



КІБЕР
ПОЛІЦІЯ



EMBROX
SOLUTIONS



LVIV IT
CLUSTER

softserve



UnderDefense

UKRAINIAN
RUST
COMMUNITY



ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської
науково-практичної конференції

27 листопада 2025 року

м. Львів

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ
ЖИТТЄДІЯЛЬНОСТІ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ПРИВАТНИЙ ЗАКЛАД ВИЩОЇ ОСВІТИ «ІТ СТЕП УНІВЕРСИТЕТ»

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської науково-практичної конференції

27 листопада 2025 року

Львів – 2025

ББК 32.81+78.362

Інформаційна безпека та інформаційні технології: збірник тез доповідей VII Всеукраїнської науково-практичної конференції, м. Львів, 27 листопада 2025 року. Львів, ЛДУ БЖД, 2025, 493 с.

РЕДКОЛЕГІЯ:

Василь ПОПОВИЧ – доктор технічних наук., професор, проректор з наукової роботи, Львівський державний університет безпеки життєдіяльності

Олександр ПРИДАТКО – кандидат технічних наук, доцент, проректор з навчально-методичної роботи Львівського державного університету безпеки життєдіяльності

Роман ЯКОВЧУК – доктор технічних наук, доцент, начальник навчально-наукового інституту цивільного захисту, Львівський державний університет безпеки життєдіяльності

Ольга МЕНЬШИКОВА – кандидат фізико-математичних наук, доцент, заступник начальника навчально-наукового інституту цивільного захисту, Львівський державний університет безпеки життєдіяльності

БУРАК Назарій Євгенович – кандидат технічних наук, доцент, начальник кафедри інформаційних технологій та систем електронних комунікацій, Львівський державний університет безпеки життєдіяльності

ІВАНУСА Андрій Іванович – кандидат технічних наук, доцент, начальник кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності

НАЗАР Юлія Сергіївна – доктор філософії, заступник начальника кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

ХЛЕВНОЙ Олександр Вікторович – кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

СМОТР Ольга Олексіївна – кандидат технічних наук, доцент, професор кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

БОРЗОВ Юрій Олексійович – кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

ГОЛОВАТИЙ Роман Русланович – кандидат технічних наук, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

ПИЛИПЕНКО Володимир Миколайович – старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

ЖЕЗЛО-ХЛЕВНА Наталія Володимирівна – викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

РАЙТА Діана Анатоліївна – старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

ДОВБНЯК Віра Йосипівна – викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

ПОЛОТАЙ Орест Іванович – кандидат технічних наук, доцент, доцент кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності

БАЛАЦЬКА Валерія Сергіївна – викладач кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності

ТКАЧУК Ростислав Львович – доктор технічних наук, професор, професор кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності

За точність наведених фактів, самостійність наукового аналізу та нормативність стилістики викладу, а також за використання відомостей, що не рекомендовані до відкритої публікації відповідальність несуть автори опублікованих матеріалів.

УДК 159.9:004.738

ПСИХОЛОГІЧНА СТІЙКІСТЬ СУСПІЛЬСТВА ЯК ЧИННИК ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Володимир СИДОРЕНКО, Олександр ДОЦЕНКО

Інститут наукових досліджень з цивільного захисту

Національного університету цивільного захисту України, м. Київ

***Анотація.** Розглядається психологічна стійкість суспільства як складова інформаційного захисту в умовах війни. Проаналізовано загрози інформаційних атак, роль критичного мислення, медіаграмотності, державної комунікації та соціальної згуртованості у формуванні психологічної стійкості населення та протидії дезінформації. Ключові слова: психологічна стійкість, інформаційний захист, війна, медіаграмотність, дезінформація, критичне мислення, суспільство, соціальна згуртованість, психологічна безпека*

В умовах гібридної війни та масштабних інформаційних атак психологічна стійкість суспільства набуває стратегічного значення. Сучасні інформаційно-психологічні операції (ІПсО) спрямовані не лише на підрив обороноздатності, а й на руйнування внутрішньої єдності, довіри до державних інституцій і морального духу населення. Тому формування психологічної стійкості громадян є ключовим елементом системи інформаційного захисту держави [1].

Психологічна стійкість суспільства – це здатність колективної свідомості зберігати емоційну рівновагу, критичне мислення та соціальну згуртованість під тиском інформаційних загроз. На індивідуальному рівні вона проявляється у вмінні не піддаватися паніці, адекватно реагувати на стрес і зберігати конструктивну поведінку. На колективному рівні – у підтримці соціальної довіри, взаємопідтримки та впевненості в спільній меті. Психологічна стійкість є основою інформаційного «імунітету» суспільства [2]. Під час війни інформаційний простір насичується величезною кількістю суперечливих повідомлень, що несуть наступні загрози:

- дезінформація та фейки, що викликають паніку або розчарування;
- маніпуляції через соціальні мережі, спрямовані на емоційний тиск;
- психологічна втома та інформаційне перевантаження, що знижують увагу й критичність сприйняття;
- цілеспрямовані ІПсО, що експлуатують страх, горе чи апатію населення [3].

Такі атаки можуть призвести до деморалізації, зниження довіри до влади та розколу суспільства.

Інформаційна безпека включає не лише технічний, а й соціально-психологічний компонент. Психологічна стійкість створює бар'єр, що зменшує ефективність ворожих інформаційних впливів. Її ключовими складовими є:

- критичне мислення (здатність розпізнавати маніпуляції та перевіряти факти);
- довіра до офіційних джерел та обережність у поширенні інформації;
- соціальна згуртованість (почуття єдності, що нейтралізує спроби посягти розбрат);
- психологічна грамотність (уміння керувати власними емоціями й підтримувати інших).

Стійке суспільство є менш уразливим до фейків і панічних настроїв, отже більш захищеним інформаційно.

Формування психологічної стійкості є комплексним процесом, що включає освітні, інформаційні, соціальні та психологічні заходи за наступними напрямками:

1) освітня діяльність і медіаграмотність. Формування критичного мислення починається з освіти. Впровадження програм медіаграмотності у школах та університетах допомагає громадянам розпізнавати фейки, аналізувати інформацію, оцінювати джерела та уникати емоційних маніпуляцій [4];

2) прозора та своєчасна державна комунікація. Доступ до достовірної інформації через офіційні канали державних органів знижує рівень паніки та недовіри [1];

3) підтримка ментального здоров'я. Державні та громадські психологічні сервіси, гарячі лінії та онлайн-консультації допомагають громадянам справлятися зі стресом і тривожністю. Особлива увага приділяється ветеранам, військовослужбовцям та членам їхніх сімей, а також людям у прифронтових регіонах;

4) громадянська солідарність та соціальна згуртованість. Волонтерські ініціативи, культурні та спортивні заходи, громадські акції допомагають підтримувати колективне почуття єдності;

5) протидія дезінформації та інформаційне просвітництво. Проекти на кшталт StopFake, Центру стратегічних комунікацій та інших платформ активно спростовують фейки і навчають населення розпізнавати маніпуляції [3, 5];

6) розвиток критичного мислення та навичок саморегуляції. Психологічна стійкість вимагає не лише знання, а й практичних умінь: управління емоціями, стресостійкість, уміння приймати рішення в умовах невизначеності;

7) міжнародний досвід та обмін практиками. Вивчення успішних моделей психологічної стійкості в інших країнах, обмін досвідом із партнерами НАТО, ЄС та ООН допомагає впроваджувати ефективні методики, адаптовані до українських реалій.

Українське суспільство під час повномасштабної війни 2022–2025 рр. продемонструвало високий рівень психологічної стійкості. Попри щоденні інформаційні загрози, кібератаки та масові спроби поширення дезінформації, громадяни зберегли віру у власні сили, довіру до Збройних Сил і готовність діяти спільно для захисту країни. Це стало можливим завдяки

комплексному підходу, який поєднав державну політику, медіаграмотність, активність громадянського суспільства та волонтерські ініціативи.

Державні структури, такі як Центр стратегічних комунікацій, своєчасно спростовували фейки та надавали громадянам достовірну інформацію, мінімізуючи паніку. Водночас широкомасштабна волонтерська діяльність, культурні події, ініціативи психологічної допомоги та взаємодопомога у громадах формували відчуття єдності та підтримки, що значно підвищувало стійкість населення. Особливо ефективною виявилася робота державних і громадських платформ, таких як StopFake, гарячі лінії психологічної підтримки, інформаційні кампанії з медіаграмотності, а також ініціативи з розвитку критичного мислення серед молоді. Ці заходи дозволили не лише нейтралізувати вплив дезінформації, а й підвищити готовність суспільства до спільних дій у кризових умовах.

Український досвід показує, що психологічна стійкість населення є не лише результатом індивідуальної витримки, а й комплексним ефектом координації держави, медіа, громадських організацій і самих громадян. Стійке суспільство стало важливою складовою національної оборони, рівнозначною армії чи кіберзахисту, і слугує прикладом для інших держав, що опинилися під інформаційним тиском та агресією.

Психологічна стійкість – це не лише риса особистості, а стратегічний ресурс держави. Вона формує інформаційний щит, який захищає суспільство від паніки, фейків і маніпуляцій. Формування цієї стійкості потребує спільних зусиль держави, освіти, медіа та кожного громадянина. У війні за свідомість людей перемагає не той, хто має більше інформації, а той, хто здатен мислити критично й залишатися внутрішньо сильним..

Література

1. Національна рада України з питань телебачення і радіомовлення. *Протидія дезінформації в умовах війни, українське законодавство та роль медіа*. URL: <https://webportal.nrada.gov.ua/protydiya-dezinformatsiyiv-umovah-vijny-ukrayinske-zakonodavstvo-ta-rol-media/> (дата звернення: 11.11.2025).
2. Корольова Н.Д., Матохнюк Л.О., Таран А.А. Психологічна стійкість молоді в умовах військової агресії. *Вісник Донецького національного університету імені Василя Стуса. Серія Психологічні науки*. 2025. Вип. 2(5). С. 72–79. DOI: 10.31558/2786-8745.2024.2(5).8.
3. StopFake.org. URL: <https://www.stopfake.org/uk/> (дата звернення: 11.11.2025).
4. Ласкова-Ярмоленко А., Слинькова Т. Медіаграмотність в системі освіти: вимоги сучасності у сфері соціальної комунікації. *Педагогічні інновації: ідеї, реалії, перспективи*. 2024. Том 1. № 32 (2024). С 100–105. DOI: 10.32405/2413-4139-2024-1(32)-100-105.
5. Центр стратегічних комунікацій. URL: <https://spravdi.gov.ua/> (дата звернення: 11.11.2025).

Середницька Х., Райта Д. АЛГОРИТМІЧНА ПРОПАГАНДА: ЯК ШІ ВИКОРИСТОВУЄТЬСЯ У СТВОРЕННІ ФЕЙКОВИХ ВІДЕО ПРО ВІЙНУ	436
Сидоренко В., Доценко О. ПСИХОЛОГІЧНА СТІЙКІСТЬ СУСПІЛЬСТВА ЯК ЧИННИК ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ	439
Сорока А., Яшук В., Балацька В. КОНЦЕПТУАЛЬНА МОДЕЛЬ МІНІМІЗАЦІЇ ВИТОКІВ ДАНИХ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ НА ОСНОВІ ПРИНЦИПІВ ZERO TRUST АРХІТЕКТУРИ.....	441
Сукач А., Яшук В., Фединець Н. КІБЕРБЕЗПЕКА В ЦИФРОВОМУ МАРКЕТИНГУ: ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У РЕКЛАМНИХ КАМПАНІЯХ.....	445
Топала Р. АНАЛІЗ МЕТОДІВ АРХІТЕКТУРНОЇ ОПТИМІЗАЦІЇ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ: ПЕРЕВАГИ ТА РИЗИКИ ZERO TOUCH PROVISIONING.....	450
Фединець Н.І., Сорока А.А. ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ ПІД ЧАС ВІЙНИ	453
Фединець Н.І., Конєпуд М.І. ХМАРНІ ТЕХНОЛОГІЇ В УМОВАХ ВІЙНИ: БАЛАНС МІЖ МОБІЛЬНІСТЮ ТА БЕЗПЕКОЮ.....	456
Ціко М., Ткачук Р., Ткаченко А. ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У СКБД НА ОСНОВІ ПОВЕДІНКОВОЇ АНАЛІТИКИ ТА НЕКОНТРОЛЬОВАНОГО НАВЧАННЯ.....	458
Cinque P. INTELLIGENT CYBERSECURITY SYSTEM BASED ON ARTIFICIAL INTELLIGENCE	461
Cinque K. IMPLEMENTATION OF ZERO-TRUST ARCHITECTURE WITH BLOCKCHAIN-BASED ACCESS AUDIT FOR CLOUD STORAGE SECURITY	463
Чінкує П. КОМБІНОВАНІ КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ.....	466

Наукове видання

**ІНФОРМАЦІЙНА БЕЗПЕКА
ТА ІНФОРМАЦІЙНІ
ТЕХНОЛОГІЇ**

Збірник тез доповідей
VII Всеукраїнської науково-практичної конференції

Відповідальні за випуск

**Назарій БУРАК
Олександр ХЛЕВНОЙ**

Оригінал-макет

**Юлія НАЗАР, Ольга СМОТР,
Роман ГОЛОВАТИЙ, Діана РАЙТА,
Віра ДОВБНЯК, Іван РОВЕЦЬКИЙ,
Наталія ЖЕЗЛО-ХЛЕВНА**

Підписано до друку 12.11.2025 р.
Формат 60×84/16. Гарнітура Times New Roman.
Друк на різнографі. Папір офсетний.
Ум. друк. арк. 30.

Друк ЛДУ БЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
тел./факс: (032) 233-32-40, 233-24-79.