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

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

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.

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-правого 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 зросла 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