіз чинників, які впливають на підвищення ефективності стратегічних комунікацій Збройних Сил України через інтеграцію інструментів публічної дипломатії"	30
<i>СЕКЦІЯ 2: ВІЙСЬКОВІ ЗВ'ЯЗКИ З ГРОМАДСЬКІСТЮ</i>	
АНТОНЕНКО КАТЕРИНА "Як креативні кампанії трансформують рекрутинг у Збройних силах України"	35
БОНДАР ЮРІЙ, ВАСИЛЕНКО КСЕНІЯ, РЯБІЧЕВ ВЯЧЕСЛАВ "Зміни українського медіаландшафту після повномасштабного вторгнення в Україну"	38
ДУДКО ОЛЕНА "Системність планування та управління інформаційними кампаніями у сфері оборони"	41
КОЗАК ВАЛЕНТИНА "Психолінгвістичні маркери маніпулятивного дискурсу в цифровому медіасередовищі"	45

КОЧМАР ТАРАС "Проблеми та виклики у створенні бригадних брендів Сил оборони України на прикладі бренду 12 бригади спеціального призначення «Азов»"	47
ЛЕЩЕНКО АНЖЕЛІКА "Мовна підготовка офіцерського складу до брифінгу"	50
ЛЮБАШЕНКО ОЛЕСЯ "Міжпрофесійна комунікативна компетентність персоналу служб першої допомоги комбатантам на фронті: кризові та стратегічні виклики"	52
СИЛКІН ЄВГЕНІЙ "Імплементация медійного виробництва підрозділів територіальної оборони як інформаційний феномен комунікаційно-контентної індустрії"	54
ТЕРЕХОВ ЮЛІЙ "Стратегічні комунікації в сучасних умовах російсько-української війни"	56
ШИДЛЮХ ВІКТОР "Розвиток культури внутрішніх комунікацій офіцерів: результати педагогічного експерименту"	61
<i>СЕКЦІЯ 3: ІНФОРМАЦІЙНІ ТА ПСИХОЛОГІЧНІ ОПЕРАЦІЇ</i>	
BENJAMIN DELHOMME "Detecting fact-agnostic influence signatures in news articles: An ontology-driven approach with DIMA-OntoToolkit"	65
HUSAK YURIY, BAZARNYI SERHIY "Methodological approach to mathematical modeling of the stability of state management in russia's multi-domain war against Ukraine"	68
LEMBERSKYI OLESANDR, CHERNIAVSKYI OLEGH "Information-psychological operations as a modern tool of geopolitics"	72
АВРАМЕНКО МАРИНА, АВРАМЕНКО ДМИТРО "Інформаційна резильєнтність як стійкість українського суспільства до інформаційних дій противника"	75
АХТИРЦЕВА ВЛАДИСЛАВА, КИРИЛЕНКО КАТЕРИНА, МАГДУН МАКСИМ "Роль і місце інформаційно-психологічних заходів в стабілізаційній операції"	78

БОНДАРЕНКО ОЛЕКСАНДР "Сучасні війни: мовно-лінгвістичний вимір"	81
ДЕМАРТИНО АНДРІЙ "Російські FIMI і втручання у вибори в європейських країнах у 2024 році"	82
МІХІНА ТЕТЯНА "Аналіз особливостей дискредитаційних кампаній рф у російсько-українській війні"	85
НАМЕСТНІК ВІКТОРІЯ, ПАВЛОВ МИКОЛА "Штучний інтелект як інструмент поширення дезінформації"	87
НЕЧАСВ ОЛЕГ "Штучний інтелект у психологічних операціях: виклики та можливості"	90
ПЕТРЕНКО КИРИЛО, ТЕМНИЙ ОЛЕГ "Протидія інформаційно-психологічному впливу противника під час реалізації комунікаційної стратегії Збройних Сил України"	92
ПРИБИЛЄВ ЮРІЙ, ЛОЗОВИЙ РОМАН "Концепція автоматизації управління психологічними операціями"	94
ПРОКОПЕНКО ОЛЕКСАНДР, ОНОФРІЙЧУК ОЛЬГА "Підвищення ефективності інформаційного впливу в інтересах інформаційної операції ОСУВ"	97
РОМАНЮК АЛЬОНА "Механізми реверсивної дезінформації: аналіз віддзеркалення фейків як складова інформаційно-психологічних операцій"	100
РУДИК АНДРІЙ "Концепція "виправлення імен" Конфуція та проведення психологічних операцій"	104
СКАРЖИНЕЦЬ АНДРІЙ "Прикладний потенціал DSM моделі в контексті аналізу цільової аудиторії"	107
ТЕРНОВИЙ ОЛЕКСАНДР "Класифікація методів та моделей генерації та поширення спеціальної інформації під час проведення інформаційної операції"	109
ФІТКАЛЕНКО НІНА "Залучення блогерів до інформаційних операцій ЗСУ: аналіз потенціалу та шляхи інтеграції"	110

ЧИЖЕВСЬКА МАРІАННА "Особливості моніторингу інформаційного простору в інтересах інформаційних операцій Збройних Сил України"	114
СЕКЦІЯ 4: ПРОБЛЕМНІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	
ZUBKO ROMAN "Disinformation as an instrument of hybrid aggression: directions for counteraction under current cyber threats"	118
АНДРУЩЕНКО ОЛЕСЯ "Інформаційна безпека як чинник легітимації політико-правових відносин у цифрову добу"	120
АРТЮЩИК АНДРІЙ "Технології захисту інформації та кібербезпека"	122
БОНДАР ВОЛОДИМИР "Трансформаційні процеси під впливом штучного інтелекту на стійкість соціоекономічних систем"	125
ВОЙНОВА ЕЛЛІНА "Сучасний інформаційний простір та його вплив на формування ідентичності молоді в умовах воєнного стану"	128
ГРОМИКО ІГОР "Пірамідальна модель доступу громадянина до державної таємниці"	131
ДЗИГА ОЛЕКСАНДР "Показники оцінювання ефективності системи забезпечення інформаційної безпеки України у воєнній сфері"	134
ЗІНЧЕНКО МИХАЙЛО, ЯКОВЧУК ОЛЕКСАНДР, ПЛУГОВА ОЛЬГА "До питання щодо вибору методів захисту інформаційних систем на основі аналізу та класифікації ризикоутворюючих факторів"	136
ІВАЩЕНКО СЕРГІЙ "Стратегічні комунікації як інструмент протидії інформаційним загрозам держави"	139
КРАЙНОВ ВАЛЕРІЙ "Основні напрямки забезпечення безпеки єдиного інформаційного простору"	141

ЛАШИН ЯРОСЛАВ, ФЕДОРІЄНКО ВІТАЛІЙ, СІВОХА ІГОР "Тематичне моделювання як інструмент підвищення ефективності інформаційної безпеки"	145
ЛИСИЧКІНА ІРИНА, ЛИСИЧКІНА ОЛЬГА "Наратив як зброя: лінгвістичні механізми конструювання реальності у когнітивній війні"	149
ЛОЙШИН АНАТОЛІЙ "Актуальні виклики інформаційної безпеки в епоху цифрової трансформації"	151
МАКАРЧЕНКО ІРИНА "Стратегія комунікації сил оборони як інструмент формування всеохоплюючої оборони в умовах стримування"	154
МАРЦУН СВІТЛАНА "Використання штучного інтелекту в кібернападах Росії на Україну"	157
МІХЄЄВ ЮРІЙ, ПАВЛЕНКО МИХАЙЛО "Використання технологій штучного інтелекту в інтересах протидії інформаційно-психологічному впливу"	161
МОРОЗ НАДІЯ "Кіберстійкість та безпека штучного інтелекту: проблеми та практичні підходи РНБО, Держспецзв'язку та Мінцифри до забезпечення національної інформаційної безпеки"	163
НІКОЛІН ЄВГЕН, ВІТРУК ЮЛІЯ "Захищений месенджер із наскрізним шифруванням і анонімізацією трафіку"	166
ПОМАЗА-ПОНОМАРЕНКО АЛІНА, ТАРАДУДА ДМИТРО, НЕВОДЧІКОВА ІРИНА "Напрямки формування системи інформаційної безпеки в Україні в умовах ризиків"	168
САЙКО ВОЛОДИМИР, ЗІНЧЕНКО МИХАЙЛО, КОМАРОВ ВОЛОДИМИР "Актуальні питання інформаційної безпеки у військовій сфері"	171

Список використаних джерел

1. *Кібербезпека та ризики цифрової трансформації компаній* — Юрій Когут
2. *Основи кіберпростору, кібербезпеки та кіберзахисту* — Богуш В. М., Богуш В. В., Бровко В. Д., Настрадін В. П.

АЛІНА ПОМАЗА-ПОНОМАРЕНКО,
д.держ.упр., професор,
Національний університет
цивільного захисту України

ДМИТРО ТАРАДУДА, к.т.н., доцент,
Інститут післядипломної освіти
Львівського державного університету
безпеки життєдіяльності

ІРИНА НЕВОДЧІКОВА,
Національний університет
цивільного захисту України

НАПРЯМКИ ФОРМУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ В УМОВАХ РИЗИКІВ

Інформаційна безпека є ключовим елементом національної безпеки будь-якої держави, оскільки саме інформаційний простір визначає стійкість суспільства до зовнішніх і внутрішніх впливів. Для України, яка перебуває у стані гібридної війни, питання інформаційної безпеки набули особливої ваги [1; 3]. Сучасні виклики полягають не лише у протидії кібератакам, а й у боротьбі з дезінформацією, інформаційними маніпуляціями, пропагандою, а також у забезпеченні технологічної незалежності держави.

Інформаційна безпека розглядається в міждисциплінарному вимірі, зокрема, на перетині галузей науки політико-правового блоку, кібернетики, соціології, конфліктології тощо. Урахування їх положень дозволяє окреслити концептуальну структуру інформаційної безпеки, що включає:

- технологічний компонент, що передбачає захист інформаційних систем і даних;
- комунікаційний компонент, що спрямований на захист від маніпуляцій, інформаційних операцій;
- гуманітарний компонент (інформаційна культура, медіаграмотність

населення);

– управлінський компонент (система державного регулювання, координації та моніторингу ризиків).

Учені слушно підкреслюють, що інформаційна безпека є не лише технічним, а й соціально-політичним феноменом. На це потрібно зважати під час забезпечення розвитку чинної правової бази у сфері інфобезпеки. Україна має необхідну законодавчу базу у сфері інформаційної безпеки, а саме:

– Закон України «Про основні засади забезпечення кібербезпеки України» (2017 р.);

– Стратегія кібербезпеки України (2021–2025 рр.);

– Стратегія інформаційної безпеки України (2021 р.);

– Укази Президента України щодо протидії інформаційній агресії, розбудови національної системи кіберзахисту.

Однак, попри наявність базових актів, залишається фрагментарність правового регулювання, відсутність узгоджених стандартів захисту критичної інформаційної інфраструктури та недостатня координація між державними структурами.

Серед основних проблем інформаційної безпеки в сучасних умовах можна виокремити такі:

1. Гібридні загрози і кібератаки. З початком повномасштабної агресії РФ кількість кібератак на українські ресурси зростає більш ніж утричі. Основними об'єктами стали державні органи, банки, енергетичні компанії, ЗМІ. Як відомо, за даними Державної служби спеціального зв'язку та захисту інформації, у 2023–2024 рр. зафіксовано понад 450 критичних інцидентів у сфері кібербезпеки.

2. Інформаційно-психологічні операції. Проти України системно ведеться інформаційна війна, спрямована на деморалізацію населення, дискредитацію Збройних сил та підрив міжнародної репутації держави. При цьому використовуються механізми протистояння фейковим новинам і дезінформаційним кампаніям, бот-мереж у соціальних медіа, псевдоаналітичних ресурсів для створення ефекту «альтернативної реальності» [2].

3. Недостатність системи державного моніторингу за станом розвитку інфосфери. Попри наявність Національного координаційного центру кібербезпеки, спостерігається недостатній рівень інтеграції баз даних, розпорошеність відповідальності між органами виконавчої влади. Не створено єдиної системи оперативного обміну інформацією між безпековими структурами [1].

4. Людський фактор та дефіцит кадрів. Дефіцит фахівців із кіберзахисту, низький рівень цифрової грамотності посадових осіб та працівників державного сектору призводять до витоків даних і технічних помилок.

5. Залежність від іноземних технологічних платформ. Проблемою залишається використання державними установами іноземного програмного забезпечення, серверних потужностей та сервісів, що створює ризики для

національної інформаційної незалежності.

Європейський Союз, НАТО та США розвивають комплексні стратегії інформаційної безпеки, які базуються на такому: інтеграції цивільного і військового секторів у забезпеченні кіберзахисту; розвитку національних центрів кіберстійкості (National Cyber Resilience Centres); інвестиціях у кіберосвіту та інформаційну грамотність. Україна вже інтегрується у цю систему через участь у Платформі кіберстійкості ЄС (EU Cyber Solidarity Act, 2023) та програмі NATO Trust Fund on Cyber Defence [4].

Щодо шляхів удосконалення державної політики у сфері інфобезпеки, можна визначити такі:

1) розробку загально державної стратегії інформаційної безпеки на середньостроковий період, яка б інтегрувала кібер, комунікаційний та освітній аспекти;

2) посилення кадрового потенціалу через створення мережі центрів підготовки спеціалістів з кіберзахисту;

3) розвиток національного софту та хмарних сервісів, зменшення залежності від зовнішніх технологій;

4) моніторинг інформаційного простору з використанням штучного інтелекту для виявлення фейків і бот-активності;

5) підвищення інформаційної культури громадян шляхом запровадження освітніх курсів медіаграмотності на всіх рівнях освіти.

Отже, інформаційна безпека є багатовимірним феноменом, що охоплює технічні, правові, політичні та культурні виміри. Основна проблема – асиметрія між швидкістю розвитку технологій і темпами адаптації управлінських систем. Для України стратегічним завданням є формування цілісної екосистеми інформаційної безпеки, що базується на принципах стійкості (resilience), міжвідомчої координації та партнерства держави, бізнесу і громадянського суспільства.

Список використаних джерел

1. Домбровська С., Помаза-Пономаренко А., Крюков О., Порока С. Інформаційні загрози та комунікативна інфраструктура в державному секторі : монографія. Харків: НУЦЗУ, 2024. 244 с.

2. Лопатченко І.М., Помаза-Пономаренко А.Л., Батир Ю.Г. Державне регулювання у сфері інформаційної безпеки України в умовах воєнного стану // Вісник Національного університету цивільного захисту України (Серія «Державне управління»). 2024. № 1 (20). С. 14–24.

3. Новіков В.О. Аналіз сучасної концепції інформаційно-гібридної війни // Державне управління: удосконалення та розвиток: елек. журнал. 2023. № 9. URL: <https://www.nayka.com.ua/index.php/dy/article/view/2133>.

4. Помаза-Пономаренко А.Л., Тарадуда Д.В. Закордонний досвід забезпечення соціальної безпеки шляхом стійкого функціонування об'єктів критичної інфраструктури та підвищеної небезпеки // Наука і техніка сьогодні. 2024. № 4 (32). С. 371-384.

ВОЛОДИМИР САЙКО, д.т.н., професор,
ВІТІ ім. Героїв Крут
E-mail: vgsaiko@gmail.com

МИХАЙЛО ЗІНЧЕНКО,
ВІТІ ім. Героїв Крут
ORCID ID: 0000-0002-1428-8231
E-mail: m030575z@ukr.net

ВОЛОДИМИР КОМАРОВ, к.т.н.,
старший дослідник, ВІТІ ім. Героїв Крут
ORCID ID: 0000-0002-4929-4527
E-mail: vladimir@komarov.in.ua

АКТУАЛЬНІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ВІЙСЬКОВІЙ СФЕРІ

Інформаційна безпека (ІБ) як узагальнююче поняття – це стан захищеності життєво важливих інтересів особи, суспільства та держави, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, моральноетичний тощо), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди.

Інформаційна безпека є критично важливою сферою для всіх типів організацій, включаючи військові організації. Способи злому баз даних стають все більш технічно складними, витонченими та ефективними. Тому необхідно забезпечити передові рішення в області ІБ, відповідаючи на виклики сучасності. Вирішення актуальних проблем ІБ потребує комплексного підходу, що включає розробку та впровадження сучасних технологій, підвищення рівня автентифікації користувачів, а також забезпечення надійності та стійкості до відмови ІТ-інфраструктури.

Під ІБ слід розуміти захист інтересів суб'єктів інформаційних відносин. Основні складові захисту - забезпечення її конфіденційності, цілісності, доступності. Головні проблеми сучасних підприємств у контексті ІБ – це хакерські атаки, різні модифікації шкідливого програмного забезпечення (ПЗ), інші зовнішні загрози. Високе занепокоєння викликають внутрішні загрози (втрата