Міністерство оборони України
Житомирський військовий інститут
імені С. П. Корольова

# “Інформаційна безпека, інформаційні та психологічні операції в умовах повномасштабної збройної агресії рф проти України”

Тези доповідей
Міжнародної науково-
практичної конференції

11 червня 2026 року

УДК 004.056.5+327.88+355.40(063)
І-74

**Інформаційна** безпека, інформаційні та психологічні операції в умовах
І–74 повномасштабної збройної агресії рф проти України : Міжнар. наук.–практ. конф., 11 червня 2026 р. : тези доп. / М-во оборони України, Житомир. військ. ін-т імені С. П. Корольова ; відп. за вип. Д. Л. Федорчук. – Житомир : ЖВІ, 2026. – 240 с.

УДК 004.056.5+327.88+355.40(063)

## ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

**Голова організаційного комітету –** кандидат технічних наук, старший дослідник ФЕДОРЧУК Дмитро Леонідович

**Заступник голови організаційного комітету –** ФРИЗ Володимир Петрович

**Члени організаційного комітету:**
доктор філософії ГОРБАЧ В. Я.;
доктор філософії САМПІР О. М.;
доктор філософії СЕРГІЄНКО О. П.;
кандидат технічних наук МАНЬКО О. В;
кандидат технічних наук ПЕРЕГУДА О. М.;
кандидат педагогічних наук СТУПАК Д. Є.;
кандидат філософських наук ФЕДОРЕНКО В. В.;
АМІРОВ А. Р.;
ЧЕРКЕС В. М.;
АЛЕКСЕЙЧУК Н. О;
НОСОВА Г. Д.

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

Адреса:
Житомирський військовий інститут імені С. П. Корольова,
просп. Миру, 22, м. Житомир, 10004

Тел. (0412) 48-30-19

---

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

## Вітальне слово начальника Житомирського військового інституту імені С. П. Корольова доктора історичних наук, професора полковника Андрія Віталійовича Слюсаренка

**Шановні колеги! Панове офіцери, науковці!**

Радий вітати вас у стінах Житомирського військового інституту імені С. П. Корольова на відкритті Міжнародної науково-практичної конференції “Інформаційна безпека, інформаційні та психологічні операції в умовах повномасштабної збройної агресії рф проти України”.

Сьогодні ми консолідуємо наші зусилля задля виконання критично важливої місії – узагальнення сучасного досвіду у сфері інформаційної безпеки, інформаційних та психологічних операцій, а також розробки новітніх і дієвих шляхів протидії загрозам з боку ворога. Повномасштабна війна, чітко довела: інформаційний та когнітивний простори є такими ж повноцінними театрами воєнних дій, як суша, море чи повітря. І перемога на цьому “невидимому фронті” безпосередньо впливає на успіх на полі бою. Для нашого військового інституту ця проблематика є сферою щоденної навчальної та наукової діяльності. Одним із ключових і стратегічних завдань інституту є якісна, всебічна підготовка висококласних фахівців у сфері психологічних операцій, інформаційної безпеки та сучасних інформаційних технологій, яка розпочалася ще в далекому 2003 році.

Сучасний офіцер має не просто аналізувати інформаційне середовище, а й досконало володіти ІТ, штучним інтелектом та інструментами кібербезпеки. Наш випускник – це фахівець, здатний виявляти та ефективно протидіяти ворожим інформаційним та кібернетичним загрозам, змінювати поведінку противника. Робота запланованих сьогодні дискусійних панелей якраз і спрямована на вдосконалення теоретичних та прикладних аспектів підготовки таких кадрів, які вже завтра посилять спроможності сил оборони України. Проте ефективна протидія ворожій пропаганді та інформаційному впливу неможлива силами лише однієї інституції. Наша сила – у міжвідомчій взаємодії, у поєднанні військової науки, інновацій, якісної підготовки, ефективного управління та бойового досвіду.

Я щиро вдячний за те, що до нашого наукового заходу долучилося широке коло партнерів, серед яких представники Міноборони, Генерального штабу, ССО, Головного управління розвідки, СБУ та провідних ВВНЗ. Саме така синергія науковців, освітян, замовників, органів військового управління та бойових підрозділів дозволяє нам вибудовувати надійну систему інформаційної стійкості. Обмін досвідом під час цієї конференції допоможе впровадити нові методики у підготовку особового складу та виробити практичні рекомендації щодо протидії ворожим впливам. Бажаю всім учасникам конференції конструктивних дискусій, плідних напрацювань задля нашої спільної Перемоги! Дякую за вашу працю та відданість справі! Слава Україні!

**ПАНЕЛЬ 1**

**Теоретичні та прикладні аспекти інформаційних і психологічних операцій**

Орищук І. О.
Ступак Д. Є., канд. пед. наук, доц.
Житомирський військовий інститут імені С. П. Корольова

# СПОСОБИ ЗАСТОСУВАННЯ КОМПЛЕКСІВ РАДІОМОВЛЕННЯ ТА ВИМОГИ ДО НИХ

В ході агресії росії проти України все більшого значення набуває фактор інформаційного та психологічного впливу (ПсВ) який посилюється інтеграцією з засобами масової комунікації, що постійно розвиваються. Присутність українських інформаційних джерел в інформаційному просторі прифронтових та захоплених ворогом територій з метою інформування населення а також забезпечення цілеспрямованого психологічного впливу на особовий склад противника в рамках психологічних операції (ПсО) залишається актуальною задачею. Її розв'язання потребує вирішення ряду частинних наукових завдань, одним з яких є розроблення нових або модернізація існуючих зразків озброєння, удосконалення способів їх бойового застосування.

Для здійснення ПсВ на цільову аудиторію шляхом радіомовлення підрозділами ПсО застосовуються зразки тактичних комплексів радіомовлення іноземного виробництва, однак їх характеристики не повністю відповідають сучасним умовам. Це ймовірно, обумовлено тактикою їх застосування, що враховувались під час їх розроблення, яка не передбачає їх знаходження у безпосередній зоні ураження вогневими засобами противника. Існуючі зразки мають антени з круговою діаграмою спрямованості в горизонтальній площині, а висота щогли значно обмежує дальність мовлення, яка для визначеного діапазону частот обмежується дальністю прямої видимості.

Необхідність максимального покриття тимчасово окупованих територій радіосигналом вимагає наближення комплексів до лінії бойового зіткнення, збільшення потужності сигналу та збільшення висоти підйому антени транслятора над поверхнею землі. Досвід застосування комплексів радіомовлення показав, що їх місце розташування (антенних систем) гарантовано виявляється противником і є для нього однією з пріоритетних цілей. Активне застосування противником FPV-дронів, КАБів та інших засобів

вимагає розташування комплексів радіомовлення за можливістю віддалено від лінії бойового зіткнення, поза зоною ураження вогневих засобів противника, що обмежує їх ефективність.

Враховуючи особливості застосування комплексів радіомовлення в сучасних умовах та мету їх застосування в інтересах ПсО можливо окреслити два основних завдання, що визначатимуть способи застосування комплексів радіомовлення, а також їх конструктивні і технічні характеристики.

Першим завданням в рамках ПсО залишається інформування населення на підконтрольних територіях, та протидія (подавлення) на визначених частотах сигналів станцій радіомовлення противника. Вирішення цього завдання можливо шляхом використання стаціонарних потужних трансляторів з круговою діаграмою спрямованості антен та стаціонарних веж, які знаходяться на безпечній відставні, або у разі їх відсутності, використання декількох невеликих мобільних комплексів з круговою діаграмою спрямованості антен.

Другим завданням є ПсВ безпосередньо на противника та на населення окупованих територій. З цією метою доцільним буде використання потужних передавачів, антен зі спрямованою діаграмою та максимальною висотою їх розміщення, для забезпечення найбільшої дальності прямої видимості, розташованих на безпечній відстані від лінії бойового зіткнення. Або застосування вздовж лінії бойового зіткнення невеликих комплексів радіомовлення, що мають малу вартість, використовують спрямовані антени, мають можливість швидкої заміни антен та кабелів у разі ураження противником. Однак, виникає ряд протиріч:

збільшення потужності передавача не є доцільним, так як дальність розповсюдження сигналу УКХ діапазону (FM) прямо залежить від дальності прямої видимості, а саме, висоти підйому антени;

збільшення дальності, для мовлення на передові позицій противника та у глибину окупованих територій, вимагає наближення до лінії бойового зіткнення, що збільшує імовірність їх ураження;

використання спрямованих антенних систем, у порівнянні з всеспрямованими, дозволяє знизити потужність передавача та вартість апаратури з однаковою дальністю розповсюдження сигналу, але висота розміщення антени значно її обмежує.

Таким чином, часткове вирішення проблеми забезпечення інформування або цілеспрямованого ПсВ на відповідну цільову аудиторію з використанням

радіомовлення можливо шляхом оптимізації характеристик комплексів радіомовлення відповідно завдань, які вони мають вирішувати та способів їх застосування в умовах бойових дій.

Брановицький В. В.
Житомирський військовий інститут імені С. П. Корольова

## ЕВОЛЮЦІЯ ТЕХНОЛОГІЙ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ У РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ

Повномасштабне вторгнення російської федерації в Україну стало безпрецедентним прикладом комплексного застосування військових, інформаційних, психологічних, кібернетичних та електронних засобів впливу. Інформаційно-психологічні операції (ІПсО) стали невід'ємним компонентом бойових дій, спрямованим на формування вигідного інформаційного середовища, деморалізацію противника та вплив на міжнародну громадську думку. На відміну від традиційного розуміння інформаційної війни як сукупності спеціальних заходів, сучасні ІПсО реалізуються в межах інтегрованого багатодоменного підходу, який поєднує спеціальну пропаганду, кібероперації, радіоелектронну боротьбу (РЕБ), застосування безпілотних літальних апаратів (БПЛА) та технології аналізу інформації з відкритих джерел (OSINT). Така інтеграція забезпечує одночасний вплив на технічні системи, інформаційні канали та когнітивну сферу цільових аудиторій.

На початковому етапі повномасштабної агресії російське керівництво розраховувало на досягнення швидкого військово-політичного результату за рахунок раптовості нападу та інформаційного шоку. Відповідно, основний акцент було зроблено не на довготривалих стратегічних інформаційних кампаніях, а на масованому застосуванні простих, але масштабних інструментів психологічного впливу: пропаганди, дезінформації, фейків та провокацій.

Водночас українська система стратегічних комунікацій, національно орієнтовані медіа, активне громадянське суспільство та високий рівень цифрової мобілізації забезпечили ефективну протидію ворожим інформаційним впливам. Це змусило росію адаптувати власні методи та перейти до багаторівневої моделі інформаційно-психологічних операцій.

Складові технологічного забезпечення інформаційно - психологічних операцій російської федерації.

1. Кібероперації. Кіберкомпонент забезпечує доступ до інформаційних ресурсів, викрадення даних, проведення атак типу DDoS, та розповсюдження шкідливого програмного забезпечення. Отримані дані використовуються як джерело компрометаційних матеріалів та інформаційних приводів.

2. Радіоелектронна боротьба. РЕБ виконує функції подавлення каналів зв'язку, навігаційних сигналів та безпілотних систем. Поряд із тактичним ефектом, РЕБ створює психологічний вплив через порушення управління, ізоляцію підрозділів та зниження довіри до технічних засобів.

3. Безпілотні літальні апарати. БПЛА використовуються не лише для розвідки та коригування вогню, а й як інструмент інформаційного впливу. Відеоматеріали з безпілотників формують символічний ефект технологічної переваги, підсилюють бойовий дух власних сил та деморалізують противника.

4. OSINT та аналітика соціальних мереж. Аналіз відкритих джерел дозволяє оперативно виявляти настрої населення, визначати ефективність інформаційних кампаній та коригувати сценарії психологічного впливу в режимі реального часу.

Російсько-українська війна демонструє, що інформаційно-психологічні операції стали ключовим елементом багатодоменного протиборства. Їх ефективність визначається не окремими пропагандистськими повідомленнями, а здатністю інтегрувати психологічний вплив із кібероперациями, радіоелектронною боротьбою, застосуванням БПЛА та аналітичними технологіями. Сучасні ІПсО спрямовані на одночасне ураження технічної інфраструктури, інформаційного середовища та когнітивної сфери людини. Саме така синергія забезпечує досягнення інформаційного домінування та суттєво впливає на перебіг і результати воєнних дій.

Опанюк Ю. В., Ph. D.
Житомирський військовий інститут імені С. П. Корольова

# ІНТЕГРАЦІЯ МАТЕМАТИЧНИХ МОДЕЛЕЙ ДИФУЗІЇ ІННОВАЦІЙ У ПРОЦЕСИ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ

Сучасна парадигма ведення бойових дій визначає когнітивний простір як ключове середовище збройного протиборства, де стратегічна перевага досягається шляхом докорінної трансформації волі та поведінкових установок противника, а саме цільової аудиторії (ЦА). Незважаючи на це, на практиці процеси вимірювання та оцінювання ефективності (Measures of Effectiveness (MOE)) психологічних операцій (ПсО) здебільшого залишаються інтуїтивними та базуються на емпіричних спостереженнях, а не на точному прогнозуванні.

Сучасна маневрена війна вимагає відмови від прямолінійної стратегії виснаження на користь завдання ударів по критичних вразливостях противника для руйнування його центру тяжіння та порушення циклу прийняття рішень. Відсутність інтегрованого математичного апарату, який би пов'язував теорію поширення інформації з алгоритмами Troop Leading Procedures (TLP), створює суттєву прогалину, унеможливлюючи точну синхронізацію когнітивних ефектів із кінетичними ударами.

Для трансформації ПсО з емпіричної практики у високоточну когнітивно-технічну дисципліну пропонується застосування комплексної методології математичного моделювання, яка розглядає психологічний вплив як процес впровадження інновації у соціальну систему ЦА. Вирішення проблеми базується на концептуальних та математичних підходах.

Одним з них є застосування диференціальної моделі Басса для прогнозування хаосу, де пропонується використання диференціального рівняння Френка Басса для розрахунку динаміки когнітивного охоплення ворожої аудиторії. Модель враховує два ключові параметри: коефіцієнт інновації (потужність зовнішнього інформаційного тиску ПсО), та коефіцієнт імітації (інтенсивність соціального зараження (чуток) всередині підрозділу). Математичне обчислення дозволяє точно визначити точку перегину (момент досягнення максимальної швидкості поширення деструктивного наративу). Це дає змогу загальновійськовому командиру призначити час вирішальної кінетичної операції на піку деморалізації ЦА.

Також, досягнення «критичної маси» та економія сил, відповідно до теорії Е. Роджерса, пропонує змістити фокус із масового впливу на суцільну аудиторію до таргетування цільових сегментів «Новаторів» та «Ранніх адоптерів» (лідерів думок). Доведено, що інфікування 15–20% ЦА створює «критичну масу», після якої процес дифузії переходить у фазу автономної самопідтримки за рахунок внутрішньої комунікації ЦА. Це дозволяє реалізувати тактичний принцип економії сил та перенаправити технічні ресурси ПсО на інші напрямки.

Крім того доцільно використовувати епідеміологічну модель (Susceptible Infected Recovered (SIR)), яка враховує перехід індивідів у стан «імунізованих» через дію ворожої системи цензури та контрпропаганди. Головним завданням фахівців ПсО є забезпечення базового репродуктивного числа інфікування, що математично гарантує експоненціальний спалах «психологічної пандемії» до моменту, коли ворожа система command and control зможе ефективно відреагувати.

Таким чином інтеграція математичних моделей Басса та SIR у доктринальну методологію ПсО забезпечує перехід до вимірюваних та об'єктивних індикаторів оцінювання. Відстеження проксі-індикаторів у реальному часі дозволяє динамічно калібрувати силу впливу, долати когнітивний імунітет противника та забезпечувати вирішальну когнітивну перевагу в умовах сучасної маневреної війни. Перспективою подальших досліджень є автоматизація графового аналізу соціальних систем із залученням технологій штучного інтелекту.

Дідушко І. І.
Житомирський військовий інститут імені С. П. Корольова

## ОЦІНКА ЕФЕКТИВНОСТІ OSINT-ІНСТРУМЕНТІВ У ВЕРИФІКАЦІЇ ІНФОРМАЦІЇ ПІД ЧАС ЗБРОЙНОГО КОНФЛІКТУ ЗА ДОСВІДОМ ПОВНОМАСШТАБНОЇ ВІЙНИ В УКРАЇНІ

Сьогодні інформація дуже сильно впливає на людей, особливо під час війни. Більшість людей зараз дізнаються новини через Telegram, TikTok, Instagram або різні сайти. Через це інформація швидко розповсюджується та

сильно впливає на думку людей. Після початку повномасштабної війни в Україні новин стало набагато більше. Кожного дня в інтернеті з'являються нові фото, відео та повідомлення. Але проблема в тому, що разом із нормальною інформацією дуже часто поширюються фейки та неправдиві новини. Через це людям стало важче розуміти, де правда, а де просто обман.

Зараз для перевірки інформації часто використовують OSINT. Для цього використовують соціальні мережі, карти, новинні сайти, фото, відео та інші відкриті джерела. Саме через доступність OSINT став таким популярним під час війни, тому що ним можуть користуватись навіть звичайні люди.

Наприклад, коли в інтернеті з'являється якесь фото або відео, його можна спробувати перевірити. Люди звертають увагу на будинки, дороги, магазини, погоду або автомобілі на фото. Навіть маленькі деталі іноді допомагають зрозуміти, чи справжня ця інформація. Також часто одну й ту саму новину перевіряють через кілька різних джерел. Якщо інформація збігається, тоді більше шансів, що це правда. Але перевіряти інформацію зараз не так просто. Новин дуже багато, і вони постійно оновлюються. Через це люди інколи просто не встигають нормально все перевіряти. Крім цього, не всі знають, як правильно шукати або аналізувати інформацію. Через це багато хто може випадково повірити фейкам або поширити їх серед інших людей.

Ще одна проблема полягає в тому, що неправдиву інформацію часто поширюють спеціально. Наприклад, можуть брати старі фото чи відео та видавати їх за нові. Або спеціально змінювати матеріали, щоб люди повірили неправдивим новинам. У таких ситуаціях навіть хороші інструменти не завжди допомагають швидко знайти правду. Тому потрібно уважно ставитися до будь-якої інформації та перевіряти її хоча б у кількох місцях.

Також велику роль у поширенні фейків відіграють соціальні мережі. Дуже часто люди пересилають новини на емоціях і навіть не задумуються, правдива ця інформація чи ні. Через це фейки дуже швидко поширюються серед великої кількості людей. І навіть коли пізніше з'являється спростування, частина людей усе одно продовжує вірити неправдивим новинам.

OSINT зараз дійсно допомагає знаходити правдиву інформацію. Його використовують журналісти, волонтери, аналітики та просто люди, які хочуть краще розуміти, що відбувається. У багатьох випадках саме завдяки OSINT вдавалося знайти фейки або підтвердити важливу інформацію.

Отже, сьогодні OSINT є дуже корисним способом перевірки інформації під час війни. Він допомагає людям менше вірити фейкам і краще розуміти події. Але багато залежить і від самих людей. Потрібно уважніше ставитися до новин та не поширювати інформацію одразу, якщо немає впевненості, що вона правдива.

Бабінов Я. Д.
Житомирський військовий інститут імені С. П. Корольова

## ПСИХОЛОГІЧНИЙ ВПЛИВ ТА ПРОТИДІЯ ЙОМУ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

У сучасних умовах поняття “війна” і способи її ведення значно змінилися. Тепер замість традиційних методів застосовують гібридну війну в асиметричних конфліктах, де психологічні операції перестали бути просто допоміжним засобом і перетворилися на самостійну форму ураження супротивника як в бойових умовах так і цивільних.

З теоретичного погляду важливо зрозуміти, що таке психологічний вплив і яка його мета на полі бою. В основі цих операцій лежить не звична лінійна модель комунікації Лассвела, а складніша нелінійна модель «рефлексивного управління». У ній об’єкт впливу втрачає власну ініціативу через нав’язані алгоритми, наративи і тиск на процес прийняття рішень.

Для розуміння практичної сторони психологічного овпливу корисно проаналізувати хід російсько-української війни. Можна виділити п’ять основних стратегій, які використовує агресор: по-перше, прив’язування вигаданих наративів до реальних резонансних подій; по-друге, заміна значень слів, наприклад, підміна слова «зрада» на «багатовекторність»; по-третє, руйнування цілісності інформаційного простору через кліпове мислення; по-четверте, застосування deep-fake та синтетичних особистостей для створення фейків; нарешті, використання соціальних мереж для масового підірвання довіри із застосуванням алгоритмів колаборативної фільтрації.

Для ефективної протидії таким методам потрібна практична реалізація заходів та підвищення рівня освіти в українському суспільстві. Цей процес повинен перейти від простої медіаграмотності до активної когнітивної безпеки.

Запропоновано концепцію «смислової інокуляції» - метод формування психологічного «імунітету» проти маніпуляцій, фейкових новин та дезінформації. Це досягається шляхом попереднього знайомства людей зі спрощеними або спотвореними варіантами хибних аргументів.

На організаційному рівні важливо впроваджувати системи раннього виявлення інформаційних загроз, орієнтуючись на лінгвістичні маркери і прояви девіантної комунікації, які включають підвищену експресивність, спрощення граматики та різку поляризацію оцінок «свій-чужий».

Отже, теоретичний аналіз психологічного впливу в російсько-українській війні демонструє, що основним полем бою є людська психіка і колективне несвідоме. Вплив здійснюється як безпосередньо на фронті, так і поза його межами. Сучасні реалії свідчать про те, що асиметричні заходи, спрямовані не на боротьбу з кожним окремим деструктивним повідомленням, а на формування стійких світоглядних орієнтирів, можуть бути набагато ефективнішими для захисту від психологічного впливу.

Буткевич Д. Д.
Збройні Сили України

## ПРОВЕДЕННЯ ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ У СУЧАСНИХ БОЙОВИХ ДІЯХ

Сучасні умови ведення бойових дій характеризуються не лише застосуванням військової сили, але й активним використанням психологічного впливу (далі - ПсВ) на противника. Психологічні операції (далі - ПсО) стали однією зі складових ведення бойових дій, оскільки вони впливають на прийняття рішень військовослужбовцями противника на полі бою та зменшують рівень їхньої мотивації до виконання подальших завдань.

Основною метою ПсВ є зміна поведінки та емоційного стану цільової аудиторії (далі - ЦА), на яку здійснюється вплив. Зазвичай, всі проведені дії спрямовані на створення панічних настроїв серед особового складу противника, його деморалізацію та зниження довіри ворожих військовослужбовців до командування тощо.

Найефективніше здійснювати вплив на ЦА, яка перебуває в програшній ситуації, тобто перебуває на ділянці фронту, де противник не має успіху, відступає

або перебуває в оточені. В таких випадках людина має найнижчий рівень мотивації та перебуває у стресі, і через свій страх стає більш вразливою до ПсВ.

З початку повномасштабного вторгнення рф в Україну, у ЗСУ в рази збільшили застосування ПсО у фізичному вимірі на різних ділянках фронту, при цьому їхній характер та інтенсивність залежать від особливостей ведення бойових дій на конкретній ділянці фронту. Основними засобами для проведення психологічних дій є використання гучномовців, радіотрансляторів, безпілотних літальних апаратів (далі - БпЛА) із засобами агітації, а також проведення демонстративних дій. Ці засоби абсолютно різні за використанням та способом донесення інформації. Тобто існують інструменти для поширення інформації за допомогою звуку, радіомовлення, графіки та тексту (наприклад, за допомогою листівок).

В залежності від поставленого завдання потрібно враховувати ряд умов: як саме буде доноситись інформація до ЦА, стан противника на цій ділянці фронту, характер місцевості та інші фактори. Це допоможе створити матеріали ПсВ, які будуть мати максимальну ефективність.

Оскільки технології на полі бою розвиваються стрімко, при виконанні завдань не можна нехтувати безпековою ситуацією, що вимагає додаткового планування. Наприклад, через розвиток засобів ураження на базі FPV-дронів зона ураження постійно зростає і на окремих ділянках фронту може становити до 50 км. Засоби ПсВ враховують ці реалії й також удосконалюються – вже є низка нових розробок, які ефективно себе зарекомендували на полі бою. Вони компактніші, мобільніші та подекуди мають кращі технічні характеристики. Особливістю деяких нових вітчизняних засобів є те, що вони не були зроблені до початку повномасштабного вторгнення та розраховані для певних завдань, а розроблені спеціально для конкретних умов і є в рази дешевшими, ніж іноземні розробки, що дозволяє масштабувати їх виготовлення.

Приклади еволюції деяких засобів:

- великі звукомовні станції замінили на менші, встановлені на БпЛА. Хоча ці пристрої мають менший радіус дії, але вони дають змогу здійснювати звукомовлення більш точково за рахунок наближення до противника;
- для збільшення відстані радіомовлення використовуються радіотранслятори збільшеної потужності;
- залистування за допомогою дефіцитних та менш точних агітаційних снарядів замінили застосуванням БпЛА різних типів, що збільшує точність поширення матеріалів ПсВ.

Практичний досвід показує, що для досягнення максимальних результатів ПсВ необхідно налаштувати чітку координацію між військовими підрозділами в зоні проведення операції та застосовувати всі наявні засоби, які будуть взаємодоповнювати один одного. Для підвищення ефекту ПсВ рекомендується поєднати фізичне та інформаційне середовища, кінетичний та некінетичний вплив, що створює додатковий психологічний тиск на ЦА.

Отже, для успішного проведення ПсО в майбутньому рекомендується постійний моніторинг та переймання передового досвіду для розробки нових або вдосконалення наявних засобів ПсВ під актуальні умови на полі бою.

Краснокутський І. В.
Житомирський військовий інститут імені С. П. Корольова

## СУЧАСНІ ТЕХНОЛОГІЇ ПСИХОЛОГІЧНОГО ВПЛИВУ

У сучасних гібридних конфліктах психологічний вплив став ключовим інструментом для досягнення воєнно-політичних цілей. Людська свідомість виступає головним полем бою, а сучасні технології дають змогу здійснювати точний, масштабний і практично непомітний вплив на поведінку окремих людей, груп і цілих суспільств. Ця тема особливо актуальна через активне використання таких технологій у російсько-українській війні, де психологічні операції поряд із традиційними бойовими діями набувають великого значення.

Основою сучасних методів психологічного впливу є поєднання психології, нейронаук, штучного інтелекту й цифрових платформ. Вони не просто поширюють інформацію - вони допомагають формувати сприйняття, емоції та процеси прийняття рішень. Особливу увагу приділяють когнітивній війні, що розглядає людський розум як нове поле бойових дій. Успішний вплив вимагає комплексного застосування технологій, психологічних знань і стратегічного планування. До сучасних технологій психологічного впливу належать: генеративний штучний інтелект і синтетичні медіа - це створення deepfake-відео, клонів голосу та персоналізованого контенту, що швидко адаптується під психографічні характеристики аудиторії для посилення довіри до певних наративів; мікротаргетинг і психографічне профілювання - використання великих даних для аналізу особистісних рис і вразливостей, що

дозволяє доставляти індивідуальні повідомлення через соцмережі й підвищувати ефективність впливу; рефлексивне управління - метод, коли інформація подається так, щоб об'єкт впливу сам приймав потрібні для впливця рішення. Цей підхід часто застосовують для маніпуляції противником та сприяння бажаним діям; алгоритмічне керування увагою - використання алгоритмів платформ, щоб створювати інформаційні бульбашки та поширювати контент, який викликає страх, гнів, апатію або ейфорію; наративне інженерство - цілеспрямоване створення й просування стратегічних наративів, які поступово змінюють світогляд аудиторії. Поєднання повторень, емоційної насиченості та зв'язку з реальними подіями підвищує їхню впливовість. У сучасних конфліктах такі технології застосовують для деморалізації, посилення розколу, дискредитації лідерів і ослаблення міжнародної підтримки, з мінімальними ресурсними витратами. Для успіху потрібне ретельне планування, координація з бойовими діями і постійний моніторинг реакцій аудиторії. Серед викликів - необхідність швидко реагувати та адаптуватися до змін у інформаційному середовищі, ризик розкриття операцій із можливими негативними наслідками, потреба у фахівцях з психології, аналізу даних і комунікацій, а також етичні й правові обмеження в демократичних країнах.

Застосування сучасних технологій психологічного впливу значно розширює можливості гібридної війни й надає психологічним операціям роль окремого інструменту для реалізації стратегічних завдань. Для їхнього ефективного використання потрібен системний підхід, поєднання наукових досягнень із технологічними можливостями. Перспективними напрямками є поглиблене інтегрування штучного інтелекту з психологічними моделями, створення спеціалізованих сил для когнітивних операцій і вдосконалення стратегічного планування комунікацій. Майстерність у цій сфері дедалі важливіша для захисту національних інтересів у сучасному світі.

Скиба І. П., Остапчук М. В.
Житомирський військовий інститут імені С. П. Корольова

# ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АВТОМАТИЗАЦІЇ РОЗРОБКИ МАТЕРІАЛІВ ПСИХОЛОГІЧНОГО ВПЛИВУ

Сучасна збройна боротьба виходить далеко за межі фізичного протистояння на полі бою. В умовах гібридної війни, в якій Україна протистоїть російській федерації з 2014 року та особливо з 24 лютого 2022 року, інформаційний простір набув стратегічного значення. Психологічні операції (ПсО) перетворилися на один із ключових інструментів досягнення оперативних і стратегічних цілей – впливу на свідомість, волю та поведінку противника та нейтральних груп.

Водночас стрімкого розвитку набули й технології штучного інтелекту (ШІ). Генеративні моделі, здатні створювати тексти, зображення, аудіо та відео, кардинально змінили технологічний прорив у створені контенту. Ці зміни безпосередньо стосуються і психологічних операцій: ШІ-інструменти дозволяють розробляти матеріали психологічного впливу (ПсВ) значно швидше, дешевше та з можливістю масштабування, недосяжного для традиційних виробничих процесів.

В умовах повномасштабного вторгнення та активної пропаганди противника підрозділи ПсО зіткнулися з необхідністю масштабувати вплив в інформаційному просторі, маючи обмежений час та людські ресурси.

Ефективність ПсО безпосередньо залежить від якості, оперативності та масштабу виробництва відповідних матеріалів впливу. Якість та ефективність матеріалів психологічного впливу (ПсВ) визначають здатність формувати настрої та поведінку цільових аудиторій (ЦА) противника та нейтральних груп.

Досвід збройного конфлікту з росією показав, що ефективність ПсО певною мірою залежить і від безпосереднього домінування в інформаційному просторі. А з розвитком ШІ проблему домінування в інформаційному просторі можна уникнути, адже технологічні потужності ШІ-системи можуть значно підвищити ефективність та масштабність ПсО, дозволяючи швидше та точніше впливати на ЦА. Це може бути особливо корисним у віртуальному просторі, де швидкість реакції та розповсюдження інформації має критичне значення.

Для систематизації ШІ-інструментів, які варто використовувати в ПсО, доцільно провести їх класифікацію за кількома критеріями.

За типом контенту виокремлюють чотири основні групи:

великі мовні моделі (LLM) для генерації текстового контенту (GPT, Claude, Gemini);

дифузійні моделі та генеративно-змагальні мережі (GAN) — для генерації зображень (Stable Diffusion, DALL-E, Midjourney);

моделі синтезу голосу та клонування (TTS, Voice Cloning) — ElevenLabs, XTTS;

відеогенеративні системи (Sora, Runway, Kling, тощо).

За режимом доступу інструменти поділяються на хмарні сервіси з API-доступом, відкриті моделі з можливістю локального розгортання та гібридні рішення. Для потреб підрозділів ПсО особливої ваги набуває можливість локального розгортання з міркувань оперативної безпеки та незалежності від зовнішніх постачальників, що потребує відповідного фінансування, обладнання та фахівців.

Таким чином, застосування технологій ШІ для автоматизації розробки матеріалів ПсВ є актуальним і практично значущим напрямком розвитку спроможностей підрозділів ПсО. ШІ виступає ефективним допоміжним засобом, здатним суттєво підвищити ефективність і результативність ПсО. Завдяки можливості автоматизувати рутинні завдання, генерувати якісний та реалістичний контент, а також масштабувати матеріали, він стає важливим інструментом у сучасній інформаційній боротьбі.

Срібний О. М.
Коваль Д. В., канд. техн. наук
Бондарчук А. А.
Житомирський військовий інститут імені С. П. Корольова

## КОНЦЕПТ АВТОНОМНОГО IOT-ВУЗЛА ЛОКАЛЬНОГО OSINT-МОНІТОРИНГУ ДЛЯ ПІДТРИМКИ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ

Сучасні інформаційно-психологічні операції (PSYOPS) значною мірою залежать від швидкості отримання інформації про зміни інформаційного середовища, появу деструктивних наративів та реакцію аудиторії на

інформаційні події. Перспективним напрямом розвитку систем інформаційного моніторингу є використання автономних IoT-вузлів, здатних здійснювати локальний збір цифрових та радіотехнічних ознак із подальшою передачею агрегованої інформації до центрального аналітичного центру.

У роботі запропоновано концепт автономного IoT-вузла локального OSINT-моніторингу, призначеного для розгортання у районах підвищеної інформаційної активності. Запропонований підхід передбачає використання компактних периферійних вузлів як локальних сенсорів інформаційного середовища. Концепт є перспективною архітектурою автономного засобу збору та попередньої обробки інформаційних ознак.

Апаратною основою вузла може виступати одноплатний комп'ютер із додатковими модулями радіо- та мережевого моніторингу. До складу вузла потенційно можуть входити SDR-приймач, зовнішній Wi-Fi-адаптер із підтримкою "monitor mode", модем мобільного зв'язку 4G/LTE, GPS-модуль, акумуляторна батарея та система автономного живлення. Конструктивно вузол може бути реалізований у вигляді компактного герметичного контейнера з можливістю прихованого або тимчасового розгортання у транспортному засобі, на будівлі, поблизу транспортних вузлів або у польових умовах.

Основною задачею вузла є локальний збір інформаційних ознак у межах окремого об'єкта або району спостереження. Під час роботи вузол потенційно може здійснювати пасивний моніторинг Wi-Fi-середовища, фіксуючи SSID мереж, MAC-адреси точок доступу та динаміку появи нових пристроїв. Реалістичний радіус такого моніторингу становить від десятків метрів у щільній забудові до кількох сотень метрів за сприятливих умов та використання зовнішніх антен. Додатково SDR-модуль дозволяє здійснювати моніторинг визначених діапазонів радіочастот та фіксувати аномальну активність у радіоефірі. Залежно від частотного діапазону та типу антени можливий прийом відкритих сигналів на відстанях від кількох до десятків кілометрів.

Паралельно через мобільне підключення до мережі Інтернет вузол може здійснювати автоматизований моніторинг відкритих Telegram-каналів, локальних веб-ресурсів та соціальних платформ. На локальному рівні виконується базова фільтрація контенту, підрахунок частоти використання визначених ключових слів та виявлення різких змін інформаційної активності. У випадку перевищення встановлених порогових значень формується подія інформаційної аномалії. Передача інформації до центрального сервера може

здійснюватися через VPN-тунелі або захищені HTTPS/MQTT-канали. При втраті зв’язку вузол потенційно здатний автономно накопичувати інформацію у локальному сховищі та передавати її після відновлення каналу.

Одним із можливих сценаріїв застосування концепту є моніторинг інформаційної ситуації у районі транспортного вузла або прикордонного населеного пункту. У випадку одночасного зростання кількості панічних повідомлень у локальних Telegram-каналах, появи нових Wi-Fi-мереж та аномального збільшення активності мобільних пристроїв система може формувати ознаки потенційної інформаційно-психологічної кампанії або кризової події. Агреговані результати передаються до центрального аналітичного центру, де із використанням AI-сервісів виконується семантичний аналіз інформації та формуються OSINT-зведення.

Запропонований концепт не є засобом радіотехнічної розвідки у класичному розумінні та не призначений для перехоплення захищених каналів зв’язку. Вузол орієнтований виключно на аналіз відкритих або технічно доступних інформаційних ознак, зокрема OSINT, SOCMINT та RF-індикаторів активності.

Таким чином, запропонований концепт автономного IoT-вузла може використовуватись підрозділами інформаційної боротьби як засіб локального OSINT-моніторингу та виявлення інформаційних аномалій у визначених районах спостереження. Подальший розвиток концепту може бути пов’язаний із інтеграцією AI-сервісів для автоматичного аналізу даних та масштабуванням системи шляхом побудови мережі взаємодіючих IoT-вузлів.

Фриз В. П., канд. техн. наук, доц.
Житомирський військовий інститут імені С. П. Корольова

## МОДЕРНІЗАЦІЯ FM-ПЕРЕДАВАЧА RIAB ЗА РАХУНОК РОЗРОБКИ СПРЯМОВАНОЇ ПЕРЕДАВАЛЬНОЇ АНТЕНИ

У сучасній російсько-українській війні досягнення успіху на полі бою визначається не лише ефективністю вогневого ураження противника, але й здатністю впливати на поведінку його особового складу. Психологічні операції (ПсО) стали невід’ємною складовою комплексного застосування сил і засобів,

спрямованих на зниження боєздатності, деморалізацію особового складу противника та руйнування його мотивації до продовження збройної боротьби.

Особливістю нинішнього етапу війни є поєднання цифрових каналів впливу на противника (соціальних мереж, месенджерів) і з класичними засобами комунікації (листівками, радіомовлення) яке зберігає високу ефективність, особливо в умовах обмеженого доступу до Інтернету.

Умови ведення психологічних операцій в районах виконання завдань потребують мобільних засобів радіомовлення, здатних забезпечувати оперативне та таргетоване поширення інформації на противника. Одним із ключових засобів у підрозділах ПсО є тактичні мобільні FM-передавачі типу RIAB (Radio in a Box), що дозволяють швидко розгортати радіомовлення в районах виконання бойових завдань для впливу на противника.

Штатна антена комплексу RIAB має кругову діаграму спрямованості, що призводить до неефективного розподілу енергії випромінювання та обмежує можливість таргетованого впливу на визначену аудиторію. У зв'язку з цим актуальним є завдання модернізації комплексу шляхом застосування спрямованої передавальної антени FM-діапазону.

Метою дослідження є вибір конструкції, розрахунок та моделювання спрямованої антени для модернізації тактичного FM-передавача RIAB.

Під час роботи були визначені основні вимоги до антени: робочий діапазон частот 87,5–108 МГц, коефіцієнт стоячої хвилі не більше 1,5, хвильовий опір 50 Ом, коефіцієнт підсилення 5–8 дБ, ширина діаграми спрямованості 30–40°, а також забезпечення мобільності та простоти розгортання в польових умовах.

На основі аналізу сучасних конструкцій антен FM-діапазону встановлено, що найбільш доцільним рішенням є використання системи з двох двоелементних дипольних антен, фазовано об'єднаних на спільній траверсі. Така конструкція забезпечує необхідну спрямованість за відносно невеликих габаритів та маси.

Для середньої частоти 100 МГц було виконано розрахунок геометричних та електричних параметрів антени. Подальше моделювання проведено в середовищі MMANA-GAL, що дало змогу оптимізувати довжини елементів, міжелементні відстані та врахувати вплив металевої щогли й конструктивних елементів на характеристики антени.

За результатами моделювання встановлено, що антена забезпечує коефіцієнт підсилення до 7,5 дБ та ширину діаграми спрямованості близько ±30–35°. Для виготовлення дослідного зразка використано алюмінієві трубки та дюралюмінієву траверсу, що забезпечило малу масу конструкції та достатню механічну міцність.

Експериментальні вимірювання, виконані із застосуванням аналізатора антенно-фідерних систем RigExpert, підтвердили резонансний режим роботи антени та високий рівень узгодження з фідером. Коефіцієнт стоячої хвилі в робочому діапазоні не перевищував 1,4:1, а реактивна складова вхідного опору була практично нульовою.

Результати випробувань у бойових умовах показали забезпечення стійкого радіоприймання на відстані до 35–40 км за потужності передавача 600 Вт. Це підтверджує ефективність запропонованої антенної системи для підвищення дальності впевненого приймання та реалізації таргетованого психологічного впливу на особовий склад противника.

Отже, розроблена спрямована антена є перспективним рішенням для модернізації мобільних FM-комплексів RIAB та може бути рекомендована до практичного впровадження у підрозділах ПсО.

Будз В. П., канд. філос. наук, доц.
Костиря С. В., канд. техн. наук
Шумлянський С. В., канд. політ. наук
Науково-дослідний центр Державної спеціальної служби транспорту

## КОГНІТИВНО-ПСИХОЛОГІЧНІ НАСЛІДКИ ІНФОРМАЦІЙНИХ ТА ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ ВОРОГА В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

На перший погляд причини російсько-української війни видаються політичними та економічними, які нібито зумовлені у першу чергу геополітичним баченням місця і ролі держав у світі та відповідно стратегічними планами розвитку суспільств. Проте, на нашу думку, справжні причини російсько-української війни, як і в більшості екзистенційних війн, мають культурно-історичні та світоглядно-ментальні основи: наприклад, російсько-

українська війна найвірогідніше не почалась би, якщо б, світогляд росіян не мав би імперських амбіцій, а світогляд та ментальність деякої частини українців не містили б ностальгії за СРСР, проросійських культурних уподобань (мова і церква) та були б проукраїнськими за своїм аксіологічним змістом.

Культурно-історичні та світоглядно-ментальні основи суттєво впливають на особливості когнітивного сприйняття дійсності, визначають мотивацію людської діяльності, орієнтують на її аксіологічний зріз. При цьому оцінювання дійсності, мотивація діяльності та постановка її цілей в аксіологічному вимірі відбувається через когнітивно-психологічні засади сприйняття дійсності, зокрема через ідеї, смисли, емоції та почуття. Ці когнітивно-психологічні засади є надзвичайно динамічними, а відповідно можуть піддаватися розмаїтим інформаційним та психологічним маніпуляціям та інспіраціям ворога на основі ведення ним інформаційно-психологічних операцій проти України.

У першу чергу росіяни, проводячи інформаційні та психологічні операції проти українців, намагаються дискредитувати українську владу в очах світової громадськості з метою викликати когнітивно-психологічний дисонанс на основі розчарування та недовіри до дій української влади, наприклад, до методів ведення мобілізації. Основна мета інформаційних та психологічних операцій росіян проти України – це вплинути на когнітивно-психологічне сприйняття дійсності на основі продукування у свідомості українців недовіри до влади, невпевненості у майбутньому, посіяти паніку, страх і хаос, що безумовно впиває на неадекватне сприйняття дійсності та помилкове прийняття рішень. У цілому, загальна мета росіян при проведенні інформаційних та психологічних операцій проти українців – це психологічна нестабільність українського суспільства, сподівання на зростання суспільного незадоволення українського населення, а на цій основі – ініціювання протестів проти української влади, оскільки українці схильні до демократичного волевиявлення та супротиву владі, про що свідчать результати Помаранчевої революції та Революції гідності.

Будь-яка загрозлива інформація, яка місить наративи і дискурс небезпеки є важливим фактором маніпулювання масовою свідомістю, що впливає, наприклад, на економічну (заощадливість), політичну (пасивність) та навіть демографічну поведінку населення – народжуваність, міграція та смертність. Зокрема смертність українського населення зростає на тлі постійної інформаційної небезпеки, яка впливає на зростання серцево-судинних хвороб.

Загрозлива інформація може бути неправдивою, тільки віртуальним інформаційним приводом, але вона здатна викликати реальні почуття та емоції, які впливають на здоров'я та на поведінку населення, а також на дії соціальних інститутів та урядів інших держав. Росіяни у процесі проведення інформаційних та психологічних операцій намагаються діяти, наприклад, на основі ідей «ядерного шантажу», загрози «наступу з Білорусі» на Україну чи країни НАТО, а це безперечно впливає на згортання політичної підтримки України, оскільки держави НАТО намагаються акумулювати військові ресурси та починають діяти обачніше на тлі можливої «ядерної загрози» та загрози наземного вторгнення росіян. Крім того росіяни у своїх інформаційних операціях намагаються мілітаризувати власне суспільство та виправдати нібито превентивність повномасштабної війни проти України у масовій свідомості росіян. Також є намагання створити образ росіян як непередбачуваних у світовій політиці, що робить імовірним будь-який сценарій, з яким потрібно рахуватись, а це розширює сферу інформаційно-психологічної війни.

Загалом, росіяни у своїх інформаційних та психологічних операціях активно застосовують когнітивно-психологічні фактори блефу, страху, терору та небезпеки, які суттєво коригують військову тактику і стратегію українців та країн-партнерів України. Тільки ідея «загрози вторгнення з Білорусі» впливає на дії української влади – відтягування та перерозподіл військових резервів та ресурсів, а також на військову логістику сил оборони України в цілому. На цій основі українці мають розробляти та проводити власні інформаційно-психологічні операції з метою послаблення ворога та дестабілізації росії.

Nosova H. D.
Zhovnovatiuk R. M., Cand. Sc. (Tech.), Senior Research Ass.
Korolov Zhytomyr Military Institute

## COUNTERING INFORMATION INFLUENCE USING SOCIAL ENGINEERING TECHNIQUES

Against the backdrop of large-scale armed aggression by the Russian Federation against Ukraine, the development of methods, forms, and means used by the enemy to shape information influence – targeted both at the civilian population of

the occupied and controlled regions of our state and at the command and personnel of our armed forces – is constantly growing. At the same time, social media has traditionally served as a distinct "battlefield."

Virtual communities, as a distinct phenomenon shaped by social media, have become a fundamentally new, stable form of social relations that surpass social groups in society in terms of organization and influence. At the same time, such formations are quite vulnerable to informational influences, a fact the enemy actively exploits by employing methods of social engineering in the creation of informational messages with a destructive impact.

The use of informational messages, the creation of which is based on methods of social engineering, is considered the most effective. Its advantage lies in the fact that a destructive influence will almost always be successful if, following timely and thorough monitoring of open-source information, the adversary is able to craft the message in such a way as to capture the target's interest and compel them to take actions beneficial to the enemy by imposing a new behavioral model on the target.

Information influence on social media using social engineering methods in today's digital society is one of the most popular avenues for developing destructive influence, given its ease of implementation, low financial investment, and minimal risk of detection and counteraction. Its use enables the adversary to achieve nearly 100% effectiveness.

The method of monitoring virtual communities, which primarily include social networks, is more effective in the long term for information countermeasures, although it requires the involvement of specialists from various scientific fields.

Резуненко Д. О.
Кузьмичев А. В.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

## ІНЖЕНЕРНЕ ЗАБЕЗПЕЧЕННЯ ПІД ВОГНЕМ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ ПРОТИВНИКА

Сучасна війна в Україні ведеться не лише за території чи вогневу перевагу, а й за психологічну стійкість військовослужбовця, його здатність приймати рішення в умовах постійного інформаційного тиску, дезінформації та

когнітивного виснаження. У цих умовах особливого значення набуває діяльність підрозділів інженерних військ, які щоденно виконують завдання в районах бойового зіткнення, залишаючись однією з пріоритетних цілей противника. Досвід бойових дій показує, що противник активно поєднує застосування артилерії, FPV-дронів, дистанційного мінування та аеророзвідки із потужним інформаційно-психологічним впливом. Особливо це проявляється під час виконання завдань з обладнання фортифікаційних рубежів, евакуації техніки, наведення переправ та проведення інженерної розвідки. Противник активно використовує: соціальні мережі, телеграм-канали, відеоматеріали з БПЛА та маніпулятивний інформаційний контент для деморалізації українських військовослужбовців. Особливо небезпечними є інформаційні вкиди щодо нібито «марності» фортифікаційних робіт, перебільшення втрат або навмисне поширення панічних настроїв після ударів по позиціях. В умовах масового застосування FPV-дронів та засобів повітряної розвідки військовослужбовці інженерних підрозділів фактично працюють у режимі безперервного психологічного виснаження. Військовослужбовці інженерних військ повинненні бути не лише технічними спеціалістами, а й психологічно стійкими фах, здатними діяти в умовах інформаційного хаосу та постійного стресу.

Показовим прикладом є виконання інженерних робіт поблизу лінії бойового зіткнення, коли після виявлення інженерної техніки противник одночасно застосовує FPV-дрони, артилерію та інформаційний вплив через Інтернет. У таких умовах навіть короткі відео з ураженням техніки противник миттєво поширює в інформаційному просторі для створення психологічного ефекту та деморалізації особового складу. Тактична ситуація часто суттєво відрізняється від тієї, яку навмисно демонструють інформаційні ресурси противника. Одним із ключових елементів стійкості підрозділу залишається професійне лідерство командира та рівень підготовки особового складу. Саме внутрішня довіра в колективі, постійна комунікація, чітке розуміння завдань та впевненість у діях командира значно знижують ефективність інформаційно-психологічного впливу противника. У сучасних умовах командир інженерного підрозділу повинен не лише організовувати виконання інженерного забезпечення, а й підтримувати морально-психологічну стійкість особового складу після обстрілів, ударів БПЛА та тривалого перебування у зоні бойового зіткнення. Особливу увагу необхідно приділяти підготовці військовослужбовців до дій в умовах інформаційного перевантаження, дефіциту часу та психологічного тиску.

Важливим аспектом підготовки є формування навичок інформаційної гігієни та критичного мислення. Військовослужбовець повинен вміти швидко перевіряти інформацію, розпізнавати дезінформацію та не допускати поширення панічних настроїв у підрозділі. Війна підтвердила, що інформаційний простір став окремим полем бою, а інформаційно-психологічні операції — одним із найбільш небезпечних інструментів впливу на бойову ефективність військ. Саме поєднання бойового досвіду, сучасних технологій, професійного лідерства та готовності діяти в умовах постійного інформаційного впливу є ключовою умовою ефективного функціонування підрозділів Сил підтримки Збройних Сил України.

Солодка О. М., канд. юрид. наук, ст. наук. співроб.
Національна академія Служби безпеки України

## ХАРАКТЕРНІ ОСОБЛИВОСТІ FIMI НА СУЧАСНОМУ ЕТАПІ

На сучасному етапі мета іноземних інформаційних маніпуляцій та втручання в інформаційний простір (FIMI) полягає у системному управлінні інформаційним середовищем через нав'язування потрібних інтерпретацій, посилення соціальної поляризації, дискредитацію державних інституцій, деморалізацію суспільства тощо. Для України ця проблема має особливе значення, оскільки FIMI є складовою російської інформаційної агресії і спрямоване не лише на внутрішню українську аудиторію, а й на міжнародне середовище з метою дискредитації України, зниження підтримки з боку партнерів, поширення антиукраїнських наративів, делегітимацію української державності та виправдання власне агресії рф. У цьому контексті FIMI виступає не допоміжним, а стратегічним інструментом, на що вказує низка характерних особливостей.

Першою особливістю є *мережевий характер впливу*. Інформаційні операції FIMI дедалі частіше здійснюються не одним джерелом, а сукупністю взаємопов'язаних каналів: офіційних представників, псевдомедіа, Telegram-каналів, акаунтів у соціальних мережах, блогерів, інфлюенсерів, бот-мереж і сайтів-клонів.

Другою особливістю є *інфраструктурність FIMI*. Сучасне інформаційне втручання спирається не лише на контент, а й на технічну та організаційну

інфраструктуру: домени, рекламні сервіси, платформи поширення, алгоритмічне підсилення, мережі фейкових акаунтів, проксі-медіа та фінансові або політичні зв'язки між учасниками операцій. Інфраструктура FIMI розроблена для того, щоб поширювати свій вплив через різноманітні цифрові медіа, коригуючи свої техніки під кожен конкретний простір.

Третьою особливістю є *поєднання онлайн та офлайн простору*. FIMI, як частина гібридної стратегії, пов'язана з діяльністю, яка відбувається як в офлайн, так і кіберпросторі.

Четвертою рисою є *комбінація відкритого й прихованого впливу*. Акторами FIMI можуть бути як державні, так і недержавні суб'єкти, включно з їхніми проксі як усередині держави, так і за її межами. Держави залишаються ключовими суб'єктами загрози у сфері FIMI. Наприклад, російські FIMI-операції реалізуються через дипломатичні мережі, спецслужби, державні медіа, соціальні платформи, приватні компанії та місцевих проксі, які взаємно підсилюють одне одного.

П'ятою особливістю є *технологізація маніпулятивного впливу*. Використання штучного інтелекту, генеративних моделей, deepfake-технологій, автоматизованого перекладу, синтетичних зображень і масового створення контенту значно знижує вартість інформаційної операції.

Шостою особливістю є *орієнтація на суспільні вразливості*. Сучасні FIMI-кампанії здебільшого використовують уже наявні лінії суспільного розколу: недовіру до влади, втому від війни, соціально-економічну нерівність, мовні, етнічні, релігійні, політичні або регіональні суперечності. Мета полягає у тому, щоб посилити внутрішню напругу, радикалізувати дискусії та зробити суспільство менш здатним до спільної реакції на загрози.

Сьомою особливістю є *втручання у демократичні процеси*. Атаки на виборчі процеси залишаються постійною загрозою, що потребує безперервного моніторингу, аналізу та протидії. Окрім цього, зазначене свідчить про те, що інформаційні маніпуляції виходять далеко за межі інформаційного простору і впливають на усі без винятку сфери.

Отже, сучасний етап розвитку FIMI характеризується переходом до складних, багаторівневих і технологічно підсилених операцій інформаційного впливу, небезпека яких у тому, що вони діють не лише на рівні фактів, а й на рівні довіри, емоцій, ідентичності та здатності суспільства до колективного спротиву. Актори загроз використовують FIMI не як ситуативну можливість для

втручання, а як системний інструмент реалізації зовнішньополітичних інтересів. У такому контексті дезінформація та інформаційні маніпуляції здатні чинити суттєвий вплив на національну та міжнародну безпеку, що обумовлює необхідність застосування комплексних, скоординованих і пропорційних заходів реагування. Ефективна протидія FIMI потребує не лише фактчекінгу, а й системного підходу: стратегічних комунікацій, кіберзахисту, міжнародної координації, правових механізмів, прозорості цифрових платформ і формування інформаційної стійкості держави. Якщо раніше основний акцент робився на спростуванні фейків, то нині досвід ЄС свідчить про поступовий перехід до комплексної моделі: виявлення мереж, атрибуції, викриття інфраструктури, санкційного тиску, дипломатичних заходів, підвищення медіаграмотності, захисту виборів і зміцнення суспільної стійкості, що передбачає зміщення акцентів від реактивної до превентивної моделі протидії.

Гавриш І. Я.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

## РОСІЙСЬКІ ІНФОРМАЦІЙНІ ЗАГРОЗИ ПОЛЬСЬКО-УКРАЇНСЬКОМУ ПАРТНЕРСТВУ В УМОВАХ ПОВНОМАСШТАБНОЇ ВІЙНИ

Польсько-українське партнерство після 24 лютого 2022 р. стало одним із ключових чинників стійкості України у протидії російській агресії. Польща виконала одразу кілька функцій: стала одним із важливих постачальників військової допомоги, головним логістичним коридором для західної підтримки України, майданчиком для прийому українських біженців та одним із найактивніших адвокатів українських інтересів у ЄС і НАТО. Саме тому польсько-українські відносини перетворилися для російської федерації на окремий об'єкт інформаційно-психологічного впливу.

Головна мета російських інформаційних операцій на польському напрямі полягає не лише у дискредитації України, а й у підриві довіри між українським і польським суспільствами. Для цього москва використовує реальні проблемні теми: зернову кризу, блокування кордону, конкуренцію на ринку праці, питання українських біженців, історичну пам'ять і Волинську трагедію. Російська

пропаганда не створює ці суперечності з нуля, але намагається радикалізувати їх, подати як доказ «неминучого розриву» між Києвом і Варшавою та сформувати у польському суспільстві образ України як економічного конкурента і політичного тягаря.

Одним із найпоширеніших наративів є твердження про нібито «втому Польщі від України» та перевагу українських біженців над польськими громадянами у доступі до соціальної допомоги. За даними спеціалізованих моніторингів, дискредитація українських біженців була одним із головних напрямів російської інформаційної кампанії у Польщі після початку повномасштабного вторгнення. Поширювалися повідомлення про «привілейоване становище» українців, їхню нібито криміналізацію, небажання працювати або загрозу для польської ідентичності. Такі меседжі були спрямовані на поступове перетворення співчуття до українців на роздратування і соціальне відторгнення.

Другий важливий напрям – використання економічних конфліктів, передусім ситуації з українським зерном і протестами польських фермерів. Російські ресурси подавали ці події як доказ краху польсько-українського союзу, нібито «колоніальних» планів Варшави щодо України або, навпаки, «зради» польських інтересів на користь Києва. EUvsDisinfo (європейська платформа з моніторингу та протидії дезінформації) фіксувала дезінформаційні повідомлення, у яких зернова суперечка трактувалася як підтвердження того, що Польща нібито прагне взяти під контроль українські ресурси або західні регіони України.

Окреме місце займає історична тематика. Російська пропаганда системно експлуатує складні сторінки польсько-української історії, передусім Волинську трагедію, намагаючись перевести сучасне стратегічне партнерство у площину взаємних історичних образ. Така тактика є особливо небезпечною, оскільки апелює не лише до раціональних аргументів, а й до емоцій, колективної пам’яті та ідентичності. У цьому випадку йдеться вже не просто про дезінформацію, а про когнітивний вплив: аудиторії пропонують інтерпретувати сучасну Україну через травматичні образи минулого.

Ще один стійкий російський наратив – твердження про те, що Польща нібито має територіальні претензії до України або планує встановити контроль над її західними областями. Цей меседж просувається як для української, так і для польської аудиторії. Для українців він має викликати недовіру до Варшави, а для поляків – підживлювати імперські або ревізіоністські уявлення. Попри

очевидну абсурдність таких тверджень, дослідження Інституту Мєрошевського 2024 р. показало, що частина української аудиторії все ж сприйнятлива до антипольських дезінформаційних тез про нібито ревізіоністські плани Польщі.

Канали поширення таких інформаційних загроз є різнорівневими. Російські наративи транслюються через державні й афілійовані медіа, псевдоаналітичні сайти, соціальні мережі, Telegram-канали, коментарі ботів, а також через маргінальні політичні середовища. У наукових і аналітичних дослідженнях згадуються як російські ресурси на кшталт RT і Sputnik, так і локальні або нішеві портали, які відтворювали російські тези, маскуючи їх під польський внутрішній дискурс.

Наслідки цих інформаційних операцій не слід перебільшувати, але й недооцінювати їх небезпечно. Польща не відмовилася від підтримки України, однак російські кампанії створюють фон недовіри, на якому будь-яка економічна чи політична суперечка швидко набуває антагоністичного звучання. Це ускладнює роботу урядів, посилює позиції радикальних політичних сил, знижує суспільну готовність до тривалої підтримки України та створює додатковий тиск на рішення у сфері військової допомоги.

Отже, російські інформаційні загрози польсько-українському партнерству мають комплексний характер. Вони спрямовані не лише на дискредитацію України або Польщі окремо, а на руйнування довіри між двома суспільствами, які в умовах війни стали важливими елементами спільної безпекової архітектури Центрально-Східної Європи. Протидія цим загрозам потребує не лише спростування окремих фейків, а й системної координації стратегічних комунікацій України та Польщі, роботи з історичною пам'яттю, прозорого пояснення економічних суперечностей і посилення медіаграмотності. Саме інформаційна стійкість польсько-українського партнерства є однією з умов збереження міжнародної підтримки України у довготривалій війні.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Курок Р. О., д-р пед. наук, доц.
Національна академія Служби безпеки України

# РОСІЙСЬКІ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ОПЕРАЦІЇ В УМОВАХ СУЧАСНОЇ ГІБРИДНОЇ ВІЙНИ

У 2025 – 2026 роках в Україні фіксується значна активізація проведення російських інформаційно-психологічних операцій, спрямованих на дестабілізацію суспільно-політичної ситуації в країні.

На сьогодні, заходи російських ІПСО мають комплексний характер і розраховані одночасно на різні цільові аудиторії. Перша – це українське суспільство, яке намагаються дестабілізувати ворог. Друга – це населення країн-партнерів, які допомагають Україні. І третя – це внутрішня російська аудиторія, оскільки державі-агресору потрібно підтримувати градус ненависті до України для формування мотивації власних громадян долучатися до т.зв. «СВО». Мета ворожих ІПСО – гіперболізувати критичність наслідків, незворотність негативних процесів у сфері державного управління, поширити у суспільстві зневіру, протестні настрої, а подекуди й паніку. Ретельно враховуючи зміни у зовнішній та внутрішній політиці України, а також ситуацію у зоні бойових дій, держава-агресор прагне створити альтернативну інформаційну реальність, у якій важко відрізнити правду від брехні, і нав'язати її цивілізованому світу.

Часто в російських ІПСО використовуються реальні факти, проте з вигідною ворогу інтерпретацією подій та висновків. При цьому, російські фахівці постійно моніторять український інформаційний простір та виявляють настрої відповідних цільових груп. Певні суспільні тенденції, навіть якщо вони поодинокі, але перспективні з погляду реалізації ІПСО, масштабуються з метою їх розповсюдження на якомога більшу цільову аудиторію. Для цього ворог активно відслідковує вітчизняний інформаційний простір, відбираючи найбільш тригерні теми, здатні максимально сколихнути українське суспільство. Водночас, використовуючи наявні ресурси, представники держави-агресора через підконтрольні медіа та інші афілійовані структури масштабують проблематику та інтерпретують її у вигідному для них напрямі на цільову аудиторію, додаючи різноманітні припущення, теорії змов і актуальні російські наративи. Таким чином, формується думка про системність проблем у сфері державного управління та неможливість їх вирішення, некомпетентність

вищого військово-політичного керівництва держави, тотальну корупцію та зраду простих людей та військових, і, як наслідок, про безглуздість опору та потребу в «мирі за будь-яку ціну».

Для провокацій держава-агресор задіює потенціал створених ботоферм, масово застосовують підконтрольні групи та фейкові акаунти в популярних месенджерах і соцмережах, найактивніше – в TikTok і Telegram. Фахівці відзначають, що соціальні мережі є особливо ефективним каналом для дезінформації через можливість охоплення великої кількості людей та таргетування на вразливі групи. Боти та фейкові акаунти використовуються для підсилення дезінформаційних повідомлень, створюючи ілюзію широкої підтримки або схвалення певної інформації. Крім того, поширення дезінформації через месенджери ускладнює контроль і виявлення фейків, оскільки повідомлення надсилаються приватно, що робить цей канал поширення одним з найскладніших для регулювання.

Ми можемо констатувати, що російські ІПСО на сьогодні залишаються одним із головних інструментів гібридної війни проти України та її союзників. Вони характеризуються високим рівнем системності, адаптивності та синхронізації з військовими, політичними й економічними подіями, комплексним підходом до охоплення різних категорій населення. Їх основна стратегічна мета – не лише послабити внутрішню стійкість українського суспільства, але й досягти розколу між Україною та її західними партнерами.

З метою підвищення ефективності інформаційного впливу, держава-агресор намагається постійно модернізувати інструментарій, який використовується для проведення ІПСО, шляхом масового використання штучного інтелекту для генерації контенту, ботоферм; глибокої локалізації наративів під конкретні країни та соціальні групи, синхронізації з подіями (вибори, саміти, енергетичні кризи, переговори) тощо.

Зазначене дає підстави стверджувати, що російські ІПСО набули статус довгострокової, високотехнологічної та багатошарової загрози для демократичної стійкості як України, так і її партнерів. Перемога у протидії цій загрозі вимагає не фрагментарних реакцій, а системної стратегії: посилення медіаграмотності населення, швидкого виявлення та блокування дезінформаційних кампаній, проведення власних наступальних спеціальних інформаційних операцій, координації зусиль між державами-партнерами, а також інтеграції протидії ІПСО в загальну систему національної та колективної безпеки НАТО та ЄС.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Наумчак Л. М.
Житомирський військовий інститут імені С. П. Корольова
Марцинкевич О. С.
В/ч А2455

# ВПЛИВ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ НА ТРАНСФОРМАЦІЮ ПІДГОТОВКИ ВІЙСЬКОВИХ ФАХІВЦІВ ДО ПРОВЕДЕННЯ ІНФОРМАЦІЙНИХ І ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ В УМОВАХ СУЧАСНОГО ЗБРОЙНОГО КОНФЛІКТУ

Сучасний збройний конфлікт характеризується зростанням ролі інформаційного, психологічного та когнітивного вимірів протиборства. Поряд із традиційними засобами ураження важливого значення набуває боротьба за сприйняття подій, довіру до державних і військових інституцій та морально-психологічну стійкість особового складу. У таких умовах інформаційні й психологічні операції (ІПсО) стають одним із ключових інструментів досягнення переваги в інформаційному середовищі. Чинником, що суттєво змінює характер інформаційного протиборства, є розвиток великих мовних моделей (LLM): їхні можливості щодо аналізу великих масивів текстових даних, виявлення наративів і генерації навчальних сценаріїв відкривають нові перспективи для підготовки військових фахівців. Водночас ці технології можуть застосовуватися і як інструмент посилення дезінформаційних кампаній та автоматизованого створення маніпулятивного контенту.

Метою роботи є визначення впливу великих мовних моделей на трансформацію підготовки військових фахівців до проведення ІПсО в умовах сучасного збройного конфлікту. Передбачається проаналізувати можливості застосування LLM для аналізу інформаційного середовища, виявлення наративів, формування навчальних сценаріїв і моделювання реакцій цільових аудиторій, а також визначити основні ризики їх використання, пов’язані з недостовірністю згенерованої інформації, упередженістю, витоком чутливих даних і можливістю застосування таких технологій противником.

Великі мовні моделі суттєво змінюють підходи до підготовки фахівців у сфері ІПсО, дозволяючи перейти від переважно теоретичного навчання до сценарного, інтерактивного та аналітично орієнтованого формату. Можна виокремити п’ять ключових напрямів такої трансформації: перехід до

сценарного навчання з моделюванням інформаційної обстановки та навчальних кейсів; розвиток аналітичних компетентностей; моделювання цільових аудиторій та їхніх реакцій; формування AI-грамотності й культури критичної перевірки результатів; зміну ролі викладача і слухача в освітньому процесі.

Особливого значення набуває застосування LLM для розвитку аналітичних компетентностей: вони дають змогу здійснювати попередню обробку великих масивів текстової інформації, узагальнювати повідомлення та формувати варіанти аналітичних висновків. Формування AI-грамотності передбачає навички постановки запитів, критичної оцінки відповідей, перевірки фактів, виявлення упередженості та дотримання вимог захисту інформації. Змінюється і роль учасників навчання: викладач виконує функцію експертного супроводу та методичного контролю, а слухач набуває досвіду активної взаємодії з AI-інструментами й прийняття рішень в умовах інформаційної невизначеності.

Попри значний потенціал, застосування LLM пов'язане з низкою ризиків. Насамперед це генерація недостовірної або логічно переконливої, але фактично хибної інформації, що в навчальному процесі може призвести до неправильних аналітичних висновків і некоректного оцінювання обстановки. Окрему загрозу становлять упередженість моделей і залежність результатів від якості навчальних даних. Критичним обмеженням є ризик витоку службової або чутливої інформації під час використання зовнішніх AI-сервісів, що вимагає застосування лише деперсоналізованих або спеціально підготовлених навчальних матеріалів. Слід також враховувати можливість використання LLM противником для автоматизованої генерації дезінформації, масштабування пропагандистських кампаній і посилення психологічного тиску.

Таким чином, великі мовні моделі є важливим чинником трансформації підготовки військових фахівців до проведення ІПсО, що посилює сценарну, інтерактивну та аналітичну складові навчання. Водночас LLM мають використовуватися виключно як допоміжний інструмент, результати якого потребують обов'язкової експертної перевірки, за умови дотримання вимог інформаційної безпеки, заборони введення чутливої інформації у зовнішні AI-сервіси та формування AI-грамотності фахівців. Перспективним напрямом подальших досліджень є розроблення методики інтеграції LLM у підготовку фахівців з ІПсО з урахуванням ризиків дезінформації та когнітивного впливу.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Рудько С. О.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

# РОСІЙСЬКІ ІНФОРМАЦІЙНІ ОПЕРАЦІЇ ПРОТИ БАЛТІЙСЬКОЇ ПІДТРИМКИ УКРАЇНИ В УМОВАХ ПОВНОМАСШТАБНОЇ ВІЙНИ

Після початку повномасштабного вторгнення російської федерації країни Балтії стали одними з найбільш послідовних прихильників військової підтримки України. Литва, Латвія та Естонія не лише активно виступали за посилення санкцій проти Росії та збільшення військової допомоги Києву, а й самі передавали Україні значну частину власних оборонних ресурсів. На цьому тлі балтійський напрям став одним із пріоритетних об’єктів російських інформаційних операцій, спрямованих на послаблення підтримки України, дискредитацію урядів країн Балтії та формування у суспільстві страху перед прямою конфронтацією з росією.

Одним із ключових російських наративів стало твердження про нібито «втягування» Литви, Латвії та Естонії у війну через підтримку України. Російські медіа та афілійовані Telegram-канали систематично поширювали повідомлення про те, що балтійські уряди діють «в інтересах НАТО», жертвуючи власною безпекою та економікою. Особливо активно ці меседжі просувалися після передачі Україні систем ППО, артилерії та бронетехніки, а також у період дискусій щодо можливого постачання винищувачів F-16 і далекобійного озброєння.

Важливим об’єктом російських інформаційних атак стала Литва після обмеження транзиту окремих санкційних товарів до Калінінградської області влітку 2022 р. Російська пропаганда намагалася представити дії Вільнюса як «блокаду Калінінграда» та «провокацію проти Росії». У російському інформаційному просторі поширювалися заяви про можливість «жорсткої відповіді» Москви, а також тези про те, що Литва нібито виконує роль «найагресивнішого члена НАТО». Насправді ж литовська влада діяла відповідно до санкційної політики Європейського Союзу, однак інформаційна кампанія рф була спрямована на створення атмосфери страху та дестабілізації в регіоні.

Окремим напрямом російських інформаційних операцій стало дискредитування балтійської військової допомоги Україні як «неефективної»

або такої, що «послаблює обороноздатність самих країн Балтії». Після передачі Литвою гаубиць PzH 2000, систем NASAMS, бронетехніки M113 та боєприпасів російські інформаційні ресурси поширювали тези про те, що литовська армія нібито «залишилася без озброєння». Подібні меседжі використовувалися і щодо Естонії після передачі Україні значної кількості 155-мм артилерійських боєприпасів та військового обладнання. Основна мета цих кампаній полягала у створенні внутрішнього суспільного тиску на уряди країн Балтії.

Російська пропаганда також активно використовувала тему економічних наслідків підтримки України. У соціальних мережах і проросійських ресурсах поширювалися твердження про «економічне самознищення» країн Балтії через санкції проти рф, енергетичну кризу та військову допомогу Україні. Особливо активно ці наративи просувалися в період зростання цін на енергоносії у 2022–2023 рр. При цьому замовчувалося, що країни Балтії ще до повномасштабної війни проводили політику скорочення енергетичної залежності від росії та пришвидшили інтеграцію до європейських енергетичних систем.

Суттєву роль у російських інформаційних операціях відіграв етнополітичний фактор. Російськомовне населення Латвії та Естонії традиційно розглядається москвою як потенційний канал інформаційного впливу. Після початку повномасштабної війни російські ресурси активно просували тези про «утиски російськомовних», «русофобію» та нібито дискримінаційну політику балтійських урядів. На практиці ці наративи використовувалися для делегітимізації підтримки України та створення внутрішніх соціальних суперечностей.

Важливим елементом інформаційної протидії з боку балтійських держав стало обмеження діяльності російських пропагандистських ресурсів. Литва, Латвія та Естонія одними з перших у Європі обмежили мовлення російських державних телеканалів RT, Sputnik та інших медіа, які використовувалися як інструмент інформаційного впливу. Паралельно посилився моніторинг соціальних мереж, інформаційних платформ і проросійських онлайн-спільнот. У країнах Балтії також активно розвивалися програми медіаграмотності та стратегічних комунікацій, орієнтовані на підвищення стійкості суспільства до дезінформації.

Російські інформаційні операції проти балтійської підтримки України мають комплексний характер і поєднують елементи залякування, економічного

тиску, історичних маніпуляцій та експлуатації соціальних суперечностей. Їхня головна мета полягає не лише у зменшенні підтримки України, а й у підриві регіональної консолідації країн Балтії та НАТО на східному фланзі Альянсу. Водночас досвід Литви, Латвії та Естонії демонструє, що поєднання активної інформаційної політики, обмеження російських пропагандистських ресурсів та високого рівня суспільної підтримки України дозволило суттєво знизити ефективність російських інформаційних кампаній у регіоні.

Пілат С. І.
Військовий інститут Київського національного університету
імені Тараса Шевченка

## РОЛЬ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ У ГІБРИДНІЙ ВІЙНІ росії ПРОТИ УКРАЇНИ

Сучасні воєнні конфлікти характеризуються активним застосуванням не лише військової сили, а й інформаційних методів впливу. В умовах розвитку цифрових технологій та глобального інформаційного простору інформаційно-психологічні операції стали одним із ключових інструментів ведення гібридної війни. Російська Федерація активно використовує такі методи проти України з метою дестабілізації внутрішньої ситуації, послаблення обороноздатності держави та впливу на свідомість населення. У зв’язку з цим дослідження ролі інформаційно-психологічних операцій у сучасній гібридній війні набуває особливої актуальності.

Інформаційно-психологічні операції (ІПСО, англ. – Psychological Operations, PSYOP) — це різновид інформаційних операцій, проведення яких передбачає використання на практиці складної сукупності узгоджених, скоординованих і взаємопов’язаних форм, методів і прийомів психологічного впливу. Складаються з політичних, військових, економічних, дипломатичних і власне інформаційно-психологічних заходів, спрямованих на конкретну людину чи групи людей з метою впровадження в їх середовище чужих ідеологічних і соціальних установок, формування помилкових стереотипів поведінки, трансформації в потрібному напрямку їх настроїв, почуттів, волі.

Особливістю гібридної війни Росії проти України є комплексне поєднання військових, політичних, економічних, інформаційних та кібернетичних засобів

впливу. Одним із головних напрямів російської агресії стало ведення масштабної інформаційної кампанії, спрямованої на підрив української державності та послаблення єдності суспільства. Важливим інструментом інформаційно-психологічних операцій є дезінформація. Російська пропаганда систематично поширює фейкові повідомлення щодо діяльності української влади, перебігу бойових дій, міжнародної підтримки України та втрат серед населення і військових.

Прикладом інформаційно-психологічної операції, спрямованої на емоційний вплив на аудиторію, став фейк Російської Федерації щодо нібито створення Україною «брудної бомби». У межах цієї інформаційної кампанії міністр оборони РФ Сєргєй Шойгу провів телефонні переговори з міністрами оборони Франції, Туреччини та Великої Британії, під час яких заявив про нібито можливу підготовку Україною застосування «брудної бомби». У відповідь міністри закордонних справ США, Франції та Великої Британії виступили зі спільною заявою, у якій засудили спроби Росії поширювати неправдиві звинувачення проти України. Зазначена інформаційно-психологічна операція була спрямована насамперед на іноземну аудиторію та базувалася на використанні страху перед можливою ядерною ескалацією. Через поширення подібних заяв Росія намагалася сформувати міжнародний тиск на Україну та схилити світову спільноту до ідеї необхідності переговорів на вигідних для РФ умовах. Як зазначав представник Головного управління розвідки Міністерства оборони України Андрій Юсов, головною метою цієї кампанії було маніпулювання громадською думкою та створення атмосфери напруги й невизначеності у міжнародному інформаційному просторі.

Досвід російсько-української війни показує, що інформаційно-психологічні операції стали невід'ємною складовою сучасного воєнного протистояння. Ефективність інформаційного впливу значною мірою залежить від рівня інформаційної стійкості суспільства, розвитку стратегічних комунікацій та здатності держави оперативно реагувати на інформаційні загрози. Саме тому важливого значення набуває підвищення рівня медіаграмотності населення, розвиток критичного мислення та вдосконалення системи інформаційної безпеки. Важливими напрямами є своєчасне інформування населення, виявлення та спростування фейкової інформації, посилення кіберзахисту та формування єдиного інформаційного простору

держави. Крім того, необхідно вдосконалювати систему стратегічних комунікацій та забезпечувати інформаційну підтримку діяльності Збройних Сил України.

Отже, інформаційно-психологічні операції відіграють одну з ключових ролей у гібридній війні Росії проти України. Інформаційний простір став окремим полем боротьби, де здійснюється вплив на свідомість населення, моральний стан суспільства та міжнародне сприйняття конфлікту. У сучасних умовах ефективна протидія інформаційним загрозам є важливою складовою забезпечення національної безпеки та стійкості держави.

Гев'юк А. М., кан. політ. наук
Костенко А. М.
Угруповання об'єднаних сил

## АРХІТЕКТУРА УЧАСТІ УГРУПОВАННЯ ОБ'ЄДНАНИХ СИЛ В ІНФОРМАЦІЙНІЙ ОПЕРАЦІЇ ТА ПОБУДОВА COGNITIVE WARFARE PLATFORM

**Актуальність.** В умовах триваючого збройного конфлікту інформаційний та когнітивний простір перетворився на повноцінний театр бойових дій, де ефективність психологічного впливу на противника безпосередньо визначає результат операцій на тактичному та оперативному рівнях, що обумовлює необхідність системного підходу до організації відповідної діяльності.

**1. Існуюча архітектура інформаційних операцій в Угрупованні об'єднаних сил (далі – УОС)**

В УОС сформувався практичний розподіл заходів інформаційного та психологічного впливу відповідно до рівнів. На тактичному рівні заходи реалізуються армійськими корпусами та підпорядкованими військовими частинами у фізичному просторі. На оперативному рівні – приданим підрозділом ПсО ССпО переважно в інформаційному просторі.

Підрозділи безпілотних систем армійських корпусів на щотижневій основі здійснюють **залистування** позицій та маршрутів висування противника, та застосовують засоби **аудіотрансляції.**

Водночас заходи тактичного рівня у фізичному просторі виконують функцію підсилення заходів впливу, що проводяться на оперативному рівні в інформаційному просторі приданим підрозділом ПсО ССпО.

Комплексне застосування каналів впливу забезпечує синергетичний ефект: повторювані меседжі в усіх операційних просторах підривають довіру особового складу противника до командування та сприяють його деморалізації.

Крім того, з метою створення ситуаційної обізнаності в УОС впроваджено систематичний аналіз морально-психологічного стану (далі – МПС) підрозділів противника з подальшою візуалізацією даних МПС підрозділів противника в інформаційно-комунікаційній системі "Delta".

**2. Виявлені проблеми та пропоновані організаційні рішення**

На цей час, масштабуванню, якісному забезпеченню зазначених заходів та отриманню інформаційної переваги над противником перешкоджає відсутність спеціалізованих підрозділів когнітивного впливу у військових частинах – для дій у фізичному просторі, в армійських корпусах – для дій у фізичному та інформаційному просторах.

Пропонується реалізувати формування загонів когнітивного впливу в армійських корпусах та взводів (рот) когнітивного впливу у військових частинах.

Підрозділ когнітивного впливу – спеціалізований підрозділ, призначений для: збору та аналізу інформації щодо МПС противника та його вразливостей; розроблення й розповсюдження матеріалів когнітивного впливу у фізичному та інформаційному просторах; здійснення дезінформаційних заходів; проведення активних дій, спрямованих на деструктивний вплив на процес прийняття рішень командуванням противника.

**3. Створення спеціалізованої цифрової платформи**

Водночас, реалізація повного спектру завдань підрозділами когнітивного впливу в умовах динамічного інформаційного середовища є неможливою без спеціалізованої цифрової платформи. Відповіддю на цю потребу є концепція платформи когнітивної війни (Cognitive Warfare Platform, CWP).

Архітектурна модель концепції платформи когнітивної війни втілюється в інформаційно-аналітичній платформі "Літопис".

Платформа "Літопис" консолідує в єдиному захищеному інтерфейсі розвідувальні джерела, засоби моніторингу інформаційного простору та інструменти аналізу, забезпечуючи повний цикл збору, обробки, координації та поширення інформації.

"Літопис" реалізує багаторівневу рольову модель доступу – від базового перегляду до повного адміністрування системи. Платформу планується

застосовувати під час проведення інформаційних та психологічних операцій, протидії дезінформації та підтримки прийняття рішень.

**Висновки**

Попри сформований в УОС практичний розподіл заходів психологічного впливу між тактичним та оперативним рівнями, відсутність спеціалізованих підрозділів когнітивного впливу залишається системним обмеженням, що унеможливлює масштабування відповідної діяльності та отримання інформаційної переваги.

Усунення цього недоліку потребує формування загонів когнітивного впливу в армійських корпусах та взводів (рот) у військових частинах, що має супроводжуватися впровадженням спеціалізованого програмно-апаратного забезпечення, зокрема інформаційно-аналітичної платформи “Літопис”.

Компанцева Л. Ф.
Національна академія Служби безпеки України
Критенко О. В.
Житомирський військовий інститут імені С. П. Корольова

## ГЕНДЕРНИЙ ВИМІР ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ СПЕЦІАЛЬНИХ ОПЕРАЦІЙ

У доповіді розглянуто інформаційні і психологічні операції як один з головних вимірів повномасштабної війни росії проти України. Операції на гендерному підґрунті – лише частина цього деструктивного впливу. Системний аналіз інформаційних операцій (ІО) і психологічних операцій (ПО) рф дозволить визначити проактивні та асиметричні засоби захисту національної безпеки.

Україна наслідує підходи держав-членів НАТО щодо визначення сутності, технологій, цільових аудиторій інформаційних і психологічних операцій.

Інформаційні операції – узгоджене за метою, завданнями, місцем і часом з іншими діями військ (сил) інтегроване використання можливостей з інформаційного впливу для порушення, зриву, перехоплення або іншого деструктивного впливу на процеси прийняття рішень противником при одночасному захисті власного інформаційного простору .

Складовими ІО є: забезпечення безпеки воєнних операцій (англ. OPSEC), введення противника в оману (англ. MILDEC), радіоелектронна боротьба (РЕБ), операції в комп'ютерних мережах (англ. CNO), психологічні операції (англ. PSYOP).

Інформаційні операції, спрямовані на зміну ставлення і поведінки цільових аудиторій противника, проводяться переважно за напрямами:

введення противника в оману – введення осіб, які приймають рішення, в оману, маніпулюючи їхнім сприйняттям дійсності та переконуючи їх іти певним курсом;

радіоелектронна боротьба – навмисне випромінювання, перевипромінювання, змінювання, поглинання або відбиття електромагнітної енергії з метою дезорієнтувати, відволікти або заманити в пастку противника чи його радіоелектронні системи;

операції в комп'ютерних мережах (англ. CNO) – комп'ютерна мережева атака, захист комп'ютерних мереж або їх використання з метою проведення операцій;

психологічні операції – сплановані заходи, які використовують комунікативні методи, а також інші засоби, спрямовані на те, щоб впливати на цільову аудиторію загалом, на сприйняття нею інформації, на формування ставлення до чогось та її поведінку, що мають вплив на досягнення певних політичних та військових цілей.

У доповіді наведено кейси інформаційних операції рф на гендерному підґрунті з початку повномасштабного вторгнення в Україну, зокрема операції в комп'ютерних мережах, введення противника в оману та інші.

ІО та ПО складаються з кількох інформаційних та психологічних атак/акцій.

Інформаційна акція/атака (ІА) – оперативна комбінація окремих способів та інструментів інформаційного впливу, об'єднаних спільним задумом, метою, завданнями, об'єктом.

Психологічна акція/атака (ПА) – організоване застосування визначених сил і засобів для виконання завдань з інформування та (або) здійснення психологічного впливу на емоційний стан, мотивацію, раціональне мислення обмеженої за масштабом та районом цільової аудиторії та зміни моделі її поведінки в спосіб, що сприятиме досягненню воєнних та політичних цілей .

Відмінність інформаційних і психологічних операцій визначається у сфері впливу. Згідно з Доктриною США FM 3-05.301 (FM 33-1-1) ІО проводяться на всіх етапах війни, інших операцій або конфліктів . ПО слугують своєрідним важелем у процесі здійснення ІО для посилення їхнього потенціалу.

Відповідно до підходів рф, ІО та ПО сприяють військовій поразці противника, що може досягатися або його знищенням, або підкоренням його волі (мета). Цільовою аудиторією можуть бути як персоналізовані особистості, так і певні групи (страти). Інформаційна зброя спрямована на оброблення психіки цільової аудиторії у такий спосіб, щоб зняти бар'єри, що захищають нервову діяльність осіб від впливу зовнішнього агресивного середовища, і поступово перевести його в змінений або пограничний стан; нанести психологічний збиток особистості (уразити живу ціль методами інформаційно-психологічного впливу).

**ПАНЕЛЬ 2**

**Інформаційно-психологічна безпека особистості та суспільства, когнітивно-психологічні аспекти впливу**

Рикун В. Л.
Свистунович І. В.
Федяєв О. Л.
Житомирський військовий інститут імені С. П. Корольова

# КОГНІТИВНО-ПСИХОЛОГІЧНІ АСПЕКТИ ІНФОРМАЦІЙНОГО ВПЛИВУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

В умовах відсічі збройної агресії рф проти України виникла гостра проблема пов'язана з активним застосуванням противником інформаційно-психологічних операцій, спрямованих на вплив на свідомість військовослужбовців, населення та міжнародної спільноти з метою створення умов для дестабілізації суспільства шляхом створення емоційної напруги та маніпуляцій громадською думкою. Враховуючи те, що сучасний інформаційний простір характеризується високою швидкістю поширення контенту, що створює умови, за яких швидкість поширення інформації значно перевищує можливості її перевірки та протидії ворожим інформаційним технологіям важливого значення набувають питання вивчення особливостей когнітивного впливу на особистість.

Когнітивно-психологічні аспекти інформаційного впливу ворога в гібридній війні спрямовані на те, щоб змінити не лише те, що людина думає, а й те, як вона це робить. Основна мета – підірвати здатність людей приймати адекватні рішення.

Серед когнітивних механізмів впливу ворога слід відмітити:

рефлексивне управління шляхом нав'язування спеціально підготовленої інформації, яка змушує людей добровільно прийняти рішення, вигідне для агресора;

використання раніше сформованих у громадян когнітивних упереджень адже люди вірять тому, що підкріплює їхні погляди;.

спотворення "здорового глузду" методом блокування або модифікації логічних зв'язків у свідомості людини для дестабілізації її психічного стану тощо.

Серед поширених психологічних методів, які застосовує ворог, можна відзначити наступні: переконання псевдологічним впливом на свідомість для зміни психічної стійкості; навіювання шляхом емоційного впливу на підсвідомість

в обхід критичного мислення; психологічне зараження методом створення емоційного стану паніки, агресії у групах людей за допомогою соціальних мереж.

Ворог спрямовує свій вплив на індивідуальну свідомість цивільних людей в цілому, з метою зміни особистих цінностей, поглядів та поведінки. Окремо ворог спрямовує свій вплив і на військовослужбовців, щоб деморалізувати особовий склад, знизити його бойовий дух та стимулювати дезертирство і на громадську думку, з метою підриву довіри до органів державної влади.

Для забезпечення захисту від когнітивного впливу, в умовах гібридної війни, основні зусилля спрямовуються на формування індивідуальних навичок критичного мислення та дотримання базової інформаційної гігієни у військовослужбовців і цивільного населення. Адже здатність аналізувати джерела інформації, перевіряти достовірність фактів і розпізнавати маніпулятивні технології суттєво знижує ефективність ворожого інформаційного впливу. Важливу роль у цьому процесі відіграють державні органи, засоби масової інформації, освітні установи, та громадські організації з їх можливостями забезпечення повноти і достовірності інформації, швидкості її розповсюдження та легкодоступності до її джерел, а також впливу на формування свідомості громадян та громадської думки. Одним з найбільш ефективних серед основних методів розвитку критичного мислення та аналізу слід відмітити, критичне ігнорування, як здатність особистості свідомо фокусуватися лише на достовірній інформації, відсікаючи фейки, спотворення, некомпетентні коментарі.

Важливим аспектом є психологічна стійкість особистості на яку негативно впливає постійне перебування в умовах інформаційного перевантаження та воєнних загроз, що може призводити до емоційного виснаження, підвищення рівня тривожності та зниження здатності до раціонального прийняття рішень. У зв'язку з цим особливої актуальності набуває впровадження програм психологічної підтримки населення, розвиток навичок емоційної саморегуляції та формування культури безпечного споживання інформації та її критичного аналізу.

Таким чином, підвищення рівня медіаграмотності, розвиток критичного мислення та зміцнення психологічної стійкості є важливими складовими національної безпеки України. Проблема забезпечення інформаційно-психологічної безпеки особистості та суспільства в умовах сучасної війни потребує комплексного підходу, який поєднує технологічні, освітні та психологічні механізми протидії деструктивним інформаційним впливам.

Добровінський Д. О.
Житомирський військовий інститут імені С. П. Корольова

# ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА БЕЗПЕКА ОСОБИСТОСТІ ТА СУСПІЛЬСТВА, КОГНІТИВНО-ПСИХОЛОГІЧНІ АСПЕКТИ ВПЛИВУ

У доповіді проаналізовано інтенсивність інформаційно-психологічних впливів в умовах сучасних гібридних конфліктів, зокрема повномасштабної агресії РФ проти України. Інформаційний простір став ключовим середовищем формування переконань, емоційних реакцій та поведінкових моделей особистості й суспільства.

Методологічну основу дослідження становлять системний підхід, аналіз наукових джерел із психології впливу, когнітивної психології та теорії інформаційної безпеки, а також узагальнення спостережень за інформаційним простором в умовах війни. Встановлено, що ключовими когнітивно-психологічними механізмами впливу ІПсО є когнітивні викривлення (ефект підтвердження, евристика доступності), емоційне зараження, інформаційне перевантаження та маніпуляція увагою. Ці механізми знижують критичність мислення та підвищують вразливість до дезінформації.

Особистість у таких умовах часто функціонує в режимі скороченої когнітивної обробки інформації, що призводить до автоматичного прийняття нав'язаних інтерпретацій подій. На рівні суспільства це формує ефект поляризації думок, зниження рівня довіри до офіційних джерел інформації та зростання соціальної напруги. Важливим результатом аналізу є те, що найбільш ефективні ІПсО базуються не лише на викривленні фактів, а й на використанні емоційно насичених наративів, які активують базові психологічні реакції страху, гніву або невизначеності. У цьому контексті інформаційно-психологічна безпека визначається як здатність особистості та суспільства зберігати критичне мислення, емоційну стабільність і стійкість до маніпулятивних інформаційних впливів.

У підсумку аналізу визначено, що інформаційно-психологічні впливи ґрунтуються на використанні універсальних когнітивних особливостей людини. Найбільш вразливими є ситуації емоційного напруження та інформаційного перевантаження. Обґрунтовано, що підвищення інформаційно-психологічної стійкості можливе через розвиток критичного мислення, медіаграмотності та навичок когнітивної саморегуляції. Це дозволяє знизити ефективність маніпулятивних впливів і зміцнити психологічну безпеку як особистості, так і суспільства.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Ільяш А. О.
Кінь Н. В.
Центральний науково-дослідний інститут Збройних Сил України

# РОЗВИТОК КОГНІТИВНОЇ СТІЙКОСТІ НАСЕЛЕННЯ І ВІЙСЬКОВОСЛУЖБОВЦІВ УКРАЇНИ НА ОСНОВІ ПІДХОДІВ НАТО ТА МЕХАНІЗМІВ СІМІС

Повномасштабна збройна агресія російської федерації проти України остаточно підтвердила трансформацію сучасних конфліктів, у яких когнітивний вимір став самостійним і критично важливим доменом протиборства. На відміну від класичної інформаційної війни, що фокусується на контролі над потоками даних, когнітивна війна (Cognitive Warfare) спрямована на зміну самих алгоритмів мислення, способів обробки інформації та механізмів ухвалення рішень як окремими індивідами, так і суспільством загалом. В умовах інтенсивного застосування ворогом генеративного штучного інтелекту, дипфейків та тактик "предикативного програмування" (завчасного формування у аудиторії необхідних ментальних установок через масову культуру та медіаконтент), формування когнітивної стійкості населення та сектору безпеки і оборони стає фундаментом національного виживання.

Згідно з підходами НАТО, стійкість розглядається не лише як оборонна здатність, а як спроможність держави й суспільства протистояти кризам, адаптуватися до них та швидко відновлювати функціонування. Концепція розвитку бойових дій Альянсу (NWCC) виокремлює шість ключових функцій випередження, де особливе місце посідають спроможності "перевершити в мисленні" (out-think) та "перевершити у витривалості" (out-last). Практична реалізація цих принципів ґрунтується на Семи базових вимогах НАТО (7 BLR), що охоплюють безперервність урядування, стійкість енергозабезпечення, цивільних комунікацій та транспорту, а також здатність долати масові втрати.

Ключовим інструментом забезпечення такої стійкості є цивільно-військове співробітництво (CIMIC). Відповідно до доктрин Альянсу, CIMIC виступає інструментом командувача для взаємодії з цивільним середовищем, дозволяючи інтегрувати цивільні фактори в оборонне планування. В українських реаліях механізми CIMIC еволюціонували у дієвий міст між Збройними Силами, органами влади, волонтерським рухом та міжнародними

організаціями. Офіцери CIMIC не лише координують гуманітарну підтримку в прифронтових районах, а й здійснюють інформаційну взаємодію, спрямовану на зміцнення довіри до сил оборони та спростування ворожих наративів безпосередньо в громадах.

Досвід 2022-2026 років засвідчив, що когнітивна стійкість напряму залежить від фіскально-інституційного здоров'я громад: спроможні громади з розвиненими горизонтальними зв'язками демонструють вищу стійкість до воєнних шоків. Водночас подальший розвиток системи CIMIC в Україні стикається з бар'єрами, такими як функціональне перевантаження підрозділів невластивими завданнями (соціальні питання, репатріація тіл) та потреба в оновленні доктринальної бази 2020 року.

Для посилення когнітивного захисту необхідно впроваджувати програми "нейро-ШІ готовності" (neuro-AI readiness) для військових та підвищувати медіаграмотності цивільного населення. Пріоритетним завданням є ухвалення Закону України "Про цивільно-військове співробітництво", який закріпить CIMIC як спільну військову функцію та чітко розмежує повноваження військових і цивільних органів. Тільки через синергію високотехнологічних рішень, стратегічних комунікацій та дієвих механізмів CIMIC Україна зможе забезпечити тривалу когнітивну перевагу та зберегти цілісність суспільної свідомості в умовах перманентних гібридних загроз.

Барановська Л. В., канд. пед. наук
Міняйло В. М.
Житомирський військовий інститут імені С. П. Корольова

## ПСИХОЛОГІЧНА СТІЙКІСТЬ ВОЛОНТЕРСЬКОГО РУХУ ЯК ФАКТОР ПРОТИДІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ОПЕРАЦІЯМ В УМОВАХ АГРЕСІЇ рф

Волонтерство в сучасній Україні є не лише формою громадянської активності, а й стратегічним психологічним явищем та елементом національної безпеки. В умовах повномасштабної збройної агресії рф тисячі людей добровільно взяли на себе функцію забезпечення критичних потреб Сил оборони та цивільного населення. Проте український волонтерський сектор,

завдяки своїй горизонтальній структурі та високій суспільній довірі, став однією з пріоритетних мішеней для російських апаратів проведення інформаційно-психологічних операцій (зокрема, 72-го головного центру спеціальної служби гру рф). Метою цих операцій є деморалізація тилу через руйнування довіри, посіяння зневіри та штучне моделювання внутрішніх соціальних розколів.

Основою стійкості волонтерів до зовнішніх маніпуляцій на початкових етапах є їхня висока внутрішня мотивація, почуття цивільної відповідальності та національної солідарності. Патріотизм, чіткі моральні імперативи та емпатія виконують роль природного психологічного захисту, трансформуючи первинний емоційний біль, страх і тривогу від війни у конструктивну, цілеспрямовану дію. Цей процес сублімації нівелює відчуття безпорадності та хронічного стресу, яке ворог намагається штучно нав'язати українському суспільству через інструменти інформаційного терору, такі як масовані ракетні обстріли чи трансляцію воєнних злочинів у медіапросторі.

Пролонгована волонтерська діяльність у парадигмі «кризового менеджменту» неминуче супроводжується деструктивними психологічними чинниками: деривацією сну, хронічною втомою, синдромом вторинної травматизації (емоційним перевантаженням через постійний контакт із людським горем, смертю та каліцтвами) та етичним дискомфортом через необхідність пріоритезації допомоги в умовах дефіциту ресурсів. Органічне когнітивне та емоційне вигорання створює критичні ментальні вразливості. Фізіологічно виснажена психіка втрачає здатність до критичного аналізу, знижує поріг когнітивного контролю та стає гіперчутливою до деструктивного контенту, що дозволяє ворожим спецслужбам успішно застосовувати цілий комплекс інструментальних моделей ІПСО.

Серед ключових деструктивних технологій ворога виділяються кампанії системної делігітимізації («корупційний контур»), спрямовані на координоване масштабування поодиноких випадків зловживань чи кримінальних проваджень у сфері гуманітарної допомоги до рівня узагальнюючого наративу «крадуть усі». Використовуються сфабриковані аудіозаписи, фейкові скриншоти листувань та проплачені публікації у медіа. Операційна мета таких дій — заблокувати фінансові потоки (донати) від населення, спровокувати у волонтерів екзистенційну кризу марності їхніх зусиль і змусити їх згорнути діяльність.

Паралельно застосовується штучна поляризація суспільства та моделювання конфліктів через експлуатацію тригерних тем для створення ліній розколу. Прикладами є штучне стравлювання категорій «тил проти фронту» (наратив про те, що цивільні нібито байдужі до війни), «великі монопольні фонди проти мікроволонтерів» (звинувачення у блокуванні зборів один одного), а також радикалізація мовних, регіональних чи політичних суперечок у волонтерських чатах за допомогою мереж ботоферм (інструменти емоційного зараження).

Окремим небезпечним інструментом є цифровий терор, залякування та доксинг — цілеспрямовані кібер-психологічні атаки. Вони включають деанонімізацію персональних даних волонтерів, збір відомостей про членів їхніх родин, злам особистих та робочих акаунтів, масований спам погрозами фізичної розправи у месенджерах. Психологічна мета — перевести волонтера зі стану «конструктивної допомоги» у стан «персонального виживання», паралізувати волю через страх за безпеку близьких. Крім того, технологія «дзеркального відчаю» та формування вивченої безпорадності через лавиноподібне заповнення коментарів під волонтерськими публікаціями депресивними повідомленнями («всі втомилися», «збори стоять, бо людям байдуже», «держава переклала свої обов'язки на нас, це безглуздо»). Ворог використовує це для активації когнітивного упередження «ефект ілюзії правди» (коли багаторазово повторена брехня сприймається виснаженим мозком як факт), що прискорює депресивні стани та відмову від діяльності. Наостанок, операції експлуатації довіри (фішинг та двійники) через створення ідентичних копій сторінок відомих волонтерів та фондів зі зміненими реквізитами для збору коштів. Окрім прямої матеріальної шкоди, ця технологія завдає глибокої психологічної травми донорам, які, дізнавшись про обман, переживають фрустрацію та повністю закриваються від подальшої фінансової участі в обороні країни.

Протидія цим комбінованим психологічним атакам ворога лежить у площині відновлення внутрішніх і колективних копінг-ресурсів спільноти. До них належать розвиток навичок психологічної саморегуляції, впровадження інституційної гігієни праці, встановлення жорстких меж між волонтерством та приватним життям, а також супервізія всередині команд. Водночас, попри деструктивний тиск, волонтерська діяльність запускає процеси посттравматичного зростання — формування вищого рівня особистісної резильєнтності, глибинної емпатії та системного переосмислення життєвих цінностей, що зрештою масштабує загальнонаціональну психологічну пружність.

Довгострокова ефективність волонтерського руху та його захищеність від ворожих ІПСО вимагають переходу від аматорської активності до розбудови внутрішньої культури ментальної турботи. Психологічний супровід, робота зі спеціалістами та участь у групах підтримки мають сприйматися як невіддільна частина загальної безпекової стратегії держави. Ментальний стан людей є головним і водночас найбільш вразливим ресурсом нашої оборони. Збереження внутрішньої рівноваги та критичного мислення волонтерів є запорукою їхньої стійкості до інформаційних інтервенцій, здатності продовжувати допомогу Сил оборони та утримувати стабільність усього українського суспільства в довгостроковій перспективі.

Горбач В. Я., Ph. D.
Горбач Т. П.
Житомирський військовий інститут імені С. П. Корольова

## КОГНІТИВНО-ПСИХОЛОГІЧНІ АСПЕКТИ ВПЛИВУ НА КУРСАНТІВ В УМОВАХ ТРАНСФОРМАЦІЇ ВІЙСЬКОВОЇ ОСВІТИ ДО СТАНДАРТІВ НАТО

Стрімкий розвиток цифрових технологій істотно змінив характер сучасних воєнних конфліктів. Поряд із бойовими діями дедалі більшого значення набуває інформаційне протиборство, спрямоване на вплив на свідомість людей, моральний стан суспільства та ефективність роботи державних інституцій. В умовах повномасштабної агресії Російської Федерації проти України питання інформаційно-психологічної безпеки набуло особливої актуальності, що потребує оновлення системи військової освіти та підготовки майбутніх офіцерів до дій у середовищі постійного інформаційного тиску.

Інформаційно-психологічна безпека є важливою складовою національної безпеки держави. Її головне завдання полягає у захисті військовослужбовців і населення від маніпулятивного впливу, дезінформації та психологічного виснаження. У сучасній війні противник активно використовує соціальні мережі, цифрові платформи й медіаресурси для поширення неправдивих повідомлень, створення панічних настроїв, дискредитації державних органів та деморалізації особового складу.

За таких умов система військової освіти повинна враховувати не лише професійну підготовку, а й формування стійкості до інформаційних загроз. Важливими напрямами підготовки курсантів мають стати розвиток критичного мислення, аналітичних здібностей, навичок роботи з інформацією та здатності швидко приймати рішення у складних і невизначених ситуаціях. Майбутній офіцер повинен уміти оцінювати достовірність джерел, виявляти ознаки маніпуляцій та протидіяти психологічному тиску.

Особливе значення має формування когнітивної стійкості — здатності зберігати емоційну рівновагу, раціональність мислення та ефективність дій під час інтенсивного інформаційного впливу. Для цього доцільно застосовувати сучасні методи навчання: тренінги, ситуаційні завдання, моделювання кризових обставин і практичні вправи в умовах, максимально наближених до бойових.

Ефективність підготовки значною мірою залежить і від професійного рівня викладачів та командирів курсантських підрозділів. Вони повинні володіти сучасними методиками інформаційної безпеки, сприяти розвитку психологічної витривалості та формувати у майбутніх офіцерів навички інформаційної гігієни. Важливими залишаються вміння критично сприймати інформацію, дотримуватись цифрової безпеки та обмежувати вплив деструктивного контенту.

Отже, сучасна система підготовки військових фахівців має орієнтуватися не лише на професійні знання, а й на розвиток психологічної стійкості та готовності до інформаційного протиборства. Це сприятиме формуванню компетентних офіцерів, здатних ефективно діяти в умовах сучасних гібридних загроз.

Дудко О. В.
Національний університет оборони України

## КОГНІТИВНІ ТА ПОВЕДІНКОВІ ЕФЕКТИ ЯК КРИТЕРІЇ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНИХ КАМПАНІЙ

Попри активне впровадження новітніх комунікаційних інструментів, у секторі оборони України все ще зберігається певна інерція застарілого процесного підходу, зорієнтованого переважно на кількісні показники поширення контенту та реактивне "гасіння пожеж". Виникає потреба переходу від фрагментарного інформування до

цільового управління довгостроковими інформаційними (комунікаційними) кампаніями, орієнтованих на досягнення верифікованих інформаційних, когнітивних та поведінкових ефектів у цільових авдиторій.

Правовою та доктринальною основою для такої трансформації є євроатлантичні стандарти стратегічних комунікацій, зокрема політика Військового комітету НАТО MC 0457 та доктрини AJP-10 і AJP-10.3, які вимагають формування у фахівців стійкого "мислення категоріями кампанії" (campaigning mindset). У межах цієї парадигми процес оцінювання ефективності комунікації категорично не може розглядатися як фінальна стадія звітування. Він має функціонувати як безперервна управлінська функція зворотного зв'язку, що базується на об'єктивних, математично вимірюваних SMART-метриках.

Наукова сутність такого оцінювання полягає у верифікації ступеня когнітивного та поведінкового залучення аудиторії на основі багаторівневих моделей, зокрема британської моделі GSC Evaluation Cycle. При цьому під когнітивним ефектом розуміють безпосередні процеси сприйняття, усвідомлення та обробки інформації. Кінцевою ж метою та головним критерієм успішності будь-якої кампанії в оборонній сфері є поведінковий ефект — соціологічно-вимірюваний результат впливу, що виражається у формуванні, модифікації або зміні поведінки людей.

Для структурування комунікаційних зусиль в оборонній практиці доречно застосовувати британську модель CORE. Вона дозволяє диференціювати ефекти за чотирма напрямами: зміна поведінки (стимулювання до виконання конкретних дій, наприклад, залучення до рекрутингових центрів), забезпечення операційної ефективності (інформаційний супровід та маскування дій військ), управління репутацією (підтримання інституційної довіри) та роз'яснення державної політики (артикуляція складних рішень для уникнення соціальної напруги).

Прикладом оцінювання комунікації за критеріями ефектів стала інформаційна кампанія "Захищаємо своє", реалізована Департаментом стратегічних комунікацій Міністерства оборони України у період з грудня 2025 року по березень 2026 року. Завдяки багатоканальності комунікації (із залученням цифрових інструментів META, Google, YouTube, Telegram, TikTok, телебачення, зовнішньої реклами та носіїв у метрополітені) було досягнуто масштабних показників охоплення.

Зокрема, інструменти Google та META у сфері підвищення обізнаності (awareness) забезпечили понад 61,4 мільйона показів та 20,1 мільйона

переглядів із унікальним охопленням 11,24 мільйона користувачів (при частоті 7.3). Інструменти показу у тих же мережах принесли понад 2,9 мільйона показів та більше 1,06 мільйона кліків. Канал TikTok згенерував понад 12,4 мільйона показів та 52,7 тисячі кліків, охопивши унікально 3,89 мільйона осіб. Посіви у Telegram-каналах та розміщення через бізнес-мережі сукупно забезпечили унікальне охоплення для більш ніж 1,45 мільйона користувачів. Крім того, значний внесок у загальне когнітивне залучення внесли OTS-показники зовнішньої реклами, які перевищили 171,5 мільйона одиниць із унікальним охопленням щонайменше 1,7 мільйона осіб.

Важливо, що оцінювання цієї кампанії не обмежилося фіксацією когнітивного охоплення. Головним показником досягнення саме поведінкових змін став перезапуск та верифікована статистика оновленого вебпорталу Army.gov.ua 2.0. Зафіксовано поведінкову активність цільової аудиторії: 461 277 унікальних користувачів здійснили 686 293 сесії та згенерували 2 368 безпосередніх заявок, що є індикатором трансформації інформаційного впливу в дію.

Таким чином, відмова від суб'єктивних чи суто кількісних метрик (на кшталт кількості випущених релізів чи "лайків") на користь жорсткого вимірювання багаторівневих когнітивних і поведінкових ефектів формує абсолютно нову інституційну культуру в оборонній сфері. Системне управління інформаційними кампаніями перетворює стратегічні комунікації з допоміжного репродуктора інформації на інструмент некінетичного впливу, який безпосередньо підтримує оперативну діяльність військ, зміцнює національну безпеку та забезпечує консолідацію зусиль суспільства і держави.

Закаблуковська О. О., Ph. D.
Біба С. А.
Воєнна академія імені Євгенія Березняка

## HUMINT І КОГНІТИВНІ ВИКРИВЛЕННЯ: МОЖЛИВОСТІ ВИЯВЛЕННЯ ТА КОРЕКЦІЇ

У сучасному інформаційному суспільстві, де обсяг даних стрімко зростає, особливого значення набуває якість їх інтерпретації. Одним із ключових факторів, що впливають на сприйняття, аналіз та прийняття рішень, є когнітивні

викривлення: систематичні помилки мислення, які виникають у процесі обробки інформації. У цьому контексті HUMINT (human intelligence) можна розглядати як ефективний інструмент не лише збору інформації, але й діагностики когнітивних процесів особистості.

HUMINT доцільно трактувати як систему міжособистісної взаємодії, що передбачає отримання, аналіз і інтерпретацію інформації через комунікацію з людиною. Його потенціал значно ширший за класичне розуміння збору даних, адже включає елементи психологічного спостереження, емпатійного слухання, аналізу невербальної поведінки та когнітивних патернів.

Когнітивні викривлення, такі як ефект підтвердження, евристика доступності, ефект якоря, упередження оптимізму чи негативізму, істотно впливають на формування суджень. Вони можуть спотворювати реальність, знижувати якість рішень та створювати ілюзію об’єктивності там, де її фактично немає. Особливо це проявляється в умовах невизначеності, емоційного напруження або обмеженого часу на обробку інформації.

Застосування HUMINT дозволяє виявляти когнітивні викривлення через аналіз мовлення, поведінкових реакцій та логіки аргументації. HUMINT виконує три взаємопов’язані функції:

1. діагностичну (виявлення когнітивних викривлень),
2. інтерпретаційну (аналіз їх впливу на судження),
3. корекційну (когнітивне коригування через комунікацію).

Окрему роль відіграє здатність HUMINT-фахівця ставити правильні запитання. Використання відкритих, уточнювальних та рефлексивних питань дозволяє не лише отримати більше інформації, але й допомагає співрозмовнику усвідомити власні когнітивні помилки. Таким чином, HUMINT стає не просто інструментом збору даних, а й механізмом когнітивної рефлексії.

Корекційний потенціал HUMINT реалізується через механізми когнітивної активації та переосмислення. Зокрема, ефективними є такі стратегії: когнітивна конфронтація (зіставленні суперечливих елементів у висловлюваннях або переконаннях суб’єкта. Вона не має характеру прямої критики, а реалізується через віддзеркалення та уточнення. Співрозмовнику демонструється невідповідність між різними його судженнями або між словами і фактами.); рефреймінг (передбачає зміну інтерпретаційної рамки, в якій суб’єкт осмислює подію. Психологічно це означає перехід від автоматизованої, часто емоційно забарвленої оцінки до більш гнучкого та багатовимірного

бачення ситуації. Рефреймінг працює через розширення контексту, той самий факт набуває іншого значення залежно від того, у яку систему координат він включений.); альтернативна гіпотеза (запропонування інших можливих причин або мотивів активізує дивергентне мислення та знижує вплив евристик. Важливим є те, що альтернативні гіпотези не нав'язуються як "правильні", а подаються як рівноправні варіанти. Це зменшує опір і сприяє формуванню когнітивної гнучкості.).

Важливо зазначити, що ефективність HUMINT у виявленні та корекції когнітивних викривлень значною мірою залежить від рівня психологічної компетентності спеціаліста. Він має володіти знаннями з когнітивної психології, комунікативних стратегій та емоційного інтелекту. Крім того, ключовими є етичні аспекти: повага до особистості, недопущення маніпуляцій та забезпечення добровільності взаємодії.

HUMINT може бути ефективно застосований у психологічному консультуванні, освіті, управлінні персоналом, переговорах та навіть у повсякденній комунікації. Його використання сприяє не лише підвищенню якості інформації, але й розвитку критичного мислення, зниженню впливу упереджень та формуванню більш об'єктивного бачення реальності.

**Висновки.** HUMINT у поєднанні з розумінням когнітивних викривлень відкриває широкі можливості для підвищення ефективності комунікації та якості прийняття рішень. Він виступає не лише інструментом отримання інформації, але й засобом глибшого розуміння людського мислення, що є особливо актуальним у сучасному складному та динамічному світі.

Khudaverdova A. O., Ph. D.
Borysenko K. M.
Ivan Kozhedub Kharkiv National Air Force University
Raikovskyi O. V.
Korolov Zhytomyr Military Institute

## SOCIO-PSYCHOLOGICAL MECHANISMS OF INFORMATION-PSYCHOLOGICAL OPERATIONS IN THE STRUCTURE OF PUBLIC OPINION FORMATION

In the architecture of hybrid conflicts, information-psychological operations (IPSYO) serve as the determining factor of large-scale transformation and modelling of public consciousness.

The experience of the russo-ukrainian war vividly demonstrates how IPSYO have become one of the most critical instruments of information warfare, as these operations are directed at the manipulation of mass consciousness, the destabilisation of public opinion, the provocation of societal conflict, and the erosion of trust in state institutions. An examination of the impact of IPSYO on public opinion during the russo-ukrainian war through the lens of socio-psychological aspects reveals a particular emphasis on the study of disinformation methods, manipulation, and propaganda systematically employed across various media channels - including social networks - as well as their psychological effects on distinct population groups.

The principal methods employed within the framework of IPSYO are the dissemination of disinformation and fake news. Propaganda resources frequently utilise emotionally charged messaging designed to cultivate fear, uncertainty, and heightened distrust toward official information sources. Such messaging may take the form of information “injections” as well as targeted disinformation campaigns oriented toward specific audiences. Under conditions of high stress and sustained psychological pressure on the population, these methods prove exceptionally effective, as individuals are prone to emotional reactions and may be susceptible to the influence of manipulative information.

Social networks play a decisive role in the conduct of IPSYO. Bots, fake accounts, and coordinated information campaigns are employed to disseminate disinformation and propaganda aimed at discrediting the government, the armed forces, and other state institutions. Notably, symbols of national identity frequently become the focus of such operations, thereby undermining the morale of the population.

The socio-psychological impact of IPSYO on public consciousness can hardly be overstated. Disinformation and manipulation generate feelings of fear, panic, and uncertainty within society. In wartime, the emotional state of the population is typically vulnerable, rendering it more susceptible to psychological influence from the adversary. IPSYO actively exploit mechanisms of cognitive distortion - in particular, confirmation bias, whereby individuals tend to seek out information that corroborates their pre-existing beliefs, and the illusory truth effect, whereby the repeated dissemination of a single piece of false information leads to its perception as true.

A significant aspect is the stimulation of societal polarisation. IPSYO are frequently directed at exacerbating social, political, and ethnic conflicts, resulting in the deepening of societal divisions. This approach is grounded in the "divide and rule" principle, whereby the adversary creates or amplifies internal conflicts within the target country in order to weaken its defensive capacity.

Social networks have emerged as a novel instrument in the hands of those who conduct IPsyO, enabling the rapid and effective dissemination of information among large numbers of people. By virtue of anonymity and the capacity for automation (bots and algorithms), IPSYO conducted via social networks allow for the manipulation of the opinions of millions of users, including through the use of "trolls" and other agitators. Platforms such as Facebook, Twitter, and Telegram are actively exploited for the dissemination of propagandistic narratives, manipulative images, and videos capable of provoking emotional responses and facilitating the further spread of disinformation. Rumours concerning events at the front, exaggerated casualty figures, or the denigration of the fighting spirit of Ukrainian military personnel all constitute elements of IPSYO directed at demoralising society and constructing an image of the enemy as an "invulnerable" adversary.

A key element of IPSYO countermeasures is the enhancement of information literacy among the population, encompassing the capacity to critically evaluate information sources and identify instances of manipulation. Relevant educational programmes, as well as the work of journalistic initiatives focused on fact-checking, can contribute to reducing the impact of disinformation. Furthermore, the development of psychological resilience within the population is a critical factor in countering the influence of IPSYO. Informing citizens about potential psychological methods of influence and conducting stress management training may contribute to diminishing the emotional impact of hostile operations. State institutions must develop countermeasure

strategies not only at the level of technical protection against cyber threats, but also in the domain of socio-psychological resistance to information attacks.

Information-psychological operations in the context of the russian-ukrainian war constitute an exceptionally significant instrument for shaping public opinion and the emotional state of the population, leading to increased levels of distrust, polarisation, and the destabilisation of social structures. In-depth investigation of the psychological and social dimensions of IPSYO enables a better understanding of the methods by which consciousness is manipulated, facilitates the development of effective countermeasures grounded in critical thinking, information literacy, and psychological resilience, and allows the Ukrainian nation to take confident strides on the path to Victory.

Ковальський О. В.
Райковський О. В.
Житомирський військовий інститут імені С. П. Корольова

## СОЦІАЛЬНІ МЕРЕЖІ ЯК СЕРЕДОВИЩЕ ПІДВИЩЕНОГО ІНФОРМАЦІЙНОГО РИЗИКУ

У сучасних конфліктах соціальні мережі стали основним засобом отримання інформації для більшості. Насамперед у сучасних умовах особливо важливим є те, що саме ці платформи найчастіше використовуються для розповсюдження дезінформації, повідомлень маніпулятивного характеру та вмістом психологічного впливу. Це питання набуває значення через зростання кількості інформаційних атак, спрямованих на підрив довіри, поділу суспільства та формування хибних уявлень як серед цивільного населення так і серед військовослужбовців.

Попри очевидні ризики, канали впливу соціальних мереж на свідомість користувачів залишаються недостатньо дослідженими. Алгоритми рекомендацій формують однорідні потоки інформації, обмежуючи можливості отримання правдивих новин, підсилюючи кількість чорної та сірої пропаганди, що сприяє радикалізації та маніпуляціям. Використання бот-каналів, фейкових акаунтів та ворожі інформаційні кампанії створюють ілюзію масової підтримки певних наративів. Користувачі часто не усвідомлюють власних когнітивних

вразливостей часто потраплячи під ефект навіювання, що робить їх мішенню для фейків, психологічного впливу та соціальної інженерії. Відсутність системної кібергігієни та низький рівень медіаграмотності посилюють ці ризики як на рівні особистості, так і на рівні суспільства.

Соціальні мережі є одним із ключових джерел інформаційних загроз для особистості та суспільства. Впровадження підходів щодо підвищення інформаційної стійкості, які включають розвиток медіаграмотності, формування навичок кібергігієни зменшать кількість випадків інформаційного та психологічного впливу на аудиторії. Використання даних заходів удосконалять інформаційно-психологічну безпеку у державному та громадських секторах. Таким чином, соціальні мережі потребують комплексного підходу до забезпечення інформаційно-психологічної безпеки, що включає як технологічні, так і когнітивно-психологічні заходи.

Коменда В. Р.
Рачкінда В. А.
Житомирський військовий інститут імені С. П. Корольова

## ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА БЕЗПЕКА ОСОБИСТОСТІ ТА СУСПІЛЬСТВА, КОГНІТИВНО-ПСИХОЛОГІЧНІ АСПЕКТИ ВПЛИВУ

Тема інформаційно-психологічної безпеки в сучасних умовах набуває особливого значення, оскільки розвиток інформаційних технологій, соціальних мереж та цифрових комунікацій суттєво змінив характер впливу на свідомість людини й суспільства. У XXI столітті інформація перетворилась не лише на засіб комунікації, а й на інструмент політичного, економічного та психологічного впливу. Особливо актуальною ця проблема є для України в умовах повномасштабної війни, коли поряд із військовими діями активно застосовуються інформаційно-психологічні операції, спрямовані на дестабілізацію суспільства, формування панічних настроїв, маніпулювання громадською думкою та підрив морально-психологічного стану населення і військовослужбовців.

Інформаційно-психологічна безпека розглядається як стан захищеності особистості, соціальних груп та суспільства від негативних інформаційних

впливів, здатних змінювати психічний стан людини, її поведінку, систему цінностей та здатність до самостійного прийняття рішень. На відміну від класичного розуміння безпеки як відсутності фізичної загрози, сучасне трактування включає також психологічний комфорт, відчуття стабільності, впевненості та здатність адекватно сприймати навколишню дійсність. Саме тому інформаційно-психологічна безпека безпосередньо пов'язана зі станом суспільної свідомості та рівнем стійкості людини до маніпулятивного впливу.

Сучасне інформаційне середовище характеризується надзвичайною швидкістю поширення інформації, значним обсягом повідомлень та практично необмеженим доступом до цифрових ресурсів. Разом із позитивними аспектами це створює і серйозні ризики. Людина фактично стає інформаційно відкритою, а її персональні дані, інтереси, поведінкові моделі та психологічні особливості можуть використовуватись для цілеспрямованого впливу. Особливу небезпеку становлять дезінформація, пропаганда, маніпулятивні технології, фейкові новини, психологічний тиск через соціальні мережі та мас-медіа. У більшості випадків такі впливи мають прихований характер і спрямовані не стільки на переконання людини, скільки на формування необхідних емоційних реакцій — страху, тривоги, агресії або апатії.

Когнітивно-психологічні аспекти інформаційного впливу пояснюють, чому людина часто стає вразливою до маніпуляцій. Когнітивна психологія досліджує процеси сприйняття, обробки, збереження та використання інформації. Її основна увага зосереджена на тому, яким чином зовнішня інформація трансформується у внутрішні знання, установки та поведінкові реакції. Людське мислення не є абсолютно об'єктивним, оскільки на нього впливають попередній досвід, емоційний стан, соціальне середовище та когнітивні викривлення.

Одним із найпоширеніших механізмів інформаційного впливу є ефект повторення. Інформація, яка систематично повторюється у медіапросторі, починає сприйматись як правдива навіть за відсутності реальних доказів. Не менш важливу роль відіграє емоційне забарвлення повідомлень. Людина значно легше запам'ятовує інформацію, що викликає сильні емоції, особливо страх або обурення. Саме тому інформаційно-психологічні операції часто будуються на створенні атмосфери паніки, невизначеності та психологічного виснаження.

Когнітивний підхід також пояснює, що людина сприймає реальність не безпосередньо, а через сформовані внутрішні моделі та уявлення. Отже, інформаційний вплив здатний змінювати не лише окремі погляди, а й саму

систему оцінювання подій. Через маніпуляцію фактами, акцентування уваги на певних темах або створення інформаційного перевантаження формується викривлене бачення дійсності

В умовах сучасної війни інформаційний простір став окремою сферою протиборства, де інформаційно-психологічні впливи використовуються для деморалізації військовослужбовців, підриву довіри до державних інституцій і створення суспільної нестабільності. Саме тому забезпечення інформаційно-психологічної безпеки є важливою складовою обороноздатності держави та потребує не лише технічного захисту інформаційних систем, а й розвитку медіа-грамотності, критичного мислення, психологічної стійкості особового складу, а також ефективної державної політики у сфері протидії дезінформації та формування якісного національного інформаційного простору.

Отже, інформаційно-психологічна безпека є однією з ключових умов стабільного функціонування держави та суспільства. Саме тому розуміння когнітивно-психологічних механізмів сприйняття інформації дозволяє ефективніше протидіяти маніпулятивним технологіям та забезпечувати психологічну стійкість особистості. Для України, яка перебуває в умовах гібридної війни, проблема інформаційно-психологічної безпеки має не лише наукове, а й стратегічне значення, оскільки без належного захисту інформаційного простору неможливе забезпечення національної безпеки та сталого розвитку держави.

Кравчук А. І.
Національна академія Служби безпеки України

## ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА БЕЗПЕКА ОСОБИСТОСТІ ТА СУСПІЛЬСТВА В УМОВАХ ПОВНОМАСШТАБНОГО ВТОРГНЕННЯ

Повномасштабне вторгнення російської федерації (далі – рф) у 2022 році радикально змінило архітектуру безпеки не лише у Європі, але й суттєво вплинуло на геополітичні процеси у всьому світі, оголивши глобальну вразливість сучасної структури міжнародної безпеки, перетворивши інформаційний простір на повноцінний театр воєнних дій.

Після повномасштабного вторгнення рф лише посилила інформаційно-психологічні впливи на суспільну свідомість українців, з метою паралізувати їх волю до спротиву. Особливо підсилює інформаційно-психологічний тиск перебування населення в умовах постійної загрози обстрілів, руйнувань та смертей, що вводить психіку людини в екстремальні стани. За таких умов інформаційно-психологічна безпека (далі – ІПБ) особистості та суспільства стає базовим чинником національної стійкості держави та спроможності її громадян чинити опір ворогу, який в рази переважає економічним та людським потенціалом.

Як було зазначено, під час війни, психіка індивіда перебуває в стані хронічного стресу, що робить її максимально вразливою до психологічних впливів та маніпуляцій. На фоні постійних обстрілів, які відбуваються як правило в ночі, що додатково виснажує людську психику через відсутність сну, паралельно ворог цілеспрямовано наносить ще й інформаційно-психологічні удари, поширюючи чутки про «неминучі катастрофи» (ядерну, техногенну, енергетичний колапс). Все це відбувається з метою викликати паніку у населення, паралізувати раціональне мислення та схилити суспільну думку до виникнення капітуляційних настроїв на вигідних для рф умовах.

Крім цього, на настрій населення суттєво впливає інформація від правоохоронних органів щодо викриття корупційних схем за участю представників вищих ешелонів української влади. Російська пропаганда відразу використовує такі інфоприводи, максимально розганяючи вкиди у інформаційному середовищі, з метою вчинити розкол суспільства та підірвати обороноздатності країни в цілому. Це здійснюється через руйнацію довіри простих людей до державних інститутів та системну дискредитацію військово-політичного керівництва країни.

В умовах повномасштабного вторгнення ІПБ особистості та суспільства вимагає проактивних дій. Розраховувати на підвищення медіаграмотності населення не достатньо і тут мали б відігравати важливу роль стратегічні комунікації, але ефективна система їх в державі досі не побудована і їх діяльність носить здебільшого епізодичний характер, який на інформаційну безпеку держави суттєвого впливу не становить.

Слід відмітити, що від початку повномасштабного вторгнення в країні було сформоване єдине, оперативно діюче джерело верифікованих новин – Телемарафон «Єдині новини», але на сьогодні його популярність значно впала

особливо серед молоді і людей середнього віку, тож такий формат подачі інформації потребує суттєвого перегляду та значних змін.

Висновок. Повномасштабне вторгнення довело, що інформаційний фронт є невід'ємною частиною кінетичної війни, коли ворог прагне завоювати не лише території, а й заволодіти розумом та серцями українців, тому перемога у цій війні залежить від когнітивної стійкості суспільства. ІПБ сьогодні – це стан безпеки суспільства, який базується на трьох стовпах: 1. довірі до власних інституцій; 2. безкомпромісній цифровій гігієні та вмінні контролювати емоції під час кризових ситуацій; 3. внутрішніх переконаннях та впевненості у перемозі України що межує із стійкою ненавистю до ворога, із усвідомленням його звірячої сутності та екзистенційній загрозі українству.

Мартинюк І. М., канд. біол. наук
Шматов Є. М.
Погребняк Т. Д.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

## КОГНІТИВНІ МЕХАНІЗМИ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ В УМОВАХ СУЧАСНОЇ ВІЙНИ

Повномасштабна збройна агресія російської федерації проти України засвідчила, що сучасна війна ведеться не лише у фізичному просторі, але й у когнітивному та інформаційному середовищі. Поряд із застосуванням високоточної зброї, безпілотних систем та кіберзасобів противник активно використовує інструменти інформаційно-психологічного впливу, спрямовані як на військовослужбовців, так і на цивільне населення. Основною метою таких дій є деморалізація особового складу, дестабілізація суспільних настроїв, підрив довіри до державних інституцій та створення атмосфери невизначеності й страху.

Сучасні інформаційні операції базуються не лише на поширенні дезінформації, а й на використанні особливостей людського мислення, емоційного сприйняття та когнітивних викривлень. Саме тому вивчення механізмів психологічного впливу та формування інформаційної стійкості військовослужбовців сьогодні набуває особливої актуальності в системі забезпечення національної безпеки України.

Інформаційно-психологічний вплив являє собою комплекс заходів, спрямованих на зміну поведінки, емоційного стану, переконань або рішень людини шляхом цілеспрямованої подачі інформації. Історичний досвід засвідчує про активне використовування пропаганди ще під час світових воєн ХХ ст., однак сучасні цифрові технології значно розширили її можливості.

В умовах російсько-Української війни інформаційні атаки здійснюються через соціальні мережі, месенджери, анонімні телеграм-канали, відеохостинги та інші цифрові платформи. Особливу небезпеку становить те, що противник враховує психологічні особливості сприйняття інформації людиною: увага, емоційність, пам’ять, схильність довіряти авторитетним джерелам, швидке реагування на загрозливий контент та її вплив багаторазового повторення.

Практика інформаційного протиборства показує, що людина не завжди аналізує інформацію раціонально. На процес оцінювання суттєво впливають когнітивні викривлення. Зокрема, люди схильні сприймати інформацію, яка підтверджує їхні попередні переконання, а багаторазове повторення певного повідомлення формує враження його достовірності навіть за відсутності доказів. Особливо ефективно працює емоційно забарвлений контент, пов’язаний зі страхом, небезпекою або загрозою життю. Саме тому російська пропаганда активно використовує повідомлення про нібито “втрати”, “зраду”, “безперспективність опору”, маніпулюючи емоціями військовослужбовців та населення. Значного поширення набули також фейкові відео, діпфейки, постановочні сюжети та інформаційні вкиди, метою яких є створення панічних настроїв і дестабілізація морально-психологічного стану.

Серед найбільш поширених методів інформаційно-психологічного впливу, які застосовуються в умовах сучасної війни, варто виділити: пропаганду, дезінформацію, маніпуляцію фактами, емоційний тиск, інформаційне перевантаження, фреймінг, соціальне програмування.

Особливу небезпеку становить фреймінг, як спосіб подачі інформації, при якому увага аудиторії акцентується лише на окремих аспектах події. Таким чином формується необхідне сприйняття ситуації навіть без прямої фальсифікації фактів. Наприклад, противник може навмисно висвітлювати лише складні або кризові епізоди бойових дій, створюючи враження постійної переваги своїх сил. Водночас позитивні результати діяльності Сил оборони України можуть замовчуватись або спотворюватись.

Окремим напрямом інформаційної агресії став кібербулінг та психологічний тиск через цифрове середовище. Це проявляється у масовому поширенні провокативних повідомлень, погроз, фейкових повідомлень родинам військовослужбовців, а також спробах морального виснаження особового складу через інформаційні канали. Крім того, сучасні технології штучного інтелекту дозволяють створювати високоякісні діпфейки – сфальсифіковані відео- та аудіоматеріали, які зовні практично неможливо відрізнити від реальних, що значно ускладнює процес перевірки інформації та створює додаткові ризики для інформаційної безпеки держави.

В умовах сучасної війни одним із ключових елементів протидії інформаційно-психологічним операціям є формування інформаційної та психологічної стійкості військових. Важливу роль у цьому процесі відіграє медіаграмотність, яка передбачає перевірку джерел інформації, вміння розпізнавати фейки, аналіз інформаційного контенту, оцінювання достовірності повідомлень, виявлення ознак маніпулятивного впливу. Не менш важливим є розвиток критичного мислення, вміння аналізувати інформацію, порівнювати факти, визначати логічні суперечності та оцінювати достовірність джерел.

Практичний досвід бойових дій демонструє безпосередній вплив психологічної стійкості особового складу на ефективність виконання бойових завдань. Саме тому підготовка військових фахівців має включати елементи психологічної підготовки, навчання емоційній саморегуляції, формування стресостійкості та навичок прийняття рішень в умовах інформаційного тиску. Доцільними є також заняття та тренінги із протидії інфоманіпуляціям, інфо безпеки, психологічної саморегуляції, дій в умовах інфоневизначеності, розпізнавання ворожих інфоопераций. Формування інфостійкості, медіаграмотності та критичного мислення має особливе значення. Інтеграція підходів до інфобезпеки, протидії ІПСО – важлива складова обороноздатності держави в умовах сучасних загроз.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Резуненко Д. О.
Кузьмичев А. В.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

# ПСИХОЛОГІЧНА АДАПТАЦІЯ ДО ВІЙНИ НОВОГО ПОКОЛІННЯ

Раніше військовослужбовець найбільше боявся артилерії чи стрілецького бою, то сьогодні одним із головних факторів психологічного виснаження стало постійне відчуття невидимої присутності противника у повітрі. FPV-дрони, безперервна аеророзвідка, інформаційний шум, телеграм-канали з відео уражень та постійне очікування удару формують новий тип бойового стресу, до якого класична військова психологія виявилася частково неготовою. Особливо гостро це відчувають військовослужбовці інженерних підрозділів. На відміну від штурмових груп, які часто працюють короткими інтенсивними епізодами, військовослужбовці нерідко виконують завдання годинами під відкритим небом, перебуваючи під постійною загрозою виявлення. Фортифікаційні роботи, обладнання позицій, евакуація техніки, розмінування маршрутів — усе це сьогодні відбувається в умовах, коли звук FPV-дрона може пролунати будь-якої секунди.

Війна ведеться не тільки за позиції, а й за нервову систему військовослужбовця. Саме тому дедалі частіше головним завданням стає не лише вижити фізично, а й не допустити когнітивного виснаження особового складу. Показовою є ситуація, коли після кількох годин інженерних робіт особовий склад починає реагувати на будь-який сторонній звук як на наближення FPV-дрона. Навіть після завершення бойового епізоду військовослужбовці ще тривалий час автоматично шукають очима небо, реагують на звук мотоцикла чи генератора як на потенційну загрозу. Це вже не просто бойовий стрес — це нова форма адаптації психіки до війни постійної присутності дрона.

Окремою проблемою стала інформаційна перенасиченість сучасного поля бою. Військовослужбовець одночасно отримує інформацію з радіостанцій, планшетів ситуаційної обізнаності, месенджерів, каналів БПЛА та команд управління. У результаті психіка працює в режимі постійного перевантаження. При цьому противник активно використовує інформаційний простір для посилення психологічного тиску: відео уражень техніки, маніпулятивні

повідомлення про втрати, емоційно навантажений контент та спроби створення атмосфери тотального контролю над полем бою.

Особливо небезпечним є ефект «невидимої присутності противника». Навіть за відсутності прямого контакту військовослужбовець постійно відчуває себе потенційною ціллю. У таких умовах формується стан хронічного психологічного виснаження, який негативно впливає на концентрацію уваги, швидкість реакції та здатність приймати рішення. Практика бойових дій показує, що тривале перебування у такому стані виснажує не менше, ніж безпосередній бій.

Водночас війна продемонструвала й інше — здатність українських військовослужбовців швидко адаптуватися до нових умов. Саме адаптивність стала одним із головних факторів виживання на сучасному полі бою. Сьогодні військовослужбовці інженерних підрозділів уже інтуїтивно змінюють маршрути руху, скорочують час роботи техніки на відкритій місцевості, використовують антидронові укриття, теплове маскування та працюють переважно короткими інтенсивними етапами.

Війна довела, що когнітивно-психологічний вплив став повноцінним елементом бойових дій. FPV-дрони, інформаційний тиск та постійна аеророзвідка змінили не лише тактику війни, а й сам психологічний стан військовослужбовця. У сучасних умовах перемогу визначає не лише кількість техніки чи озброєння, а й здатність людини адаптуватися до постійного стресу, зберігати критичне мислення та діяти ефективно навіть тоді, коли FPV чути раніше, ніж команду командира.

Беззубцева Т. Г.
Ринський І. М.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

## ІНФОРМАЦІЙНА СТІЙКІСТЬ ПІДРОЗДІЛІВ СИЛ ТЕРИТОРІАЛЬНОЇ ОБОРОНИ В УМОВАХ КОГНІТИВНОГО ВИСНАЖЕННЯ ВІЙНОЮ

Умови широкомасштабної збройної агресії російської федерації проти України суттєво змінили роль інформаційного середовища у забезпеченні бойової спроможності військових формувань. Якщо на початкових етапах війни

інформаційний вплив противника був спрямований на дезорганізацію управління, деморалізацію особового складу та поширення панічних настроїв, то в умовах тривалої війни високої інтенсивності основним об'єктом впливу дедалі більше стає когнітивна стійкість людини, тобто здатність військовослужбовця зберігати критичність мислення, адекватність сприйняття інформації та функціональну ефективність в умовах тривалого інформаційного й психологічного перевантаження. Для підрозділів Сил територіальної оборони зазначена проблема має особливе значення. Особовий склад одночасно перебуває у військовому, цивільному та цифровому інформаційному середовищах, що створює додаткові умови для інформаційного перевантаження, емоційного виснаження та зниження психологічної стійкості. Додатковим чинником є сучасний характер застосування Сил ТрО. Бригади і батальйони ТрО виконують завдання у складі угрупувань військ як механізовані, стрілецькі підрозділи, що суттєво підвищує рівень бойового, інформаційного та психологічного навантаження на особовий склад. На п'ятому році широкомасштабної агресії змінився і характер інформаційного впливу ворога, який активніше використовує механізми когнітивного виснаження через поєднання масованих ракетно-дронових ударів, інформаційно-психологічних операцій, маніпулятивного висвітлення тем втрат, мобілізації, соціальної несправедливості, тривалості війни та перспектив її завершення. Метою такого впливу є зниження здатності суспільства і військовослужбовців підтримувати психологічну готовність. Однією з проблем інформаційної стійкості підрозділів Сил ТрО є постійне перебування особового складу в умовах надлишкового та хаотичного інформаційного потоку. Сучасний військовослужбовець одночасно отримує інформацію з офіційних каналів управління, соціальних мереж, цивільного медійного середовища, відкритих Telegram-ресурсів та неформальних інформаційних спільнот. За умов постійного використання мобільних засобів зв'язку фактично стираються межі між бойовим і цивільним інформаційним простором, що ускладнює підтримання психологічної стійкості та інформаційної дисципліни. Суттєву небезпеку становить і поширення деструктивних інформаційних наративів окремими представниками внутрішнього інформаційного середовища, які через емоційність, політичну заангажованість або недостатнє усвідомлення наслідків власної діяльності фактично підсилюють інформаційний вплив противника. В умовах когнітивного перевантаження це призводить до зростання конфліктності, втрати довіри до

управлінських рішень, поширення чуток, порушень режиму інформаційної безпеки та загального зниження ефективності виконання бойових завдань. Практика бойових дій підтверджує, що навіть фрагментарне оприлюднення фото-, відеоматеріалів або геолокаційних ознак може використовуватися противником для ведення розвідки, коригування вогню та проведення інформаційно-психологічних операцій. Одночасно накопичувальний ефект тривалої війни, постійний бойовий стрес та інформаційна перенасиченість поступово формують стан психологічного виснаження і звикання до критичних умов. За таких умов забезпечення інформаційної стійкості підрозділів Сил ТрО має розглядатися як комплексне завдання, що поєднує питання інформаційної безпеки, цифрової дисципліни, інформаційної гігієни, підготовки командирів та адаптації особового складу до дії в умовах тривалого когнітивного перевантаження. Особливого значення набуває роль командирів усіх рівнів у підтриманні внутрішньої інформаційної стабільності підрозділів, своєчасному доведенні достовірної інформації та попередженні деструктивних інформаційних впливів. Водночас забезпечення інформаційної стійкості не може обмежуватися лише заборонами та адміністративними обмеженнями. Необхідним є поступове включення елементів підготовки до дії в умовах інформаційного та когнітивного перевантаження до системи бойової підготовки підрозділів Сил ТрО.

Таким чином, в умовах війни на виснаження інформаційна стійкість Сил ТрО перетворюється на один з фундаментальних чинників бойової ефективності та керованості. Від якості вирішення цих завдань залежатиме здатність системи територіальної оборони, як складової національного спротиву, зберігати функціональну стійкість в умовах довготривалого інформаційного і психологічного тиску противника.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Зиков В. Г.
Черняхівський І. В.
Житомирський військовий інституту імені С. П. Корольова

# КОГНІТИВНИЙ ВПЛИВ НА ОСОБОВИЙ СКЛАД ПІД ЧАС ВЕДЕННЯ БОЙОВИХ ДІЙ

Сучасна наступальна операція — це пікове, екстремальне навантаження на психіку солдата. Під час штурму когнітивний вплив ворога, висока динаміка бою та загроза загибелі діють синергетично. Вони намагаються паралізувати волю бійця, зруйнувати його тактичне мислення та повністю зірвати темп наступу. Для командира захист когнітивного ресурсу підлеглих у штурмовій фазі є базовою умовою виконання бойового завдання та збереження життів. Особливо гостро це питання постає під час залучення до штурмів молодого, необстріляного поповнення, чий ментальний контур ще не має бойового гартування.

Тактика когнітивного тиску під час штурму має певну специфіку.

У фазі наступу мозок штурмовика атакується одночасно з кількох напрямків. Противник цілеспрямовано використовує такі методи когнітивного придушення:

акустично-візуальний шок: надщільний артилерійський вогонь, хаотичні вибухи, використання світлошумових засобів та дронів-камікадзе. Це викликає сенсорне перевантаження, блокує раціональне мислення та вводить бійця в стан первинного жаху.

штучний хаос та дезорієнтація: застосування засобів РЕБ для подавлення нашого зв'язку та підміни GPS-координат. Втрата орієнтації на незнайомій місцевості вмикає когнітивний ступор — солдат не розуміє, де свої, а де противник.

цифрові пастки безпосередньо перед атакою: закидання в тактичні чати фейків про підхід резервів ворога, замінування всього маршруту або наказ про скасування операції тощо. Мета — посіяти сумнів у доцільності штурму за хвилини до виходу на рубіж.

Внаслідок цих факторів у бійців виникає “тунельний зір” (вони бачать лише те, що прямо перед ними, і пропускають флангові загрози), втрата відчуття часу та нездатність адекватно оцінювати команди.

Командир підрозділу повинний вчасно виявляти ознаки граничного когнітивного виснаження та виявляти військовослужбовців, чий мозок вже відмовив під впливом добойового стресу, ще на етапі висування на вихідний рубіж.

Головними ознаками граничного виснаження є:

поведінковий ступор або гіперреактивність: солдат або застигає, безцільно дивлячись в одну точку і не реагуючи на звернення, або здійснює хаотичні, безглузді рухи (нескінченно перевіряє порожній магазин, перекладає речі).

порушення координації та моторики: нездатність з першого разу спорядити магазин, тремтіння рук і хитка хода за відсутності фізичних поранень.

вегетативні прояви: виражена блідість або синюшність шкіри обличчя, часте поверхневе дихання, повна відсутність реакції зіниць на зміну освітлення, забудькуватість елементарних інструкцій, почутих хвилину тому.

Виявлення таких маркерів — сигнал для негайного втручання командира, оскільки такий військовослужбовець у штурмовій групі стане першою мішенню і підставить під удар весь підрозділ.

Введення в наступ необстріляних бійців вимагає від командира особливого когнітивного супроводу. Їхня психіка ще не має сформованих бойових шаблонів, тому будь-який непередбачуваний фактор може викликати паніку.

Робота з ними базується на трьох правилах:

1. Закріплення за кожним молодим бійцем у штурмовій парі або трійці (має бути закріплений досвідчений, обстріляний сержант чи солдат-ветеран). Молодий повинен копіювати дії наставника автоматично: "роби як я". Це знімає з його мозку тягар прийняття тактичних рішень у стресі.

2. Мікрозавдання замість глобальної мети: не ставити перед необстріляним солдатом абстрактне завдання, наприклад "взяти позицію ворога". Його мозок заблокується від масштабу загрози. Штурм діліться на кроки: "дійти до того дерева", "кинути гранату за цей бруствер", "переповзти на п'ять метрів вправо".

3. Голосове та фізичне супроводження: під час висування досвідчені військовослужбовці повинні постійно розмовляти з молодими, коментувати обстановку вголос, плескати по плечу. Звук голосу побратима та фізичний контакт не дають необстріляному бійцю провалитися у внутрішній простір власного страху.

Завдання командира: управління когнітивним станом під час наступу.

Його роль як лідера під час штурму — тримати ментальний каркас підрозділу. Він повинен діяти за наступним алгоритмом:

1. Когнітивне розвантаження (детальний брифінг): перед штурмом кожен солдат має знати свій маневр до автоматизму. Чіткі орієнтири, схеми

зачистки та покрокові дії знижують рівень невизначеності — головного джерела когнітивного стопору.

2. Надлишковий дуплюючий зв'язок: підготувати візуальні, світлові та звукові сигнали на випадок глушіння радіостанцій. Боєць повинен постійно відчувати управління; втрата зв'язку під час наступу миттєво руйнує ментальну стійкість.

3. Фільтрація інформації на рубежі: за 2-3 години до штурму повністю вилучити мобільні телефони. Інформаційний вакуум у цей період має бути заповнений виключно бойовими наказами та чіткими командами офіцерів.

Для швидкої стабілізації стану штурмовика існує методика Peer-to-Peer.

Якщо під час штурму боєць застиг, впав у паніку або діє хаотично, командир застосовує жорсткий алгоритм повернення до бою:

фізичне повернення: різко схопити за бронежилет, зафіксувати погляд очі в очі. Голосно та впевнено прокричати: “Дивись на мене! Ти в бою, я з тобою!”;

дихальний замок: змусити зробити один глибокий вдих і тривалий видих. Це збиває тремор та серцебиття;

переключення на тактичну дію: негайно дати простий, однозначний наказ, що вимагає мислення та руху. Наприклад: “Працюй по тому вікну!”, “Прикрий лівий фланг!”. Дія миттєво вимикає панічний контур мозку.

Таким чином, у штурмових діях перемагає не той, у кого більше зброї, а той, чий розум залишається холодним та керованим. Захист когнітивного простору штурмовика, своєчасне виявлення виснажених та правильна інтеграція новобранців — це пряма відповідальність командира. Тільки ментально захищений та сфокусований підрозділ здатний проламати оборону ворога та виконати бойове завдання.

Колодяжний О. С.
Скиба І. П.
Житомирський військовий інститут імені С. П. Корольова

## КОГНІТИВНА БЕЗПЕКА ОСОБИСТОСТІ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

В умовах російсько-української війни інформаційний простір став окремим полем бою, де ціллю стає не фізична оболонка, а свідомість людини, її емоції, переконання та цінності. Агресор активно використовує різні методи

психологічного впливу для просування своїх наративів та пропаганди, що суттєво впливає на український народ, створюючи панічні настрої в суспільстві та підриваючи довіру до державних інституцій. На відміну від традиційної зброї, інформаційно-психологічний вплив можна здійснювати з будь-якого куточка Землі. Тому питання когнітивної безпеки особистості є вкрай актуальним для сьогодення.

Когнітивна безпека - це, насамперед, вміння критично аналізувати інформацію. За рахунок відкритого інформаційного простору в Україні, що, безумовно, є ознакою демократичної держави, водночас створює вразливість до зовнішнього інформаційно-психологічного впливу на населення. В той час країна-агресор, створила умови «інформаційної бульбашки» всередині власної країни, водночас активно використовує можливість для проведення когнітивного та психологічного впливу на наше населення шляхом поширення власних наративів, пропаганди та маніпулятивного контенту.

Емоції – найгірший противник когнітивної безпеки особистості, який знижує вміння піддавати інформацію сумніву. У різних емоційних станах, таких як гнів, страх, паніка, безвихідність, вміння розпізнати та запобігти інформаційно-психологічному впливу суттєво знижується. Зазвичай агресор обирає найслабші місця нашого суспільства, такі як: примусова мобілізація, тема «ухилянтів», проблема енергетики, корупція, втрати на фронті тощо. Через необізнаність та незацікавленість більшості суспільства втрачається повнота дійсності. В цей момент, скролячи Facebook чи TikTok, користувачі потрапляють в емоційно забарвлену пастку. Фільтр вимикається, і бомба сповільненої дії вже запущена. Починається з малого: сумніви, недовіра до влади та може перерости до бажаної противником зміни поведінки.

Для ефективної протидії ворожому інформаційно-психологічному впливу необхідно систематично інформувати населення, розвивати медіаграмотність та особливу увагу приділяти інформаційному щепленню. Тобто завчасно ознайомлювати населення з основними методами дезінформації та маніпуляції, наводячи приклади, що дозволить виробити, так званий, «інформаційний імунітет» до ворожого контенту та покращить когнітивну безпеку.

Отже, в умовах російсько-української війни когнітивна безпека особистості відіграє важливу роль, як складова національної безпеки держави. Український інформаційний простір водночас забезпечує повний доступ до

інформації, при цьому стає вразливим для просування ворожої пропаганди й наративів. Особливо при використанні емоційно забарвленої інформації, що вимикає наш «фільтр» сприйняття. Тому ключовими напрямами є розвиток інформаційної гігієни та впровадження концепції інформаційного щеплення. Таким чином, це дозволить зменшити ефективність інформаційно-психологічного впливу ворога та покращить когнітивну безпеку в країні.

Корнійчук С. В.
Єфімов Г. В.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

## ІНФОРМАЦІЙНА ВТОМА СУСПІЛЬСТВА В УМОВАХ ТРИВАЛОЇ ВІЙНИ: РИЗИКИ ДЛЯ СИСТЕМИ НАЦІОНАЛЬНОГО СПРОТИВУ

Агресія російської федерації проти України пройшла етапи гібридної війни, широкомасштабного збройного вторгнення і сьогодні набула ознак довготривалої війни на виснаження, у межах якої ворог системно поєднує воєнний, інформаційний, психологічний, економічний та соціальний тиск. За таких умов одним із лакмусових показників спротиву дедалі більше стає внутрішня стійкість українського суспільства, його здатність утримувати тривалу мобілізаційну, психологічну та інформаційну напругу.

Інформаційна втома, у контексті викладеного матеріалу, вбачається як поступове зниження рівня суспільної концентрації, емоційної стійкості, критичності сприйняття інформації та готовності до тривалого функціонування в умовах війни. І це не втрата патріотизму чи підтримки держави, це – конденсаторний ефект постійного стресу, інформаційного перевантаження, невизначеності, втрат, емоційного виснаження. Особливої актуальності означена проблема набуває для системи національного спротиву, ефективність якої безпосередньо залежить від рівня внутрішньої стійкості суспільства, довіри до державних інституцій, готовності населення підтримувати Сили оборони України та зберігати здатність до організованого спротиву в умовах затяжної війни. Специфікою сучасної війни є те, що ворог прагне не лише досягти

військових результатів на полі бою, а й виснажити здатність українського суспільства до довготривалого опору. Саме тому зі зниженням його просування на фронті зростає температура його інформаційної агресії. І саме тому інформаційний вплив ворога частіше спрямовується не на миттєве переконання чи зміну поглядів, а на формування атмосфери постійної психологічної втоми, безперервної тривожності, емоційного виснаження та втрати внутрішньої концентрації. Одним із індикаторів інформаційної втоми є постійне перебування суспільства у стані надлишкового інформаційного навантаження. Масовані повітряні удари, втрати, мобілізація, руйнування, економічні проблеми та тривалість війни формують безперервний негативний інформаційний фон, який поступово виснажує механізми психологічної адаптації людини.

Особливо небезпечним стає звикання суспільства до критичних умов. Постійна присутність війни в інформаційному просторі призводить до зниження рівня внутрішньої мобілізації, втрати відчуття гостроти загрози та формування хибного уявлення про можливість «адаптації» до війни без активної участі у спротиві держави. Вкрай важливо чітко усвідомлювати: для України ця війна не має компромісного або «відкладеного» характеру, оскільки рф веде боротьбу не лише проти державності України, а й проти самої здатності українського суспільства існувати як окрема політична, культурна та безпекова спільнота. За таких умов інформаційна втома стає не лише психологічною проблемою, а одним із чинників ризику існування системи національного спротиву. Отже, протидія інформаційній втомі суспільства потребує системної державної політики, яка має поєднувати інформаційні, психологічні, організаційні та безпекові механізми і центральним її напрямом вбачається формування культури інформаційної стійкості суспільства, зокрема, розвитку критичного сприйняття інформації, усвідомлення механізмів інформаційно-психологічного впливу, зниження залежності від маніпуляцій, підвищення рівня інформаційної відповідальності. Особливого значення набуває підтримання довіри між суспільством, державою та Силами оборони України. Інформаційний вакуум, затягування офіційних роз'яснень, реагувань на провокативні публікації внутрішніх опонентів, ігнорування суспільно чутливих проблем створюють сприятливі умови для поширення маніпулятивних наративів. Не менш важливим є збереження внутрішньої єдності суспільства. Ворог активно експлуатує теми мобілізації, соціальної нерівності, регіональних відмінностей, мовних, політичних суперечностей для посилення внутрішньої конфліктності.

Штучне протиставлення «фронту і тилу», військових і цивільних, різних соціальних груп безпосередньо спрацьовує на виснаження України.

В свою чергу, військова складова територіальної оборони, - Сили ТрО відіграють важливу роль у підтриманні суспільної стійкості, адже саме вони, завдяки зв'язку з громадами, населенням, є одним елементом збереження суспільної організованості та локальної стійкості в умовах тривалої війни.

Таким чином, інформаційна втома суспільства в умовах тривалої війни поступово перетворюється на один із визначальних індикаторів ризику для системи національного спротиву України.

За таких умов суспільна стійкість, інформаційна дисципліна, внутрішня єдність та здатність протидіяти деструктивному інформаційному впливу стають не лише питаннями інформаційної безпеки, а складовими збереження державності та самого існування України.

Маковський В. Ю.
Москалик С. В.
Вінник В. В.
Житомирський військовий інститут імені С. П. Корольова

## РОЗВИТОК КОГНІТИВНОЇ ГНУЧКОСТІ ЯК ІНСТРУМЕНТУ ПРОТИДІЇ ВТОМІ ТА ПРОФЕСІЙНОМУ ВИГОРАННЮ ПЕРСОНАЛУ З РОЗМІНУВАННЯ

Діяльність фахівців із розмінування (саперів) характеризується екстремальними когнітивними та емоційними навантаженнями. Постійна концентрація уваги в умовах смертельної небезпеки неминуче призводить до накопичення втоми та ризику професійного вигорання. Традиційні методи підготовки часто фокусуються на технічних навичках, проте психологічна стійкість потребує розвитку когнітивної гнучкості — здатності мозку швидко перемикатися між завданнями та адаптуватися до мінливих умов.

Робота сапера пов'язана зі станом «хронічного пильного очікування».

Основні фактори навантаження включають:

монотонність при високій ціні помилки;

сенсорну депривацію або перевантаження (робота в захисному костюмі, використання металодетекторів);

когнітивний дисонанс при зіткненні з новими типами «мінних пасток».

Ці фактори призводять до когнітивного ригідизму — стану, за якого фахівець починає діяти за шаблоном, втрачаючи пильність, що є першою стадією вигорання.

Когнітивна гнучкість дозволяє фахівцеві зберігати продуктивність завдяки:

дивергентному мисленню: здатності бачити нестандартні рішення у стандартних ситуаціях (наприклад, розпізнавання замаскованого ВНП);

ефективному перемиканню уваги: швидкому переходу від процесу пошуку до аналізу загрози без втрати концентрації;

зниженню рівня стресу: гнучкість дозволяє сприймати зміни обстановки не як загрозу, а як робоче завдання, що знижує психоемоційне виснаження.

При накопиченні втоми у персоналу спостерігається звуження «поля уваги» та уповільнення реакцій. Когнітивна гнучкість виступає буфером, дозволяючи мозку оптимізувати використання нейронних ресурсів. Розвинена навичка адаптації допомагає саперу вчасно ідентифікувати момент зниження власної ефективності (метакогнітивний моніторинг) та ініціювати перерву, запобігаючи нещасному випадку.

Для профілактики вигорання та протидії втомі пропонується впровадження таких технік:

сценарні тренінги з елементами невизначеності: навчання роботі в умовах, коли стандартні протоколи потребують швидкої модифікації «на ходу»;

майндфулнес-техніки: розвиток навички усвідомленої присутності для контролю за рівнем автоматизму в діях;

нейропластичні вправи: використання спеціалізованих тренажерів на перемикання уваги та придушення домінуючої реакції (тести Струпа та їх аналоги).

Розвиток гнучкості мислення сприяє формуванню «активного копінгу» (active coping). Замість емоційного відсторонення, характерного для вигорання, фахівець зберігає інтерес до професії та когнітивну залученість. Це не лише підвищує безпеку поточних операцій, а й подовжує професійне довголіття персоналу.

Когнітивна гнучкість є критично важливим компонентом інформаційно-психологічної безпеки сапера. Інтеграція методів розвитку адаптивного мислення в систему підготовки персоналу з розмінування дозволяє суттєво знизити рівень професійного вигорання, нівелювати негативний вплив втоми та забезпечити високу надійність виконання завдань в умовах підвищеного ризику.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Варламова І. Є.
Ухо Д. В.
Військовий інститут Київського національного університету
імені Тараса Шевченка

# ЗАГРОЗИ КОМПРОМЕТАЦІЇ OPSEC УКРАЇНСЬКИХ ВІЙСЬК ЧЕРЕЗ ЦІЛЬОВІ ФІШИНГОВІ АТАКИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

OPSEC (Operations Security) – стосується процесу ідентифікації, контролю та захисту конфіденційної інформації, яка може бути використана проти ворога (особи, організації або державним органом влади). Мета OPSEC - запобігти витоку критичної інформації, яка може бути використана ворогом для зловмисних цілей. Безпека особистості досягається шляхом дотримання певного алгоритму, а саме: ідентифікація інформації, аналіз загроз, вразливостей, оцінка ризиків, протидія. При цьому важливо ідентифікувати загрозу, як таку, що має намір та можливості, оскільки без одного з цих факторів загроза не буде сприйматися (необхідно поставити питання: “Яка мета? Які можливості зашкодити об’єкту впливу?”).

Для збору інформації про цільову аудиторію, розглянемо Збройні Сили України (ЗСУ), які систематично піддаються кібератакам зі сторони російської федерації. Противник збирає інформацію через: соціальні мережі (наприклад Instagram, Facebook, TikTok, Treads, які можуть зберігати фото, відео, відмітки геолокацій, Meta дані тощо) та месенжери (наприклад Telegram, WhatsApp, Viber, Signal, де безпосередньо зберігаються переписки та важливі дані). Також ворог може прослуховувати особисті телефонні розмови або спілкування через месенджери, таким чином визначаючи проблеми військовослужбовців та відслідковуючи вразливості та страхи, якими через особисті телефонні розмови часто переймаються військовослужбовці. Серед найпоширеніших методів соціальної інженерії, можна виділити фішинг. Невинне на перший погляд посилання або файл масово розсилаються військовослужбовцям та їх родинам, для подальшого зламування акаунтів.

Противник шукає вразливості, які основані на зборі даних методами, розглянутими вище, потім створює контент, який зачіпає потреби військовослужбовців (або їх сімей), буквально змушуючи їх перейти за посиланням, або надати доступ до своїх конфіденційних даних тощо. Хакери та

зловмисники не одразу використовують дані, які вони отримали у ході фішингової атаки. Ворог може систематично збирати дані з акаунтів або одразу починати викачувати потрібну інформацію безпосередньо з того пристрою, який був взламаний. Психологічними тригерами для українських військовослужбовців, в першу чергу, являється тема родини (наприклад, смс повідомлення із дитячого садочку на медичні потреби доньки, перегляд нових фотографій сина з футболу тощо). Також чутливою є тема збору на техніку для підрозділів або допомогу пораненим побратимам. Такі повідомлення можуть надходити в месенджери, E-mail адреси, смс в телефоні, телефонні дзвінки. Вони можуть пересилатися навіть від рідних, які, як і військовослужбовці ЗСУ, переймаються за родину, побратимів їх члена родини.

Технічний аспект полягає у тому, що військовослужбовці відкриваючи небезпечний файл можуть заразити свої пристрої шкідливим програмним забезпеченням (ПЗ) і надати дані стороннім особам. Витік інформації є небезпечним не лише через те, що стороння особа отримує доступ до конфіденційної інформації військовослужбовця, а й через ризики заволодіти критичною інформацією про підрозділи (кількісний, якісний склад, розташування, переміщення ЗСУ тощо). Наприклад, військовослужбовцю надходить файл із такими назвами, як "терміновий звіт від начальника штабу" або "новий порядок нарахування грошового забезпечення", відкриваючи цей файл він дозволяє гаджету з автоматичними налаштуваннями завантажити шпигунську програму. Військовий може навіть не зрозуміти, що так просто відбулася фішинг-атака, яка в подальшому може розширитись на особисті пристрої побратимів або інше ПЗ підрозділу. Найгучніші випадки таких атак фішингу були у 2024-2025 роках, коли військовим надходили файли з назвами "список нарядів", "звіт наради", "маршрут виїзду на завтра" тощо на месенджери Signal та WhatsApp.

Отже, для максимального забезпечення безпеки критичної інформації недостатньо тільки встановити якісне ПЗ, яке буде виявляти всі підозрілі програми. В першу чергу, треба навчити себе та підрозділ базовим навичкам OPSEC, щоб чітко знати як діяти у різних ситуаціях. Свідомі та вмілі дії щодо інформаційної гігієни, зможуть знешкодити атаку ще на початковому етапі, не давши противнику жодного шансу на подальше розповсюдження.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Колотуша Я. В.
Військовий інститут Київського національного університету
імені Тараса Шевченка

# СОЦІАЛЬНІ МЕРЕЖІ ЯК СЕРЕДОВИЩЕ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ

Інформаційно-психологічні операції – це комплекс заходів, спрямованих на вплив на свідомість, емоційний стан, поведінку та прийняття рішень цільовою аудиторією шляхом поширення спеціально сформованої інформації. Основною метою таких операцій є зміна ставлення аудиторії до певних подій, явищ або суб'єктів, формування необхідних поведінкових моделей та створення вигідного інформаційного середовища.

Ключова мета ворожих ІПСО – викликати паніку, посіяти страх, підірвати довіру до державних інституцій та схилити громадян до рішень, вигідних противнику. Фактично, інформація стала повноцінним елементом гібридної війни.

Інтернет-середовище створює ідеальні умови для проведення інформаційних операцій з кількох причин. По-перше, швидкість поширення інформації в мережі практично миттєва, що дозволяє досягнути максимального охоплення за мінімальний час. По-друге, анонімність створює безпечні умови для маніпуляторів – можна легко сформувати мережу фейкових акаунтів, які виглядатимуть правдиво.

Ще одним чинником ефективності соціальних мереж як середовища інформаційно-психологічного впливу є алгоритмічна організація інформаційних потоків. Сучасні алгоритми формують для користувачів індивідуалізований інформаційний простір, у межах якого посилюється ефект так званої «інформаційної бульбашки». У таких умовах людина здебільшого отримує контент, який підтверджує її наявні переконання, що знижує критичне сприйняття інформації та підвищує вразливість до маніпуляцій.

Серед основних методів реалізації інформаційно-психологічних операцій у соціальних мережах можна виокремити поширення дезінформації, використання бот-мереж, створення фейкових акаунтів, маніпуляцію емоційно забарвленим контентом та використання візуальних засобів впливу. Особливу небезпеку становить застосування технологій штучного інтелекту для генерації правдоподібного маніпулятивного контенту, зокрема deepfake-матеріалів, що значно ускладнює виявлення фальсифікацій.

Психологічний механізм впливу в соціальних мережах ґрунтується на активації когнітивних викривлень, зокрема ефекту повторення, соціального доказу та емоційного зараження. Багаторазове повторення певних повідомлень створює враження їхньої достовірності, навіть за відсутності фактичного підтвердження. Крім того, масова підтримка або схвалення певної інформації іншими користувачами формує у реципієнта відчуття її суспільної значущості.

В умовах зростання масштабів інформаційно-психологічних операцій важливого значення набуває розробка ефективних механізмів протидії. До основних напрямів належать підвищення рівня медіаграмотності населення, удосконалення алгоритмів автоматизованого виявлення маніпулятивного контенту, розвиток систем моніторингу інформаційного простору та формування навичок критичного мислення.

Таким чином, соціальні мережі виступають потужним середовищем реалізації інформаційно-психологічних операцій завдяки своїй масовості, швидкості поширення інформації, персоналізації контенту та високому рівню залучення користувачів. Це зумовлює необхідність комплексного підходу до вивчення механізмів інформаційного впливу та розробки ефективних інструментів захисту інформаційного простору.

Плаксій А. В.
Стафійчук В. В.
Військовий інститут київського національного університету
імені Тараса Шевченка

## ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Тема інформаційної безпеки України в умовах гібридної війни є надзвичайно актуальною в сучасному світі, оскільки інформаційний простір став одним із ключових інструментів впливу на суспільство, державу та міжнародну спільноту. В умовах російсько-української війни інформаційні атаки, дезінформація, пропаганда та психологічний тиск використовуються не менш активно, ніж військова сила. Саме тому питання захисту інформаційного простору України набуває особливого значення для забезпечення національної безпеки та збереження державного суверенітету.

Проблему інформаційної безпеки активно досліджували українські та зарубіжні науковці, серед яких Георгій Почепцов, Валерій Іванов, а також фахівці у сфері стратегічних комунікацій і кібербезпеки. Особливої уваги це питання набуло після 2014 року, коли Україна зіткнулася з масштабною інформаційною агресією з боку Російської Федерації, а після повномасштабного вторгнення у 2022 році проблема стала однією з центральних у сфері державної політики та медіакомунікацій.

У контексті гібридної війни проти України Росія активно застосовує інформаційні атаки як один із ключових інструментів впливу на населення. Зокрема, на початку повномасштабного вторгнення в інтернеті поширювалися фейкові новини про нібито капітуляцію України чи втечу вищого керівництва з Києва. Ці повідомлення були спрямовані на те, щоб посіяти паніку серед людей і підірвати моральний дух громадян. Іншою формою такої агресії стало створення й розповсюдження неправдивої інформації про дефіцит продуктів, пального чи відключення банківської системи. Унаслідок цього населення почало масово скуповувати товари та вилучати кошти, що додатково сприяло хаосу.

Одним із важливих компонентів гібридної війни стали кібератаки. Державні сайти, банківські установи та енергетичні компанії неодноразово ставали їх об’єктами, що тимчасово порушувало роботу окремих сервісів і сприяло поширенню внутрішнього безладу та недовіри до систем влади. Також противник активно використовує Telegram-канали та соціальні мережі для проведення інформаційно-психологічних операцій. Приклади включають фейкові новини про нібито великі втрати ЗСУ або хибні «інсайди» щодо рішень керівництва країни — усе це робиться для послаблення морального духу українців.

Окрему загрозу становлять дипфейки—змонтовані відео за допомогою технологій штучного інтелекту. Одним із найвідоміших випадків стало фейкове відео із закликами нібито від імені президента Володимира Зеленського до українських військових скласти зброю. Хоча цей матеріал і був викритий як підробка, його поширення підкреслило небезпеку сучасних технологій в умовах інформаційної війни. У відповідь Україна робить кроки для посилення захисту інформаційного середовища: розвиває фактчекінг, підвищує рівень медіаграмотності населення та впроваджує вдосконалені системи кіберзахисту.

Отже, інформаційна безпека є важливою складовою національної безпеки України в умовах гібридної війни. Захист інформаційного простору, розвиток

медіаграмотності населення, посилення кібербезпеки та ефективна державна інформаційна політика є необхідними умовами для протидії сучасним загрозам. Успішна боротьба на інформаційному фронті впливає не лише на внутрішню стабільність держави, а й на міжнародний імідж України та її здатність протистояти зовнішній агресії.

Райковський О. В.
Шевчук В. О.
Житомирський військовий інститут імені С. П. Корольова

## СОЦІАЛЬНІ МЕРЕЖІ – СЕРЕДОВИЩЕ ФОРМУВАННЯ КОЛЕКТИВНИХ ПЕРЕКОНАНЬ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Соціальні мережі — це платформи та додатки, призначені для спілкування, обміну інформацією, створення віртуальних спільнот. Вони дозволяють користувачам створювати профілі, публікувати власний контент, обмінюватися повідомленнями та взаємодіяти.

Соціальні мережі, характеризуються властивостями, які мають чималі відмінності від традиційних медіа. Зокрема вони полягають в охопленні та доступності до контенту. В соцмережах кожен користувач може бути автором, читачем і глядачем. Люди можуть ділитися інформацією, коментувати, та навіть впливати на створення самого матеріалу. Ця інтерактивність і є тією, значною відмінністю від традиційних медіа, де комунікація зазвичай одностороння. Тобто цифрові медіа більш доступніші до звичайного споживача. Таким чином у сучасному інформаційному світі соціальні мережі стали чи не основним каналом комунікації, поширення інформації та формування суспільної думки. В умовах збройного конфлікту їх роль ще більше зростає, адже всесвітня медіа мережа є не просто джерелом останніх новин, а часто і першоджерелом, яке формує суспільну думку.

За даними міжнародної платформи Statista, яка спеціалізується на зборі статистичних даних у 2025 році Facebook та Instagram мали понад три мільярди користувачів, майже два мільярди у TikTok і мільярд у Telegram. Ці мережі стали основним джерелом інформації про хід війни в Україні і не лише для світового співтовариства, а й українців зокрема. Відтак, дослідження процес формування

суспільної думки є важливим елементом розуміння сучасної інформаційної війни, адже ворог їх активно використовує і намагається дестабілізувати українське суспільство і світову громадську думку. Саме тому, соцмережі стали об'єктом у боротьбі за людський розум і основним інструментом інформаційно-психологічного впливу.

Завдяки часто спотвореному, а іноді й просто фейковому контенту, окремі наративи можуть швидко закріплюватися у свідомості. Цьому сприяють алгоритми роботи соцмереж і сам контент, який повинен викликати потрібні емоції, що мають найбільший рівень поширення (репостів) та впливу. Страх, тривога, гнів, розчарування, чи презирство сприяють швидкому розповсюдженню таких матеріалів, які під час ретельної перевірки виявляються домислом, чи навіть відверто брехнею. Проте "колективному інформаційному розуму" правда не завжди потрібна, адже емоційно поданий матеріал з "гарячими фактами" в в мережі людина схильна сприймати, як беззаперечну істину. Відтак, поширення дезінформації через соціальні мережі стає тим, ще одним "полем бою" на яке необхідно зважати, адже психологічний стан суспільства здатен повністю переломити хід реальних бойових дій. Саме тому, важливо протидіяти негативному інформаційному впливу, через соціальні мережі. Цьому сприятиме розвиток медіа грамотності, яка допоможе користувачам соцмереж критично сприймати матеріали та не зважати на різноманітні маніпулятивні технології.

Підсумовуючи можна зазначити, що соціальні мережі під час ведення бойових дій є не тільки можливістю швидкої комунікації у суспільстві, а й тим сучасним і потужним інструментом, який формує суспільну думку, впливаючи на емоційний стан населення. Зважаючи на всі описані ризики ця тема потребує подальшого наукового дослідження та розробки дієвих механізмів інформаційної протидії і навчання суспільства для розвитку медіа грамотності.

Світлічний І. В.
Науково-дослідний центр Державної спеціальної служби транспорту

# БІБЛІОГРАФІЧНИЙ АНАЛІЗ КОГНІТИВНО-ПСИХОЛОГІЧНИХ АСПЕКТІВ ВПЛИВУ ІНФОРМАЦІЙНИХ І ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ НА МОЛОДЬ В УМОВАХ ПОВНОМАСШТАБНОЇ ЗБРОЙНОЇ АГРЕСІЇ рф ПРОТИ УКРАЇНИ

**Постановка проблеми.** Для узагальнення сучасного досвіду у сфері інформаційної безпеки, інформаційних і психологічних операцій, шляхів протидії інформаційним загрозам в умовах повномасштабної збройної агресії рф проти України насамперед необхідно здійснити бібліографічний аналіз існуючих досліджень когнітивно-психологічних аспектів впливу ІПСО у поєднанні з аналітичним моніторингом цифрового інформаційного середовища. Окреслимо дану тематику в контексті впливу на молодь особовий склад Сил оборони України. Дослідження та міжнародні огляди доводять, що ІПСО противника системно таргетують молодь, спричиняють зниження довіри до інститутів держави, підвищення тривожності та когнітивні спотворення. Емпіричні оцінки вказують на зниження довіри до уряду на 15–25% у разі тривалих кампаній, що є лише однією з цілей зазначених ІПСО.

**Стан наукових досліджень.** В українському науковому дискурсі вказана проблематика має ґрунтовну теоретичну базу. Зокрема, психоемоційні наслідки впливу дезінформації досліджує Я. Бондаренко (2024), фокусуючи увагу на дестабілізації стану цільової аудиторії, зростанні рівня тривожності, стресу та розчарування. А. В. Ковалевська-Славова (2023) виокремлює сугестивні вербальні й екстралінгвістичні маркери пропаганди, які спричиняють когнітивну викривленість реципієнтів. Навчальні модулі репрезентовано в посібнику А. Мегель та М. Яремчук (2022). Вагомий внесок зробили вітчизняні дослідники Г. Почепцов, В. Лизанчук, І. Валюшко (2022–2024 рр.), а також сучасні науковці М. Кувік (2020), О. Уманець (2022), І. Живоглядов (2024), А. Галата, І. Ковілько, Є. Хоменко, В. Будз, С. Шумлянський та інші.

**Виклад основного матеріалу.** У контексті війни та молоді ключову роль почали відігравати соціальні мережі, месенджери (зокрема Telegram, TikTok), блоги та агенти штучного інтелекту, які підсилюють маніпулятивний потенціал інформаційного середовища, провокують сумніви щодо доцільності подальшої

підтримки Сил оборони України та сприяють деградації довіри до командування й уряду.

Нині (на травень 2026 р.) ІПСО противника охоплюють переважно три напрями: дискредитація процесу мобілізації та військового командування, президента та його оточення, корупційні та економічні скандали. Для реалізації цих планів створюються скомпрометовані документи начебто від органів влади (НБУ, ДФС, СБУ тощо). У відеоконтенті, а також у вербальних і екстралінгвістичних маркерах у 2026 році репрезентовано низку фейкових наративів: про те, що ломбарди почали масово приймати протези ветеранів як заставу; що західні спецслужби буцімто використовують територію для глобального транзиту наркотиків під прикриттям військової допомоги; що телефонні шахраї виманили у французів 42 мільйони євро на ППО для іноземних баз Франції; що в Харківській області здійснюється примусова мобілізація жінок; що в кабінеті Президента України помітили оригінальне полотно Поля Сезанна, викрадене з Італії; що влада видає пенсіонерам елітні супові набори зі свинячих голів та копит; мігрантів з Індії помітили за пранням у гірській річці на Івано-Франківщині; парафіянам Української православної церкви доведеться проходити процедуру перехрещування; а також подібне. Продовжують поширюватися й теми про "бойових комарів", біолабораторії, бойових птахів, біологічну зброю, згадується Памела Андерсон, наркотрафік, а також твердження про те, що православні храми в Україні нібито переобладнують на кінотеатри та дискотеки, а WADA буцімто дозволило українським спортсменам вживати седативні препарати через психологічний стрес.

Проте парадоксальний адаптивний потенціал емоційно-абсурдних фейків у формуванні психологічної стійкості українців полягає в тім, що фейки стають тригером психологічної резильєнтності. Спостерігається **феномен когнітивної адаптації:** міфи про бойових комарів чи перетворення храмів на дискотеки втрачають силу і набувають терапевтичної функції. Згідно з теорією когнітивної оцінки стресу, зіткнення з гіперболізованою дезінформацією запускає процес раціоналізації. Коли зміст повідомлення (наприклад, прийом протезів у ломбардах) кардинально суперечить емпіричній реальності реципієнта, первинна реакція страху трансформується у комічне сприйняття. Гумор у цьому контексті діє як захисний механізм подолання стресу. Висміювання наративів знижує рівень кортизолу, зменшує психологічну напругу та сприяє емоційному розвантаженню від перманентного дистресу.

Генерація мемів на основі фейків виконує функцію соціальної консолідації. Віртуальна деконструкція пропаганди шляхом створення сатиричного контенту формує відчуття колективної переваги над супротивником. Українці, трансформуючи загрозу (дезінформацію) на об'єкт кепкування, повертають собі локус контролю над інформаційним середовищем. Як наслідок, непрофесійність і карикатурність російських ІПСО не досягають мети підриву морального духу, але й парадоксальним чином підвищують когнітивну стійкість українського суспільства до інформаційних атак.

*Когнітивно-психологічні аспекти впливу ІПСО на військовослужбовців.*

Військовослужбовці є цільовою групою, оскільки їхній психічний стан безпосередньо пов'язаний із боєздатністю підрозділів. У вітчизняних дослідженнях відповідні фейки поділяють на дві групи: деморалізуючі (про оточення, відсутність підтримки, зраду, втечі тощо) та гротескно‑абсурдні (про голод, тотальну корупцію, торгівлю протезами, непокору та СЗЧ).

З позицій стресово‑травматичної парадигми перші фейки націлені на підрив базових відчуттів безпеки та передбачуваності, підсилюють бойову втому, формують уявлення про знецінення жертви й відсутність справедливості, збільшують ризики емоційного вигорання. Натомість другий тип – надмірно абсурдні, легко спростовувані наративи – у сучасному дискурсі зафіксовано як тригер для протилежної реакції: зневаги, іронії та позитиву. Так, польові спостереження демонструють, що регулярне викриття й висміювання фейків ворога може виконувати для військових функцію психологічного щеплення. Розпізнавання, розбір маніпуляцій та перетворення їх на жарти підвищують медіаграмотність, зміцнюють довіру до власних джерел інформації, а тому формують стійкі когнітивні схеми опору дезінформації.

Завдяки бібліографічному аналізу когнітивно-психологічних аспектів впливу ІПСО на молодь у поєднанні з аналітичним моніторингом цифрового інформаційного середовища було виявлено основні патерни поширення (за емоційно-комунікативним відгуком та ступенем психологічного впливу типів):

*тематика міжнародної допомоги* (корупція, фінансування, забезпечення) має найвище загальне охоплення (понад 15 млн), оскільки ці наративи орієнтовані не лише на внутрішню, а й на західну аудиторію (час реакції аудиторії становить близько 3,8 години);

*емоційно-абсурдні фейки* мають порівняно невелике (близько 5,4 млн) охоплення, а час офіційної реакції на них становить понад 12 годин. Утім, саме

ця категорія генерує найвищий рівень емоційного та комунікативного відгуку як серед молоді, так і серед статистично значущої частки людей старшого віку, хоча й із діаметрально протилежними психологічними наслідками.

*Окремої класифікації потребує вектор вербування неповнолітніх через цифрові платформи* (сегмент із рівнем латентного залучення до 3–9%). Цей тип прицільно експлуатує когнітивну незрілість, схильність до ризикованої поведінки та фінансову вразливість підлітків, трансформуючи когнітивний вплив у реальні деструктивні та кримінальні дії.

Структура тематичного розподілу реакцій молодіжної аудиторії свідчить про нерівномірну сприйнятливість (ступінь впливу) різних типів ІПСО:

*емоційно-абсурдні фейки* (90%) про комарів, ломбарди з протезами, біолабораторії, індусів демонструють найвищий рівень залучення, трансформуються в меметичні форми комунікації, стікерпаки у Telegram та тренди в TikTok, слугують інструментами іронії та психологічного відновлення;

*тема міжнародної допомоги* (80%) викликає значний інтерес, пов'язаний із майбутнім, молодь активно слідкує за постачанням сучасної зброї (F-16, далекобійні ракети) і обговорює у профільних чи територіальних спільнотах;

*наративи щодо ухилення від мобілізації* (55%) викликають помірний стійкий інтерес, особливо у контексті обговорення правил виїзду за кордон;

*дискредитація командирів, військового керівництва та політиків* (45%) є класичними пропагандистськими наративами, проте характеризується нижчим рівнем резонансу серед молодіжної аудиторії та військовослужбовців.

**Висновки та пропозиції.** Бібліографічний аналіз когнітивно-психологічних аспектів досліджень впливу ІПСО на молодих людей та особовий склад Сил оборони України в умовах повномасштабної збройної агресії рф у поєднанні з аналітичним моніторингом цифрового інформаційного середовища засвідчив домінування теоретичних підходів у сучасному українському науковому дискурсі. Наявність поведінкових загроз, зокрема вербування неповнолітніх, зумовлює необхідність у коротко- та середньостроковій перспективі активізувати прикладні наукові дослідження, орієнтовані на отримання емпірично верифікованих результатів когнітивних, емоційних і поведінкових наслідків впливу, розроблення практико-орієнтованих моделей підвищення резильєнтності молодих людей, включаючи неповнолітніх та створення практичних інструментів протидії дослідженому деструктивному впливу.

Стафійчук В. В.
Плаксій А. В.
Військовий інститут Київського національного університету
імені Тараса Шевченка

# РОЛЬ МЕДІАГРАМОТНОСТІ У ЗМІЦНЕННІ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ СТІЙКОСТІ НАСЕЛЕННЯ УКРАЇНИ

У сучасному світі боротьба за території дедалі частіше супроводжується боротьбою за свідомість людей. Інформаційний вплив став важливим інструментом досягнення політичних і воєнних цілей, а тому здатність громадян критично сприймати інформацію перетворюється на важливий елемент стійкості держави та суспільства.

У цьому контексті медіаграмотність виступає важливим інструментом захисту особистості від інформаційних загроз. Медіаграмотність – це сукупність знань, умінь і навичок, які дають можливість критично оцінювати інформацію, визначати її джерела, виявляти маніпулятивні технології та приймати обґрунтовані рішення на основі перевірених фактів. Медіаграмотна людина здатна аналізувати інформаційні повідомлення, розрізняти факти та судження, а також усвідомлювати можливі цілі інформаційного впливу.

Важливою складовою інформаційно-психологічної стійкості є здатність громадян протистояти деструктивному інформаційному впливу. Розвинені навички медіаграмотності дозволяють зменшити ризик поширення фейків, знижують рівень паніки та сприяють формуванню об'єктивного сприйняття подій. Крім того, критичне мислення допомагає громадянам уникати маніпуляцій, що особливо актуально в умовах ведення інформаційної війни.

Суттєву роль у розвитку медіаграмотності відіграють освітні заклади, засоби масової інформації та державні інституції. В Україні реалізуються різноманітні освітні програми та інформаційні кампанії, спрямовані на формування навичок критичного сприйняття інформації серед різних вікових груп населення. Особливо важливим є впровадження елементів медіаосвіти у систему підготовки молоді, майбутніх військовослужбовців та фахівців сектору безпеки й оборони.

Таким чином, медіаграмотність є одним із ключових чинників забезпечення інформаційно-психологічної стійкості населення України в

умовах повномасштабного вторгнення Російської Федерації в Україну. Вона сприяє підвищенню здатності громадян протидіяти дезінформації, критично оцінювати інформаційні повідомлення та зберігати психологічну стійкість в умовах постійного інформаційного тиску. Подальший розвиток медіаграмотності має розглядатися як важлива складова системи національної безпеки та ефективної протидії сучасним інформаційним загрозам.

Жураковська О. Р.
Військовий інститут Київського Національного університету
імені Тараса Шевченка

## ІНФОРМАЦІЙНЕ ПЕРЕВАНТАЖЕННЯ ЯК ФАКТОР ПСИХОЛОГІЧНОЇ ДЕСТАБІЛІЗАЦІЇ ОСОБИСТОСТІ

Сучасне інформаційне суспільство характеризується постійним збільшенням обсягів інформації, яку людина отримує через соціальні мережі, новинні ресурси та цифрові платформи. В умовах воєнного стану та активного розвитку медіапростору інформаційний вплив на особистість значно посилюється. Це створює підвищене когнітивне навантаження та негативно впливає на психоемоційний стан людини. У зв’язку з цим проблема інформаційного перевантаження набуває особливої актуальності в контексті інформаційно-психологічної безпеки особистості та суспільства.

Інформаційне перевантаження — це стан, за якого обсяг інформації перевищує можливості людини щодо її сприйняття, аналізу та критичного осмислення. Постійний потік повідомлень, новин і медіаконтенту знижує здатність особистості до концентрації уваги та раціонального аналізу інформації. Одним із наслідків такого впливу є формування кліпового мислення, за якого інформація сприймається фрагментарно та поверхнево. Це, у свою чергу, знижує рівень критичного мислення та підвищує ризик маніпулятивного впливу через дезінформацію, фейкові новини та емоційний контент.

Негативний вплив інформаційного перевантаження проявляється також в емоційній сфері. Постійне споживання новин про воєнні дії, кризові події та соціальні конфлікти спричиняє підвищення рівня тривожності, психологічної напруги та емоційного виснаження. У деяких випадках це може призводити до

хронічного стресу, апатії та інформаційної залежності. Особливу небезпеку становить неможливість ефективної фільтрації інформації, оскільки велика кількість суперечливого контенту ускладнює формування об'єктивного сприйняття подій та створює умови для інформаційно-психологічного впливу на свідомість людини.

Важливими засобами протидії негативним наслідкам інформаційного перевантаження є розвиток критичного мислення, формування навичок медіаграмотності та дотримання інформаційної гігієни. Людина повинна вміти аналізувати інформацію, перевіряти джерела та свідомо контролювати власний інформаційний простір. Важливе значення має також психологічна саморегуляція, яка сприяє збереженню емоційної стійкості в умовах постійного інформаційного впливу.

Отже, інформаційне перевантаження є одним із чинників психологічної дестабілізації особистості в сучасному суспільстві. Надмірний інформаційний вплив негативно позначається на когнітивній та емоційній сферах людини, знижує рівень критичного мислення та психологічної стійкості. Формування медіаграмотності та інформаційної культури є необхідною умовою забезпечення інформаційно-психологічної безпеки особистості та суспільства.

Нечаєв О. О.
В/ч А0987

## ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ ІНФОРМАЦІЙНИХ І ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ

Сучасне безпекове середовище характеризується постійним зростанням ролі інформації як одного з ключових ресурсів для досягнення інтересів, просування та нав'язування власних наративів від тактичного до стратегічного рівня. Поряд з традиційними формами застосування військових сил та засобів, дедалі більшого значення набувають психологічні операції (далі – ПсО), спрямовані на вплив на свідомість, поведінку та процес ухвалення рішень визначених цільових аудиторій. В умовах російсько-української війни ПсО стали невід'ємним елементом забезпечення національної безпеки та важливим інструментом підтримки воєнних, політичних і соціальних процесів.

Теоретичне підґрунтя ПсО базується на міждисциплінарному підході, який поєднує елементи психології, соціології, стратегічних комунікацій, інформаційної безпеки в поєднанні із застосуванням сучасних тенденцій розвитку інформаційних технологій та військового управління. Основною метою ПсО є формування необхідного інформаційного середовища, здатного забезпечити сприятливі умови для досягнення визначених політичних або воєнних цілей в інтересах держави як всередині, так і поза її межами. У сучасних умовах ефективність ПсО значною мірою залежить не лише від змісту повідомлень, але й від швидкості їх поширення, адаптивності до змін інформаційного простору (інформаційної повістки, трендів, течій тощо) та здатності враховувати особливості конкретних цільових аудиторій.

Одним із ключових аспектів ПсО є процес аналізу цільової аудиторії. Визначення мотивації, потреб, вразливостей, врахування географіних, культурних, соціальних та інформаційних звичок аудиторії дозволяє формувати повідомлення, які здатні досягти визначених об’єктів впливу та спонукати їх до зміни поведінки. Водночас особливого значення набуває оцінювання ефективності проведених заходів через використання показників результативності та аналіз змін у поведінці цільових аудиторій – чи спонукали дії до необхідної поведінкової зміни.

Практичний досвід сучасних конфліктів демонструє, що ПсО дедалі більше інтегруються як з традиційними засобами досягнення переваги на полі бою: від взаємодії з піхотними підрозділами та підрозділами безпілотних систем, так і в поєднанні з рухом опору та кіберпідрозділами. У результаті формується комплексний підхід до планування та проведення заходів впливу в інформаційному середовищі, у межах якого важливу роль відіграє координація дій між різними суб’єктами сектору безпеки і оборони Збройних Сил України.

Окремої уваги заслуговує вплив цифрових технологій та штучного інтелекту на розвиток ПсО. Використання автоматизованих систем аналізу даних, алгоритмів персоналізації контенту, генеративних моделей створення текстових, аудіо- та відеоматеріалів значно розширює можливості інформаційного впливу. Водночас це створює нові виклики, пов’язані з поширенням дезінформації, маніпулятивного контенту та зростанням складності виявлення інформаційних загроз.

Важливим практичним аспектом ПсО є забезпечення їх адаптивності до змін оперативної обстановки. Інформаційне середовище характеризується

високою динамікою, тому при плануванні та проведенні заходів в інформаційному та/або фізичному середовищі необхідно постійно враховувати можливість адаптації повідомлень, каналів комунікації, засобів та способів впливу залежно від реакції цільових аудиторій і дій (протидії) противника. Особливого значення набуває також здатність прогнозувати вторинні інформаційні ефекти, небажані результати та ймовірні контрзаходи противника з метою кореляції ведення психологічного впливу.

Таким чином, ПсО у сучасних умовах є важливим інструментом забезпечення інформаційної та воєнної безпеки держави. Їх ефективність визначається рівнем інтеграції теоретичних підходів, сучасних цифрових технологій та практичного досвіду застосування в умовах реального конфлікту.

Нечаєв О. О.
Огієнко С. С.
В/ч А0987

## УКРАЇНСЬКИЙ ТИСЯЧОЛІТНІЙ СВІТОГЛЯД ЯК ФУНДАМЕНТ КОГНІТИВНОЇ СТІЙКОСТІ НАЦІЇ В УМОВАХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ АГРЕСІЇ московії

Сучасна повномасштабна агресія московії проти України остаточно підтвердила: війна XXI століття – це насамперед війна за свідомість, історичну пам'ять і національну ідентичність. Інформаційно-психологічна складова стала одним із головних інструментів противника, спрямованим на руйнування суб'єктності України через системну фальсифікацію історії, крадіжку культурної спадщини та нав'язування ідеології "руского міра".

У цих умовах когнітивна безпека особистості та суспільства держави набуває стратегічного значення. Її основою є український національний світогляд, який формувався протягом тисячоліть на засадах свободи, вічевого звичаю, правдолюбства та духовно-природної єдності з рідною землею.

Мета дослідження – обґрунтування ролі тисячолітнього українського світогляду як головного чинника когнітивної стійкості нації та визначити стратегічні напрями його захисту й розвитку в умовах гібридної війни.

Український світогляд – один із найдавніших у Європі, його витоки сягають Трипільської та інших хліборобських культур, які існували на території

сучасної України. Для них характерні культ поклоніння Землі-Матері та органічна єдність людини з природою. Кругове планування протоміст із центральними майданами та оборонними спорудами свідчить про існування прото-вічевих форм колективного самоврядування – загальних зборів громади для вирішення спільних питань. Вже тоді (V–III тис. до н.е. ÷ III–V ст. н.е.) сформувався ***національний код світоглядності,*** який ***ґрунтується на: свободі, вічевому звичаю, любові до рідної землі та готовності їх захищати***.

Ця традиція набула класичного розвитку в період Русі (IX–XIII ст.) у формі вічевого права – верховного органу народовладдя, що вирішував питання війни, миру, обрання князів і розподілу ресурсів. У козацьку епоху (XV–XVIII ст.) вона еволюціонувала в Січову Раду – військово-соціальну форму народоправства з чіткою процедурою та принциповою рівністю козаків.

На противагу цьому, московська модель формувалася під впливом деспотичних традицій Орди і характеризується централізмом, підкоренням особистості державі та відсутністю традиції народовладдя. Вічева традиція стала наскрізним маркером цивілізаційної відмінності: український шлях – європейський, вічовий; московський – азійсько-ординський, авторитарний.

Саме цей тисячолітній світогляд є фундаментом української національної ідентичності та головною складовою когнітивної стійкості нації в протистоянні ворогам України.

московія століттями веде системну стратегічну когнітивну операцію: фальсифікує історію, привласнює спадщину Русі, нав’язує міф "триєдиного народу" та ідеологію "руского міра". Її мета – знищити українську суб’єктність, сформувати комплекс історичної меншовартості та позбавити народ права на власне минуле.

Для ефективної протидії необхідний перехід від оборонної тактики до наступальної стратегії:

1. Інституційне розмежування та термінологічна гігієна – офіційне закріплення термінів "Русь-Україна" та "московія" як маркер цивілізаційної межі "свій – чужий".

2. Ревізія системи історичної освіти та патріотичного виховання – викладання історії як боротьби двох цивілізаційних моделей: європейської – вічевої (української) проти азійської – деспотичної (московської).

3. Наступальна інформаційна стратегія на міжнародній арені – активне руйнування московоцентричних наративів у світовій історичній науці, освіті та медіа.

4. Формування когнітивного імунітету суспільства через освітні програми, засновані на усвідомленні глибинних цінностей українського світогляду – свободи, справедливості, вічевого звичаю та любові до рідної землі.

У сучасній гібридній війні збереження та зміцнення автентичного українського світогляду набуває характеру стратегічного завдання національної безпеки. Фальсифікація історії, апропріація спадщини Русі та ідеологія "руского міра" є інструментами світоглядного наступу, спрямованого в перетворення українців на безсуб'єктну периферію імперії.

Перемога у когнітивній сфері – повернення українському народові повної історичної правди та усвідомлення своєї цивілізаційної ідентичності. Це є важливою та необхідною передумовою загальної Перемоги над ворогами України. Нація, яка твердо усвідомлює свою тисячолітню ідентичність, здатна остаточно подолати ворогів як на полі бою, всередині країни так і у своїй свідомості.

Молодецька К. В., д-р техн. наук, проф.
Національний університет «Києво-Могилянська академія»

## РЕЗИЛЬЄНТНІСТЬ СУСПІЛЬСТВА В УМОВАХ ШІ-КЕРОВАНИХ ДЕЗІНФОРМАЦІЙНИХ КАМПАНІЙ

Повномасштабна збройна агресія рф проти України актуалізувала потребу переосмислення інформаційної безпеки не лише як захисту каналів комунікації чи протидії окремим кампаніям, а як забезпечення стійкості соціальної системи до цілеспрямованого впливу на довіру, судження та колективну поведінку. У цьому контексті резильєнтність суспільства доцільно визначати як спроможність індивідів, спільнот та інституцій своєчасно розпізнавати маніпулятивні інформаційні впливи, зберігати функціональну довіру до офіційних джерел, підтримувати якість публічного дискурсу та відновлювати комунікативну цілісність після дезінформаційних атак.

Сучасні концепції інформаційної безпеки дедалі більше зміщують аналітичний фокус із верифікації змісту повідомлень на вивчення інфраструктури впливу. Ідеться про когнітивну безпеку, протидію інформаційному маніпулюванню та втручанню, мережеву оборону від скоординованої неавтентичної поведінки, а також про стратегічні комунікації,

зорієнтовані на довгострокове зміцнення суспільної довіри. Спільним для цих підходів є розуміння дезінформації як адаптивного процесу, у якому повідомлення, платформи, псевдоавтентичні актори, емоційні тригери та алгоритмічна логіка поширення утворюють єдину операційну систему впливу.

Якісно новий рівень загроз пов'язаний із використанням систем штучного інтелекту (ШІ) для автоматизації інформаційних операцій. За матеріалами NATO Strategic Communications Centre of Excellence, сучасні ШІ-керовані системи здатні здійснювати розвідку цільових спільнот, створювати синтетичні персоналії з узгодженими біографіями та поведінковими моделями, генерувати контекстуально релевантний контент, координувати поширення повідомлень і коригувати тактику на основі зворотного зв'язку. Показовим є експериментальний сценарій, у якому протягом семи днів кампанія охопила понад 85 тис. користувачів, а 347 автентичних користувачів почали самостійно відтворювати тези кампанії. Отже, головним результатом стає не лише охоплення аудиторії, а перетворення реальних користувачів на вторинні вузли ретрансляції потрібного наративу.

Цей кейс демонструє обмеженість традиційної моделі протидії, зосередженої на спростуванні неправдивого змісту після його поширення. У разі ШІ-керованих кампаній загрозою є не окреме повідомлення, а фабрикація соціального доказу: створення видимості органічної згоди, масової підтримки або експертної легітимації. Такі кампанії експлуатують не лише інформаційні прогалини, а й когнітивні вразливості: потребу в належності до групи, схильність довіряти повторюваним твердженням, емоційну реактивність і залежність від рекомендаційних алгоритмів. Відтак резильєнтність має вимірюватися не тільки рівнем медіаграмотності, а й спроможністю суспільства не піддаватися штучно сконструйованим сигналам консенсусу.

Перспективною видається багаторівнева модель суспільної резильєнтності. На індивідуальному рівні вона передбачає розвиток навичок латеральної перевірки, розпізнавання емоційно насичених маніпулятивних повідомлень та усвідомлення меж власної когнітивної автономії. На рівні спільнот важливими є сталі практики взаємної верифікації, підтримка якісної модерації та формування довіри до локальних авторитетів, здатних пояснювати складні події без спрощень і поляризації. На інституційному рівні необхідні прозорі кризові комунікації, системне викриття скоординованих мереж впливу,

співпраця держави, медіа, громадянського суспільства й платформ. На технологічному рівні пріоритетом є не лише маркування синтетичного контенту, а й виявлення координації, поведінкових аномалій та неавтентичних мережевих патернів.

Отже, резильєнтність суспільства в інформаційній безпеці слід розглядати як комплексну спроможність захищати епістемічну інфраструктуру демократії - довіру, перевірюваність, відповідальну публічну дискусію та сталі механізми ухвалення рішень. В умовах поширення ШІ-керованих дезінформаційних кампаній ефективна протидія має переходити до превентивного посилення когнітивної, інституційної та технологічної стійкості. Для України, яка перебуває в умовах тривалої інформаційно-психологічної агресії, така модель є необхідною умовою збереження суспільної суб'єктності та демократичної керованості.

**ПАНЕЛЬ 3**

**Актуальні проблеми інформаційної безпеки**

Киричик С. М.
Військовий інститут танкових військ НТУ «ХПІ»

# ЕЛЕКТРОМАГНІТНІ ПРОЯВИ МОБІЛЬНИХ ПРИСТРОЇВ ЯК ФАКТОР ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДРОЗДІЛІВ ТАКТИЧНОГО РІВНЯ

У сучасних умовах ведення бойових дій інформаційна безпека підрозділів нерозривно пов’язана з контролем електромагнітного середовища. Широке використання особовим складом смартфонів та інших мобільних пристроїв створює додаткові джерела радіовипромінювання, які можуть бути виявлені засобами радіоелектронної розвідки противника та використані як демаскуючі ознаки активності військ. Особливої актуальності ця проблема набуває на тактичному рівні, де навіть короткочасне порушення електромагнітної дисципліни здатне призвести до розкриття місцезнаходження підрозділу.

Метою роботи є експериментальна оцінка впливу режимів роботи мобільних пристроїв та їх групового використання на електромагнітну обстановку і визначення практичних наслідків для забезпечення інформаційної безпеки підрозділів.

Дослідження проведено із застосуванням портативного аналізатора спектру SA6 у діапазонах 800-900 МГц, 1710-1785 МГц та 2400-2483 МГц, що відповідають роботі систем стільникового зв’язку та бездротових мереж Wi‑Fi. Вимірювання виконувалися у відкритій місцевості та в міському середовищі. У ході експерименту аналізувалися такі режими роботи мобільних пристроїв: режим польоту, режим очікування, передача даних, голосовий зв’язок і робота в режимі точки доступу Wi‑Fi. Окремо досліджувався вплив одночасної роботи групи з 13 смартфонів.

Установлено, що навіть у режимі очікування мобільні пристрої періодично передають службові сигнали до базових станцій стільникового зв’язку. Під час передачі даних і голосового зв’язку інтенсивність випромінювання істотно зростає. Найбільш виражені зміни електромагнітної обстановки спостерігаються під час одночасного виходу групи пристроїв із режиму польоту, коли відбувається їх реєстрація в мережі та виникають короткочасні, але потужні спектральні сплески.

У діапазоні 2,4 ГГц встановлено, що робота смартфонів у режимі точки доступу Wi‑Fi формує стійке широкосмугове випромінювання. Якщо один пристрій створює локальний вплив, то одночасна робота групи смартфонів

призводить до значного підвищення рівня електромагнітного фону та ускладнення спектральної картини. Це свідчить про наявність ефекту масштабування: зі збільшенням кількості пристроїв зростає ймовірність їх виявлення технічними засобами спостереження.

Практичне значення отриманих результатів полягає у підтвердженні того, що мобільні пристрої є потенційним джерелом витоку інформації про активність підрозділів. Сформовані ними електромагнітні прояви можуть використовуватися противником для виявлення районів зосередження особового складу, пунктів управління та інших важливих об'єктів. У цьому контексті дотримання режимів радіомовчання, обмеження використання персональних засобів зв'язку та контроль бездротових інтерфейсів є важливою складовою операційної безпеки та захисту інформації.

Таким чином, результати експериментального дослідження підтверджують, що навіть побутові мобільні пристрої здатні суттєво впливати на електромагнітне середовище та створювати характерні демаскуючі ознаки. Отримані закономірності доцільно враховувати під час організації електромагнітної дисципліни, підготовки військових фахівців та розроблення практичних рекомендацій щодо забезпечення інформаційної безпеки підрозділів тактичного рівня.

Кліщ А. Р.
Шейгас В. В.
Житомирський військовий інститут імені С. П. Корольова

## СТВОРЕННЯ АЛГОРИТМУ МОДЕЛЮВАННЯ ТА АНАЛІЗУ СПЕКТРАЛЬНИХ ПРОФІЛІВ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ СИГНАЛІВ ЯК МЕТОД ДІАГНОСТИКИ ТА ЗАПОБІГАННЯ ВИТОКАМ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Сучасні системи інформаційного захисту стикаються з дедалі витонченішими загрозами, серед яких побічні канали витоку (електромагнітне випромінювання, акустичні сигнали, вібрації тощо) займають особливе місце. Їхня особливість у тому, що вони не порушують логіку функціонування інформаційної системи, а отже – не помітні для звичайного програмного захисту. Основний інструмент боротьби з цими загрозами – інструментальний

контроль, який передбачає виявлення таких каналів за допомогою спеціалізованих технічних засобів.

Втім, ефективність інструментального контролю значною мірою залежить від кваліфікації фахівця, що його здійснює. Неправильне розташування антен, неврахування резонансних частот, невірна інтерпретація спектрального аналізу – усе це призводить до пропущених загроз. Крім того, ручна перевірка великої кількості пристроїв є вкрай трудомісткою, особливо у бойових військових частинах. Тому людський фактор стає серйозною вразливістю в системі технічного захисту інформації.

Усунути або мінімізувати вплив людського фактору можливо за рахунок автоматизації процесу інструментального контролю. Це передбачає створення комплексної системи, що складається з апаратних і програмних компонентів. Апаратна частина включає сенсори, які здатні фіксувати широкий спектр побічних сигналів – від низькочастотних коливань до високочастотних електромагнітних хвиль. Ці сенсори підключаються до центрального блоку обробки, де на базі заздалегідь закладених шаблонів і алгоритмів відбувається розпізнавання потенційно небезпечних сигналів.

Програмна частина забезпечує аналіз отриманих даних з використанням методів машинного навчання, зокрема кластеризації та виявлення аномалій. Це дає змогу системі вивчати попередні результати, адаптуючи свої критерії до нових загроз. Таким чином, система здатна виявляти навіть ті типи витоків, які не були закладені в початковому шаблоні. Оператор у такій системі виступає не як контролер, а як спостерігач і аналітик, що отримує вже оброблені дані з висновками.

Для подальшого розвитку, є можливість створення інтелектуальних розподілених систем інструментального контролю, де точки збору даних розміщені у різних зонах об’єкта і взаємодіють між собою через захищені канали. Така система зможе аналізувати витоки в реальному часі, створювати карту «загрозливих зон» і навіть прогнозувати напрямок потенційного витоку.

Крім того, інтеграція систем автоматичного контролю з інформаційними панелями кіберзахисту військової частини, дозволить об'єднати технічний і програмний моніторинг у єдину платформу. Це сприятиме прийняттю рішень на рівні керівництва без залучення вузькопрофільних інженерів. Зрештою, розвиток штучного інтелекту відкриває шлях до створення самонавчальних

систем, які будуть не тільки виявляти витоки, але й пропонувати контрзаходи у відповідь на загрозу.

Отже, інструментальний контроль захищеності від витоку побічними каналами є критично важливим для збереження конфіденційної та службової інформації. Проте його ефективність часто обмежується людськими можливостями. Автоматизація процесу контролю дозволяє підвищити точність, прискорити обробку сигналів і мінімізувати ризик пропущених витоків. Розвиток таких систем – це крок до сучасного інформаційного війська, де технічна безпека буде забезпечена не лише засобами, а й інтелектом.

Романчев А. М.
Шейгас В. В.
Житомирський військовий інститут імені С. П. Корольова

## ІНТЕГРАЦІЯ СЕНСОРНИХ СИСТЕМ У ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЯК ЗАСІБ ВИЯВЛЕННЯ МУЛЬТИКАНАЛЬНИХ ЗАГРОЗ

На сучасних об'єктах інформаційної діяльності спостерігається значне ускладнення структури інформаційних потоків. Поширеним залишається витік інформації через так звані технічні канали, зокрема: електромагнітні випромінювання, акустичні хвилі, вібрації, теплові сигнатури тощо. Існуючі системи аналізу здебільшого вузькопрофільні – кожна з них охоплює лише один тип сигналу або не має можливості повного міжканального аналізу. У результаті значна частина потенційних загроз залишається не виявленою, та у противника залишається можливість несанкціонованого доступу до службової інформації.

Запропоноване рішення полягає у створенні єдиного інтелектуального програмного середовища, яке здатне обробляти інформацію з різнорідних сенсорів та здійснювати комплексний інженерний аналіз. Це програмне забезпечення має включати:

1. Модулі збору даних з електромагнітних, акустичних, оптичних, вібраційних та інших датчиків.
2. Єдину платформу обробки сигналів – для зменшення перешкод, виявлення закономірностей і синхронізації між каналами.
3. Алгоритми штучного інтелекту та машинного навчання – для виявлення нетипових або підозрілих сигналів, що можуть свідчити про витік інформації.

4. Систему оповіщення для оперативного реагування на загрози безпеці.

Таке програмне забезпечення дозволяє здійснювати аналіз не лише кожного каналу окремо, а й виявляти комплексні мультиканальні загрози, наприклад, коли електромагнітне випромінювання супроводжується аномальними акустичними шумами, які у сукупності можуть свідчити про втручання.

Найперспективнішим напрямом розвитку такого програмного забезпечення є його інтеграція з хмарними обчислювальними сервісами та аналітичними платформами, що дозволить:

1. Масштабувати обчислення та скоротити час реакції на події.
2. Застосовувати аналіз великих даних (Big Data) для накопичення та прогнозування загроз.
3. Розвивати здатність до самонавчання системи, коли вона самостійно вдосконалює свої аналітичні алгоритми на основі попередніх ситуацій.

Отже, інтеграція сенсорних систем у єдину програмну платформу забезпечує ефективний інженерний аналіз усіх можливих технічних каналів витоку інформації. Такий підхід дозволяє оперативно виявляти багатокомпонентні загрози, підвищує надійність захисту об'єкта та відкриває перспективи для подальшого розвитку інтелектуальних систем безпеки.

Єськов Є. В.
Шейгас В. В.
Житомирський військовий інститут імені С. П. Корольова

## АДАПТИВНЕ ТА МОДУЛЬНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЯК ОСНОВА ПЕРСОНАЛІЗОВАНОГО ЗАХИСТУ ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

В умовах сучасних можливостей кібератак, більшість рішень з аналізу технічних каналів витоку інформації не враховують індивідуальні характеристики кожного об’єкта. Наприклад, стандартне програмне забезпечення може бути ефективним для одного об’єкту інформаційної діяльності (далі – ОІД) з незначною кількістю автоматизованих робочих місць, але абсолютно не придатним для великого об'єкта з численними технічними

приміщеннями, різним типом конструкцій або специфічними електромагнітними умовами. Це призводить до низької ефективності виявлення витоків, помилкових спрацьовувань або ж повного ігнорування реальних загроз.

Рішенням є розробка модульного та адаптивного програмного забезпечення, яке дозволяє конфігурувати функціонал відповідно до реальних умов об'єкта.

Основні риси такого програмне забезпечення:

Модульність, яка можливість додавання чи видалення функціональних блоків для роботи з конкретними типами загроз (наприклад, акустичний аналіз, теплове моделювання, аналіз мережевих викидів).

Адаптивність – налаштування під індивідуальні особливості об'єкта (матеріали стін, наявність ізоляції, кількість кабельних ліній тощо).

Гнучка аналітика, тобто кожен експерт з технічного захисту інформації може створювати власні профілі ризику, сценарії моделювання загроз, шаблони виявлення аномалій, а також окремий обліковий запис для кожної військової частини.

Підключення до зовнішніх систем: зокрема систем відеоспостереження, контролю доступу, охоронної сигналізації тощо – для формування єдиного простору безпеки.

Таке програмне забезпечення дозволяє не лише захищати об'єкти інформаційної діяльності, а й прогнозувати появу нових загроз на основі зміни параметрів середовища.

У майбутньому розвиток адаптивного програмне забезпечення орієнтується на такі напрямки:

1. Автоматичне сканування об'єкта та створення його цифрового двійника, що дозволить виявляти вразливі точки у віртуальній моделі.
2. Використання штучного інтелекту для постійного аналізу поведінкових патернів обладнання, виявлення прихованих витоків або шкідливих впливів.
3. Вбудований симулятор загроз, який дозволяє відтворити можливі сценарії атак і в реальному часі оцінити ефективність контрзаходів.
4. Підтримка роботи з мобільних пристроїв, що забезпечить гнучкий моніторинг стану безпеки в будь-який момент часу.

Модульність та адаптивність програмного забезпечення дозволяє забезпечити високоточний, персоналізований інженерний аналіз технічних каналів витоку інформації на будь-якому об'єкті інформаційної діяльності. Це

відкриває можливості для динамічного розвитку систем безпеки, підвищує ефективність реагування на загрози та робить систему гнучкою до змін у середовищі.

Сірош І. О.
Павлюк І. С.
Житомирський військовий інститут імені С. П. Корольова

## ЗАСТОСУВАННЯ КЛАВІАТУРНОГО ПОЧЕРКУ ДЛЯ ПІДВИЩЕННЯ РІВНЯ АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ В УМОВАХ ВОЄННОГО СТАНУ

В умовах повномасштабної збройної агресії рф проти України особливого значення набуває забезпечення захисту інформаційних систем, що використовуються у військовій сфері, державних структурах та критичній інфраструктурі. Одним із важливих напрямків розвитку інформаційної безпеки є вдосконалення механізмів автентифікації користувачів з метою запобігання несанкціонованому доступу до інформаційних ресурсів.

Традиційні методи автентифікації, засновані лише на використанні логіна та пароля, мають низку недоліків, оскільки пароль може бути перехоплений, вкрадений або переданий стороннім особам. У зв’язку з цим перспективним напрямком є використання біометричних методів автентифікації, зокрема клавіатурного почерку користувача.

Клавіатурний почерк являє собою поведінкову біометричну характеристику, що базується на аналізі індивідуальних особливостей набору тексту. До основних параметрів належать інтервали між натисканнями клавіш, швидкість введення символів, ритм набору та час утримання клавіш. Навіть при введенні однакового пароля різні користувачі мають унікальний ритм друку, що дозволяє використовувати даний метод як додатковий фактор автентифікації.

З метою дослідження даного питання розроблено програму автентифікації користувачів із застосуванням клавіатурного почерку. Програмний засіб реалізований мовою Python із використанням графічного інтерфейсу Tkinter. Система забезпечує перевірку логіна, пароля та ритму введення пароля користувачем.

Розроблена система підтримує розподіл ролей між користувачами, адміністраторами та супер-адміністратором, ведення журналів входів і дій адміністратора, механізми блокування облікових записів після багаторазових невдалих спроб входу, а також можливість перезапису біометричного шаблону користувача. Для формування шаблону клавіатурного почерку використовується багаторазове введення пароля з подальшим обчисленням середніх часових інтервалів між натисканнями клавіш.

Особливістю системи є використання буфера ритму введення, автоматичного запису часових інтервалів та механізму перевірки середнього і максимального відхилення між еталонним та поточним шаблонами. Це дозволяє підвищити стійкість системи до підбору паролів та використання викрадених облікових даних.

Отже, використання клавіатурного почерку як додаткового фактора автентифікації дозволяє підвищити рівень захисту інформаційних систем в умовах воєнного стану, зменшити ризик несанкціонованого доступу та забезпечити додатковий рівень контролю доступу до критично важливих ресурсів. Перспективами подальших досліджень є вдосконалення алгоритмів аналізу поведінкових характеристик користувачів, використання методів машинного навчання та підвищення точності розпізнавання клавіатурного почерку.

Талавер В. О.
Павлюк Н. А.
Житомирський військовий інститут імені С. П. Корольова

## МЕТОДОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ ОРГАНІЗАЦІЇ РОБОТИ РЕЖИМНО-СЕКРЕТНИХ ОРГАНІВ В УМОВАХ ВЕДЕННЯ БОЙОВИХ ДІЙ

Повномасштабна збройна агресія російської федерації проти України кардинально змінила умови функціонування системи забезпечення національної безпеки, висунувши нові жорсткі вимоги до захисту інформації з обмеженим доступом. У сучасних реаліях високотехнологічної війни, що характеризується інтенсивним вогневим впливом, активним застосуванням ворогом безпілотних літальних апаратів та засобів технічної розвідки, охорона державної таємниці набуває стратегічного значення. Будь-який витік

відомостей про плани командування, бойові розпорядження, райони зосередження чи переміщення підрозділів на рівні пунктів управління може призвести до катастрофічних наслідків, зриву військових операцій та втрати особового складу і техніки.

Аналіз чинного вітчизняного законодавства у сфері охорони державної таємниці, зокрема Постанова Кабінету Міністрів України від 18 грудня 2013 року № 939 (зі змінами) "Про затвердження Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України", Постанова Кабінету Міністрів України від 04 жовтня 2017 року № 750 "Про затвердження Порядку забезпечення охорони державної таємниці в Збройних Силах, інших утворених відповідно до законів військових формуваннях, правоохоронних, розвідувальних органах, органах спеціального призначення з правоохоронними функціями, які залучені до відсічі збройної агресії" свідчить про те, що чинні нормативно-правові акти орієнтовані переважно на стаціонарні умови функціонування військових частин. Разом з тим, динаміка сучасного бойового зіткнення вимагає від режимно-секретних органів (РСО) максимальної мобільності та живучості. Виникає гостра науково-практична потреба у відході від статичних безпекових моделей та розробленні адаптивної методики організації роботи РСО поза межами пунктів постійної дислокації у виїзних умовах – у тимчасових фортифікаційних спорудах або спеціальних апаратних.

Доцільно розробити методику організації роботи виїзного РСО в умовах ведення бойових дій, яка базуватиметься на комплексному поєднанні організаційно-правових, інженерно-технічних та оперативно-тактичних заходів. Ключовим елементом підходу є впровадження динамічного "мобільного режиму секретності", який передбачає суворе регламентування доступу посадових осіб до секретної інформації безпосередньо на пунктах управління за допомогою спрощених, але надійних алгоритмів ідентифікації.

Особливу увагу в методиці доцільно приділити мінімізації ризиків від технічних розвідок противника шляхом впровадження жорстких правил протидії технічним розвідкам і технічного захисту інформації.

Крім того, враховуючи наявний кадровий дефіцит та специфіку комплектування РСО у період воєнного стану, доцільно оптимізувати процеси

секретного діловодства шляхом розробки чітких алгоритмів дій військовослужбовців, що суттєво зменшує вплив "людського фактора".

Критично важливим аспектом повинно бути планування заходів на випадок екстрених та кризових ситуацій. Створення деталізованих чек-листів та часових регламентів (таймінгів) для оперативного згортання роботи виїзного РСО, негайної евакуації матеріальних носіїв секретної інформації або безповоротного фізичного чи програмно-апаратного знищення МНСІ у разі виникнення безпосередньої загрози захоплення позицій ворогом.

Практичне впровадження розробленої методики дозволить суттєво підвищити оперативність опрацювання секретних документів командуванням, оптимізувати використання наявних сил і засобів, а головне – гарантуватиме надійний захист секретної інформації від витоку в умовах нестабільної та швидкозмінної оперативної обстановки.

Таким чином, розроблена методика стане дієвим інструментом підвищення живучості системи управління військами. Сформовані практичні рекомендації можуть бути безпосередньо інтегровані в діяльність органів військового управління та військових частин, які виконують бойові завдання в районах ведення бойових дій, задля забезпечення надійного збереження державної таємниці та ефективності тактичних дій наших військ (сил).

Гуменюк І. В., канд. техн. наук, доц.
Косюк С. О.
Житомирський військовий інститут імені С. П. Корольова

## ШЛЯХИ ВДОСКОНАЛЕННЯ ЗАСОБІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ШЛЯХОМ УПРОВАДЖЕННЯ ПРОГРАМНОЇ АВТОМАТИЗАЦІЇ ЇХ ФУНКЦІОНУВАННЯ

В умовах повномасштабної збройної агресії російської федерації проти України забезпечення безперервного, оперативного та захищеного обміну інформацією між органами військового управління різних рівнів набуває критично важливого значення. Особливе місце в системі військового зв'язку займає передача інформації з обмеженим доступом у вигляді зашифрованих повідомлень засобами криптографічного захисту інформації (КЗІ). Значний

обсяг інформаційних потоків, висока інтенсивність обміну повідомленнями, дефіцит часу на прийняття рішень, а також людський фактор обумовлюють необхідність впровадження програмно-апаратних комплексів автоматизації обробки зашифрованих повідомлень. Поряд з цим має місце суттєве навантаження на підрозділи КЗІ, що у свою чергу, призводить до зниження оперативності оброблення криптограм, доведення їх до виконавців та, як наслідок, несвоєчасність виконання завдань, які зазначені у бойових документах.

Саме тому автоматизація обробки криптограм апаратно-програмними комплексами КЗІ є актуальним та необхідним завдання. Для розв'язання такого класу задачі запропоновано узагальнену схему методики, яка включає в себе: проведення апаратного та організаційного налаштування засобу КЗІ, безпосереднє проведення оброблення криптограм та заповнення форми технічного журналу. Основну увагу у роботі зосереджено на використанні параметрів під час апаратного та організаційного налаштування. Такий підхід значно зменшує кількість операцій черговою зміною (операторами), час на опрацювання вхідних (вихідних) криптограм та суттєво підвищує оперативність доведення до виконавців розпорядчих, інформаційно-аналітичних документів. Це, у свою чергу, забезпечує зниження ймовірності зриву управління підрозділами (військами), втрати їх боєздатності підрозділів тощо.

Лагодний О. В., канд. техн. наук, доц.
Колеснік Л. О.
Житомирський військовий інститут імені С. П. Корольова

## ПРИСТРІЙ ОХОРОННОЇ ЛАЗЕРНОЇ СИГНАЛІЗАЦІЇ ДЛЯ ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

У сучасних умовах питання інформаційної безпеки стає все більш актуальним, особливо у сфері технічного захисту інформації. Однією з ключових загроз є несанкціонований доступ (далі – НСД) до об'єкта інформаційної діяльності (далі – ОІД), де здійснюється обробка та зберігання інформації з обмеженим доступом (далі – ІзОД).

На ОІД ІзОД може перебувати у вигляді матеріальних носіїв секретної інформації, на жорстких дисках персональних комп'ютерів, серверах, флеш-

накопичувачах, а також циркулювати в автоматизованих системах. У разі несанкціонованого проникнення на ОІД існує ризик витоку, викрадення або пошкодження ІзОД, що може призвести до порушення режиму безпеки та негативних наслідків для діяльності об'єкта.

Зростання рівня кіберзагроз, а також постійний розвиток методів фізичного проникнення вимагають створення багаторівневих та надійних систем охорони. Традиційні методи охорони часто мають вразливості, такі як «сліпі зони», можливість обходу або необхідність значного людського ресурсу для моніторингу.

Для захисту ІзОД від НСД на ОІД застосовуються різні технічні засоби охорони, зокрема системи відеоспостереження, датчики руху, герконові датчики відкриття дверей і вікон, охоронна сигналізація, системи контролю та управління доступом.

Для підвищення рівня захисту ІзОД від НСД запропоновано впровадження пристрою охоронної лазерної сигналізації (далі – ПОЛС).

ПОЛС функціонує шляхом створення контрольованого простору за допомогою лазерного випромінювання. У разі порушення цілісності лазерного променя система фіксує факт проникнення та формує сигнал тривоги. Даний принцип роботи дозволяє здійснювати контроль доступу до окремих зон, приміщень або периметра об'єкта без необхідності постійної присутності персоналу охорони.

ПОЛС може застосовуватися для охорони службових приміщень, режимних зон, архівів та інших об'єктів, де здійснюється обробка та зберігання ІзОД. Використання даного пристрою дозволяє підвищити рівень безпеки ОІД, зменшити ризик НСД та забезпечити оперативне реагування на загрозу.

Таким чином, реалізація ПОЛС підвищує рівень захисту ІзОД на ОІД. Система забезпечує своєчасне виявлення несанкціонованого проникнення та зменшує ризик витоку ІзОД, підвищуючи надійність охорони в умовах сучасних загроз.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Kosterev D. S.
Korolyov Zhytomyr Military Institute

# INFORMATION SECURITY OF UNMANNED AERIAL VEHICLES IN SWARM OPERATIONS

The swarm deployment of unmanned aerial vehicles is one of the most advanced concepts in modern warfare. A swarm is a decentralized, self-organizing system in which each unmanned aerial vehicle (UAV) interacts with others to achieve a common goal. From an information security perspective, this is an extremely complex ecosystem where traditional protection methods often prove ineffective due to the high dynamics and specific network architecture.

The foundation of communication in such systems is Flying Ad Hoc Networks, known as FANET. This architecture lacks a single central router, and each UAV acts simultaneously as both an end node and a signal relay. The high mobility of the devices leads to constant changes in the network topology, and decentralization means that overall security depends on the security of each individual node. In addition, UAVs have strict limitations on size, weight, and power consumption, which makes it practically impossible to use computationally intensive encryption algorithms typical of stationary systems.

These architectural features create numerous vectors for cyberattacks at various levels of the swarm's operation. At the physical and channel levels, the adversary employs electronic jamming to disrupt communications, spoofs satellite coordinates to divert the UAV from its intended course, and intercepts traffic to gather intelligence. At the network level, the system may be vulnerable to threats such as a "black hole" attack, where a compromised UAV captures and destroys data packets, or replay attacks (where the enemy intercepts a legitimate command—such as "return to base"—and transmits it with a delay); resulting in a disruption of synchronized actions through the deliberate delay of legitimate commands. The most specific attacks target the swarm intelligence logic itself. For example, during an attack involving the generation of a large number of fictitious nodes in the swarm network, the enemy artificially gains a numerical advantage. This allows it to manipulate collective consensus algorithms and impose its own decisions on legitimate devices, seizing control over the selection of priority targets. Additionally, the enemy's capabilities allow it to carry out an attack in which one or more UAVs it has captured

begin transmitting contradictory or false information to other swarm members in order to sow chaos and disrupt the Ukrainian defense forces' ability to carry out their assigned mission.

Ensuring the cyber resilience of the swarm and countering these threats requires a comprehensive approach that is flexibly adapted to the limited resources of unmanned aerial vehicles. The foundation of this protection is lightweight cryptography, capable of ensuring robust encryption with minimal energy consumption, closely integrated with dynamic key management systems to instantly isolate compromised UAVs within the swarm. At the software level, blockchain technologies and lightweight smart contracts are increasingly being integrated to build a system of collective trust, in which no change in route or strategy is accepted without confirmation by a majority of nodes. This is organically complemented by AI-based intrusion detection systems that continuously analyze the behavior of neighboring UAVs and block them in the event of anomalies. On the hardware side, security is significantly enhanced by the use of isolated chips for the secure storage of cryptographic keys, as well as the application of frequency-hopping methods and alternative communication channels, such as laser optical communication, which makes swarm communication as resistant as possible to enemy electronic warfare.

Given the above, it must be concluded that the information security of swarm-based unmanned aerial vehicle applications extends far beyond traditional data protection. It is a fundamental prerequisite for maintaining controllability, the integrity of collective intelligence, and the overall viability of autonomous systems in a highly competitive and hostile environment. This requires the development of solutions that provide an optimal balance between cryptographic resilience, data transmission speed, and energy efficiency for each individual element of the swarm network.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Makovskyi I. Yu.
Budzinska O. O.
Netrebko R. V.
Korolov Zhytomyr Military Institute

# IMPLEMENTATION OF NIST SP 800-37 INTO THE NEW INFORMATION SECURITY ARCHITECTURE OF UKRAINE

The modern geopolitical context and the steadily increasing intensity of cyberattacks on Ukraine's public and private sectors demand a fundamental shift in the philosophy of information security. The national system's historic transition from the concept of static asset protection to a risk-based model has established a new security paradigm.

In this context, the methodological experience of leading technological nations becomes exceptionally relevant. The most comprehensive and field-proven tool is the U.S. National Institute of Standards and Technology Special Publication, NIST SP 800-37, "Risk Management Framework for Information Systems and Organizations" (RMF). Its primary conceptual shift from legacy approaches lies in abandoning a static posture in favor of continuous dynamism. The traditional approach was frequently reduced to freezing the system's configuration at the exact moment of its security certification. Consequently, any subsequent dynamic modifications rendered defense a mere formality that lagged behind real-world threats.

The RMF outlines a seven-step cyclical process that integrates security and privacy into the system development life cycle (SDLC) across three levels:

1. Organization (strategy, risk tolerance and perception);
2. Mission and processes (missions and functions);
3. Information systems (system-level implementation).

The first and most critical stage of the RMF implementation is the adaptation of the system categorization process. Within the Ukrainian legal framework, the criteria for designating facilities as critical infrastructure, alongside new system security profiles, have become the foundation for determining criticality.

At the same time, a methodological gap exists: the national approach frequently categorizes the institution as a whole, whereas NIST SP 800-37 focuses on the specific information system and the types of data it processes. To achieve successful synergy, the following mapping is proposed:

- impact assessment based on the CIA triad: instead of a generalized system classification, implement a discrete assessment of potential impact for Confidentiality (C), Integrity (I), and Availability (A) across Low, Moderate, and High levels;

- function-centric approach: an electronic document management system (EDMS) and a process control system located at the exact same facility should be assigned different NIST categories, thereby optimizing security expenditures.

A key element of NIST SP 800-37 is the role of the Authorizing Official (AO) – the senior official responsible for granting the Authorization to Operate (ATO) a system. Crucially, the AO formally signs off on the acceptance of residual risk, thereby creating room for dynamic information security management.

New Ukrainian legislation takes a step in this direction by placing personal legal liability for cyber defense directly on the heads of institutions. However, domestic practice is still dominated by a tendency to shift this responsibility onto an external regulator or auditor. Implementing the provisions of NIST SP 800-37 requires developing internal tools for executives, enabling them to make informed risk assessments and management decisions based on a balance between security and operational feasibility.

The final step of the RMF – Monitor – serves as a bridge to true cyber resilience. In Ukraine's current reality, where infrastructure faces persistent attacks, monitoring cannot be limited to quarterly log reviews.

The implementation of this step requires:

- the automation of security metrics collection and integration with government cyber defense centers (Government CERT);

- the implementation of the Continuous Authorization concept, whereby the ATO is automatically renewed as long as risk indicators remain within acceptable thresholds;

The implementation of NIST SP 800-37 provisions into the national information security system is not merely a technical task, but a vital step toward integration into the Euro-Atlantic security space. Transitioning from rigid compliance to adaptive risk management will enable the state to protect real-world processes by rapidly responding to the dynamic evolution of threats.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Цабик В. Ю.
Кулініч Ю. М.
Житомирський військовий інститут імені С. П. Корольова

# ПРОГРАМНИЙ ЗАСІБ АВТОМАТИЧНОГО РЕЗЕРВУВАННЯ ДАНИХ КОРИСТУВАЧІВ АВТОМАТИЗОВАНИХ СИСТЕМ КЛАСУ 1

У сучасних умовах повномасштабної збройної агресії рф проти України питання забезпечення інформаційної безпеки держави набувають особливої актуальності. Значне зростання кількості кібератак, спроб несанкціонованого доступу до інформаційних ресурсів та впливу шкідливого програмного забезпечення створює підвищені ризики втрати або пошкодження критично важливої інформації.

Особливого значення набуває захист інформації з обмеженим доступом, що обробляється в автоматизованих системах класу 1. У процесі функціонування таких систем існує ймовірність втрати даних унаслідок технічних збоїв, відмов обладнання, помилок користувачів, дії шкідливого програмного забезпечення або навмисних дій порушників. Реалізація зазначених загроз може призвести до порушення функціонування інформаційних систем, втрати службових даних та зниження ефективності виконання завдань.

Одним із ключових способів забезпечення збереженості інформації є організація резервування даних. Відповідно до вимог нормативних документів у сфері технічного захисту інформації, резервне копіювання є невід’ємною складовою комплексної системи захисту інформації та повинно забезпечувати можливість відновлення даних у разі їх втрати або пошкодження.

У роботі проведено аналіз існуючих методів резервування даних та сучасних програмних засобів резервного копіювання. За результатами аналізу визначено, що найбільш ефективним підходом для автоматизованих систем класу 1 є комбінований метод резервування, який поєднує повне та інкрементне копіювання даних.

Для реалізації програмного засобу автоматичного резервування даних було обрано мову програмування Python. Вибір обумовлений простотою реалізації алгоритмів, широкими можливостями роботи з файловими системами, підтримкою автоматизації процесів та наявністю бібліотек для архівування й контролю цілісності даних.

Розроблений програмний засіб забезпечує:
автоматичне створення резервних копій;
архівування даних;
контроль цілісності резервних копій;
ведення журналу операцій;
можливість подальшого відновлення інформації.

Використання програмного засобу дозволяє підвищити рівень захищеності інформації, мінімізувати ризик втрати даних та забезпечити безперервність функціонування автоматизованих систем в умовах сучасних кіберзагроз.

Джансиз І. І.
Лутченко В. І.
Житомирський військовий інститут імені С. П. Корольова

## МЕТОДИКА ВИЗНАЧЕННЯ ПЕРЕЛІКУ ЗАХОДІВ ДЛЯ БЛОКУВАННЯ МОЖЛИВИХ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

В умовах сучасної гібридної агресії та стрімкого розвитку інформаційних технологій особливої актуальності набуває питання технічного захисту інформації на об'єктах інформаційної діяльності (ОІД). Активне використання електронно-обчислювальної техніки, автоматизованих систем та телекомунікаційних мереж у військових частинах і державних установах створює додаткові ризики витоку інформації через технічні канали, зокрема канали побічних електромагнітних випромінювань та наведень (ПЕМВН).

Технічний захист інформації є складовою системи національної безпеки держави та спрямований на забезпечення конфіденційності, цілісності й доступності інформації з обмеженим доступом. Основною проблемою залишається недостатня систематизація процесу визначення необхідних заходів захисту інформації на ОІД та складність прийняття обґрунтованих рішень під час проєктування комплексів технічного захисту інформації (далі ТЗІ).

З огляду на існуючі технічні канали витоку інформації, причини виникнення ПЕМВН, паразитних зв'язків та наведень, а також методів й засобів

захисту інформації, особливу увагу під час визначення заходів ТЗІ на ОІД, необхідно приділити питанням екранування, заземлення, фільтрації небезпечних сигналів, просторового та лінійного зашумлення.

Методика визначення переліку заходів для блокування можливих технічних каналів витоку на ОІД дозволяє систематизувати процес виявлення технічних каналів витоку інформації, формування моделі загроз і вибору комплексу інженерно-технічних та організаційних заходів захисту. Її застосування дає можливість мінімізувати вплив людського фактору, підвищити ефективність прийняття рішень та забезпечити необхідний рівень захищеності інформації.

Мяновська Д. О.
Завірюха Д. О.
Житомирський військовий інститут імені С. П. Корольова

## ІДЕНТИФІКАЦІЯ РОЗВІДУВАЛЬНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ЯК ЕЛЕМЕНТ ЗБЕРЕЖЕННЯ ВАЖЛИВОЇ ІНФОРМАЦІЇ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Повномасштабне вторгнення в Україну та аналіз досвіду ведення російсько-української війни свідчить, що в ході бойових дій збройні сили російської федерації збільшують інтенсивність ведення повітряної оптичної розвідки, коригування вогню артилерії за допомогою безпілотних авіаційних комплексів із метою визначення об’єктів вогневого ураження. Крім того, неможливо обійти стороною інтенсивність застосування БпЛА типу баражуючих боєприпасів та FPV-дрони, які також оснащені та є носіями засобів оптичної розвідки. Зростання кількості та різноманіття БпЛА призводить до збільшення ризиків для особового складу, цивільного населення та критичної інфраструктури.

З позицій інформаційної безпеки, ворожий БпЛА є активним засобом несанкціонованого доступу до закритої інформації: він здійснює аерофотозйомку позицій, перехоплює радіообмін, визначає дислокацію особового складу та засобів зв’язку, чим безпосередньо загрожує відомостям, що становлять державну таємницю. Тому своєчасна ідентифікація БпЛА є не

лише тактичним, а й критично важливим завданням у сфері захисту інформації з обмеженим доступом.

Із досвіду виконання завдань підрозділами забезпечення охорони державної таємниці, існує проблематика щодо низького рівня підготовки особового складу залученого до виконання бойових (спеціальних) завдань, а також відсутність узагальненого методичного матеріалу з розвідувальними ознаками ворожих БпЛА.

Своєчасне виявлення, ідентифікація типу, походження та намірів безпілотного літального апарата відіграє важливу роль у визначенні та застосуванні дієвих методів, способів та заходів протидії. Мобільні групи протидії технічним розвідкам із активними засобами протидії інколи ідентифікують за принципом "свій-чужий". При цьому порівняльний візуально-програмний аналіз спектрів радіосигналів та пеленгів із джерел радіовипромінення, іноді дозволяє встановити лише сам факт наявності ймовірно ворожого безпілотного літального апарата. Для проведення всебічного і повного аналізу радіосигналів з метою ідентифікації БпЛА доцільно розробити та запровадити програмний застосунок, який буде допомагати вищеназваним підрозділам у ідентифікації БпЛА.

Проблематика ідентифікації БпЛА в контексті інформаційної безпеки полягає у такому:

велика кількість однотипних сигналів телеметрії та передавання даних із безпілотних літальних апаратів ускладнює розмежування власних та ворожих джерел радіовипромінення, що створює умови для прихованого збору розвідувальної інформації;

завантаженість певних діапазонів частот та накладання одних сигналів на інші унеможливлює чітке визначення форми сигналів та джерела загрози витоку інформації;

низький рівень підготовки особового складу в розрізі знань про середовище поширення радіохвиль, форми сигналів ворожих і дружніх БпЛА послаблює режим захисту інформації з обмеженим доступом;

відсутність єдиної автоматизованої системи допомоги операторів активних засобів протидії технічним розвідкам із базами даних, які значним чином будуть допомагати, в контексті, протидії виявленим БпЛА, що також в свою чергу знижує ефективність захисту відомостей, що становлять державну таємницю.

З позицій інформаційної безпеки програмний застосунок має на меті виконувати такі функції: захист від несанкціонованого збору інформації –

шляхом оперативної ідентифікації та вибору засобу протидії скорочується час роботи ворожої розвідувальної системи; захист від витоку відомостей, що становлять державну таємницю, – придушення каналів телеметрії та передачі даних БпЛА запобігає передачі розвідувальних даних про дислокацію об’єктів; підтримка режиму захисту інформації – база даних тактико-технічних характеристик зберігається локально без передачі мережею.

Ідентифікація БпЛА – це комплексна багаторівнева задача інформаційної безпеки, яка вимагає поєднання технічних інновацій, організаційних рішень та якісної підготовки особового складу. Лише системний підхід до створення автоматизованої системи підтримки оператора активного засобу протидії технічним розвідкам забезпечить ефективний захист інформації з обмеженим доступом та мінімізацію ризиків несанкціонованого збору розвідувальних відомостей засобами безпілотної авіації.

Соловей В. А.
Житомирський військовий інститут імені С. П. Корольова

## МЕТАДАНОНЕЙТРАЛЬНА АРХІТЕКТУРА РОЗПІЗНАВАННЯ «СВІЙ-ЧУЖИЙ» ДЛЯ БЕЗПІЛОТНИХ СИСТЕМ

Сучасні системи розпізнавання «свій-чужий» типу NATO Mode 5 (NM5) базуються на підтвердженні володіння криптографічним секретом шляхом формування коректної відповіді на запит радіолокаційної станції (РЛС). Такі системи залишаються вразливими до накопичення метаданих, кореляційного аналізу та побудови довготривалих графів мережевої. Ключовою проблемою системи NM5 є існування стабільного криптографічного стану, який проявляється через повторювані процедури автентифікації та наявність у радіоефірі криптографічної відповіді на запит системи розпізнавання.

У роботі пропонується гібридна архітектура SAIC (Self-Adaptive Implicit Communications – самоадаптивні імпліцитні комунікації), у якій механізм NM5 використовується як прихований механізм початкової ініціалізації SAIC-взаємодії без передачі криптографічної відповіді NM5 у радіоефір.

У архітектурі SAIC-NM5 РЛС формує випадковий запит та локально обчислює у межах NM5 набір криптографічних значень (КЗ) для очікуваних

платформ. Отримані КЗ не передаються в радіоефір та не використовуються як класична відповідь системи «свій-чужий» NM5. Натомість кожне з них застосовується як вектор ініціалізації окремого унікального фазового простору SAIC для всіх очікуваних платформ. Безпілотна платформа (БП) криптографічно обробляє запит від РЛС у системі NM5 та використовує отримане криптографічне значення (КЗ) для формування початкового фазового стану своєї системи взаємодії SAIC. Після цього БП передає у радіоефір не КЗ, а SAIC-пакет даних (ПД), який є подієво-залежною фазово узгодженою структурою відносно тільки одного унікального SAIC на РЛС.

РЛС отримує від БП відповідь у вигляді ПД та виконує логічну безпарольну автентифікацію (ЛБА) його структури. У разі успішної ЛБА на одній із систем SAIC – РЛС визначає статус відповідного БП як «свій» і тільки після цього реконструює КЗ. У межах такого підходу ідентифікація будь-якого БП здійснюється не через верифікацію КЗ, а через визначення допустимості структури отриманого ПД всередині відповідного онтологічного простору взаємодії у межах архітектури SAIC. І тільки після цього локально виконується перевірка КЗ згенерованого у межах системи NM5.

У запропонованій архітектурі відбувається концептуальний перехід від моделі «належність через знання секрету» до моделі «належність через операційну допустимість». Подальша валідність БП визначається вже не знанням секрету, а здатністю підтримувати допустиму фазову та подієву узгодженість усередині комунікаційної взаємодії архітектури SAIC.

Після першого успішного встановлення SAIC-взаємодії всі ключі NM5 – видаляються. Автентифікація здійснюється вже всередині SAIC-каналу шляхом постійної ЛБА кожного отриманого ПД незалежно від його інформаційного змісту. У межах SAIC будь-який ПД генерується в унікальному операційному стані, що з точки зору безпеки – відповідає унікальному ключу для кожного шифрокоду у NM5. Взаємодія SAIC+NM5 забезпечує одночасну реалізацію безперервної автентифікації (ЛБА) та безпечної інформаційної взаємодії між платформами без жодного випромінювання стабільних автентифікаційних структур у радіоефір.

Особливістю SAIC-взаємодії для РЛС-БП, чи БП-БП є наявність додаткового небітового математичного каналу взаємодії, який формується структурою всередині ПД, не збільшує його розмір, та не обмежує інформаційну ємкість основного закритого архітектурою SAIC – бітового

каналу зв’язку. Це створює передумови для реалізації для додаткового прихованого управління ройовими безпілотними системами та формування динамічних метаданонейтральних бойових мереж.

Метаданонейтральність комунікаційної взаємодії SAIC не дозволяє ворогу визначити адресата ПД, напрямок та факт передачі інформації, розмір інформаційного повідомлення, визначити структуру інформаційної взаємодії. Логічна адресація ПД приховано формується всередині його структури, внаслідок чого семантична реконструкція інформації можлива лише для тієї платформи, для якої відповідний пакет даних є операційно допустимим.

SAIC забезпечує неможливість непомітної модифікації, оскільки будь-яка зміна структури ПД призводить до втрати логічної автентичності пакета.

На відміну від NATO Mode 5, запропонована архітектура формує онтологічно замкнений канал взаємодії, функціонування якого не потребує використання зовнішньої криптографічної інфраструктури.

У SAIC відсутній криптографічний об’єкт, який може бути використаний противником, що нівелює атаки повторного відтворення, кореляційного аналізу, побудови графів мережевої взаємодії, статистичної реконструкції активності платформ тощо.

Sribnyi O. M.
Koval D. V., Ph. D.
Bondarchuk A. A.
Korolov Zhytomyr Military Institute

## GENERAL PRINCIPLE OF THE USE OF SOCIAL ENGINEERING DURING CYBERATTACKS AGAINST INFORMATION SYSTEMS

In the context of modern armed conflict, particularly during the period of the full-scale invasion of Ukraine by the Russian Federation, intelligence units of various states conduct activities aimed at obtaining information on the operation of critical infrastructure facilities, public administration bodies, and especially the leadership of the Security and Defense Forces of Ukraine. Given the considerable technological complexity of directly penetrating information systems in order to gain unauthorized access to their resources, such operations are often preceded by obtaining

authorization credentials, session tokens, authentication cookies, or the capability for remote control over specific system components through the use of social engineering techniques. At the same time, modern artificial intelligence technologies enable the automation of information gathering on potential targets and the creation of highly credible personalized messages.

According to the official report of CERT-UA, the Government Computer Emergency Response Team of Ukraine operating under the State Service of Special Communications and Information Protection of Ukraine, in 2025 the team processed 5,927 cyber incidents, which is 37.4% more than in the previous year. The most widespread types of cyberattacks included:

mass distribution of messages through electronic communication channels (e-mail, social networks, messengers) containing malicious software attachments;

phishing emails and messages containing links to fraudulent electronic resources requesting authentication credentials;

targeted spear phishing campaigns using legitimate cloud services and compromised accounts;

attacks aimed at stealing session tokens, browser cookies, and other authentication data.

All these types of cyberattacks share a common principle – the target of the cyberattack must personally interact with the means of unauthorized access in a manner required for the attacker to achieve their objective. For this purpose, before creating the aforementioned messages and emails, open-source intelligence analysis of the target audience is conducted, including individuals interacting with the target, their leadership, subordinates, relatives, friends, and others. Social networks, messengers, publicly available documents, leaked personal data, geotagged photographs, file metadata, and other accessible OSINT sources are used for this purpose. Based on the obtained results, the content of the message or email is designed in such a way as to force the target to perform actions required by the attacker. Additionally, adversaries may use generative artificial intelligence technologies to automatically create personalized messages imitating real officials or acquaintances of the target.

However, even after obtaining stable access to a specific component of the target's information system, the attacker, in addition to technical manipulations, may study the management capabilities of this component and the individual operating it,

and use psychological manipulation techniques to expand privileges and gain access to other system components. For example, by using malicious software that enables remote control of the target's workstation, the attacker, after gaining appropriate access, may terminate individual processes, capture keyboard input, steal authentication tokens and browser cookies, and use built-in operating system tools without installing additional software. By monitoring user actions and the working environment, the attacker may obtain authorization credentials for email clients, web resources, remote access systems, file repositories, databases, and other elements of the information system.

Considering the above, administrators of information systems within units and command bodies of the Security and Defense Forces of Ukraine must implement the necessary measures to counter attempts by adversaries to gain unauthorized access in such ways. In addition to the official recommendations of the State Service of Special Communications and Information Protection of Ukraine, since phishing emails and messages are distributed through Internet-based electronic communication channels, the automated workstation intended for receiving and processing public correspondence (for example, the official email account of a military unit) should:

ensure physical or logical isolation from the internal information system using principles of network segmentation, separate VLANs, DMZs, or other access separation mechanisms;

prohibit the processing and storage of any information except downloading correspondence to designated external media;

prevent the installation of additional software, as well as the use of unauthorized PowerShell scripts, macros, and other automation tools;

restrict access to web resources through the use of URL filtering, DNS filtering, and web access control systems;

implement multi-factor authentication, user privilege management, and centralized security event monitoring systems.

Other elements of the information system require the implementation of appropriate security policies, antivirus protection tools, EDR/XDR solutions, as well as centralized monitoring and analysis of information security events. Personnel of military units must be instructed about the threat posed by the use of social engineering techniques by adversaries, and training sessions on personal cyber hygiene, identification of fraudulent web resources, phishing emails, and messages

should be conducted. Additionally, under the supervision of information system administrators, periodic exercises aimed at countering such cyberattacks should be organized, during which personnel must identify test phishing emails and messages without prior warning. Based on the results of these exercises, administrators will improve the resilience of information systems against cyberattacks involving social engineering techniques and ensure readiness for rapid detection, localization, and response to cyber incidents.

Чмир А. О.
Ворон В. В.
Житомирський військовий інститут імені С. П. Корольова

## ЕКСТРЕНЕ ЗНИЩЕННЯ НОСІЇВ ІНФОРМАЦІЇ ЯК ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЗОНІ БОЙОВИХ ДІЙ

Питання екстреного знищення машинних носіїв інформації (МНІ) об'єктів електронно-обчислювальної техніки у Збройних Силах України сьогодні набуває особливої актуальності. В умовах активної збройної агресії проти України традиційний паперовий облік переходить на електронну систему, що забезпечує оперативність управління та ефективність роботи, але водночас може створювати ризики витоку інформації. Захоплення машинних носіїв інформації противником може мати негативні наслідки, що призведуть до витоку важливих даних, що становлять загрозу для виконання поставлених бойових завдань та збереження державної таємниці.

Проблемою екстреного знищення машинних носіїв інформації у зоні бойових дій являється те, що чинні нормативні та керівні документи переважно розраховані на мирний час. Водночас, що стосується умов особливого періоду то екстрене знищення викладено стисло та немає певної послідовності дій, що може призвести до не надійного знищення машинних носіїв, що може потрапити до противника з частковим або повним відновленням інформації.

Тому виникає необхідність розроблення методичних рекомендацій щодо екстреного знищення МНІ в особливий період. Вони мають визначати порядок дій особового складу та загрози захоплення носіїв противником, способи, засоби та послідовність їх знищення в умовах обмеженого часу й дії бойових факторів з урахуванням сучасних загроз та досвіду бойових дій.

Порядок знищення МНІ регламентується Постановами №939 (мирний час) та №750 (особливий період). Для виконання цих вимог військовослужбовці на навчаннях вивчають керівні документи, складають заліки та відпрацьовують навички знищення носіїв у бойових умовах, що запобігає витоку інформації. Особовий склад зобов'язаний забезпечувати збереження МНІ та запобігати витоку інформації. Відповідальність за інструктаж, маскування, вибір методу знищення та контроль покладається на начальника підрозділу. Найефективнішим методом для екстреного знищення МНІ являється фізичне руйнування, оскільки перебування підрозділу можливе, в населених пунктах чи в лісовій місцевості, де застосування інших способів знищення може бути неможливим. Для фізичного руйнування можуть використовуватись підручні матеріали, які є в кожному підрозділі, до них відносяться: молоток, ковадла, плоскогубці, вогнесуміші та інші інженерні засоби знищення (міни, тротилові шашки),що забезпечать надійне знищення деталей носіїв інформації.

Екстрене знищення здійснюється з дозволу командира, а за його відсутності – старшим на пункті управління або начальником підрозділу. У випадку раптового нападу рішення може прийматись самостійно особовим складом, якщо вказівку не можливо отримати. В першу чергу знищуються машинні носії з критично важливою інформацією про угрупування військ, плани бойових дій та персональні дані військовослужбовців. Результатом проведення екстреного знищення є документальне оформлення у вигляді заздалегідь складеного акту або письмової доповіді, в якій зазначається: коли, ким та за чиїм розпорядженням, місце, яким способом та за яких обставин проведено знищення, а також здійснюється фото- або відеофіксація результатів знищення.

Таким чином**,** в умовах ведення бойових дій питання екстреного знищення МНІ об'єктів електронно-обчислювальної техніки набуває особливо важливого значення, оскільки своєчасне виконання поставлених заходів дозволяє запобігти витоку інформації та потраплянню до рук противника. Вирішення цього завдання є невід'ємною складовою системи технічного захисту інформації та забезпечення стійкості інформаційної безпеки у Збройних Силах України. Виявлені невідповідності між керівними документами та умовами бойових дій свідчать про необхідність розроблення методичних рекомендацій, які враховують дій особового складу, обмеженість часу та ресурсів, а також високий рівень ризику витоку даних. Ефективність знищення визначається своєчасністю прийняття рішень, розподілом обов'язків та документальним підтвердженням результатів. Саме поєднання організаційних, технічних та правових заходів гарантує надійність захищення важливої інформації, а система захисту даних

залишається захищеною в умовах бойових дій. Це підкреслює важливість удосконалення нормативної бази та підготовки особового складу для підвищення рівня інформаційної безпеки та надійності технічного захисту.

Митрофанова М. С.
Військовий інститут Київського національного університету
імені Тараса Шевченка

## СОЦІАЛЬНІ МЕДІА ЯК СЕРЕДОВИЩЕ ДЛЯ ПОШИРЕННЯ НЕГАТИВНИХ ІНФОРМАЦІЙНИХ ВПЛИВІВ

У сучасному інформаційному просторі соціальні медіа перетворилися на один із головних каналів комунікації, що визначає формування громадської думки, політичних настроїв та поведінки суспільства. Після початку повномасштабного вторгнення Російської Федерації в Україну роль соціальних мереж значно посилилася. Такі платформи як Telegram, TikTok, Facebook, Instagram, YouTube та X стали не лише джерелом оперативної інформації, а й середовищем активного поширення дезінформації, психологічного впливу, пропаганди та маніпуляцій. Соціальні медіа сьогодні виконують функцію інформаційного поля бою, де поряд із реальними подіями ведеться боротьба за свідомість аудиторії.

Соціальні медіа створюють умови для формування так званих інформаційних «бульбашок», у межах яких користувачі отримують переважно контент, що підтверджує їхні переконання. Алгоритми платформ орієнтовані насамперед на утримання уваги аудиторії, тому найбільше поширення отримує емоційний, конфліктний або провокативний контент. Дослідження науковців Массачусетського технологічного інституту показало, що неправдива та емоційно забарвлена інформація поширюється у соціальних мережах значно швидше, ніж правдива. Фейкові повідомлення частіше викликають страх, гнів, здивування та обурення, що підвищує рівень їх вірусності в інформаційному просторі.

Одним із найбільш поширених негативних інформаційних впливів у період повномасштабної війни стала кремлівська дезінформація. У перші тижні вторгнення соціальні мережі були переповнені фейковими повідомленнями про

«капітуляцію українських міст», «здачу військових частин» та нібито втечу українського керівництва. Значна частина таких повідомлень поширювалася через Telegram-канали та мережі ботів. Основною метою було створення паніки серед населення, деморалізація військових та підрив довіри до державних інституцій.

Особливо активним інструментом негативного впливу став Telegram. Через анонімність адміністраторів та відсутність ефективної модерації платформа стала середовищем поширення неперевіреної інформації, фейкових новин та проросійських наративів. У 2022–2024 роках Центр протидії дезінформації при РНБО України неодноразово повідомляв про діяльність мереж каналів, які координовано поширювали панічні настрої щодо мобілізації, втрат ЗСУ та ситуації на фронті. Одним із прикладів стала хвиля повідомлень про нібито «тотальний дефіцит зброї» та «неминучу поразку України» восени 2023 року, які активно просувалися через анонімні Telegram-ресурси.

Ще одним прикладом негативного інформаційного впливу стало масове поширення маніпулятивних відео у TikTok. Через короткий формат та алгоритмічне просування контенту платформа стала ефективним інструментом інформаційно-психологічних операцій. Російська пропаганда активно використовувала TikTok для створення емоційних відео про «втому українців від війни», «конфлікти між військовими та цивільними», а також для дискредитації міжнародної підтримки України. У 2024 році активно поширювалися змонтовані ролики про нібито масові протести українців проти мобілізації, які згодом були спростовані фактчекерами.

Окремою проблемою стало поширення дипфейків та контенту, створеного за допомогою штучного інтелекту. У березні 2022 року було опубліковано фейкове відео із нібито зверненням Президента України Володимир Зеленський про капітуляцію. Хоча відео швидко спростували, цей випадок продемонстрував небезпеку використання технологій штучного інтелекту у межах інформаційної війни. Подібні приклади свідчать про те, що сучасні інформаційні впливи стають дедалі технологічнішими та складнішими для розпізнавання. Водночас соціальні медіа залишаються важливим інструментом протидії негативним інформаційним впливам. Українські державні структури, незалежні медіа та громадські організації активно використовують платформи для спростування фейків, проведення фактчекінгу та підвищення медіаграмотності населення. Важливу роль у цьому процесі

відіграють проєкти StopFake, VoxCheck та Центр протидії дезінформації. Науковці підкреслюють, що розвиток медіаграмотності є одним із найефективніших механізмів боротьби з дезінформацією.

Охрімчук В. В., канд. техн. наук, доц.
Охрімчук І. А.
Житомирський військовий інститут імені С. П. Корольова

## ЗМІЩЕННЯ ВЕКТОРА РОСІЙСЬКИХ КІБЕРВПЛИВІВ

У XXI столітті кіберпростір став одним із ключових театрів ведення гібридної війни. Російська федерація активно використовує кібероперації як інструмент політичного тиску, дестабілізації та збору розвідувальної інформації. Особливо помітним це стало після початку російської агресії проти України у 2014 році та повномасштабного вторгнення у 2022 році. Якщо на початкових етапах російські кібератаки були спрямовані переважно на державні установи, критичну інфраструктуру та великі організації, то згодом спостерігається суттєве зміщення вектору кібеатак у бік персональних пристроїв військовослужбовців. Така трансформація пов'язана зі зміною характеру сучасної війни, де інформація та оперативність відіграють вирішальну роль.

Перші масштабні російські кібератаки проти України були орієнтовані на порушення роботи державних структур та критичної інфраструктури. Одним із найбільш відомих прикладів стала атака на українську енергосистему у 2015 році, коли внаслідок втручання хакерів тисячі громадян залишилися без електропостачання. У 2017 році вірус NotPetya завдав значних економічних збитків як українським установам, так і міжнародним компаніям. Метою подібних атак було створення хаосу, підрив довіри до державних інституцій та демонстрація вразливості української системи кібербезпеки.

Аналіз сучасних кіберінцидентів свідчить про перехід від масових деструктивних атак до таргетованих операцій проти окремих військовослужбовців. Із розвитком цифрових технологій та активним використанням мобільних пристроїв у військовій сфері російські спецслужби змінили підхід до кібероперацій. Замість масштабних атак виключно на

установи дедалі більше уваги приділяється персональним гаджетам військовослужбовців: смартфонам, планшетам, ноутбукам та засобам зв'язку. Такий вектор є значно ефективнішим у тактичному вимірі, адже дозволяє отримувати оперативну інформацію про пересування військ, координати позицій, контакти між підрозділами та морально-психологічний стан військових.

Одним із методів впливу є використання шкідливого програмного забезпечення, яке маскується під мобільні додатки або файли для обміну інформацією. Через заражені програми російські кіберугруповання можуть отримувати доступ до геолокації, фотографій, повідомлень та контактів військових. Особливу небезпеку становлять атаки через месенджери та соціальні мережі, де здійснюється фішинг або поширення дезінформації. У деяких випадках противник використовує психологічні методи впливу, надсилаючи військовослужбовцям повідомлення із погрозами чи неправдивою інформацією з метою деморалізації.

Важливою причиною зміщення вектору кібератак є також зростання ролі мобільного зв'язку у сучасних бойових діях. Мобільні пристрої стали складовою інформаційно-комунікаційної інфраструктури військових підрозділів: через нього здійснюється координація дій, передача фото- та відеоматеріалів, використання картографічних сервісів та спеціалізованих застосунків. Відтак компрометація одного пристрою може створити загрозу для цілого підрозділу. Російські кібератаки дедалі частіше мають точковий характер, орієнтований на конкретних осіб, що робить їх складнішими для виявлення та протидії.

Крім збору розвідданих, атаки на персональні пристрої мають і пропагандистську складову. Через доступ до акаунтів військових противник може поширювати фейкові повідомлення або використовувати особисту інформацію для інформаційно-психологічних операцій. Таким чином кіберпростір стає не лише технічним, а й психологічним інструментом ведення війни.

Отже, російські кібероперації проти України еволюціонували від кібератак на державні інституції та критичну інфраструктуру до цілеспрямованого впливу на персональні пристрої військовослужбовців. Така зміна вектору пояснюється прагненням отримати швидкий доступ до тактичної інформації та посилити інформаційно-психологічний тиск на представників Сил оборони України. У сучасних умовах ефективна кібербезпека повинна охоплювати не лише захист державних систем, а й цифрову грамотність та кібергігієну кожного військовослужбовця. Саме людський фактор дедалі більше стає ключовим елементом у протистоянні сучасним кіберзагрозам.

Письменний О. О., канд. політ. наук, ст. досл.
Воєнна академія імені Євгенія Березняка

# ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ФАКТОР ПОЛІТИЧНОЇ СТАБІЛЬНОСТІ ДЕРЖАВИ

Політична стабільність держави є однією з необхідних умовою для національної безпеки, стабільного розвитку та соціальної єдності суспільства. Політично стабільна держава здатна протидіяти конфліктам, економічним потрясінням, зовнішньому тиску та іншим викликам без руйнування основ політичної системи. Така держава характеризується спроможністю державних інститутів адаптуватися до змін, підтримувати суспільний порядок, забезпечувати виконання законів і зберігати довіру громадян до влади.

У сучасних умовах розвитку глобалізованого інформаційного суспільства інформаційна безпека стала одним із ключових чинників забезпечення політичної стабільності держави. Стрімкий розвиток цифрових технологій, соціальних мереж, штучного інтелекту та інформаційно-комунікаційних систем суттєво змінив характер політичних процесів, механізми державного управління та способи впливу на суспільну свідомість. У зв'язку з цим інформаційний простір перетворився не лише на середовище комунікації, але й на арену політичного протиборства, інформаційних загроз та конфліктів.

Для України особливої актуальності проблема інформаційної безпеки набула з початку активної фази російської воєнної агресії. Російська федерація активно використовує всі інструменти інформаційної війни з метою дестабілізації політичної ситуації в Україні, підриву довіри до державних інституцій, поширення панічних настроїв та розколу суспільства. У таких умовах забезпечення інформаційної безпеки стає важливим елементом національної безпеки та передумовою збереження політичної стабільності держави.

Забезпечення інформаційної безпеки передбачає виконання комплексу заходів, спрямованих на захист інформаційних ресурсів, державних інформаційних систем, суспільної свідомості та інформаційного суверенітету держави. Її важливість обумовлена тим, що сучасні конфлікти дедалі частіше здійснюються не лише у військовій чи економічній площині, а й через інформаційно-психологічний вплив, маніпуляцію громадською думкою, кібератаки та дезінформаційні кампанії.

Однак інформаційна безпека не має розглядатися виключно як інструмент контролю над інформаційним простором. Надмірне обмеження свободи слова та доступу до інформації може негативно впливати на демократичний розвиток держави та спричиняти суспільне невдоволення. Тому у забезпеченні інформаційної безпеки важливим є пошук балансу між забезпеченням національної безпеки та дотриманням демократичних прав і свобод громадян.

Особливу роль у зміцненні інформаційної безпеки відіграє розвиток медіаграмотності населення. Підвищення рівня критичного мислення, здатності аналізувати інформацію та розпізнавати маніпулятивний контент сприяє формуванню стійкості суспільства до інформаційних загроз. У сучасних умовах медіаграмотність стає важливим елементом громадянської культури та фактором політичної стабільності.

Світовий досвід демонструє, що ефективне забезпечення інформаційної безпеки потребує комплексного підходу, який поєднує діяльність державних органів, громадянського суспільства, наукових установ та міжнародних організацій.

Отже, інформаційна безпека є одним із фундаментальних чинників політичної стабільності держави. Вона є похідною інформаційного суверенітету, сприяє підтриманню суспільної довіри до державних інституцій, мінімізує ризики зовнішнього інформаційного впливу та створює умови для стабільного функціонування політичної системи. В умовах сучасних глобальних викликів роль інформаційної безпеки постійно зростає, що обумовлює необхідність подальшого вдосконалення державної політики у цій сфері.

Забезпечення інформаційної безпеки відбувається в системі особа – суспільство – держава. Кожен з її елементів служить на користь своїм інтересам. Часто потреби одного елемента є загрозами для іншого або мають конфліктогенну природу, тому, на нашу думку, доцільно розділяти поняття інформаційної безпеки на окремі рівні (особовий, колективний, суспільний, державний), оскільки кожен із них зазнає специфічних зовнішніх впливів і усуває властиві саме йому загрози. Однак оцінити загальний стан інформаційної безпеки як фактора політичної стабільності держави неможливо без урахування впливів на кожен із рівнів системи особа – суспільство – держава.

Бєлова В. С.
Національна академія Служби безпеки України

# OSINT ЯК ОДИН ІЗ КЛЮЧОВИХ ЕЛЕМЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ПРОТИДІЇ РОСІЙСЬКІЙ АГРЕСІЇ

В умовах повномасштабної збройної агресії російської федерації проти України проблема протидії проявам гібридної війни в інформаційному просторі набуває дедалі більшої актуальності та значущості.

Поряд із безпосередніми бойовими зіткненнями на лінії фронту, ворог продовжує активно застосовувати й інформаційно-психологічні операції, спрямовані на формування у громадян України викривленої картини реальності, маніпуляцію суспільною свідомістю, психологічне навантаження та емоційну дестабілізацію, підрив довіри до державних інституцій тощо.

У таких умовах особливого значення набуває медіаграмотність населення як здатність критично сприймати, аналізувати та оцінювати інформацію. Адже під час гібридної війни ворог діє витончено: дипфейки та маніпуляції з "візуалом": фото- та відеодокази фабрикуються або беруться з інших конфліктів минулих років; ботоферми та штучний інтелект; легітимізація фейків, тобто інформація вкидається через мережу анонімних Telegram-каналів, а потім розповсюджується "сміттєвими медіа" ("жовта преса", клікбейт-видання тощо). У таких умовах підходи до медіграмотності потребують доповнення практичними інструментами перевірки даних, серед яких важливе місце займає знання OSINT-технологій.

Так, інтеграція OSINT у систему медіаграмотності забезпечує перехід від теоретичного аналізу інформації до її практичної верифікації. Завдяки опануванню інструментів OSINT, розумінню принципів роботи з відкритими джерелами, що дозволяє виявляти потенційні загрози та запобігти витоку інформації, користувачі можуть: перевіряти правдивість фото- та відеоматеріалів; виявляти фейки та маніпулятивний контент; встановлювати першоджерела інформації; аналізувати контекст поширення повідомлень. Таким чином, OSINT виступає важливим практичним інструментом для реалізації медіаграмотності у цифровому середовищі.

У той же час, країна-агресор перетворює технології OSINT на потужну зброю, автоматизуючи збір та аналіз розрізнених даних із відкритих джерел. Це дозволяє

отримувати детальні цифрові профілі політиків, військових, а також здійснювати пошук "слабких точок" у безпеці об'єктів критичної інфраструктури.

Тому слід наголосити на необхідності впровадження контр-OSINT (Counter-OSINT) – набору методів і стратегій, спрямованих на захист інформації від збору, аналізу та використання зловмисниками через відкриті джерела, а також обмеження доступу до чутливих даних, дезінформацію та контроль за цифровим слідом.

Серед найдоступніших методів в протидії OSINT-діяльності ворога можна виділити такі, як *мінімізація цифрового сліду* (обмеження особистої інформації, використання анонімних акаунтів для роботи в мережі Інтернет, відмова від безкоштовних сервісів, які збирають і аналізують персональні дані); *дезінформація та введення в оману* (створення фейкових профілів: наповнення їх некоректною інформацією, яка відволікатиме аналітиків; маніпуляція даними: зміна дат, геолокації, подій, використання фальшивих цифрових слідів; підміна технічної інформації: маскування реальної IP-адреси, використання шифрованих комунікацій, таких як Signal, ProtonMail тощо); *контроль за витоком інформації* (використання багаторазової автентифікації – 2FA; регулярний аудит безпеки: перевірка витоку паролів, доступності інформації про користувача в пошукових системах, наприклад Google Dorking); *захист від OSINT-аналізу зображень і відео* (видалення EXIF-метаданих перед публікацією фото; уникнення публікації геолокації або розмиття важливих деталей на зображеннях; затримка у часі при публікаціях для унеможливлення визначення поточного місцезнаходження); *захист корпоративної та державної інформації* (обмеження відкритого доступу до документів у форматах PDF, DOCX, що можуть містити метадані про організацію; моніторинг згадок у мережі, зокрема Google Alerts, Meltwater, Mention для запобігання витоку інформації; проведення тренінгів з кібергігієни для співробітників для мінімізації ризиків ненавмисного розкриття інформації).

Отже, в сучасних умовах, де інформаційний простір є ареною протистояння, а гібридний характер агресії ворога передбачає синхронне застосування кібератак та інформаційно-психологічних операцій, OSINT-технології стали ключовим елементом інформаційної безпеки України, оскільки дозволяють у реальному часі отримувати, верифікувати та використовувати дані з відкритих джерел. Тому інтеграція базових OSINT-навичок у освітні програми з медіаграмотності суттєво підвищує когнітивну стійкість населення до

дезінформації. Для подальшого посилення інформаційної безпеки необхідна інституціоналізація OSINT-структур, державне фінансування відповідних проєктів та гармонізація роботи волонтерських і офіційних OSINT-спільнот.

Гладич Р. І.
Житомирський військовий інститут імені С. П. Корольова

## АКТУАЛЬНІ ЗАГРОЗИ БЕЗПЕЦІ ХМАРНИХ АРХІТЕКТУР У РАЗІ МІГРАЦІЇ ДЕРЖАВНИХ ТА ВІЙСЬКОВИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Повномасштабна збройна агресія рф проти України зумовила радикальну трансформацію підходів до забезпечення національної безпеки в кіберпросторі, висунувши на перший план завдання екстреного захисту критичної інформаційної інфраструктури від фізичного та віртуального знищення. Масовані ракетні удари по вітчизняних центрах обробки даних (ЦОД) створили пряму загрозу втрати державних реєстрів та оперативних військових баз даних. Термінове внесення змін до чинного законодавства дозволило здійснити масштабну міграцію державних та військових інформаційних систем до закордонних хмарних середовищ провідних світових гіперскейлерів (AWS, Microsoft Azure, Google Cloud). Цей крок став стратегічним інструментом збереження цифрового суверенітету, забезпечивши безперервність функціонування органів влади та Збройних Сил України. Проте перенесення стратегічних масивів даних із локально ізольованих периметрів у глобальну хмару сформувало новий ландшафт кіберзагроз. Актуальність дослідження зумовлена необхідністю глибокого науково-практичного аналізу вразливостей хмарних технологій в умовах воєнного стану. Метою роботи є системна класифікація критичних загроз безпеці хмарних архітектур, що виникають під час міграції державних та оборонних систем, а також визначення науково обґрунтованих шляхів їх нейтралізації.

Концептуальна безпека хмарних рішень базується на моделі спільної відповідальності (Shared Responsibility Model). У її межах провайдер гарантує виключно безпеку інфраструктури хмари (фізичну цілісність серверів та ізоляцію віртуальних середовищ), тоді як замовник несе повну відповідальність

за безпеку даних у ній (конфігурацію мереж, управління доступами, шифрування). Досвід відбиття кібератак, скоординованих російськими проурядовими хакерськими угрупованнями, свідчить, що форсована міграція систем під час бойових дій суттєво підвищує ризик виникнення помилок конфігурації (Misconfiguration). В умовах дефіциту часу технічні фахівці часто припускаються помилок у налаштуванні прав доступу, залишають відкритими хмарні сховища даних або використовують вразливі, незахищені інтерфейси програмування додатків (API). Це створює передумови для прихованого, несанкціонованого збору класифікованої та розвідувальної інформації силами кіберпідрозділів ворога.

Іншим критичним вектором уразливості хмарних архітектур є компрометація систем управління ідентифікацією та доступом (IAM). Російські хакери активно застосовують високотехнологічний таргетований фішинг (Spear Phishing) та методи соціальної інженерії для компрометації облікових записів системних адміністраторів державних та військових відомств. Нехтування обов'язковим використанням апаратних ключів багатофакторної автентифікації (MFA) та надмірне делегування повноважень дозволяють зловмисникам перехопити легітимні облікові записи та отримати повний контроль над хмарною інфраструктурою підрозділу, що дає їм змогу непомітно модифікувати дані або повністю знищувати інформаційні масиви.

Особливу загрозу становлять складні атаки на ланцюжки постачання (Supply Chain Attacks). Хмарні системи тісно інтегрують стороннє програмне забезпечення та автоматизовані інструменти управління від зовнішніх комерційних підрядників. Шляхом компрометації систем розробки приватних ІТ-компаній хакери отримують можливість обійти передові технічні системи кіберзахисту хмари безпосередньо зсередини. Окрім технічних чинників, виникають проблеми юридичного суверенітету даних через розміщення інформації поза межами національної юрисдикції, а також вразливість гібридних каналів зв'язку, які піддаються деструктивному впливу ворожих засобів радіоелектронної боротьби (РЕБ) та атак на маршрутизацію (BGP hijacking).

Ефективна нейтралізація зазначеного комплексу загроз вимагає негайного переходу до архітектурної моделі Нульової довіри (Zero Trust). Головними технічними заходами мінімізації ризиків мають стати глибока мікросегментація хмарних мереж, яка локалізує потенційне ураження, впровадження суворого

рольового доступу за принципом найменших привілеїв, а також обов'язкове використання наскрізного криптографічного шифрування даних. Крім того, критично важливим є впровадження інструментів CSPM (Cloud Security Posture Management) для автоматизованого аудиту налаштувань хмари у реальному часі.

Підсумовуючи, міграція державних та військових систем у хмарний простір стала історично необхідним та високоефективним кроком для збереження працездатності України. Водночас забезпечення довгострокової стійкості оборонного потенціалу країни в кіберпросторі можливе лише за умови системного впровадження архітектури Zero Trust, жорсткого дотримання кібергігієни та регулярного технічного аудиту хмарних середовищ.

Давиденко М. О., канд. юрид. наук
Національна академія Служби безпеки України

## ЩОДО МЕТОДІВ МАНІПУЛЮВАННЯ СУСПІЛЬНОЮ СВІДОМІСТЮ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ АГРЕСІЇ рф

У сучасних умовах повномасштабного вторгнення російської федерації на територію України інформаційна агресія держави-агресора проти України розглядається через призму систематичної та ґрунтовно побудованої дезінформації, нових технологій маніпулятивного впливу і удосконалених форм і методів поширенні деструктивної пропаганди з метою впливу на різні верстви українського суспільства (зокрема військових та членів їх родин) з метою поширення радикалізму, екстремізму, тероризму і сепаратизму, зниження міжнародної підтримки України під час повномасштабного вторгнення.

Маніпулювання суспільною свідомістю виступає основоположним елементом інформаційної агресії рф, який має довгострокові наслідки на суспільні інститути і державу. Використовуючи медіа-середовище, створюється специфічний інформативний контент, спрямований на поляризацію суспільства, розпалювання конфліктів, зокрема і релігійних, та підрив усталених соціальних інститутів.

Одним із методів маніпулювання суспільною свідомістю є стратегічне конструювання поляризованої картини світу в антиукраїнських інформаційних операціях рф. За допомогою цього методу складна соціальна реальність редукується до жорсткого протиставлення «своїх» і «чужих». Це характерно для

більшості спеціальних інформаційних операцій рф, у яких він має особливо виразний геополітичний вимір. Зокрема, Україна, ЄС і НАТО подаються як частини ворожого блоку, що нібито прагне принизити, розчленувати чи знищити «справжню» росію або традиційний соціальний порядок.

Для української цільової аудиторії ця поляризація часто маскується під внутрішньополітичні антагонізми, що може також впливати на думку електорату під час виборчого процесу. Використовуючи цей метод, російські інформаційні кампанії намагаються перетворювати політичні розбіжності, етнічні та мовні відмінності, ставлення до мобілізації, конфесійні суперечки чи регіональні особливості на радикально несумісні табори. Як результат співгромадяни із відмінною світоглядною позицією починають сприйматися як ворожі опоненти і дедалі більше розглядаються як т.зв. «зрадники», «агенти ворожого впливу», «релігійні вороги або носії нелегітимної ідентичності».

У західноєвропейському контексті поляризація суспільства нерідко вибудовується довкола інших ліній: «народ» проти «глобалістських еліт», «традиційні європейці» проти мігрантів чи мультикультуралізму, «захисники суверенітету» проти Брюсселя. Російські інформаційні меседжі тут не завжди прямо прославляють кремль – значно частіше вони посилюють уже наявні крайні антиелітні та антиінституційні настрої, створюючи сприятливе середовище для нормалізації проросійських або антиукраїнських інтерпретацій.

Фактично можемо зауважити, що інформаційна агресія починається не з прямого пропагування радикальних дій чи закликів до насильства або знищення опонента, а скоріше зі зміни способу класифікувати соціальні відносини. Коли, наприклад, соціальна чи політична множинність замінюється бінарною схемою, різко звужується простір для компромісу, а отже – зростає ймовірність прийняття суспільством крайніх рішень та радикальних ідей. Саме тому, на наш погляд, метод поляризації у маніпулюванні суспільною свідомістю варто вважати одним із ключових: він створює базовий т.зв. «когнітивний каркас», на якому вибудовуються та розвиваються інші методи інформаційної агресії.

Вищевикладене апелює до побудови злагодженої інституційної архітектури інформаційно-психологічного протиборства у державі. Зокрема, створення в Україні Центру протидії дезінформації відіграє важливу роль у інформаційно-психологічному протиборстві, що сприяє виявленню та протидії дезінформації, пропаганді, деструктивним інформаційним впливам і кампаніям у медіа-середовищі, запобігання спробам маніпулювання суспільною свідомістю.

Також, пріоритетним є удосконалення правового регулювання відносин у сфері забезпечення інформаційної безпеки держави щодо посилення спроможностей протидії інформаційній агресії рф, захисту інформаційного простору України, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборонного потенціалу держави, попередження загроз державному суверенітету та територіальній цілісності України.

Жуков А. О.
Мірошніченко С. І.
Житомирський військовий інститут імені С. П. Корольова

## ПІДВИЩЕННЯ РІВНЯ ЗАХИСТУ АВТОМАТИЗОВАНИХ РОБОЧИХ МІСЦЬ ВІД ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ USB-НОСІЇ

У статті доктора технічних наук, професора, академіка НАН України М. З. Згуровського «Загальні питання інформаційної безпеки. Правове забезпечення захисту інформації. Міжнародне співробітництво у сфері захисту інформації» визначено, що характерною рисою нинішнього етапу науково-технічного прогресу є масове використання обчислювальної техніки в усіх сферах суспільного життя. Але це накладає і достатньо велику кількість інформаційних загроз по зчитуванню, копіюванню, знищенню інформації тощо.

Тому питання захисту інформації набуває особливої актуальності. Значна кількість інцидентів інформаційної безпеки пов'язана з використанням зовнішніх носіїв інформації, зокрема USB-накопичувачів. Завдяки компактності, високій швидкості передачі даних та великому обсягу пам'яті USB-носії стали одним із поширених засобів зберігання та перенесення інформації. Водночас їх використання створює потенційну загрозу витоку конфіденційних даних, особливо у випадках несанкціонованого підключення до автоматизованих робочих місць (АРМ).

Будь-яка організація, що працює з конфіденційною інформацією, повинна забезпечувати контроль за захистом інформації. Це можливо зробити або документальним обліком носіїв, що використовуються або програмним. Документальний облік не завжди є ефективним (є випадки порушення виконавцем цих норм), тому більш актуальним є впровадження систем

контролю USB-пристроїв (програмний спосіб обліку) які дозволяють визначати, які саме носії можуть використовуватися на конкретному ПК. Таким чином, актуальним завданням є підвищення рівня захищеності автоматизованих робочих місць від витоку інформації шляхом впровадження програмних засобів контролю використання USB-носіїв.

Для забезпечення захисту автоматизованих робочих місць пропонується система контролю використання USB-носіїв, яка реалізує механізм авторизації пристроїв. Основна ідея полягає у формуванні списку дозволених USB-носіїв, з якими дозволено працювати на конкретному комп'ютері.

При підключенні USB-пристрою система автоматично виконує перевірку його унікальних параметрів, зокрема серійного номера, ідентифікатора пристрою та виробника. Після перевірки система може виконати одну з дій:

- дозволити доступ, якщо даний пристрій є у списку дозволених;
- блокувати пристрій, якщо підключений носій відсутній у списку дозволених. Тоді система формує повідомлення користувачу та передає інформацію про подію адміністратору безпеки.
- надати обмежений доступ, наприклад тільки читання.

Основними перевагами запропонованого підходу є забезпечення повного контролю за використанням зовнішніх носіїв інформації з можливістю їх прив'язки до конкретного користувача, запобігання несанкціонованому копіюванню чи знищенню даних, ведення журналу безпеки з автоматичним інформуванням адміністратора, а також централізоване управління списком дозволених пристроїв і гнучке розмежування прав доступу для різних виконавців.Принцип роботи системи полягає у постійному моніторингу USB-портів комп'ютера. При підключенні нового пристрою виконується його ідентифікація та перевірка відповідності параметрів базі дозволених носіїв.

Структура роботи системи моніторингу наступна:

Користувач → USB-пристрій → модуль перевірки ідентифікаторів пристрою та виробника → база дозволених пристроїв → система прийняття рішення → рішення(дозвіл, блокування, обмежене використання тощо).

Система контролю USB-пристроїв безперервно моніторить порти комп'ютера, ідентифікуючи кожен підключений носій за базою дозволених пристроїв. Авторизовані накопичувачі отримують доступ до системи, тоді як незареєстровані - миттєво блокуються із одночасною фіксацією інциденту в журналі безпеки та сповіщенням адміністратора й користувача. Головною

особливістю клієнтського програмного забезпечення є регулярна перевірка наявності пристрою під час сесії: у разі його відключення або спроби підміни доступ до даних автоматично та негайно блокується. Модульна структура системи дозволяє забезпечити гнучкість та можливість подальшого розширення функціональних можливостей.

Запропонований підхід дозволяє забезпечити контроль використання зовнішніх носіїв інформації, запобігти несанкціонованому копіюванню даних та підвищити рівень інформаційної безпеки комп'ютерних систем в умовах функціонування сучасних інформаційно-комунікаційних систем.

Красенець М. В.
Національна академія Служби безпеки України

## ФУНКЦІОНУВАННЯ БОТОФЕРМ ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ ВІЙНИ російської федерації ПРОТИ УКРАЇНИ

Повномасштабна збройна агресія рф проти України супроводжується системними інформаційними та психологічними операціями. У цифровому середовищі вони не обмежуються діяльністю офіційних медіа або відкритих пропагандистських каналів. Значну роль відіграють ботоферми - приховані мережі акаунтів, які створюють видимість «самостійної» думки громадян, пришвидшують поширення маніпулятивних повідомлень і переносять кремлівські наративи у локальні онлайн-спільноти, які доцільно розглядати як інструмент не допоміжного, а безпосереднього впливу на інформаційну безпеку держави.

Під ботофермою у цьому дослідженні розуміється організована сукупність технічних засобів, програмного забезпечення та людських операторів, що забезпечують масове створення, підтримку й використання фіктивних або анонімізованих облікових записів. Її типовими елементами є SIM-карти або віртуальні номери, пристрої чи емулятори мобільних телефонів, проксі-інфраструктура, шаблони контенту, таблиці завдань, канали координації та фінансова мотивація виконавців. На відміну від поодинокого «бота», ботоферма має операційну стійкість: вона може швидко відновлювати заблоковані акаунти, змінювати платформи, адаптувати мову повідомлень і розподіляти ролі між автоматизованими та ручними діями.

Перша функція ботоферм — імітація суспільного консенсусу. Масові коментарі, однотипні дописи, «лайки», скарги та репости формують хибне враження, що певна позиція є поширеною або «народною». Для російських операцій це особливо важливо, адже відкрито проросійський меседж в українському інформаційному просторі часто сприймається критично. Тому він маскується під голос «розчарованого громадянина», «родича військового», «місцевого мешканця», «волонтера» або «експерта». У такий спосіб ботоферма не стільки переконує аргументами, скільки створює соціальний тиск: користувачеві здається, що навколо вже існує масове невдоволення, паніка або недовіра. Друга функція — прискорене розповсюдження наративів. Ботоферми працюють як «підсилювачі» інформаційних вкидів: вони швидко поширюють потрібне формулювання, виводять його у тренди, підхоплюють матеріали з анонімних каналів, підроблених сайтів або російських ресурсів і легітимізують їх через повторення. Типовими темами є дискредитація мобілізації, перебільшення втрат, твердження про «зовнішнє управління» Україною, корупцію у військовій допомозі, «втому» партнерів, протиставлення військових і цивільних, а також просування тези про «мир за будь-яку ціну». У міжнародній аудиторії ці самі меседжі трансформуються у заклики зменшити підтримку України, сумніви щодо санкцій або спроби представити агресора «стороною переговорів», а не джерелом війни. Третя функція — психологічний тиск у кризові моменти. Найбільш ефективними ботоферми стають під час ракетних обстрілів, відключень електроенергії, складних рішень органів влади або резонансних подій на фронті. У такі періоди аудиторія має підвищену потребу в інформації, а швидкість перевірки фактів знижується. Координовані акаунти можуть поширювати неперевірені дані про нібито «масові руйнування», «зраду командування», «евакуацію посадовців», «закриття кордонів» чи «капітуляційні домовленості». Мета полягає в тому, щоб збільшити тривожність, спровокувати конфлікти між групами населення і знизити довіру до офіційних повідомлень. Четверта функція — зв’язок інформаційної операції з кіберзагрозами. Українська практика демонструє, що ботоферми можуть бути не лише каналом пропаганди, а й інфраструктурою для фішингу, збору даних і підготовки атак. У 2024-2026 роках СБУ повідомляла про нейтралізацію ботоферм, які допомагали російським спецслужбам зламувати телефони українських військових і водночас поширювати кремлівські наративи; для

цього використовувалися анонімні номери та акаунти, зареєстровані в українському сегменті.

Отже, між інформаційною безпекою та кібербезпекою немає жорсткого поділу: одна й та сама мережа може формувати довіру до фейкового профілю, надсилати шкідливе посилання, а потім використовувати викрадені дані для нових інформаційних вкидів. П'ята функція — масштабування за допомогою штучного інтелекту. Генеративні моделі здешевлюють виробництво текстів, зображень, аватарів, перекладів і псевдолокальних коментарів. У липні 2024 року Міністерство юстиції США повідомило про зрив російської урядової AI-enabled bot farm, яка створювала фіктивні профілі у соціальній мережі X для поширення дезінформації у США та інших країнах, зокрема для підриву підтримки України. Це свідчить про перехід від простих «коментарних фабрик» до гібридних мереж, де люди задають політичні цілі й контролюють якість, а алгоритми забезпечують обсяг і варіативність повідомлень.

Протидія ботофермам має бути багаторівневою. На технічному рівні потрібні системи раннього виявлення координованої неавтентичної поведінки, обмін індикаторами між державними органами, платформами, дослідниками та громадським сектором. На правовому рівні важливими є документування доказів, встановлення організаторів, блокування фінансових каналів і притягнення до відповідальності осіб, які надають інфраструктуру для ворожих операцій. На платформному рівні необхідні швидкі процедури маркування, обмеження охоплення, видалення мереж і прозорі звіти про причини таких рішень. На суспільному рівні пріоритетом є інформаційна грамотність: користувач повинен розуміти, що «багато однакових коментарів» не дорівнює реальній громадській думці. Особливої уваги потребує захист військовослужбовців, волонтерів, посадовців органів місцевого самоврядування та журналістів. Для них ботоферми становлять подвійну загрозу: репутаційну, коли через скоординовані атаки дискредитується конкретна особа чи підрозділ, і технічну, коли через фейкові профілі здійснюється соціальна інженерія. Мінімальними практиками мають бути двофакторна автентифікація, перевірка контактів у месенджерах, обмеження публікації персональних даних, навчання розпізнаванню фішингових повідомлень і фіксація підозрілої активності для подальшого розслідування.

Таким чином, можна стверджувати, що ботоферми є одним із найбільш гнучких інструментів інформаційної війни рф проти України, оскільки

поєднують дешевизну, масштабованість, анонімність і можливість швидко пристосовуватися до змін інформаційного порядку денного. Їхня мета полягає не лише у поширенні окремих фейків, а у довготривалому виснаженні довіри: до держави, війська, медіа, міжнародних партнерів і співгромадян. Через це боротьба з ботофермами не може зводитися до видалення окремих акаунтів. Вона має бути частиною національної системи інформаційної та психологічної стійкості. Перспективним напрямом подальших досліджень є створення міждисциплінарної методики оцінювання впливу ботоферм, яка враховуватиме не тільки кількість акаунтів чи повідомлень, а й зміну поведінки аудиторії, поширення недовіри, емоційну поляризацію та зв'язок із реальними кризовими подіями. Для України така методика має прикладне значення: вона допоможе швидше відрізняти органічну критику від ворожої координації, захищати демократичну дискусію і водночас не допустити перетворення протидії дезінформації на необґрунтоване обмеження свободи слова.

Охота К. О.
Рачкінда В. А.
Житомирський військовий інститут імені С. П. Корольова

## АКТУАЛЬНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Ключові проблеми інформаційної безпеки в сучасному світі зумовлена стрімким розвитком цифрових технологій та глибокою інтеграцією інформаційних систем у всі сфери життєдіяльності суспільства. Сьогодні інформація є одним із найцінніших ресурсів держави, бізнесу та окремої особи. Вона використовується для управління, комунікації, прийняття рішень та забезпечення функціонування критичної інфраструктури. Водночас зростання залежності від інформаційних технологій призводить до появи нових загроз, які можуть мати як локальний, так і глобальний характер.

Особливої гостроти ця проблема набуває в умовах гібридних конфліктів, коли інформаційний простір стає окремим полем протиборства. Противники активно використовують кіберзасоби для впливу на громадську думку, дестабілізації соціально-політичної ситуації та отримання несанкціонованого доступу до конфіденційних даних. У таких умовах інформаційна безпека

перетворюється на важливий елемент національної безпеки, від якого залежить стабільність державних інституцій та суспільства в цілому. Особливо небезпечними є атаки на критичну інфраструктуру, зокрема енергетичні системи, транспортні мережі та фінансові установи, оскільки їх порушення може призвести до масштабних наслідків для економіки та безпеки держави.

Ще однією суттєвою проблемою є недостатній рівень захищеності інформаційних систем у багатьох державних установах та приватних структурах. У ряді випадків використовується застаріле програмне забезпечення, відсутні сучасні системи моніторингу та реагування на дії інциденти, що створює додаткові вразливості.

Важливе значення має вдосконалення нормативно-правової бази у сфері захисту інформаційних систем. Держава повинна забезпечити ефективне регулювання інформаційних відносин, встановлення відповідальності за кіберзлочини та створення умов для взаємодії між державними органами, приватним сектором і міжнародними партнерами. Особливе значення має міжнародне співробітництво, оскільки кіберзагрози часто не мають чітких географічних меж.

Окремої уваги потребує підготовка кваліфікованих фахівців у сфері інформаційної безпеки. Освітні програми повинні відповідати сучасним вимогам та враховувати реальні виклики кіберпростору. Крім того, необхідно підвищувати рівень цифрової грамотності населення, формувати культуру безпечної роботи з інформацією та навчати базовим правилам кібергігієни.

Обґрунтування важливості вирішення зазначених проблем полягає в тому, що стабільне функціонування сучасного суспільства безпосередньо залежить від надійності інформаційних систем. Будь-яке порушення їх роботи може призвести до значних економічних втрат, зниження ефективності державного управління та активізації деструктивних соціальних проявів. У крайніх випадках кібератаки можуть становити загрозу національній безпеці та суверенітету держави.

Таким чином, інформаційна безпека є одним із ключових елементів сучасної системи безпеки держави. Вона потребує постійного розвитку, адаптації до нових викликів та впровадження інноваційних технологій захисту. Лише системний підхід, що поєднує технічні засоби, правове регулювання та підготовку кадрів, дозволить ефективно протидіяти сучасним кіберзагрозам і забезпечити стабільний розвиток інформаційного суспільства.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Пащетник О. Д., канд. техн. наук, ст. наук. співроб.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

# АРХІТЕКТУРНІ ВИМОГИ ДО ВИКОРИСТАННЯ ХМАРНИХ РІШЕНЬ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Сучасні інформаційно-комунікаційні системи (ІКС) військового призначення функціонують в умовах постійного зростання обсягів інформації, необхідності безперервного обміну даними між органами військового управління та скорочення циклу прийняття рішень. Особливої актуальності це набуває в умовах сучасних бойових дій, де ефективність управління підрозділами безпосередньо залежить від швидкості збору, оброблення та передачі інформації між різнорідними системами, пунктами управління, засобами розвідки та вогневого ураження. Одним із перспективних напрямів розвитку таких систем є впровадження хмарних рішень, які забезпечують масштабованість обчислювальних ресурсів, централізоване зберігання даних та оперативний доступ до інформації з різних рівнів управління. Разом із тим, використання хмарних технологій в ІКС супроводжується суттєвими ризиками у сфері інформаційної безпеки. Публічні та гібридні хмарні середовища характеризуються обмеженим рівнем фізичного контролю над ресурсами, залежністю від зовнішніх телекомунікаційних каналів та складністю контролю життєвого циклу даних. За таких умов традиційні підходи до побудови комплексних систем захисту інформації не забезпечують необхідного рівня ізоляції та контролю доступу.

Особливої уваги потребує проблема оброблення різнорівневої за класифікацією інформації в межах єдиної хмарної інфраструктури. У сучасних ІКС можуть одночасно циркулювати службові, оперативні, розвідувальні дані та інформація з обмеженим доступом. Це створює необхідність побудови архітектури, здатної забезпечити ізоляцію інформаційних потоків, розмежування прав доступу та виключення неконтрольованого перетину даних між сегментами системи. Однією з базових вимог до такої архітектури є реалізація принципу повної сепарації ролей користувачів та адміністративних доменів. Жоден користувач або сервісний обліковий запис не повинен мати

повного контролю над критичними компонентами системи, включаючи механізми керування доступом, журнали подій та криптографічні сервіси. Для цього в архітектурі ІКС має використовуватись централізований домен ідентичностей, який забезпечує єдину систему автентифікації, авторизації та управління ролями користувачів і сервісів.

Критичні операції, пов'язані зі зміною політик доступу, управлінням ключами шифрування або видаленням даних, повинні виконуватись за принципом колективного контролю із повним журналюванням супутніх метаданих. Важливим елементом архітектури є застосування моделей керування доступом RBAC та ABAC, що дозволяють враховувати не лише роль користувача, а й контекст доступу: тип пристрою, мережеве середовище, рівень допуску та тип інформації.

Окремого значення набуває реалізація концепції Zero Trust Architecture, відповідно до якої жоден користувач, сервіс або сегмент мережі не розглядається як довірений за замовчуванням. У межах такого підходу кожна дія суб'єкта доступу повинна супроводжуватися перевіркою автентичності, контексту доступу та відповідності політикам безпеки. Реалізація принципів Zero Trust дозволяє знизити ризики поширення атак у разі компрометації окремих компонентів системи. У сучасних умовах важливим компонентом захищеної хмарної інфраструктури є підсистема спостережуваності та аудиту. Усі дії користувачів, зміни політик, операції з даними та криптографічними ключами повинні фіксуватись у незмінних журналах подій із забезпеченням цілісності записів. При цьому система журналювання має бути архітектурно відокремленою від доменів адміністрування, що мінімізує ризик приховування слідів несанкціонованої діяльності. Не менш важливою вимогою є створення окремої криптографічної підсистеми, призначеної для генерації, перевірки, зберігання та вилучення ключів шифрування і цифрових підписів. Компрометація криптографічної інфраструктури в умовах військових ІКС може призвести до втрати контролю над усією системою захисту інформації, тому механізми управління ключами повинні бути максимально ізольованими та захищеними від несанкціонованого доступу.

Таким чином, в доповіді пропонується підхід до побудови архітектури захищеної хмарної інфраструктури для ІКС військового призначення, який базується на принципах Zero Trust Architecture, повної сепарації ролей

користувачів і адміністративних доменів, ізоляції даних різних рівнів доступу, централізованого управління ідентичностями, обов'язкового аудиту подій безпеки та використання окремої криптографічної підсистеми для забезпечення цілісності, конфіденційності та доступності інформаційних ресурсів.

Петренко С. В.
Національна академія Служби безпеки України

## НАРАТИВНІ МЕХАНІЗМИ РОСІЙСЬКОГО КОГНІТИВНО-ГЕОПОЛІТИЧНОГО ВПЛИВУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

У сучасних умовах гібридної конфронтації інформаційний простір став окремим полем геополітичного протиборства. Суперництво держав відбувається не лише у військовій, економічній чи дипломатичній сферах, а й у сфері смислів та інтерпретацій подій. У цьому контексті стратегічні наративи є важливим інструментом впливу, який формує способи сприйняття реальності та опосередковано впливає на політичні рішення як усередині країн, так і на міжнародному рівні.

Росія використовує наративні механізми як частину комплексної системи гібридного впливу, де інформаційні, військові, дипломатичні та економічні інструменти діють у взаємозв'язку. У цій системі наратив виконує не допоміжну, а ключову роль, оскільки забезпечує смислову єдність усіх форм впливу. Його основна функція полягає у легітимації дій росії та формуванні альтернативного пояснення міжнародних подій. Стратегічний наратив можна розглядати як спосіб конструювання політичної реальності. Він визначає, як пояснюються події, які причини їм приписуються та яку роль отримують різні учасники конфлікту. У результаті контроль над наративами означає вплив на те, як аудиторія думає і оцінює ситуацію. Тому наративи фактично набувають ознак когнітивного інструменту впливу на суспільство.

У російській стратегії важливе місце займає делегітимація української державності. Це реалізується через поширення тез про «штучність» України, її «зовнішнє управління» та «відсутність історичної самостійності». Такі наративи спрямовані на підрив міжнародного визнання України як повноцінної держави та створюють підґрунтя для виправдання російської агресії.

Пов'язаним з цим наративом є маніпулятивне трактування історії. Історичні події використовуються для політичних цілей, зокрема для заперечення самостійного існування української нації. Також росія активно застосовується наратив «неонацизму», який має кілька функцій: виправдання війни, мобілізацію внутрішньої аудиторії та формування негативного образу України на міжнародному рівні. Ще одним напрямом є дискредитація українських державних інституцій і сектору безпеки та оборони України. Через інформаційні операції поширюються твердження про «неефективність влади», «корупцію» та «виснаження армії». Усередині України це знижує довіру до держави, а за її межами впливає на ставлення до підтримки України.

Російські наративи поширюються через різні канали: традиційні медіа, соціальні мережі, телеграм-канали, дипломатичні заяви та мережі псевдоекспертів. Така багатоканальність створює ефект «багатьох джерел», коли одна і та сама ідея виглядає підтвердженою з різних сторін і сприймається як правдива. Важливою рисою цих наративів є їхня адаптивність. Вони змінюють форму залежно від ситуації, але зберігають головну мету. Будь-які події військові, політичні чи економічні використовуються для повторення вже знайомих меседжів про «втому Заходу», «неефективність санкцій» або «необхідність переговорів на умовах росії».

На міжнародному рівні російські наративи спрямовані на різні аудиторії. У західних країнах акцент робиться на економічних витратах і ризиках ескалації. У країнах Глобального Півдня використовуються теми антиколоніалізму та критики «подвійних стандартів», що дозволяє росії виглядати альтернативним центром впливу. Окремим завданням є підрив санкційної політики. Через поширення ідей про «неефективність санкцій» і «втому Європи» створюється інформаційне середовище, яке послаблює єдність держав-партнерів і ускладнює ухвалення спільних рішень. У результаті російська наративна експансія створює загрозу не лише інформаційній безпеці, а й когнітивній стійкості суспільства, тобто здатності критично сприймати інформацію, зберігати довіру до інституцій і протистояти маніпуляціям. Тому поняття когнітивної безпеки набуває особливого значення в системі національної безпеки. Протидія цьому впливу потребує не лише спростування дезінформації, а й формування власних послідовних стратегічних наративів. Важливими є координація державних інституцій, розвиток стратегічних комунікацій та підвищення медіаграмотності суспільства.

Отже, російська наративна експансія є системним інструментом геополітичного впливу, який поєднує пропаганду, дезінформацію та когнітивні операції. Її мета полягає у впливі на міжнародне сприйняття війни та послабленні підтримки України. Тому в сучасних умовах ключового значення набувають когнітивна безпека та ефективні стратегічні комунікації як засоби нейтралізації деструктивного інформаційного впливу.

Резуненко Д. О.
Кузьмичев А. В.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

## ІНФОРМАЦІЙНА БЕЗПЕКА ОСОБОВОГО СКЛАДУ

Однією з особливостей бойових дій останніх років стало різке зростання впливу інформаційного середовища на морально-психологічний стан військовослужбовців. Інформація сьогодні здатна не лише допомагати в управлінні військами, а й створювати додаткові загрози для особового складу. Для військовослужбовців інженерних підрозділів це питання набуває особливого значення, оскільки їхня діяльність пов’язана з високим рівнем відповідальності, тривалим фізичним навантаженням та роботою у небезпечних умовах.

Психологічне виснаження дедалі частіше виникає не лише через фізичні фактори, а й через постійне перебування в інформаційному полі. Військовослужбовець змушений одночасно працювати з великою кількістю джерел інформації. Надлишок інформації у стресових умовах негативно впливає на концентрацію уваги та підвищує ризик помилкових рішень. Особливо небезпечними є неперевірені повідомлення та емоційний контент. Практика бойових дій показує, що навіть короткочасний інформаційний вплив здатний суттєво змінювати морально-психологічний стан особового складу. Для військовослужбовців проблема інформаційної безпеки має декілька важливих аспектів. Значна частина завдань виконується в умовах високої відповідальності та потребує максимальної уважності.

Під час виконання завдань із розмінування деокупованих територій особовий склад інженерних підрозділів часто працює у режимі багатогодинного

психологічного напруження. Найбільш стійкими залишалися ті підрозділи, де командири підтримували постійну комунікацію з особовим складом. Підготовлений, психологічно стійкий та інформаційно захищений військовослужбовець здатний ефективно діяти в умовах високого навантаження, постійного ризику та невизначеності бойової обстановки. У сучасних умовах вирішальне значення має не лише рівень професійної підготовки, а й здатність військовослужбовця зберігати самоконтроль, критичне мислення та психологічну рівновагу під впливом стресових факторів. Військовослужбовець, який уміє працювати в умовах інформаційного перевантаження, протидіяти дезінформації та швидко адаптуватися до змін оперативної обстановки, значно ефективніше виконує поставлені завдання та знижує ризики для особового складу. Саме поєднання професійної компетентності, психологічної витривалості, інформаційної грамотності та згуртованості підрозділу сьогодні є одним із ключових чинників збереження боєздатності інженерних військ та успішного виконання завдань у складних умовах воєнного стану.

Ясінський Р. А.
Рачкінда В. А.
Житомирський військовий інститут імені С. П. Корольова

## ПРОГРАМА ФОРМУВАННЯ СЛОВНИКА ПЕРЕГОВОРНИХ ТАБЛИЦЬ

Повномасштабне вторгнення російської федерації в Україну суттєво підвищило значення захищеного та оперативного обміну інформацією між підрозділами. В умовах активного застосування перехоплення сигналів особливої актуальності набуло використання переговорних таблиць і систем кодування повідомлень. Саме тому автоматизація процесу формування словника переговорних таблиць стала важливим завданням для забезпечення ефективного управління та координації дій підрозділів.

Отже швидкість передачі інформації безпосередньо впливає на ефективність виконання поставлених завдань та безпеку особового складу. Використання спеціалізованих програм дозволяє значно скоротити час створення та обробки переговорних таблиць, мінімізувати помилки оператора

та забезпечити надійне збереження службових даних. Крім того, впровадження таких програмних засобів сприяє підвищенню стійкості систем зв'язку до впливу противника та відповідає сучасним вимогам ведення війни.

Переговорні таблиці застосовуються для заміни окремих слів, фраз або команд спеціальними кодами чи умовними позначеннями. Використання таких таблиць значно спрощує процес обміну інформацією між абонентами та дозволяє уникати відкритої передачі важливих відомостей. Проте традиційний спосіб створення словників переговорних таблиць має низку недоліків. Насамперед це значні витрати часу на ручне внесення термінів, висока ймовірність помилок під час введення даних, складність редагування та пошуку необхідної інформації. Крім того, при роботі з великою кількістю кодових слів виникає проблема впорядкування та швидкого доступу до потрібних термінів.

Для вирішення зазначених проблем було запропоновано створення спеціалізованої програми формування словника переговорних таблиць. Основною метою такої програми є автоматизація процесу створення, редагування, збереження та використання переговорних таблиць. Програма дозволяє значно скоротити час роботи оператора та мінімізувати ризик виникнення помилок.

Структура програми передбачає наявність бази даних, у якій зберігаються терміни та відповідні їм коди. Користувач має можливість додавати нові записи, редагувати вже існуючі або видаляти непотрібні елементи. Однією з важливих функцій є автоматичне генерування кодів для термінів, що значно спрощує процес створення переговорних таблиць. Також програма може підтримувати імпорт готових словників із файлів формату Excel, що дозволяє швидко завантажувати великі обсяги інформації без необхідності ручного введення.

Важливою перевагою програми є зручний інтерфейс користувача. Для реалізації графічної частини можуть використовуватися сучасні бібліотеки програмування, зокрема Tkinter у мові Python. Це дозволяє створити просте та зрозуміле середовище для роботи користувача. Інтерфейс може містити таблиці з термінами, поля для пошуку, кнопки додавання та редагування даних, а також систему авторизації для захисту доступу до інформації.

Окрему увагу приділено забезпеченню безпеки даних. Оскільки переговорні таблиці можуть містити важливу службову інформацію, програма повинна забезпечувати захист від несанкціонованого доступу. Для цього може використовуватися парольний захист, шифрування файлів або система резервного копіювання даних.

Таким чином, програма формування словника переговорних таблиць є ефективним засобом автоматизації роботи з кодованою інформацією. Її впровадження дозволяє підвищити швидкість обробки даних, зменшити кількість помилок та покращити організацію роботи користувачів. Використання сучасних технологій програмування та автоматизації робить таку програму перспективним інструментом для застосування у військовій сфері, системах зв'язку та інших галузях, де важливими є оперативність, точність та захист інформації яка передається і її адресатам.

Гута С. С.
Воєнна академія імені Євгенія Березняка

## ІНФОРМАЦІЙНА БЕЗПЕКА ТА РОЗВІДУВАЛЬНІ СПРОМОЖНОСТІ МАЛИХ ДЕРЖАВ: ДОСВІД КАТАРУ ТА ЙОГО ЗНАЧЕННЯ ДЛЯ УКРАЇНИ

У сучасних умовах трансформації міжнародної системи питання інформаційної безпеки та розвідувальних спроможностей держав набувають особливого значення, наприклад посилення глобальної конкуренції, розвиток інформаційних технологій, гібридні конфлікти та поширення кіберзагроз суттєво змінили підходи до забезпечення національної безпеки.

У XXI столітті ефективність держави дедалі більше визначається не лише військовими чи економічними ресурсами, а й здатністю здійснювати інформаційний вплив, формувати міжнародний порядок денний та забезпечувати аналітичну підтримку стратегічних рішень, особливо актуальним це питання є для малих держав, які в умовах обмежених ресурсів змушені шукати нові механізми забезпечення власної безпеки та міжнародного впливу.

Одним із найбільш показових прикладів такої держави є Катар. Незважаючи на невелику територію, обмежений демографічний потенціал та складне геополітичне оточення, Катар зумів сформувати ефективну модель зовнішньої політики, яка базується на поєднанні дипломатії, інформаційного впливу, енергетичних ресурсів та розвідувальних інструментів, їхній досвід демонструє, що в сучасному багатополярному світі навіть малі держави можуть виступати активними суб'єктами міжнародних відносин та впливати на регіональні процеси.

Теоретичні підходи сучасної політичної науки свідчать про поступову трансформацію розуміння державної сили, якщо представники класичного реалізму розглядали міжнародні відносини переважно крізь призму військової могутності та балансу сил, то сучасні концепції акцентують увагу на інформаційних, дипломатичних та інституційних механізмах впливу. Зокрема концепція "м'якої сили" Дж. Ная, а також сучасні підходи до "розумної сили" (smart power) підтверджують, що інформація, комунікація та міжнародна репутація стають важливими інструментами реалізації зовнішньополітичних інтересів держави. Катар активно використовує ці інструменти у власній зовнішній політиці. Важливу роль у формуванні міжнародного впливу держави відіграє глобальна медіамережа Al Jazeera, яка фактично стала інструментом стратегічної комунікації та інформаційного впливу, через міжнародний інформаційний простір Катар отримав можливість впливати на формування громадської думки, висвітлення регіональних конфліктів та просування власних політичних позицій.

Катар зумів побудувати систему координації між дипломатичними структурами, медіаресурсами, аналітичними центрами та безпековими органами, що дозволяє швидко реагувати на зміни міжнародного середовища, так держава активно використовує політику стратегічного хеджування, підтримуючи відносини з різними центрами сили та уникаючи надмірної залежності від одного союзника.

Для України досвід Катару має важливе практичне значення, де російсько-українська війна продемонструвала, що сучасні конфлікти ведуться не лише на полі бою, а й в інформаційному просторі. Кібератаки, інформаційно-психологічні операції, дезінформація та маніпуляція громадською думкою стали складовими сучасної гібридної війни. У таких умовах особливого значення набуває розвиток системи стратегічних комунікацій, інформаційної протидії та аналітичного забезпечення державної політики.

Україна вже має значний досвід у сфері інформаційної безпеки та міжнародної комунікації, але сучасні виклики потребують подальшого вдосконалення механізмів координації між дипломатичними структурами, розвідувальними органами, медіасектором та кібербезпековими інституціями. Важливим напрямом також залишається розвиток міжнародного інформаційного партнерства та формування позитивного міжнародного іміджу України як держави, що протистоїть зовнішній агресії та захищає демократичні цінності.

Отже, сучасне розуміння інформаційної безпеки виходить далеко за межі технічного захисту інформаційних систем. Воно охоплює питання стратегічних комунікацій, дипломатії, медіавпливу, розвідки та міжнародного позиціонування держави. Тому, досвід Катару підтверджує, що навіть малі держави здатні компенсувати обмежені матеріальні ресурси за рахунок ефективного використання інформаційних і дипломатичних інструментів. Також, використання для України подібних підходів може стати важливим чинником зміцнення національної безпеки, підвищення міжнародної суб'єктності та ефективної протидії сучасним гібридним загрозам.

Заєць Я. Г., канд. техн. наук, ст. досл.
Давіденко С. В., канд. техн. наук, доц.
Чорняк І. І.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

## ФАКТОРИ, НА ЯКІ СЛІД ЗВЕРТАТИ УВАГУ ВІЙСЬКОВОСЛУЖБОВЦЮ ПІД ЧАС ВИКОРИСТАННЯ МОБІЛЬНОГО ТЕЛЕФОНУ

Не таємниця, що дані з вашого мобільного телефона можуть розповісти про вас ворогу все. І річ не тільки в тому, що окремі військовослужбовці, попри заборону, не тільки користуються на «нулях» гаджетом, але ще й викладають із району бойових дій певну інформацію й світлини в соціальні мережі, не усвідомлюючи, що іноді один кадр може надати ворогу більше інформації, ніж тактична та агентурна розвідки.

Слід пам'ятати, що з першим ввімкненням придбаного гаджета ви погоджуєтеся з умовами використання його програмного забезпечення, поставивши галочку в полі «Я прочитав та погоджуюся з умовами». Отже, з цього моменту, ви довіряєте клавіатурі, камері та мікрофону все своє віртуальне життя – разом із листуваннями, паролями, іншими секретами.

Яким же чином, не маючи спеціальних знань, виявити, які «вшиті» або завантажені пізніше додатки й програми вас таємно контролюють та отримують від вас інформацію?

На практиці все доволі просто – до прикладу, необхідно встановити програму Safe Dot чи будь-який її аналог. Такі програми вміють подавати тривожні сигнали,

коли хтось приховано використовує ваш мікрофон або камеру, бази даних. Ви можете налаштувати вібросигнал – і щоразу, коли будь-яка чужа програма під'єднається до вашої камери чи мікрофона, телефон буде вібрувати. Ви можете відстежувати, які програми й коли мали доступ до вашої камери й мікрофона. У такому разі можна прибрати через їхні налаштування свій дозвіл на доступ до мікрофона й камери або просто їх видалити, знищуючи шпигуна.

Не менш просто впоратися зі шпигунською клавіатурою. Щоб убезпечити себе з цього боку, можна встановити на свій девайс клавіатуру від будь-якого стороннього виробника, якому ви довіряєте. Наприклад, з магазину відкритого програмного забезпечення F-Droid. Те саме стосується доступу до вашого екрана. Зайдіть у налаштування програм і перевірте надані для кожної з них дозволи – серед них не має бути дозволу на запис екрана (окрім програм, яким він справді необхідний, як-от Zoom).

Доступ до вашої камери для ворожих програм складніший. Тому що стежити за вами через камеру зможуть лише ті програми, яким ви самі надали такий дозвіл під час встановлення. Тож слід звертати увагу на всі згоди, які вона вимагає. Коли софт для відеоконференцій просить доступу до камери девайсу – це нормально. А от коли такий доступ просить мобільна гра – виникає серйозний привід задуматися.

Необхідно пам'ятати, що за допомогою підконтрольного ворогу смартфона можна:

контролювати місце вашого розташування в реальному часі;

«читати» все, що ви вводите на клавіатурі;

відстежити історію вашого місцеперебування та переміщень;

передати сповіщення про те, що ви покинули певне місце або прибули до нього;

«побачити» вас та навколишні події за допомогою вбудованої камери;

прослухати все, що ви говорите, дізнатися, що відбувається навколо вас.

Яким чином самостійно можна уникнути зараження телефону шпигунською програмою?

Не давайте стороннім людям користуватися вашим смартфоном. Якщо заряджаєте смартфон від джерела в громадському місці, переконайтеся, що адаптер живиться від мережі, а на кабелі немає додаткових електронних пристроїв.

Не переходьте за посиланнями в листах та месенджерах, тримайте увімкненим антивірус й регулярно його оновлюйте.

Вивчайте відгуки й рейтинги програм, які ви збираєтеся завантажити.

Не використовуйте Jailbreak (root-доступ, права суперкористувача тощо) на своєму телефоні. Переваги, які це дає, непорівнянні із загрозами конфіденційності.

Перевірте налаштування безпеки вашого пристрою щодо дозволу встановлення програм із невідомих джерел. Завантажувати програми з невідомих джерел ні в якому разі не можна.

Видаліть усі непотрібні програми якими ви не користуєтесь, щоб легше орієнтуватися в процесах і контролювати свій пристрій.

Регулярно оновлюйте смартфон. Якщо програмне забезпечення вашого гаджету не оновлюється і його підтримка завершена виробником – саме час змінити пристрій.

Регулярно змінюйте паролі. Щоб покращити безпеку, використовуйте менеджери паролів. Це дозволить вам генерувати та зберігати складні паролі для кожного сервісу, мінімізуючи ризик їх витоків. Вибирайте якісні менеджери паролів, які забезпечують шифрування даних та захист від атак грубої сили.

Касаткін Є. В.
Микитин В. Ф.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

## ІНФОРМАЦІЙНА ФРАГМЕНТАЦІЯ ЯК ЗАГРОЗА КЕРОВАНОСТІ СИСТЕМИ ТЕРИТОРІАЛЬНОЇ ОБОРОНИ

Перебіг подій широкомасштабної агресії рф проти України підвищив залежність системи територіальної оборони, як складової національного спротиву від ефективності функціонування інформаційного середовища. Сучасна війна характеризується стрімким зростанням рівня інформаційної фрагментації, тобто розподілу єдиного інформаційного простору на значну кількість неузгоджених, конкуруючих або слабо контрольованих інформаційних середовищ, що створює додаткові ризики для збереження керованості системи управління, у т.ч. військового. Особливої актуальності проблема набуває в умовах тривалої війни високої інтенсивності, коли поряд із зовнішнім інформаційним впливом противника дедалі більшу роль починають відігравати внутрішні процеси інформаційної дезорганізації, емоційного виснаження та

зниження довіри до окремих управлінських рішень. За таких обставин формується інформаційний простір одночасного функціонування великої кількості паралельних джерел. Особовий склад підрозділів Сил ТрО, представники місцевої влади, волонтерське середовище, населення одночасно отримують інформацію з офіційних каналів, соціальних мереж, Telegram-ресурсів, медіа, особистих контактів та неформальних інформаційних спільнот, в результаті, відбувається розмиття пріоритету офіційної інформації, зниження рівня централізованої керованості інформаційним середовищем. Небезпеку для інформаційно залежного суспільства становить поширення емоційно забарвленої інформації. Негативні повідомлення часто поширюються швидше за офіційні роз'яснення. В умовах війни на виснаження це створює передумови для формування локальних осередків недовіри, поширення чуток та виникнення деструктивних інформаційних кампаній навіть без прямого втручання ворога. Окремою проблемою є поступовий розвиток неформальних центрів інформаційного впливу: окремі Telegram-канали, блогери, медійні особи здатні впливати на психологічний стан військовослужбовців, населення, формувати альтернативні інтерпретації подій або підсилювати конфліктність інформаційного поля. Практика підтверджує: навіть непідтверджені вкиди про нібито «оточення», «зраду», «обвал фронту», поширені через популярні цифрові ресурси, створюють локальні осередки дезорганізації швидше, ніж офіційні джерела встигають реагувати. Ускладнює ситуацію перебування підрозділів Сил ТрО у складі угрупувань військ як механізованих, що загострює реагування та відповідний негативний вплив не лише на морально-психологічний стан, а й на рівень дисципліни, довіри до командування, ефективність управління та виконання бойових завдань. Відтак, забезпечення єдиного інформаційного контуру системи територіальної оборони потребує комплексного підходу, який має поєднувати організаційні, інформаційні та психологічні механізми. Головним має стати посилення ролі офіційних каналів внутрішньої комунікації. Оскільки інформаційний вакуум заповнюється маніпулятивним контентом, особовий склад повинен своєчасно отримувати достовірну інформацію. Важлива підготовка командирів до функціонування в умовах високої інформаційної турбулентності, адже лідер дедалі більше виконує функцію не лише організатора бойових дій, а й стабілізатора внутрішнього інформаційного середовища, а від оперативності його реагувати на деструктивні інформаційні явища залежить рівень керованості підрозділу. Не менш важливим є формування системної інформаційної гігієни особового складу. Мова про

навички критичного сприйняття інформації, дотримання цифрової дисципліни, усвідомлення ризиків неконтрольованого поширення інформації. Досвід підтверджує, що навіть фрагментарне оприлюднення інформації про переміщення підрозділів, наслідки ударів або особливості бойової роботи негайно використовується ворогом. Тут небезпеку становить і деструктивний вплив окремих представників внутрішнього інформ середовища, які через політичну заангажованість і гонитву за аудиторією підсилюють інформаційний тиск ворога. Таким чином, інформаційна фрагментація в умовах сучасної війни поступово перетворюється на один із суттєвих чинників ризику для забезпечення керованості системи територіальної оборони України. Поєднання високої залежності від цифрових комунікацій, значної кількості горизонтальних інформаційних зв'язків, тривалого психологічного виснаження суспільства та активного інформаційного впливу противника створює передумови для дезорганізації інформаційного середовища та зниження ефективності управління. За таких умов забезпечення інформаційної стійкості та формування єдиного інформаційного контуру системи територіальної оборони повинні розглядатися як один із визначальних елементів функціональної стійкості, дисципліни та бойової ефективності Сил ТрО.

Петлюк І. В., канд. техн. наук, ст. досл.
Пащетник О. Д., канд. техн. наук, ст. наук. співроб.
Чорняк І. І.
Гелета С. М.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

## КІБЕРБЕЗПЕКА ЛОГІСТИЧНИХ СИСТЕМ ПІДРОЗДІЛІВ ЗБРОЙНИХ СИЛ УКРАЇНИ

Аналіз російсько-української війни 2014–2026 років показує, що в умовах активних бойових дій питання кібербезпеки логістичних систем стає надзвичайно актуальним. Однією з ключових складових надійного та безперебійного забезпечення підрозділів під час бойових дій є кібербезпека логістичних систем військових підрозділів. Логістичні мережі стають все більш вразливими до кібератак, які можуть призвести до зриву постачань, втрати

важливої інформації та навіть повного виходу з ладу систем управління логістичними операціями. Кожна із воюючих сторін намагається втрутитися у логістичні процеси, спотворюючи дані про запаси та руйнуючи канали зв'язку між логістичними підрозділами, створюючи фальшиві маршрути постачання,. Масовані атаки на критичну інфраструктуру та цифрові системи управління порушують безперервність постачань, дезорієнтують командування та створюють небезпеку для військових підрозділів. Злом систем управління запасами може призвести до прийняття хибних рішень щодо розподілу ресурсів, а спотворення даних про маршрути доставки – до втрати вантажів та збільшення ризику для особового складу.

Одним із перспективних напрямів для підвищення кібербезпеки є впровадження стандартів безпеки на кожному етапі логістичного процесу, а саме: шифрування даних; контроль доступу до систем управління запасами; регулярні аудити безпеки для виявлення вразливостей.

Для швидкої ідентифікації потенційних загроз та запобіганню їх реалізації важливу роль відіграє інтеграція штучного інтелекту та машинного навчання, які спроможні автоматично виявляти та аналізувати аномальну активність в логістичних системах. Досвід російсько-української війни показує, що ключовими напрямами захисту логістичних систем є створення багаторівневих систем кібербезпеки з можливістю швидкої адаптації до нових загроз, використання інструментів кіберрозвідки для активного виявлення атак та забезпечення оперативного реагування з мінімальним впливом на логістичні операції. Враховуючи специфіку бойових дій та постійні зміни у тактичній обстановці українські логістичні підрозділи активно розвивають та вдосконалюють цей напрям. Використання інноваційних рішень, таких як автономні системи моніторингу та захисту даних, дозволяють підвищити стійкість логістичних операцій та забезпечити надійне постачання підрозділів у найскладніших умовах.

Наявність чітких протоколів захисту логістичних процесів зменшить можливість втрати контролю над ланцюгами постачання, витоку інформації та виходу з ладу критично важливих елементів логістичних систем.

Інформаційна безпека на даному етапі виступає не лише технічним інструментом, а й стратегічним чинником, що визначає ефективність та життєздатність військових підрозділів в умовах сучасної війни. Поєднання

кіберзахисту, навчання особового складу основам кібергігієни є комплексною системою оборони військових підрозділів силових структур ЗС України. Інформаційна безпека є фундамент сучасної військової стратегії, гарантом ефективності бойових дій, збереження суверенітету держави.

Таким чином, впровадження комплексного підходу до кіберзахисту та інформаційної безпеки логістичних систем дозволяє не лише захистити поточні операції від кібератак, а й створити більш стійку та адаптивну логістичну мережу, здатну ефективно підтримувати військові підрозділи навіть у критичних умовах. Захист логістичних операцій від кіберзагроз та інформаційної безпеки є одним із найважливіших аспектів забезпечення безпеки та боєздатності військових частин на сучасному етапі розвитку збройних конфліктів.

Польцев І. В.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

## ВИКОРИСТАННЯ OSINT У ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ПІД ЧАС РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Повномасштабна російсько-українська війна продемонструвала, що інформаційний простір став одним із ключових театрів сучасного протистояння. Поряд із бойовими діями російська федерація активно застосовує дезінформаційні кампанії, інформаційно-психологічні операції та маніпулятивні наративи, спрямовані як проти українського суспільства, так і проти міжнародної підтримки України. У цих умовах особливого значення набули інструменти OSINT – аналізу та верифікації інформації з відкритих джерел.

Під час російсько-української війни OSINT перестав бути вузькоспеціалізованим інструментом розвідувальних структур і фактично перетворився на важливий елемент інформаційної протидії. Відкриті джерела – супутникові знімки, соціальні мережі, відео з мобільних телефонів, Telegram-канали, геолокаційні сервіси, онлайн-бази даних – дозволили оперативно спростовувати російські фейки та документувати перебіг бойових дій.

Одним із перших прикладів ефективного використання OSINT стало викриття російської дезінформації щодо концентрації військ біля українського кордону наприкінці 2021 – початку 2022 р. Незважаючи на офіційні заяви Москви про «навчання» та відсутність намірів вторгнення, супутникові знімки Maxar Technologies, Planet Labs та інших компаній дозволяли фіксувати накопичення техніки, польових госпіталів, логістичних баз і підготовку до масштабної операції. Після початку вторгнення саме відкриті супутникові дані стали одним із ключових доказів російської агресії.

Важливу роль OSINT відіграв і під час документування воєнних злочинів. Після деокупації Бучі у квітні 2022 р. російська федерація намагалася поширювати твердження про «постановочний характер» масових убивств цивільного населення. Однак супутникові знімки компанії Maxar, проаналізовані журналістами The New York Times та незалежними дослідниками, підтвердили наявність тіл мирних мешканців на вулицях міста ще в період російської окупації. Таким чином, OSINT став інструментом доказової бази для міжнародних розслідувань.

Значного розвитку під час війни набули й українські OSINT-спільноти. Проєкти DeepState, InformNapalm, Molfar, OSINTtechnical та низка волонтерських аналітичних груп систематично здійснюють моніторинг бойових дій, геолокацію відео, верифікацію втрат противника та аналіз російської інформаційної активності. Наприклад, InformNapalm ще з 2014 р. використовував дані із соціальних мереж російських військових для встановлення участі підрозділів ЗС рф у бойових діях на Донбасі. Під час повномасштабної війни ці практики масштабувалися та стали значно швидшими завдяки розвитку цифрових платформ і доступності відкритих даних.

Окремим напрямом використання OSINT стала протидія фейковим відео та маніпулятивному контенту. Російська пропаганда регулярно поширювала старі відеозаписи, кадри з інших конфліктів або змонтовані матеріали як «докази» успіхів російської армії чи злочинів української сторони. Верифікація через геолокацію, аналіз погодних умов, архітектурних об’єктів, метаданих і порівняння з архівними зображеннями дозволяла швидко викривати подібні маніпуляції. У багатьох випадках спростування з’являлися вже через кілька годин після публікації фейку.

Суттєвим фактором стало й використання OSINT для аналізу російських інформаційно-психологічних операцій у соціальних мережах. Дослідники

фіксували діяльність бот-мереж, координоване поширення однакових повідомлень, штучне просування панічних або антиукраїнських наративів. Особливо активно такі кампанії застосовувалися під час ударів по енергетичній інфраструктурі України, контрнаступальних операцій ЗСУ та дискусій навколо міжнародної військової допомоги.

Водночас використання OSINT має і низку проблем. Відкриті джерела можуть містити недостовірну або навмисно викривлену інформацію, а швидкість поширення даних часто перевищує можливості їх перевірки. Окрему небезпеку становить оприлюднення інформації, яка може розкрити позиції українських військ або результати ударів до офіційних повідомлень. Саме тому ефективне використання OSINT потребує не лише технічних навичок, а й сформованого критичного мислення, навичок верифікації та розуміння інформаційної безпеки.

Таким чином, російсько-українська війна показала, що OSINT став важливим елементом сучасного інформаційного протиборства. Використання відкритих джерел дозволяє оперативно виявляти дезінформацію, документувати воєнні злочини, аналізувати діяльність противника та підтримувати інформаційну стійкість суспільства. Водночас розвиток цифрового середовища та масштабування інформаційних операцій роблять необхідним подальше вдосконалення методів OSINT і підготовку фахівців, здатних ефективно працювати з відкритими даними в умовах сучасної війни.

Чорняк І. І.
Заєць Я. Г., канд. техн. наук, ст. досл.
Давіденко С. В., канд. техн. наук, доц.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

## РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Аналіз ризиків інформаційної безпеки у Збройних Силах України є дуже важливим аспектом оборони в умовах сучасної високотехнологічної та мережецентричної війни. У сучасних збройних конфліктах інформаційний простір став повноцінним полем бойових дій, де для української армії забезпечення безпеки даних є питанням безпосереднього збереження життів

військовослужбовців та успіху бойових операцій. Основні загрози формуються під впливом технічних, людських та інфраструктурних чинників, які постійно еволюціонують під дією ворожих спецслужб.

Головну технічну небезпеку становлять кібератаки та поширення шпигунського програмного забезпечення з боку російських хакерських угруповань. Ворог активно використовує методи цільового фішингу, маскуючи шкідливі посилання або документи під офіційні накази та бойові розпорядження, які розсилаються через месенджери та електронну пошту. Зараження особистих або службових мобільних пристроїв дозволяє супротивнику збирати геолокаційні дані, перехоплювати аудіоповідомлення та текстове листування, що може призвести до критичних наслідків для підрозділів в цілому та втрат особового складу.

Людський фактор та розвідка на основі відкритих джерел залишаються одними з найуразливіших елементів оборони. Публікація військово-службовцями фото чи відеоматеріалів у соціальних мережах без попереднього очищення метаданих або з наявністю впізнаваних елементів ландшафту дозволяє ворогу оперативно вираховувати позиції. Крім того, обговорення службових питань, передача координат чи внутрішніх розпоряджень через незахищені месенджери створює умови для перехоплення цієї інформації силами противника.

Окремим викликом є захист цифрових систем управління боєм та ситуаційної обізнаності, які активно впроваджуються в ЗСУ. Ризики пов'язані зі спробами ворога перехопити права доступу до централізованих мереж через компрометацію окремих терміналів, планшетів чи ноутбуків безпосередньо на лінії фронту. Також існує серйозна залежність від супутникових каналів зв'язку, які піддаються постійному локальному глушінню та спробам кібератакам з метою дезорганізації управління військами.

Наслідки реалізації цих ризиків у військовому секторі мають катастрофічний характер, адже будь-який витік даних миттєво перетворюється на розкриття позицій та особового складу з наступним вогневим ураженням артилерією, ударними дронами чи ракетами. Компрометація інформаційних систем веде до зриву бойових операцій через передчасне розкриття планів маневрів, а викрадення персональних даних військових та їхніх родин стає основою для проведення потужних ворожих інформаційно-психологічних операцій, спрямованих на підрив морального духу.

Недопущення таких ризиків потребує комплексного підходу, який поєднує технологічний захист та сувору інформаційну гігієну. Впровадження архітектури нульової довіри, де кожен користувач і пристрій постійно підтверджують свої права, разом із використанням сертифікованих військових засобів зв'язку та функцією автоматичного знищення даних у разі втрати пристрою суттєво підвищують стійкість систем. Водночас вирішальну роль відіграє жорстка дисципліна щодо обмеження використання особистих комунікаційних мобільних пристроїв у зоні бойових дій та безперервне навчання особового складу протидії методам кібератакам.

З вище вказаного можна зробити висновок що інформаційна безпека в Збройних Силах України виступає не лише технічним інструментом, а й стратегічним чинником, що визначає ефективність та життєздатність армії в умовах сучасної війни. Вона забезпечує безперервність управління військами, захист критичних даних та протидію кібератакам, які є невід'ємною складовою агресії проти України. Поєднання кіберзахисту, навчання особового складу основам кібергігієни та інтеграція з міжнародними партнерами створюють комплексну систему оборони, здатну протистояти як зовнішнім, так і внутрішнім загрозам. Саме тому інформаційна безпека стає фундаментом сучасної військової стратегії, адже без її належного рівня неможливо гарантувати ані ефективність бойових дій, ані збереження суверенітету держави.

Алєксєєва М. В.
Кикоть О. О.
Військовий інститут Київського національного університету
імені Тараса Шевченка

## ІНФОРМАЦІЙНА ПРОТИДІЯ РОСІЙСЬКИЙ ПРОПАГАНДІ У ВОЄННИЙ ЧАС

Повномасштабне вторгнення російської федерації в Україну супроводжується активним веденням інформаційної війни з боку країни агресора. Російська пропаганда спрямована на поширення дезінформації, деморалізацію українського народу та дискредитацію Збройних Сил України. У таких умовах особливого сзначення набуває інформаційна протидія, що є ключовою складовою системи стратегічних комунікацій держави.

Інформаційна війна передбачає використання загальних медіа, соціальних мереж та решти каналів комунікації для впливу на суспільну думку. Основними способами російської пропаганди є фейкові новини, маніпуляції фактами, інформаційні вкиди та використання бот-мереж у соціальних мережах, нерідко можна побачити згенеровані ШІ відеозвернення президента України та інших посадових осіб. Такі дії спрямовані на створення масової тривоги в українців та зниження довіри до державних інституцій.

У протидії дезінформації важливу роль відіграють державні органи, зокрема Міністерство оборони України, Головний офіс президента України, Головне управління комунікацій, а також військові журналісти і пресслужби Збройних Сил України. Їх діяльність спрямована на оперативне інформування суспільства, оскарження неправдивої інформації та формування об'єктивної ситуації в країні та на фронті.

Суттєвою складовою інформаційної протидії є використання сучасних медіаплатформ. Соціальні мережі, офіційні сайти державних установ та цифрові медіа стали ефективним інструментом комунікації між військовими структурами та суспільством. Завдяки цьому суспільство має можливість отримувати достовірну та перевірену інформацію безпосередньо від офіційних джерел. Важливим елементом протидії дезінформації є робота спеціалізованих державних та громадських структур, які здійснюють моніторинг інформаційного середовища. Серед них є Центр протидії дезінформації при Раді національної безпеки і оборони України, який виявляє та аналізує ворожі інформаційні операції, а також оперативно публікує спростування фейків. Громадські ініціативи, такі як StopFake та VoxCheck, займаються перевіркою фактів у медіа, аналізом маніпуляцій та викриттям недостовірних новин.

Крім того, важливу роль у боротьбі з російською пропагандою відіграє підвищення медіаграмотності населення. Усвідомлення механізмів маніпуляції інформацією допомагає населенню критично оцінювати отриману інформацію та не піддаватися впливу дезінформації. У сучасних умовах формування інформаційної стійкості суспільства є одним із головних завдань державної інформаційної політики.

Отже, інформаційна протидія російській пропаганді є важливою складовою національної безпеки України. Ефективна комунікація державних органів, діяльність військових журналістів та розвиток медіаграмотності населення сприяють зміцненню стійкості до інформаційних впливів суспільства та протидії ворожим ІПСО.

Буряк А. А.
Військовий інститут Київського національного університету
імені Тараса Шевченка

# СОЦІАЛЬНІ МЕРЕЖІ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ ВІЙНИ: РИЗИКИ ВПЛИВУ ТА ІНСТРУМЕНТИ ПРОТИДІЇ

В наш час соціальні мережі перетворилися на один із ключових інструментів формування громадської думки та поширення інформації. В умовах гібридних конфліктів вони стали повноцінним полем інформаційного протиборства, де поряд із легітимною комунікацією активно застосовуються маніпулятивні технології, дезінформація та психологічний вплив на аудиторію. Масовість, швидкість поширення контенту та низький поріг входу для створення інформаційних повідомлень роблять соціальні медіа зручним середовищем для проведення інформаційних операцій.

Одним із головних ризиків є поширення дезінформації та фейкових новин. Алгоритми соціальних платформ орієнтовані на залучення користувачів, тому емоційно забарвлений або сенсаційний контент поширюється значно швидше за перевірену інформацію. Це сприяє поширенню маніпуляцій, викривленню інформаційного середовища та поглибленню розколу в суспільстві.

Ще одним важливим викликом є персоналізація інформаційного середовища. Алгоритми формують так звані «інформаційні бульбашки», в яких користувач отримує переважно контент, що відповідає його попереднім інтересам і поглядам. У результаті знижується критичне сприйняття інформації, а маніпулятивні повідомлення легше інтегруються в уже сформовану систему переконань. Це посилює ризики радикалізації та підриву суспільної довіри до державних інституцій і медіа.

У контексті протидії інформаційним загрозам ключову роль відіграє підвищення рівня медіаграмотності населення. Формування навичок критичного мислення, перевірки джерел інформації та розпізнавання маніпулятивних технік є базовим елементом інформаційної безпеки. Важливим напрямом також є розвиток систем фактчекінгу, співпраця державних органів із технологічними платформами та створення ефективних механізмів виявлення та блокування мереж координованої дезінформації.

Сучасним прикладом впливу соціальних мереж у контексті інформаційної війни стало масове поширення відео та повідомлень про діяльність ТЦК та СП. У TikTok, Telegram, YouTube та Facebook активно з'являлися ролики із затриманнями чоловіків на вулицях або конфліктами під час перевірки документів. Часто такі відео публікувалися без повного контексту та супроводжувалися емоційними підписами, що формувало однобічне сприйняття подій і швидко набувало вірусного поширення.

Показовим став випадок із відео, яке набрало значну кількість переглядів: на ньому жінка стукає у двері квартири та веде розмову з чоловіком, тоді як поруч нібито очікують представники ТЦК, щоб затримати його після відкриття дверей. Попри відсутність підтвердженого контексту, ролик викликав хвилю страху, обурення та масові обговорення, а користувачі активно поширювали припущення і поради щодо «уникнення мобілізації».

Ці приклади демонструють, як алгоритми соціальних мереж підсилюють емоційний і конфліктний контент, що може сприяти зростанню напруги, поширенню фейків і недовіри. Водночас вони підкреслюють важливість офіційної комунікації, фактчекінгу та розвитку медіаграмотності як ключових інструментів протидії інформаційним загрозам.

Таким чином, соціальні мережі залишаються одночасно інструментом комунікації та потужною зброєю інформаційної війни. Ефективна протидія загрозам можлива лише за умови комплексного підходу, що поєднує технологічні рішення, освітні ініціативи та інституційну взаємодію. Розвиток стійкості суспільства до інформаційних впливів є необхідною передумовою забезпечення національної інформаційної безпеки.

Кикоть О. О.
Алєксєєва М. В.
Військовий інститут Київського національного університету
імені Тараса Шевченка

# РОЛЬ ВІЙСЬКОВОЇ ЖУРНАЛІСТИКИ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІД ЧАС РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Військова журналістика під час повномасштабного російського вторгнення перетворилася на важливий елемент національної інформаційної безпеки України. Вона вийшла за рамки традиційного висвітлення подій і стала активним учасником гібридної війни, де інформаційний простір є справжнім фронтом.

Сучасні конфлікти демонструють, що контроль над наративом і контроль над територією є взаємопов'язаними складовими війни. Українські військові журналісти, кореспонденти при підрозділах ЗСУ та мілітарні медіа щоденно протидіють російській пропаганді, фейкам і інформаційно-психологічним операціям. Їхня робота безпосередньо впливає на суспільну стійкість, моральний дух війська та міжнародну підтримку.

Однією з головних функцій стало оперативне спростування ворожих наративів про «нацизм», «біолабораторії» чи втрати ЗСУ. Завдяки польовим репортажам і верифікації фактів журналісти швидко нейтралізують дезінформацію, часто у взаємодії з державними структурами.

Важливим залишається дотримання операційної безпеки (OPSEC). Журналісти уникають розголошення чутливих даних, дотримуються правил акредитації та рекомендацій Генштабу. Це дозволяє зберігати баланс між свободою слова та національною безпекою.

Водночас військові кореспонденти самі стають цілями кібератак. DDoS-атаки, фішинг, doxing і deepfake-відео є частими інструментами тиску. Тому кібергігієна стала обов'язковою складовою їхньої роботи.

Професійна військова журналістика також виконує документувальну функцію. Фіксація воєнних злочинів створює доказову базу для міжнародних трибуналів і формує глобальну думку. Якісні репортажі з передової допомагають протидіяти паніці та підтримувати суспільну resilience.

Звичайно, постають етичні виклики. Необхідно поєднувати об'єктивність із принципом «не нашкодити своїй армії». В умовах війни українська військова журналістика розвивається як модель відповідальної журналістики.

Нові технології, такі як OSINT, Starlink та інструменти штучного інтелекту, значно розширюють можливості, але водночас створюють додаткові ризики.

Отже, військова журналістика стала невід'ємною частиною системи інформаційної безпеки держави. Вона поєднує інформування, протидію агресору та підтримку суспільної стійкості. Для її подальшого розвитку потрібні системні тренінги з кібербезпеки, національні стандарти роботи медіа в умовах війни та тісніша співпраця з військовим керівництвом.

Саме професійна та військова журналістика, яка доводить факти здатна ефективно протистояти сучасній інформаційній агресії.

Колотуша Я. В.
Військовий інститут Київського національного університету
імені Тараса Шевченка

## ДЕЗІНФОРМАЦІЯ ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ ВІЙНИ: РОЛЬ МЕДІА В ПРОТИДІЇ

У сучасному інформаційному суспільстві дезінформація стала одним із ключових інструментів впливу на громадську думку, політичні процеси та безпеку держав. В умовах гібридних конфліктів інформація перетворюється на ресурс і зброю, а медіапростір – на поле боротьби за свідомість аудиторії. Швидкий розвиток цифрових технологій, соціальних мереж і месенджерів значно спростив поширення як правдивої, так і неправдивої інформації, що підвищило ризики масових інформаційних маніпуляцій.

Дезінформація – це навмисне створення та поширення неправдивої або викривленої інформації з метою впливу на думки, поведінку або рішення людей. Вона відрізняється від помилкової інформації тим, що має цілеспрямований характер. У контексті інформаційної війни дезінформація використовується для досягнення політичних, військових або економічних цілей. Її основними завданнями є формування потрібного емоційного фону в суспільстві, підрив довіри до державних інституцій і медіа, створення паніки, а також дезорієнтація населення.

Сучасна дезінформація поширюється через різні канали. Найбільш активно використовуються соціальні мережі, такі як Telegram, Facebook, TikTok та інші платформи, де інформація може ставати вірусною за лічені години. Також значну роль відіграють псевдоновинні сайти, боти та автоматизовані акаунти, які імітують реальних користувачів. Окремим потужним інструментом стали технології штучного інтелекту, зокрема генерація текстів, зображень і відео, включаючи deepfake, що ускладнює виявлення фальсифікацій.

В інформаційній війні медіа займають подвійне становище. З одного боку, вони можуть бути об'єктом атак і каналом поширення дезінформації, з іншого –виступають ключовим інструментом її протидії. Саме журналістика забезпечує суспільство перевіреною інформацією, здійснює фактчекінг і викриття фейків, а також формує критичне мислення аудиторії. Надійні медіа відіграють важливу роль у підтриманні довіри до інформаційного простору, що є критично важливим у кризових умовах.

Одним із головних методів протидії дезінформації є фактчекінг – перевірка інформації на основі офіційних джерел, експертних оцінок та відкритих даних. Також активно застосовується OSINT-аналіз, тобто використання відкритих джерел для перевірки фото, відео та текстової інформації. Важливим напрямом є розвиток медіаграмотності населення, що дозволяє людям самостійно критично оцінювати інформацію та розпізнавати маніпуляції. Крім того, медіа співпрацюють із цифровими платформами для маркування неправдивого контенту та обмеження його поширення. Попри існуючі методи протидії, проблема дезінформації залишається складною. Основними викликами є надшвидке поширення інформації, використання штучного інтелекту для створення реалістичних фейків, низький рівень медіаграмотності населення, а також складність оперативної перевірки великих обсягів контенту. Додатковим фактором є політична заангажованість інформаційного простору, що ускладнює об'єктивне сприйняття новин.

Таким чином, дезінформація є потужним інструментом інформаційної війни, який впливає на суспільну свідомість і стабільність держав. У цих умовах роль медіа є надзвичайно важливою, адже саме вони забезпечують перевірену інформацію, викривають маніпуляції та сприяють формуванню інформаційної безпеки суспільства. Ефективна протидія дезінформації можлива лише за умови поєднання професійної журналістики, технологічних рішень та високого рівня медіаграмотності населення.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Стрілець К. С.
Кухарська О. С.
Піковська І. Д.
Військовий інститут Київського національного університету
імені Тараса Шевченка

# АКТУАЛЬНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: МІСЦЕ ВІЙСЬКОВИХ ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ В МЕДІЙНОМУ ПРОСТОРІ УКРАЇНИ

У повномасштабній війні з Росією інформаційна безпека стала не менш важливим фронтом, ніж лінія зіткнення. Військові ЗМІ – офіційні канали Міноборони, Генштабу, «АрміяInform», пресслужби бригад і підрозділів – відіграють ключову роль: вони дають суспільству оперативну інформацію, протидіють ворожій пропаганді та підтримують моральний дух. Але їхнє місце в загальній медійній системі досі чітко не визначене, через що виникають серйозні вразливості.

Одна з головних проблем – фрагментація військових комунікацій. Багато бригад і навіть окремих підрозділів ведуть власні Telegram-канали та сторінки без єдиної координації. Через це з’являються суперечливі повідомлення, а іноді й порушення правил операційної безпеки (OPSEC). Ворог відразу використовує такі розбіжності, щоб поширювати дезінформацію та підривати довіру до офіційних джерел. Наказ Головнокомандувача ЗСУ від 3 березня 2022 року (з пізнішими доповненнями) намагається врегулювати взаємодію з медіа, але на практиці єдиного центру стратегічних комунікацій, який би жорстко контролював усе, досі немає.

Друга гостра проблема – баланс між прозорістю та безпекою. Суспільство хоче знати, що відбувається на фронті, але надмірні деталі:геолокація, фото техніки з прив’язкою, конкретні втрати в реальному часі створюють прямі загрози для військових. Були неодноразові випадки, коли контент з військових пабліків допомагав ворогу коригувати удари. Цивільні ЗМІ часто просто репостять такий матеріал, і ризик лише зростає. Доктрина інформаційної безпеки України та рішення РНБО щодо єдиної інформаційної політики під час воєнного стану підкреслюють необхідність цього балансу, але механізмів його дотримання поки недостатньо.

Ще один виклик – взаємодія військових і цивільних медіа. Військові

пресслужби дедалі частіше стають головним джерелом для журналістів. З одного боку, це добре: офіційна інформація поширюється швидше. З іншого – з'являються звинувачення в надмірній «мілітаризації» інформаційного простору та обмеженні свободи слова. Відсутність чітких і прозорих правил акредитації та роботи в зоні бойових дій тільки посилює напругу. Технічна вразливість теж не на останньому місці. Офіційні військові акаунти регулярно стають мішенню для хакерів, фейків і підміни контенту. Велика залежність від Telegram робить систему ще чутливішою – месенджер уже блокували українські держоргани через ризики.

Щоб виправити ситуацію, потрібні конкретні кроки: створити потужний єдиний координаційний центр стратегічних комунікацій ЗСУ, запровадити обов'язкові стандарти OPSEC та INFOSEC для всіх військових пресслужб, розробити сучасні стандарти військової журналістики та системно готувати фахівців, які розуміють і журналістику, і інформаційну безпеку.

Військові ЗМІ сьогодні – це реальний щит у інформаційній війні. Але поки їхній статус і правила роботи залишаються недорегульованими, вони можуть мимоволі створювати слабкі місця, якими користується ворог. Чітке визначення їхньої ролі в загальній медійній системі – це не питання зручності, а питання національної безпеки.

Zubelevych D. I.
Kirieiev O. V.
Korolov Zhytomyr Military Institute

## EVOLUTION OF SOFTWARE SUPPLY CHAIN ATTACK VECTORS AND POSSIBLE SECURITY STRATEGIES

Modern software development process depends heavily on the open-source components and automated Continuous Integration and Continuous Deployment (CI/CD) pipelines. The proportion of third-party components in contemporary software products can reach up to 90% of the total amount of code. While the integration of third-party libraries and frameworks significantly accelerates the development process, it also introduces severe security risks to information systems. The compromising of a single open-source element can cause a critical threat to numerous downstream projects that rely on it as a dependency.

Software Supply Chain Attacks have become a prevalent vector of cyber threats in recent years. Traditionally, these incidents involved long-term, stealthy malicious code injections, as evidenced by the attack on SolarWinds Orion software in 2020 and the backdoor discovered in the XZ Utils library (CVE-2024-3094) in 2024, which enabled unauthorized SSH access to Linux systems in bypass of authentication mechanisms. But the "Megalodon" incident (detected in May 2026) demonstrated a strategic shift toward high-speed, automated, infrastructure-level attacks directly targeting the development environment.

Investigations into the "Megalodon" incident revealed that the attack was entirely automated and executed within a six-hour window. The vulnerability technical workflow included:

1) Trusted entity spoofing by pushing malicious modifications to repositories under the guise of automated service build-bots;

2) CI/CD configuration poisoning through malicious tampering with GitHub Actions workflows, deploying new workflows triggered on push/pull requests or replacing configurations to establish dormant backdoors;

3) Platform constraint evasion by utilizing the workflow_dispatch trigger to bypass GitHub's built-in anti-recursion mechanisms for remote API activation;

4) Sensitive data exfiltration specifically engineered to harvest secrets from CI/CD environments, including environment variables, cloud provider credentials (AWS, GCP, Azure), private SSH keys, and Docker/Kubernetes configurations.

Consequently, the "Megalodon" incident compromised 5,561 unique GitHub repositories via more than 5,700 malicious commits. This breach illustrated the severe transitive dependency risks inherent in complex software ecosystems.

This incident demonstrates the insufficiency of traditional cybersecurity approaches, such as signature-based detection and known vulnerability analysis, for identifying compromised supply chains. To mitigate these threats, automated Software Composition Analysis (SCA) tools are increasingly essential. A foundational component of this approach is the generation of a Software Bill of Materials (SBOM) to track component provenance under controlled build conditions. Furthermore, employing the Vulnerability Exploitability eXchange (VEX) mechanism allows organizations to ascertain whether a specific vulnerability is practically exploitable within a given product, thereby reducing false positives during automated security audits.

The "Megalodon" incident shows that effective security strategies against the modern threats requires a comprehensive, defense-in-depth approach through the implementation of DevSecOps practices across all stages of the software development lifecycle. Key strategies include adopting a Zero Trust model for CI/CD processes by restricting GITHUB_TOKEN permissions to read-only by default, and enforcing strict branch protection rules that require cryptographically signed commits and mandatory human code reviews (preventing service bots from pushing unverified changes directly). Additionally, software artifact integrity must be enforced by pinning third-party CI/CD actions to unique cryptographic identifiers (SHA commit hashes) rather than mutable version tags. These measures align with the implementation of SLSA (Supply-chain Levels for Software Artifacts) standards and the use of cryptographic signing infrastructures, such as Sigstore, to verify artifact provenance and immutability.

Also, the complementary direction for enhancing security is the utilization of isolated execution environments to verify third-party components prior to their integration during the build and compilation phases. Deploying virtual machines, containerization technologies (Docker, containerd, LXC/LXD), system restrictions (AppArmor/SELinux), and WebAssembly (Wasm)-based environments enables the behavioral analysis of libraries and dependencies under strictly controlled conditions. Thus, effective counteraction to modern software supply chain attacks requires a strategy that combines automated composition analysis, CI/CD infrastructure control, integrity verification of software artifacts, and behavioral analysis of third-party components.

Чіпєра В. В.
Поливаний С. В.
Житомирський військовий інститут імені С. П. Корольова

## ВИКОРИСТАННЯ МЕТОДУ ВІДДАЛЕНОЇ ІН'ЄКЦІЇ В ПАМ'ЯТЬ ПРОЦЕСУ ЗА ДОПОМОГОЮ POWERSHELL ДЛЯ ТЕСТУВАННЯ АНТИВІРУСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Одним із важливих елементів кібербезпеки є перевірка комп'ютерних систем на проникнення, що часто називається тестуванням на проникнення (penetration testing). Це процес імітації атаки на систему з метою виявлення

вразливостей, які можуть бути використані зловмисниками для отримання несанкціонованого доступу.

Основними цілями перевірки на проникнення є:

виявлення слабких місць у системі безпеки;

оцінка ефективності існуючих заходів захисту;

надання рекомендацій щодо усунення виявлених вразливостей;

підвищення загального рівня безпеки організації.

Ключовим елементом тестування на проникнення є перевірка антивірусного захисту на стійкість до сучасних методів обходу системи безпеки та здатність виявляти приховані загрози.

Шкідливе програмне забезпечення постійно намагається уникнути виявлення антивірусними засобами, використовуючи два основні методи:

ухилення на диску;

ухилення в пам’яті.

Ухилення на диску зосереджується на модифікації шкідливих файлів, фізично збережених на носіях даних, з метою уникнення виявлення механізмами файлового сканування антивірусного програмного забезпечення.

Ухилення в пам’яті полягає у впровадженні шкідливого коду в оперативну пам’ять (in-memory injection). Основними методами такого впровадження є:

ін’єкція шкідливого коду в інший легітимний процес;

впровадження відбиваючих DLL-бібліотек (reflective DLL injection);

вивільнення процесів (process hollowing).

Віддалена ін’єкція шкідливого коду в інший легітимний процес за допомогою PowerShell надає можливість взаємодіяти з API Windows та реалізовувати механізми ін’єкції в пам’ять. Однією з головних переваг використання скриптів замість виконуваних файлів є складність визначення їх шкідливості антивірусним програмним забезпеченням, оскільки скрипт виконується всередині інтерпретатора і сам по собі не є компільованим виконуваним кодом.

Крім того, навіть якщо скрипт буде ідентифікований як шкідливий, його можна легко модифікувати. Антивірусне програмне забезпечення часто аналізує імена змінних, коментарі та логіку виконання, однак ці елементи можуть бути змінені без необхідності перекомпіляції коду.

Такі скрипти зазвичай використовують імпорт функцій VirtualAlloc і CreateThread із бібліотеки kernel32.dll, а також функції memset із бібліотеки

msvcrt.dll. Методи ухилення від антивірусного виявлення, зокрема ін'єкції коду в пам'ять, становлять серйозну загрозу для сучасних інформаційних систем. Використання PowerShell та API Windows дозволяє реалізовувати приховане виконання шкідливого коду, що ускладнює його виявлення традиційними засобами захисту.

Тому під час проведення тестування на проникнення важливо оцінювати не лише наявність антивірусного програмного забезпечення, а й його здатність протидіяти сучасним технікам обходу захисту. Це сприяє підвищенню ефективності систем кібербезпеки та своєчасному виявленню потенційних вразливостей.

Осадчук М. В.
Житомирський військовий інститут імені С. П. Корольова

## ПРОГРАМНО-АПАРАТНА СИСТЕМА ФОРМУВАННЯ ІМІТАЦІЙНИХ ПЕРЕШКОД РАДІОЛОКАЦІЙНИМ СТАНЦІЯМ ТАКТИЧНОГО РІВНЯ

Сучасні збройні конфлікти характеризуються широким застосуванням засобів радіолокаційної розвідки та виявлення повітряних цілей. Ефективність роботи радіолокаційних станцій значною мірою визначає можливості протиповітряної оборони, управління військами та контролю повітряного простору. У зв'язку з цим особливого значення набуває розвиток засобів радіоелектронної боротьби, здатних впливати на роботу радіолокаційних систем противника шляхом створення активних радіоперешкод різного типу.

Одним із перспективних напрямів розвитку засобів радіоелектронного подавлення є застосування імітаційних перешкод. На відміну від маскувальних шумових завад, імітаційні перешкоди не лише знижують ефективність роботи радіолокаційної станції, а й створюють у її інформаційному полі неправдиву обстановку. Це дозволяє формувати хибні відмітки цілей, ускладнювати процес супроводження реальних об'єктів та збільшувати навантаження на операторів радіолокаційних комплексів.

Сучасний розвиток технологій програмно визначеного радіо відкриває нові можливості для побудови гнучких та відносно недорогих систем формування радіоперешкод. Використання SDR-платформ дозволяє

реалізовувати складні алгоритми генерації сигналів у програмному середовищі, забезпечуючи оперативну зміну параметрів випромінювання залежно від характеристик виявлених радіолокаційних засобів.

У роботі розглянуто підхід до створення програмно-апаратної системи формування імітаційних перешкод радіолокаційним станціям тактичного рівня на базі SDR-технологій. Запропонована система забезпечує пошук та аналіз параметрів сигналів радіолокаційних станцій, визначення їх робочих характеристик і подальше формування сигналів перешкод із заданими параметрами. Програмна частина реалізує алгоритми обробки радіосигналів, визначення параметрів випромінювання та генерації імітаційних сигналів, а апаратна частина забезпечує приймання, обробку та передачу сформованих сигналів у реальному масштабі часу.

Особливу увагу приділено можливості застосування сучасних SDR-платформ для роботи в широкому діапазоні частот, характерному для радіолокаційних станцій тактичного рівня. Запропонований підхід дозволяє підвищити адаптивність системи до різних типів радіолокаційних засобів та забезпечити оперативне налаштування параметрів перешкод без необхідності внесення змін до апаратної частини комплексу.

Отримані результати підтверджують доцільність використання програмно визначеного радіо для побудови перспективних засобів радіоелектронної боротьби. Розроблена система може бути використана як основа для створення мобільних комплексів формування імітаційних перешкод, призначених для протидії радіолокаційним станціям тактичного рівня та підвищення ефективності заходів радіоелектронного подавлення.

Критенко О. В.
Житомирський військовий інститут імені С. П. Корольова
Саєнко І. В.
Військова академія (м. Одеса)

# ОСОБЛИВОСТІ ТА ЗНАЧЕННЯ ГЕНДЕРНИХ КОНСТРУКТИВНИХ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Разом з актуалізацією забезпечення рівних прав і можливостей жінок і чоловіків розвивається нормативно-правова база інтеграції гендерних аспектів у стратегічні комунікації.

Ключовими документами, що регулюють стратегічні комунікації в Україні, є: Стратегія національної безпеки України (затверджена Указом Президента № 392/2020 від 14.09.2020), Стратегія інформаційної безпеки України (затверджена Указом Президента № 685/2021 від 28.12.2021), Стратегічний оборонний бюлетень України (затверджений Указом Президента № 473/2021 від 17.09.2021), Концепція комунікації у сфері гендерної рівності.

Особливості гендерних конструктивних стратегічних комунікацій у секторі безпеки і оборони України:

1. Ефективне використання цифрових технологій: Україна значно активізувала стратегічні комунікації за допомогою використання цифрових платформ, таких як Facebook, Instagram, YouTube та ін., що дозволяє доносити до громадськості важливу інформацію в режимі реального часу.

2. Інститут гендерних радників/радниць: гендерні радники/радниці виконують важливу роль у впровадженні та моніторингу політики гендерної рівності в інституціях сектору безпеки і оборони України (СБОУ), підтримуючи зусилля щодо створення інклюзивного робочого середовища, надають консультативну підтримку з питань рівних прав та можливостей жінок і чоловіків, рекомендації щодо адаптації міжнародних стандартів у цій царині та підтримують реалізацію стратегічних комунікацій для підвищення обізнаності особового складу щодо гендерних аспектів.

3. Розвиток цивільно-військового партнерства: активна співпраця з громадським сектором підсилює ефективність комунікацій та підтримку ініціатив з питань гендерної рівності, що сприяє прозорості роботи СБОУ та

впливає на рівень довіри населення до інституцій СБОУ. Наприклад, регіональні коаліції 1325 долучаються до аналізу гендерних проблем та вивченню запитів жінок СБОУ в областях та здійснюють моніторинг для регіональних планів заходів для локалізації порядку денного «Жінки, мир, безпека», формують рекомендації для оновлення НПД 1325.

Згідно з аналізом тенденцій, зроблених Центром передового досвіду стратегічних комунікацій НАТО, можна виокремити ключові виклики, що є актуальними для сучасного інформаційного середовища:

1. Зміна підходів до дезінформації та протидії гібридним загрозам, що вимагає залучення ресурсів та нових тактик, спрямованих на блокування фальшивих новин та деструктивних наративів. Активізація пропагандистських кампаній демонструє, як дезінформація стає центральним елементом у впливі на суспільну думку та маніпуляції аудиторіями.

2. Інтеграція нових технологій, зокрема штучного інтелекту: сучасні дослідження наголошують на ролі штучного інтелекту та його використанні в інформаційних операціях для автоматизованого створення контенту, що значно посилює ефективність дезінформації. Актуалізуються механізми захисту та контролю штучного інтелекту, а також можливості його використання для покращення стратегічних комунікацій, аналізу масивів даних та швидкого виявлення фейкових наративів.

3. Співпраця та підтримка медіа містить боротьбу з негативним впливом пропаганди та інформаційних маніпуляцій.

4. Протидія цифровому втручанню шляхом моніторингу та оцінювання цифрового середовища, що допомагає виявляти та реагувати на загрози в режимі реального часу.

## ПАНЕЛЬ 4

## Проблеми та аспекти підготовки фахівців у сфері психологічних операцій, інформаційної безпеки та інформаційних технологій

Кримець Л. В., Ph. D., ст. наук. співроб.
В/ч А0987

# ЗНАЧЕННЯ ВИВЧЕННЯ ТА ВПРОВАДЖЕННЯ ДОСВІДУ ДЛЯ ПІДГОТОВКИ ВІЙСЬКОВИХ ФАХІВЦІВ

Досвід збройної боротьби російської федерації та України продемонстрував особливе значення адаптивності та здатності збройних сил швидко реагувати на нові виклики сучасної війни та потреби випереджати ворога в протиборстві інновацій в усіх доменах та на всіх рівнях. Практика російсько-української війни засвідчує, що проведення успішних бойових дій, спеціальних операцій та заходів впливу в сучасних умовах неможлива без вчасного, постійного та комплексного збору, аналізу, узагальнення та впровадження передового досвіду, що протягом 2022-2026 рр. активно здійснюється підрозділами Сил спеціальних операцій Збройних Сил України (далі – ССпО ЗС України). Адже, наразі, Збройні Сили України володіють значним практичним досвідом протидії тривалій повномасштабній агресії ворога, якого не мають армії інших країн світу.

У фокусі вивчення та впровадження досвіду – підвищення адаптивності ЗС України та інших складових сил оборони держави, що визначається їх здатністю оперативно реагувати на зміни у безпековому середовищі, ефективно інтегрувати здобутий досвід в систему підготовки та застосування сил (військ) та розвиток їх спроможностей. В умовах збройного конфлікту, процес вивчення та впровадження досвіду виконання бойових (спеціальних) завдань має бути прискореним, щоб відповідати темпу зростаючих викликів, випереджаючи у цьому противника та водночас зберігаючи високу дієвість.

Підготовка військових фахівців у ВВНЗ, ВНП ЗВО, ЗФПВО, НЦ і центрах підготовки підрозділів має ґрунтуватись виключно на основі аналізу сучасного досвіду виконання бойових (спеціальних) завдань підрозділами за напрямом відповідальності і враховувати фундаментальні принципи системи вивчення і впровадження досвіду:

1. Підтримка командирами (начальниками) всіх рівнів – без розуміння керівником необхідності організації процесу ВВД у підпорядкованій військовій організаційній структурі неможливо забезпечити виконання коригувальних дій для впровадження ідентифікованого уроку (потенційної найкращої практики). Інституалізація ВВД забезпечується виключно лідерством командирів (начальників) всіх рівнів.

2. Зрозумілий розподіл ролей і обов'язків – всі учасники процесу ВВД повинні розуміти свою роль і місце у ньому. Для забезпечення цього принципу у кожній військовій організаційній структурі повинна проводитись підготовка з ВВД.

3. Розподіл ресурсів – пріоритет розподілу наявних ресурсів, визначення необхідних ресурсів для виконання коригувальної дії або впровадження найкращої практики дозволяє командиру (начальнику) зрозуміти порядок їх впровадження.

4. Забезпечення комунікації – вона повинна бути простою, доступною та швидкою. Важливе значення для реалізації системи ВВД є максимально прискорений обмін досвідом як по горизонталі, між військовими підрозділами одного рівня підпорядкування зі спільним напрямком діяльності, так і по вертикалі, між військовими підрозділами і органами військового управління (установами) за підпорядкованістю. Забезпечення ефективної комунікації вимагає обов'язкового зворотного зв'язку.

Мета актуалізації системи вивчення і впровадження досвіду для підготовки військових фахівців полягає у постійному вдосконаленні змісту навчальних програм з одночасним підвищенням рівня засвоєння матеріалу.

Ця мета досягається: оптимізацією програм і планів підготовки; впровадженням інновацій у педагогічні практики; постійною адаптаціїю методик підготовки; удосконаленням матеріально-технічної бази; підвищення методичної майстерності викладачів, інструкторів тощо.

Рекомендованими формами ВВД підготовки є: проведення науково-практичних конференцій із досвіду підготовки; проведення нарад (круглих столів); розповсюдження матеріалів проведення навчань, тренувань, занять тощо; розроблення відеоуроків (навчальних відеофільмів); досвід підготовки за кордоном тощо.

На завершення важливо підкреслити, що система вивчення та обміну досвідом важлива і в контексті досягнення взаємосумісності спроможностей

сил оборони України з НАТО. Для покращення аналітичної спроможності Системи ВВД вже створено Об'єднаний центр Україна – НАТО з аналізу, підготовки та освіти (Ukraine-NATO Joint analysis, Training and Education Center, далі – JATEC). Мета його створення – спільне нарощування спроможностей оборонного та безпекового сектору України та НАТО, досягнення взаємосумісності безпекових та оборонних інституцій України з відповідними інституціями Альянсу, підвищення якості освіти, діяльності аналітичної складової та підготовки кадрів, системи вивчення та впровадження досвіду.

Плотнікова Д. С.
Папуш О. Г.
Житомирський військовий інститут імені С. П. Корольова

## ОПТИМІЗАЦІЯ ПРОЦЕДУРИ ПЕРЕВІРКИ ЗНАНЬ У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ДЛЯ НАДАННЯ ДОСТУПУ ДО СЕКРЕТНОЇ ІНФОРМАЦІЇ ТА ЇЇ МАТЕРІАЛЬНИХ НОСІЇВ

В умовах повномасштабної збройної агресії проти України та постійного зростання загроз у сфері інформаційної безпеки питання забезпечення охорони державної таємниці набувають особливої актуальності. Сучасні умови ведення бойових дій характеризуються активним використанням інформаційно – психологічних операцій, кібератак, технічної розвідки та інших засобів отримання інформації, що створює додаткові ризики витоку відомостей, які становлять державну таємницю.

У зв'язку з цим одним із ключових напрямів забезпечення національної безпеки є удосконалення системи контролю за дотриманням режиму секретності та підвищення рівня підготовки особового складу, який має доступ до секретної інформації та її матеріальних носіїв. Тому важливе місце у системі охорони державної таємниці займає професійна підготовка військовослужбовців і працівників, діяльність яких пов'язана з використанням інформації з обмеженим доступом. Саме рівень їхніх знань щодо вимог законодавства, порядку поводження з матеріальними носіями секретної інформації, правил роботи в умовах режимних обмежень та дій у разі виникнення загрози витоку інформації значною мірою визначає ефективність

функціонування всієї системи захисту державної таємниці. Недостатній рівень обізнаності особового складу може призводити до порушення встановлених процедур, втрати документів, розголошення секретної інформації або неналежного виконання вимог режиму секретності, що, у свою чергу, створює безпосередню загрозу обороноздатності держави.

Аналіз стану дотримання режиму секретності у військових частинах свідчить, що значна частина інцидентів трапляється через поверхневе засвоєння нормативної бази та брак практичних навичок. Важливо розуміти, що подібні правопорушення, окрім дисциплінарних стягнень, тягнуть за собою сувору кримінальну відповідальність (зокрема за розголошення державної таємниці чи втрату її носіїв). Традиційні підходи до оцінювання знань, які переважно базуються на усних опитуваннях або письмовому тестуванні, є малоефективними. Вони потребують значних часових витрат на підготовку матеріалів, друк бланків, перевірку відповідей і ведення паперового документообігу. Крім того, відсутність стандартизованих інструментів контролю знижує об’єктивність оцінювання та ускладнює подальший аналіз і систематизацію результатів.

Перспективним шляхом розв'язання цієї проблеми є впровадження спеціалізованого програмного застосунку для контролю та оцінювання знань особового складу. Використання цифрового інструменту дозволяє уніфікувати процедуру перевірки, сформувати єдині підходи до створення тестових завдань та мінімізувати вплив людського фактора. Завдяки централізованій базі матеріалів забезпечуватимуться рівні умови для всіх, хто проходить перевірку, а час на обробку результатів скорочується до мінімуму. При цьому архітектура програмного застосунку має гнучко враховувати категорії військовослужбовців, їхні посадові обов'язки та чинний рівень доступу.

Особливу увагу під час проєктування та розробки такого програмного застосунку слід приділити питанням інформаційної безпеки, надійності та автономності. Програмний засіб повинен гарантувати захист результатів тестування від несанкціонованого модифікування чи копіювання, стабільно функціонувати без підключення до глобальних мереж (в ізольованому контурі) та бути адаптованим до роботи в умовах обмеженої ІТ-інфраструктури. Не менш важливими критеріями є ергономічність, інтуїтивно зрозумілий інтерфейс та невибагливість до апаратного забезпечення, що дозволить інтегрувати рішення у повсякденну діяльність підрозділів без тривалого попереднього навчання користувачів.

Інтеграція програмного застосунку щодо оцінювання знань з питань охорони державної таємниці сприятиме підвищенню рівня підготовки особового складу, покращенню якості контролю знань та формуванню більш відповідального ставлення до дотримання вимог режиму секретності. Використання сучасних програмних рішень дозволить зменшити кількість порушень, пов'язаних із людським фактором, підвищити ефективність роботи режимно – секретних органів та зміцнити загальний рівень інформаційної безпеки у Збройних Силах України. Таким чином, оптимізація процедури перевірки знань шляхом впровадження автоматизованих систем є важливим напрямом удосконалення системи охорони державної таємниці в сучасних умовах.

Канкін І. О., канд. техн. наук
Житомирський військовий інститут імені С. П. Корольова

## ОРГАНІЗАЦІЯ ТА ПРОВЕДЕННЯ ЗАХОДІВ ВВЕДЕННЯ ПРОТИВНИКА В ОМАНУ ПІД ЧАС ВІДБИТТЯ ЗБРОЙНОЇ АГРЕСІЇ рф ПРОТИ УКРАЇНИ

Під час оперативного планування в органах військового управління особливу роль відводять питанням безпеки застосування військ (сил), а саме введенню противника в оману та приховуванню власної діяльності. Саме від ефективності проведення заходів дезінформації, імітації, демонстративних та демонстраційних дій суттєво залежить успіх дезорієнтації противника щодо напрямку головного удару (у ході наступальної операції) або збереження бойового потенціалу й ефективність виконання бойового завдання (у ході оборонної операції).

Планування та проведення заходів введення противника в оману у Збройних Силах України покладається на підрозділи психологічних операцій (ПсО) Сил спеціальних операцій, безпеки застосування військ (сил) органів військового управління (ОВУ), та повинно реалізовуватись в рамках інформаційних операцій.

В органах військового управління, будь-якого рівня, під час процесу оперативного планування операції, це напрямок враховується у планувальних та розпорядчих документах з безпеки застосування військ (сил) шляхом

планування та проведення заходів дезінформації, імітації, демонстративних та демонстраційних дій.

Досвід проведення заходів введення противника в оману під час оперативного планування та виконання завдань ведення демонстративних та демонстраційних дій у складі угруповань військ (сил) командування десантно-штурмових військ Збройних сил України показав, що незважаючи не певні успішні приклади, існує низка проблемних питань, що потребують вивчення та усунення, а саме:

високий рівень обізнаності противника про наші війська (за рахунок використання усіх видів розвідки) значно ускладнює успішну реалізацію заходів щодо дезорієнтації противника;

відсутність централізованого управління плануванням та реалізацією заходів інформаційної операції (ІО) за єдиним замислом в ОВУ різних рівнів (відсутність директивних (розпорядчих) документів в ОВУ оперативного рівня щодо заходів введення противника в оману за єдиним задумом);

відсутність ранньої інтеграції представників тактичних груп ПсО у процес планування загальновійськової операції ОВУ;

відсутність додатків до плану операції ОВУ у вигляді планів ІО та ПсО, згідно з тимчасовою доктриною планування операцій;

відсутність в ОВУ структурного підрозділу планування участі в ІО та обмежена кількість підготовлених фахівців для планування заходів впливу на противника;

низький рівень використання автоматизованих засобів моніторингу інформаційного простору для своєчасного виявлення інформаційних загроз та можливого витоку інформації не завжди дозволяє оперативно реагувати на них, своєчасно враховувати їх під час планування та реалізації відповідних заходів;

недостатня взаємодія між структурними підрозділами штабу ОВУ та тактичними групами ПсО ССпО, представниками підрозділів ІО, Служби безпеки України та військової контррозвідки не дозволяє ефективно й системно здійснювати заходи з дезінформації противника;

відсутність достатньої кількості каналів поширення інформації (дезінформації) суттєво зменшує можливості її донесення до противника (обраної цільової аудиторії) та підтвердження з різних джерел;

наявність регулярних випадків витоку інформації з обмеженим доступом технічними каналами суттєво впливає на обізнаність противника про наші війська;

неефективний розподіл сил і засобів під час використання макетів зразків озброєння та військової техніки, а також складність використання засобів імітації поблизу лінії зіткнення через збільшення можливостей вогневого ураження з боку противника (постійне застосування розвідувальних та ударних БпЛА);

складність оцінювання ефективності проведених заходів із введення в оману для корегування впливу на противника.

Тому метою доповіді є підвищення ефективності проведення заходів введення противника в оману, за рахунок чіткої організації їх планування та реалізації, забезпечення контролю та взаємодії на всіх етапах будь-якої операції Сил оборони України.

Koval D. V., Ph. D.
Koval M. V.
Sribnyi O. M.
Korolov Zhytomyr Military Institute

## INNOVATIVE TECHNOLOGIES FOR ENSURING ACADEMIC INTEGRITY IN PROFESSIONAL TRAINING: EXPERIENCE OF IMPLEMENTING THE VEX SYSTEM

Even with the dominance of traditional offline learning formats, the digitalization of the educational process dictates the need for objective and automated assessment of student knowledge during in-person classes. The training of highly qualified professionals requires not only the provision of relevant lecture content but also the creation of reliable mechanisms for controlling its assimilation. A key challenge in this context is ensuring academic integrity during computerized testing held in university computer laboratories. A decline in academic integrity directly impacts the quality of graduates' training, their actual competence, and the overall image of the educational institution.

Standard computerized testing platforms used in physical classrooms often prove vulnerable to various methods of rule circumvention. Despite the physical presence of an instructor, monitoring every student's screen simultaneously is virtually impossible, allowing students to use unauthorized external resources, switch tabs, or collaborate. To address these issues, the VEX system was developed and

implemented – a web-based platform whose architecture was designed with strict security and anti-cheating requirements tailored specifically for classroom deployment. The VEX platform offers a comprehensive approach that combines cryptographic protection, content randomization, and continuous algorithmic monitoring of user behavior.

The primary preventive mechanism in the VEX system is the deep individualization of test tasks. During session initialization, the platform's algorithms generate a unique sequence of questions and shuffle the answer options individually for each test-taker. This completely eliminates the possibility of using pre-prepared numerical answer templates. Furthermore, it renders cheating by looking at a neighbor's screen entirely ineffective, as even visually identical questions possess a different configuration of correct options.

An important aspect of the system is strict session control and time limitation, customized for the duration of an offline class. Registration for a specific assessment event is open for a strictly defined, brief period at the beginning of the lesson. Each student receives a unique access token, which is strictly bound to their IP address at the database level. In an offline context, this ensures that students are accessing the test exclusively from the designated laboratory network, preventing attempts to take the test remotely for an absent peer. Upon expiration of the allocated time, the system automatically and forcibly closes the session, recording the current result and blocking any further manipulations.

For continuous monitoring of the testing process during the class, a special anti-cheat module was developed. It records suspicious student actions, specifically the loss of active page focus or switching between browser tabs (e.g., attempting to search for answers online). Each such action is logged by the system as a distinct violation. The system automatically calculates and applies penalty points for each attempt at dishonest behavior, dynamically deducting them from the final score. Simultaneously, the instructor gains access to a real-time monitoring dashboard on their device, displaying each participant's progress and the number of recorded violations, allowing for immediate in-class response and the forced cancellation of violators' sessions.

The implementation of the VEX platform during offline professional training demonstrates a significant reduction in academic cheating. The comprehensive use of dynamic randomization methods, localized session protection, strict time management, and algorithmic penalty calculation allows educators to obtain the most objective picture of knowledge. The use of such specialized systems is a necessary

step to improve the quality of higher education and foster a responsible, professional attitude among future specialists toward the results of their labor.

Жовноватюк Р. М., канд. техн. наук, ст. наук. співроб.
Манько О. В., канд. техн. наук, ст. наук. співроб.
Житомирський військовий інститут імені С. П. Корольова

## АВТОМАТИЗАЦІЯ ОСВІТНЬОЇ ДІЯЛЬНОСТІ В ХОДІ ПІДГОТОВКИ ФАХІВЦІВ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Широке розповсюдження систем штучного інтелекту (далі - ШІ) змінило вже звичний для усіх порядок роботи у мережі інтернет. Традиційне формування пошукового запиту, з подальшим почерговим переглядом за посиланнями результатів пошукової видачі змінилося на отримання уже готових відповідей. Таким чином, отримання результату не потребує синтезу вихідних даних. Такий порядок речей має достатньо суттєвий вплив і на процеси освітньої діяльності. Причиною цього є зміна вже усталеної послідовності дій під час освоєння матеріалу (рис. 1).

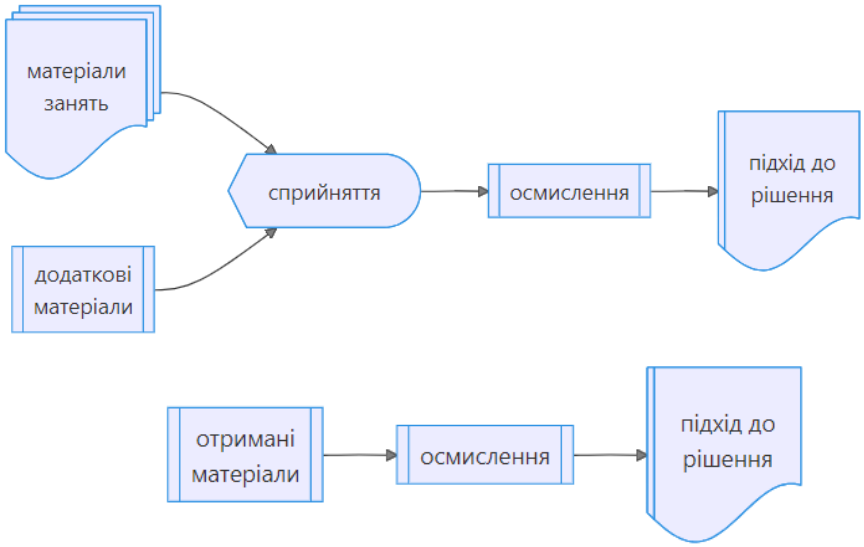


Рис. 1

Оскільки матеріал інформаційними системами з ШІ уже надається опрацьованим, фаза осмислення і сприйняття поєднується. Окрім того, потенційно втрачається можливість опрацювання розширеного контексту

питання (дані із першоджерела), що вивчається, та розгляду варіантів альтернативних рішень.

Для вирішення даних питань пропонується застосування інформаційно-комунікаційної системи (далі - ІКС) , яка дозволить автоматизувати процеси проведення навчальних занять, а також контролювати використання ШІ. А враховуючи особливості та сфери підготовки фахівців у військових навчальних закладах, така ІКС зможе функціонувати і у локальних мережах (без доступу до мережі інтернет).

У доповіді запропоновано прототип такої ІКС, описуються її підсистеми: авторизації користувачів, адміністрування, проведення занять та тестування.

Підсистеми авторизації та адміністрування забезпечують формування та доступ до індивідуального простору для кожного користувача. до підготовленої саме для них інформації. Це дозволяє формувати індивідуальну траєкторію для кожного здобувача вищої освіти. Авторизація дозволяє вести також і облік часу для кожного учасника навчального процесу. Це стосується і аудиторних годин, і годин самостійної підготовки.

Для здобувачів освіти, профіль користувача відображає показники, що характеризують проходження освітньої компоненти. Є основою для надання рекомендацій як персональних, так і групових, у разі виявлення загальних тенденцій і закономірностей.

Для викладача, система адміністрування передбачає інструмент для: розробки / редагування матеріалів занять; підготовки тестів та практичних завдань; управління доступом здобувачів освіти до матеріалів навчальних занять; обліку виконаних завдань (практичних, лабораторних, курсових, індивідуальних); перевірки виконаних здобувачами завдань; висвітлення успішності; створення загальних та персональних повідомлень здобувачам освіти; аналізу показників, обраних для контролю процесу проходження здобувачами освітньої компоненти.

Для функціонування підсистеми адміністрування передбачено використання інформації згенерованої веб-сервісами на основі ШІ. Також підсистема дозволяє використовувати локальні системи машинного навчання для автоматизованої перевірки завдань.

Підсистема проведення занять та тестування передбачає наявність функціоналу для інтерактивної взаємодії із здобувачами освіти, а саме:

відображення презентаційних матеріалів, та управління ходом відображення; проведення тестування здобувачів освіти; робочі місця для виконання практичних завдань; засіб для обміну повідомленнями (чат).

У доповіді запропоновані подальші напрями вдосконалення представленої ІКС, варіанти врахування специфіки викладання різних дисциплін.

Сергієнко О. П.
Скиба І. П.
Житомирський військовий інститут імені С. П. Корольова

## НАПРЯМИ ПІДГОТОВКИ СПЕЦІАЛІСТІВ ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ

Триваюча російсько-українська війна поєднує сучасні технології кінетичного ураження та потужного інформаційно-психологічного впливу. Розвиток роботизованих, цифрових систем та технологій на основі штучного інтелекту дають новий поштовх у використанні сил і засобів психологічних операцій. Уміле застосування методів інформаційно-психологічного впливу дозволяють мати Україні потужну інформаційну зброю, не менш важливу ніж безпілотні та інші бойові системи.

Нинішній інформаційний простір, переповнений безперервними комунікаційними потоками, дедалі активніше впливає на формування світогляду, системи цінностей та поведінкових моделей людини. В умовах постійного перенасичення інформації в медіа та соціальних мережах, значна частина громадян не завжди усвідомлює, що їхні переконання, уподобання та рішення виникають не спонтанно, а ймовірно, є наслідком цілеспрямованого інформаційно-психологічного впливу.

Застосування засобів масової інформації, соціальних платформ, цифрових технологій, а також розважального контенту створює можливості для прихованого, проте результативного впливу на суспільні настрої та громадську думку. У нинішньому інформаційному середовищі такі інструменти дають змогу досягати стратегічних цілей в тому числі у поєднанні із використанням засобів вогневого ураження на території агресора для дестабілізації держави із середини та формування вигідних світоглядних установок серед окремих соціальних груп.

Важливе місце у даному контексті відіграє інформаційно-психологічний вплив на морально-психологічний стан військовослужбовців ворога. Зниження мотивації, посилення страху, недовіра до командування, все це зазвичай впливає на виконання бойових завдань військовослужбовців держави агресора.

Стрімкий розвиток програмних продуктів на основі штучного інтелекту розширюють можливості психологічних операцій щодо генерування текстів меседжів, зображень, відеоматеріалів, клонування реального голосу людини, музичних композицій для матеріалів інформаційно-психологічного впливу на цільові аудиторії агресора, які розповсюджуються з використанням соціальних мереж та месенджерів.

Переорієнтування у зміні тактик на полі бою щодо ведення вогневого ураження противника з використанням безпілотних систем призвів і до зміни засобів доставки аудіовізуальних продуктів психологічного впливу.

Розвиток безпілотних систем для деморалізації противника у районах виконання бойових завдань, доставки листівок та інших продуктів психологічного впливу до аудиторії агресора, є одним із напрямів застосування безпілотних літальних апаратів у розрізі ведення психологічних операцій. Такі системи поєднують апарати повітряної доставки, автоматизовані механізми скиду та засоби психологічного впливу, що дозволяє знизити ризик ураження персоналу розрахунків екіпажів психологічних операцій, здійснити цільове розповсюдження матеріалів інформаційно-психологічного впливу.

Отже, сутність російсько-української війни переконливо демонструє, що психологічні операції сьогодні виступають невід’ємним елементом військового протистояння, у межах якого саме перевага в інформаційному просторі дедалі частіше визначає динаміку та характер військових операцій (бойових дій). В умовах агресії проти України, в тому числі й інформаційної, особливої ваги набувають нові напрямки підготовки спеціалістів психологічних операцій з урахуванням стрімкого розвитку програмного забезпечення на основі штучного інтелекту та безпілотних і роботизованих систем.

Умінський В. В., канд. техн. наук, ст. наук. співроб.
Молош О. С.
Житомирський військовий інститут імені С. П. Корольова

# АВТОРИЗАЦІЯ КОРИСТУВАЧІВ АВТОМАТИЗОВАНОЇ СИСТЕМИ ЗА ІДЕНТИФІКАТОРОМ НА ЕЛЕКТРОННОМУ НОСІЇ ІНФОРМАЦІЇ

Сучасний розвиток інформаційних технологій, поширення автоматизованих систем та постійне зростання кількості кіберзагроз зумовлюють необхідність удосконалення механізмів контролю доступу до інформаційних ресурсів. Метою роботи є розробка застосунку авторизації користувачів автоматизованої системи за ідентифікатором на електронному носії інформації та дослідження методів підвищення рівня захисту доступу до інформаційних ресурсів.

У межах дослідження проаналізовано сучасні методи ідентифікації, автентифікації та авторизації користувачів, а також принципи функціонування таких протоколів, як OAuth, Kerberos, LDAP, SAML та JWT. Визначено, що найбільш ефективним підходом до підвищення рівня безпеки є поєднання декількох факторів автентифікації, зокрема знання пароля та володіння фізичним носієм інформації.

У розробленому програмному застосунку реалізовано двофакторну автентифікацію користувача. Перший етап передбачає перевірку логіна та пароля користувача, другий – перевірку унікального ідентифікатора, що зберігається на електронному носії інформації.

Окрему увагу приділено реалізації механізму безперервної автентифікації (Continuous Authentication). Система постійно контролює фізичну присутність електронного носія інформації під час активної сесії користувача. У разі вилучення USB-токена доступ до автоматизованої системи миттєво блокується, а користувач автоматично повертається до форми входу. Це дозволяє мінімізувати ризики несанкціонованого використання відкритої сесії та підвищує відповідність системи принципам концепції Zero Trust Security.

Запропонований підхід дозволяє підвищити рівень інформаційної безпеки автоматизованих систем, забезпечити захист від несанкціонованого доступу та зменшити вплив людського фактора на безпеку оброблюваної інформації.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Губатюк М. О.
Житомирський військовий інститут імені С. П. Корольова

# ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У ПІДГОТОВЦІ ФАХІВЦІВ ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ

Сучасний розвиток інформаційних технологій суттєво змінює характер інформаційного протиборства та висуває нові вимоги до професійної підготовки фахівців психологічних операцій. Зростання обсягів інформації, активне використання цифрових платформ і соціальних мереж, а також поширення автоматизованих систем аналізу даних зумовлюють необхідність впровадження технологій штучного інтелекту в освітній процес. У цих умовах підготовка фахівців повинна бути орієнтована не лише на опанування традиційних методів інформаційно-психологічного впливу, а й на здобуття навичок роботи із сучасними інтелектуальними системами.

Штучний інтелект відкриває нові можливості для аналізу інформаційного середовища, прогнозування поведінки цільових аудиторій та оцінювання ефективності інформаційно-психологічних заходів. Використання алгоритмів машинного навчання дозволяє здійснювати автоматизований моніторинг інформаційного простору, виявляти тенденції поширення інформації, аналізувати настрої аудиторій та прогнозувати можливі інформаційні загрози. Водночас сучасні великі мовні моделі здатні підтримувати процес аналізу текстових матеріалів, формування аналітичних висновків і моделювання інформаційних кампаній.

Однією з актуальних проблем залишається недостатня інтеграція засобів штучного інтелекту в систему професійної підготовки. У багатьох випадках освітні програми не встигають адаптуватися до швидких технологічних змін, що призводить до розриву між сучасними практичними потребами та змістом навчання. Крім того, важливим завданням є формування у майбутніх фахівців навичок критичного оцінювання результатів роботи алгоритмів, оскільки автоматизовані системи можуть генерувати неточні або упереджені висновки.

Підвищенню якості підготовки сприятиме оновлення освітніх компонентів з урахуванням сучасних досягнень у сфері штучного інтелекту, впровадження практикоорієнтованих занять із використанням спеціалізованого програмного забезпечення, а також розроблення навчальних кейсів, що

моделюють реальні інформаційно-психологічні операції. Особливого значення набуває формування культури безпечного та етичного використання технологій штучного інтелекту в професійній діяльності.

Отже, інтеграція технологій штучного інтелекту в систему підготовки фахівців психологічних операцій є необхідною умовою підвищення ефективності їх професійної діяльності в умовах сучасного інформаційного протиборства. Використання інтелектуальних систем аналізу даних сприятиме розвитку аналітичних компетентностей, удосконаленню процесів прийняття рішень та підвищенню готовності майбутніх фахівців до виконання завдань за призначенням.

Беньковський С. Ю., канд. юрид. наук, доц.
Інститут Військово-Морських Сил Національного університету
"Одеська морська академія"

## ПРОБЛЕМИ АДАПТАЦІЇ СТАНДАРТІВ НАТО В СИСТЕМІ ПІДГОТОВКИ ФАХІВЦІВ ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ В УКРАЇНІ

Сучасні безпекові виклики, пов'язані з повномасштабною агресією проти України, актуалізували необхідність удосконалення системи підготовки військових фахівців, зокрема у сфері психологічних операцій (PsyOps). В умовах гібридної війни інформаційно-психологічний вплив став одним із ключових інструментів досягнення стратегічних цілей. Саме тому особливого значення набуває питання адаптації стандартів НАТО у системі професійної підготовки фахівців психологічних операцій в Україні.

Психологічні операції в країнах НАТО є важливою складовою стратегічних комунікацій та інформаційного забезпечення військових операцій. Альянс приділяє значну увагу підготовці висококваліфікованих фахівців, здатних здійснювати інформаційно-психологічний вплив на визначені цільові аудиторії, протидіяти дезінформації, формувати позитивний імідж військових структур та забезпечувати інформаційну підтримку операцій. У зв'язку з євроатлантичним курсом України постає необхідність гармонізації національної системи військової освіти зі стандартами НАТО.

Водночас процес адаптації стандартів НАТО у сфері підготовки фахівців психологічних операцій супроводжується низкою проблем організаційного,

методичного, кадрового та технологічного характеру. Це потребує комплексного аналізу та пошуку ефективних шляхів модернізації системи професійної підготовки.

У країнах НАТО психологічні операції розглядаються як складова інформаційної діяльності, спрямованої на вплив на емоції, мотивацію, поведінку та прийняття рішень цільових аудиторій. Основною метою PsyOps є формування сприятливого інформаційного середовища для досягнення військових і політичних цілей.

Система підготовки фахівців психологічних операцій у країнах НАТО базується на принципах міждисциплінарності, практичної орієнтованості, інтеграції сучасних цифрових технологій та розвитку критичного мислення. Особлива увага приділяється комунікативній підготовці, психології масових комунікацій, стратегічним комунікаціям, медіаграмотності, роботі з інформаційними ресурсами, аналізу інформаційного середовища, іншомовній підготовці, навичкам міжкультурної комунікації.

Важливою особливістю стандартів НАТО є орієнтація на практичне моделювання реальних інформаційних ситуацій та проведення тренувань у максимально наближених до бойових умовах.

Однією з головних проблем адаптації стандартів НАТО в Україні є недостатня нормативно-правова та методична база у сфері підготовки фахівців психологічних операцій. Незважаючи на активне реформування сектору безпеки й оборони, окремі елементи системи військової освіти все ще функціонують відповідно до застарілих підходів, які не повною мірою відповідають сучасним вимогам інформаційної війни.

Суттєвою проблемою є також недостатній рівень кадрового забезпечення. Підготовка фахівців PsyOps потребує залучення висококваліфікованих викладачів, які мають не лише теоретичні знання, а й практичний досвід участі в інформаційно-психологічних операціях. Крім того, важливим є володіння іноземними мовами для роботи з міжнародними стандартами, документами НАТО та участі у спільних навчаннях.

Ще одним викликом є обмеженість сучасної матеріально-технічної бази. Ефективна підготовка фахівців психологічних операцій передбачає використання мультимедійних платформ, цифрових симуляторів, систем аналізу інформаційного простору, програм для моніторингу соціальних мереж, технологій штучного інтелекту.

У багатьох закладах військової освіти України рівень технічного забезпечення ще не повністю відповідає сучасним вимогам.

Складною залишається проблема інтеграції міждисциплінарного підходу. Підготовка фахівців психологічних операцій вимагає поєднання знань із психології, соціології, лінгвістики, інформаційних технологій, журналістики, стратегічних комунікацій та військової справи. На практиці навчальні програми часто мають фрагментарний характер, що ускладнює формування комплексної професійної компетентності.

Важливою проблемою є також недостатній рівень розвитку іншомовної комунікативної компетентності майбутніх фахівців. У системі НАТО англійська мова є основним інструментом професійної взаємодії. Тому низький рівень володіння професійною англійською мовою обмежує можливості українських фахівців щодо участі у міжнародних навчаннях, стажуваннях та спільних операціях.

Сучасний розвиток цифрових технологій суттєво змінює характер інформаційно-психологічного впливу. Соціальні мережі, цифрові медіа, штучний інтелект та аналітичні системи стали важливими інструментами психологічних операцій. У зв'язку з цим підготовка фахівців PsyOps повинна враховувати нові технологічні тенденції.

Особливого значення набуває використання технологій штучного інтелекту у професійній підготовці. ШІ може застосовуватися для аналізу інформаційних потоків, прогнозування інформаційних загроз, автоматизованого моніторингу соціальних мереж, створення навчальних симуляцій, розвитку комунікативних навичок, персоналізації навчання.

Використання інтерактивних платформ, кейс-методу, ситуаційного моделювання та технологій змішаного навчання сприяє підвищенню ефективності професійної підготовки та формуванню практичних навичок майбутніх фахівців.

Для успішної адаптації стандартів НАТО у сфері підготовки фахівців психологічних операцій необхідно реалізувати комплекс заходів.

Передусім важливим є оновлення освітніх програм відповідно до сучасних вимог інформаційної безпеки та стандартів Альянсу. Навчальні дисципліни повинні бути орієнтовані на практичну підготовку, розвиток критичного мислення та формування навичок роботи в умовах інформаційного протиборства.

Доцільним є розширення міжнародного співробітництва із закладами освіти країн НАТО, участь у спільних тренінгах, стажуваннях та міжнародних навчаннях. Це сприятиме обміну досвідом та впровадженню сучасних методик підготовки.

Особливу увагу необхідно приділяти розвитку іншомовної підготовки майбутніх фахівців. Володіння професійною англійською мовою є важливою складовою ефективної взаємодії у багатонаціональному середовищі.

Перспективним напрямом є також активне впровадження технологій штучного інтелекту та цифрових освітніх платформ у систему військової освіти. Це дозволить підвищити адаптивність навчання та ефективність формування професійних компетентностей.

Отже, адаптація стандартів НАТО у системі підготовки фахівців психологічних операцій в Україні є важливим напрямом реформування військової освіти в умовах сучасних безпекових викликів. Психологічні операції відіграють важливу роль у забезпеченні інформаційної безпеки держави та протидії інформаційній агресії.

Основними проблемами адаптації залишаються недостатня нормативно-методична база, кадрові труднощі, обмеженість матеріально-технічного забезпечення, потреба в міждисциплінарній інтеграції та недостатній рівень іншомовної підготовки.

Подальше вдосконалення системи професійної підготовки фахівців PsyOps повинно ґрунтуватися на впровадженні сучасних освітніх технологій, розвитку міжнародного співробітництва, інтеграції стандартів НАТО та активному використанні цифрових технологій і штучного інтелекту. Це сприятиме формуванню висококваліфікованих фахівців, здатних ефективно діяти в умовах сучасного інформаційного протиборства.

Богуславець А. В., канд. психол. наук, ст. досл.
Воєнна академія імені Євгенія Березняка

# ПСИХОЛОГО-ПЕДАГОГІЧНІ ЗАСАДИ ФОРМУВАННЯ В МАЙБУТНІХ ФАХІВЦІВ КОГНІТИВНОЇ БЕЗПЕКИ ТА КУЛЬТУРИ ЦИФРОВОЇ АНОНІМНОСТІ

Нові виклики та загрози системі національної безпеки, які з'явилися після повномасштабного вторгнення рф на територію України, спонукають науково-педагогічних працівників (НПП) закладу вищої освіти (ЗВО) до комплексної трансформації освітнього процесу. В умовах безперервного інформаційно-психологічного протиборства підготовка майбутніх фахівців сектору безпеки і оборони України (СБіО України) до виконання ними спеціальних завдань потребує принципово нових педагогічних підходів.

Ураховуючи специфіку завдань майбутньої професійної діяльності, ключовими векторами підготовки фахівців є глибоке розуміння та практичне застосування принципів абсолютної цифрової анонімності та успішної роботи в умовах перманентного стрес-впливу віртуального інформаційного простору (ВІП).

Забезпечення цифрової анонімності під час виконання майбутніми фахівцями СБіО України спеціальних завдань має розглядатися не крізь призму суто технічних дисциплін, а як складний інтрапсихічний процес. НПП ЗВО мають спрямувати зусилля на формування у них особливих патернів мислення та когнітивну установку "нульової довіри" до ВІП, перевівши фокус із захисту апаратних пристроїв на захист власної психіки та поведінкових реакцій.

З цією метою НПП ЗВО рекомендується впроваджувати у освітній процес такі методичні підходи:

розвиток рефлексивного контролю за поведінковим слідом – замість технічного аналізу метаданих чи геолокацій, ННП бажано акцентувати увагу на психологічній складовій "цифрового сліду". Майбутні фахівці СБіО України мають навчитися аналізувати власні неусвідомлені патерни поведінки у мережі (ритми активності, емоційні реакції в текстах, вибір специфічної лексики та швидкість відповідей). Тому, тренінг оперативної пильності має сформувати звичку до постійного самомоніторингу, щоб майбутній фахівець розумів, як його лінгвальні та паралінгвальні маркери можуть видати ворогу його реальний психотип, рівень стресу чи фахову приналежність;

формування навичок психологічної компартменталізації (ізоляції ідентичностей) – використання багаторівневого проксіювання (VPN, Tor) має супроводжуватися відповідною ментальною ізоляцією. НПП ЗВО доцільно навчати майбутніх фахівців СБіО України чітко розмежовувати реальне "Я" та створену ідентичність, вони мають навчитися так би мовити "вмикати" і "вимикати" свій образ синхронно із запуском захищеного ВІП. Це запобігає емоційному вигоранню та перенесенню психологічного напруження, яке виникає в результаті виконання спеціальних завдань у реальне життя. Згідно з компетентнісним підходом, будь-яка емоційна дифузія (втрата контролю над почуттями створеного образу) під час навчальної вправи має оцінюватися як зрив завдання та деанонімізація (розконспірація);

стрес-інокуляція (мікрострес у формі психологічного щеплення) проти маніпулятивного впливу сторонніх осіб – навчальні ситуації "зворотного фішингу" (наприклад фейкові бази даних) мають розглядатися насамперед як таргетовані когнітивні впливи з боку сторонніх осіб. Завдання НПП – не просто навчити майбутніх фахівців не відкривати небезпечні URL-адреси, а допомогти їм ідентифікувати власні психологічні вразливості (надмірну цікавість, професійну емпатію, страх втратити контроль чи реакцію на авторитет). Моделювання таких соціально-інженерних маніпуляцій під час викладання спеціальних дисциплін формує у них стійкий психологічний імунітет та здатність блокувати імпульсивні реакції в умовах стресу.

Означений методичний блок логічно доповнить систему психологічної підготовки майбутніх фахівців СБіО України, перетворюючи його в професійно реалізованого, успішного керівника (менеджера). Застосування цих методичних рекомендацій сприятиме підготовці майбутніх фахівців СБіО України нової формації, здатних дистанційно керувати діяльністю осіб в умовах агресивного полігібридного протистояння.

Молдован В. Д., канд. техн. наук, доц.
Семібаламут К. М., канд. техн. наук, доц.
Воєнна академія імені Євгенія Березняка

# ПРАВОВІ АСПЕКТИ ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ТЕХНІЧНИХ ЗАСОБІВ НЕГЛАСНОГО ОТРИМАННЯ ІНФОРМАЦІЇ

У сучасних умовах правового режиму воєнного стану та умовах стрімкого розвитку технологій, особливої актуальності набуває питання правового регулювання використання спеціальних технічних засобів (СТЗ) для негласного отримання інформації. До таких засобів належать пристрої, які становлять загрозу інформаційній безпеці на об'єктах інформаційної діяльності а також праву людини на приватність. У правовому полі, відповідно статті 2 наказу Служби безпеки України від 23.12.2020 № 383 "Про затвердження Зводу відомостей, що становлять державну таємницю", спеціальні технічні засоби – це технічні засоби, устаткування, апаратура, прилади, пристрої, програмне забезпечення, препарати та інші вироби, призначені (спеціально розроблені, виготовлені, запрограмовані або пристосовані) для негласного отримання інформації. Йдеться про засоби, здатні здійснювати аудіо-, відеофіксацію або перехоплення інших даних. Ключовою ознакою таких пристроїв є їхня прихованість, тобто здатність працювати непомітно для оточуючих.

Важливим критерієм належності таких засобів до СТЗ є функціональне призначення пристрою. СТЗ повинні мати можливість реєструвати, передавати або зберігати інформацію, часто – дистанційно та без явних демаскуючих ознак їх роботи. Крім того, значну роль відіграє конструктивне виконання: такі пристрої маскуються під звичайні побутові, офісні предмети, сам засіб має мініатюрні розміри для прихованого встановлення.

З правової точки зору, вирішальним є не лише технічний аспект, але й мета застосування СТЗ, його придатність для негласного збору інформації у скритний (прихований) спосіб, характерний для оперативно-розшукової, розвідувальної діяльності.

В Україні правове регулювання цієї сфери здійснюється низкою нормативно-правових актів. Зокрема, Кримінальний кодекс передбачає відповідальність за незаконне придбання, збут або застосування таких засобів. Також відповідні норми містяться у інших нормативно-правових актах та

Законах України у оперативно-розшуковій діяльності та у сфері технічного захисту інформації (ТЗІ). Обіг СТЗ є обмеженим. Їх застосування дозволяється лише уповноваженим органам у межах закону. Для інших осіб придбання чи застосування таких засобів може мати правові наслідки.

Важливим елементом віднесення технічних засобів негласного отримання інформації до СТЗ є їх експертне дослідження. При цьому важливим є наступні етапи: коректне вилучення виявленого технічного засобу та його підготовка до передачі на експертне дослідження. Порядок проведення експертних досліджень СТЗ визначається загальною методикою "Експертиза спеціальних технічних засобів негласного отримання інформації" та відповідною окремою методикою.

**Висновок.** Таким чином, з правової точки зору регулюється застосування СТЗ, їх виявлення, вилучення та проведення експертного дослідження, що є одним із ключових напрямків технічної підготовки фахівців у сфері ТЗІ.

Попова К. А.
Твердохвалова В. О.
Житомирський військовий інститут імені С. П. Корольова

## ЕМОЦІЙНЕ ВИГОРАННЯ КУРСАНТІВ ЯК ЗАГРОЗА ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІЙ БЕЗПЕЦІ МАЙБУТНЬОГО ВІЙСЬКОВОГО ФАХІВЦЯ

Інформаційно-психологічна безпека особистості є однією з визначальних умов надійного виконання завдань фахівцями військових спеціальностей. Її основу становить здатність людини зберігати психічну стійкість, адекватно сприймати й оцінювати інформацію та протистояти деструктивним інформаційно-психологічним впливам. У процесі підготовки курсантів ця здатність формується в умовах підвищеного психоемоційного навантаження, що актуалізує питання про внутрішні чинники, які її послаблюють. Одним із таких чинників є емоційне вигорання.

Емоційне вигорання розглядається у працях Г. Фройденбергера та К. Маслач як синдром емоційного виснаження, деперсоналізації та зниження відчуття власної ефективності; В. В. Бойко описав його стадійну динаміку, виокремивши фази напруження, резистенції та виснаження. Специфіку

вигорання курсантів закладів вищої освіти висвітлено у дослідженнях Ю. Адамчука, Л. П'янківської, Д. Кисленка. Проте вигорання рідко аналізується саме як загроза інформаційно-психологічній безпеці особистості.

Мета – обґрунтувати розгляд емоційного вигорання курсантів як загрози їхній інформаційно-психологічній безпеці на основі результатів емпіричного дослідження.

Дослідження проведено на базі Житомирського військового інституту імені С. П. Корольова; у ньому взяли участь 75 курсантів старших курсів. Використано методику діагностики рівня емоційного вигорання В. В. Бойка та опитувальник професійного вигорання К. Маслач.

Результати засвідчили, що приблизно у шостої частини курсантів сформовано симптоми всіх трьох фаз вигорання, а значна частина вибірки перебуває у стадії його формування. Переважають середні й високі показники емоційного виснаження та редукції професійних досягнень, а найвираженішою виявилася фаза резистенції з її економією емоцій та спрощеним ставленням до службових обов'язків. Кореляційний аналіз підтвердив поетапність розвитку синдрому – від напруження через резистенцію до виснаження, що супроводжується зростанням емоційного виснаження, деперсоналізації та зниженням оцінки власної ефективності.

Кожен із виявлених проявів вигорання послаблює інформаційно-психологічну безпеку особистості. Емоційне виснаження знижує концентрацію уваги, погіршує пам'ять та критичність мислення, унаслідок чого курсант гірше фільтрує й оцінює інформацію. Деперсоналізація та емоційне відчуження зменшують залученість до взаємодії в підрозділі й послаблюють групову згуртованість як ресурс протидії інформаційно-психологічному тиску. Редукція професійних досягнень супроводжується зниженням мотивації та впевненості у власних силах, що підвищує вразливість до тривожних і деморалізуючих повідомлень.

Тривожно-депресивні переживання та фіксація на психотравмуючих обставинах роблять курсанта чутливішим до маніпулятивних впливів, що експлуатують страх і невизначеність. Таким чином, вигорання діє як внутрішня загроза: воно не пов'язане безпосередньо із зовнішнім інформаційним нападом, проте створює сприятливе психологічне підґрунтя для його впливу, знижуючи захисні ресурси особистості.

Значущість цієї проблеми зростає з огляду на те, що випускники інституту виконуватимуть завдання у сферах, безпосередньо пов'язаних з опрацюванням

інформації та протидією інформаційним загрозам. Знижена внаслідок вигорання психологічна стійкість може негативно позначатися на якості та надійності виконання таких завдань. Особливу групу ризику становлять курсанти старших курсів, а також ті, хто має досвід контакту з травматичними подіями. Це підкреслює потребу в ранній діагностиці та профілактиці синдрому вже на етапі навчання.

Висновки. Емоційне вигорання курсантів доцільно розглядати як чинник зниження їхньої інформаційно-психологічної безпеки, а профілактику вигорання – як складову системи її забезпечення. Емпірично підтверджено наявність ознак вигорання у частини курсантів старших курсів. Профілактична робота має охоплювати індивідуальний рівень – формування навичок емоційної саморегуляції, стресостійкості та критичного сприйняття інформації; груповий – розвиток згуртованості підрозділів і взаємопідтримки; організаційний – оптимізацію навчально-службового навантаження та системний психологічний моніторинг стану курсантів. Реалізація цих заходів сприятиме збереженню психічного здоров'я й підвищенню стійкості майбутніх фахівців до інформаційно-психологічних впливів.

Присяжнюк М. М., канд. техн. наук, ст. наук. співроб.
Воєнна академія імені Євгенія Березняка
Карпович О. М.
В/ч А0193

## ФІЗІОГНОМІКА В ПРОЦЕСІ ДОСЛІДЖЕННЯ ПСИХОЛОГІЧНИХ ОСОБЛИВОСТЕЙ ОСОБИСТОСТІ ЯК ОБ'ЄКТА ВПЛИВУ

Підготовка і проведення інформаційних і психологічних операцій з метою протидії гібридним загрозам в умовах повномасштабної збройної агресії рф потребує якісної підготовки фахівців у сфері психологічних операцій, інформаційної безпеки та інформаційних технологій.

Важливою складовою цих операцій є здійснення інформаційно-психологічного впливу на визначені об'єкти противника з метою змушення їх до відмови від збройної агресії проти України.

Сучасний розвиток науки і техніки набув такого рівня, коли створена реальна можливість застосовувати засоби та методи прямого й непрямого впливу на нервову систему людини з метою зміни її функціонування.

Процес підготовки та здійснення інформаційно-психологічного впливу на відповідний об'єкт в інформаційних і психологічних операціях зазвичай складається з трьох етапів.

На першому етапі відбувається визначення об'єкта впливу й дослідження характерних його особливостей, слабких і сильних сторін. Цей етап займає найбільше часу в процесі підготовки і здійснення інформаційно-психологічного впливу – від 80 до 95 відсотків усього процесу здійснення впливу.

Другий етап – це вибір способів і засобів інформаційно-психологічного впливу на визначений об'єкт, який займає від 5 до10 відсотків усього процесу здійснення впливу.

І третій етап – це безпосередньо сам інформаційно-психологічний вплив на визначений об'єкт, який також займає від 5 до10 відсотків усього процесу здійснення впливу.

Тобто, перший етап визначення об'єкта впливу й дослідження його характерних особливостей потребує найбільше часу та ресурсів у процесі підготовки і здійснення інформаційно-психологічного впливу на обраний об'єкт, що, у свою чергу, знижує ефективність проведення інформаційно-психологічних операцій.

Скоротити час визначення об'єкта впливу і дослідження його особистих характеристик допомагає аналіз психологічних особливостей особистості як об'єкта впливу за допомогою методу фізіогноміки. Цей метод дозволяє в неінструментальний спосіб визначити психологічний тип особистості людини, її психологічні характеристики шляхом аналізу зовнішніх рис обличчя *(маркерів)*. Аналіз проводиться шляхом спостереження статичного виразу обличчя об'єкта обстеження (досліджуваної особи). За маркерами кожної риси обличчя, проводиться опис притаманних їй індивідуально-психологічних властивостей. Це дозволяє зробити висновок про особистість (психологічний портрет особистості), який включає в себе: психологічні характеристики, прогноз поведінки, ефективну стратегію комунікації, слабкі та сильні сторони обраного об'єкта впливу.

*У психологічному портреті розкриваються* індивідуально-психологічні особливості людини, надається прогноз поведінкових реакцій у стресовій ситуації та повсякденній діяльності, описуються способи ефективної взаємодії з об'єктом дослідження.

Зовнішні риси обличчя *(маркери)* визначеного об’єкта впливу поділяють на *вроджені* й *набуті*.

*До вроджених маркерів відносять*: форму голови, форму нижньої щелепи, пропорції рота, висоту та кут лоба, ширину і втиснутість перенісся, розвиненість вилиць, особливості підносового жолобка та особливості підборіддя.

*До набутих маркерів відносять*: розвиненість і форму губ, носогубні складки, особливості зморшок, густоту та форму брів, розташування очей, будову щік, розвиненість жувальних м’язів і кут нахилу кінчика носа.

Поєднання цих маркерів при дослідженні індивідуально-психологічних особливостей особистості дає можливість визначити ефективні стратегії інформаційно-психологічного впливу на визначений об’єкт відповідно до його аналізу за допомогою методу фізіогноміки, а також суттєво скоротити час першого етапу щодо вибору і вивчення характерних особливостей об’єкта впливу, його слабких і сильних сторін та вибору способів і засобів інформаційно-психологічного впливу.

**Висновки.** Впровадження в навчальний процес дисципліни з вивчення сучасних технологій інформаційного впливу, а також методу фізіогноміки для аналізу психологічних особливостей особистості як об’єкта впливу дозволить воєнним фахівцям з інформаційного впливу та протидії дезінформації підвищити ефективність цього важливого напряму.

Староконь Є. Г., канд. психол. наук
Магалецький О. О.
Житомирський військовий інститут імені С. П. Корольова

## ПРОПОЗИЦІЇ ЩОДО ОРІЄНТОВНОГО ЗМІСТУ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ “ПРИКЛАДНА ПСИХОЛОГІЯ” ДЛЯ ФАХІВЦІВ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ

Всі зусилля фахівців інформаційно-психологічних операції (ІПсО) приречені на невдачу, якщо інформаційний продукт створений без урахування механізмів сприйняття і обробки інформації інформаційною системою людей, що складають цільову аудиторію. Доставлене до цільової аудиторії інформаційне повідомлення, якщо воно не враховує свідомість і психіку людей, не варте витрат на її аналіз та його трансляцію.

Тому зміст підготовки фахівців інформаційно-психологічного впливу повинен бути сконцентрований саме на особливостях вивчення функціонування психіки людини та психології мас в ході сприйняття, усвідомлення та оцінки інформації.

Пропонуємо до освітньо-професійної програми фахівців відповідного профілю включити дисципліну "Прикладна психологія", яка охопить широке коло професійних проблем з такими орієнтовними темами.

Змістовний модуль1. Психологія впливу

Тема 1. Теоретичні основи соціального впливу. Три складові впливу: установка, поведінка, когніція. Зміна поведінки в результаті соціального научіння. Зовнішній вплив як джерело внутрішніх змін. Супротив і підпорядкування впливу. Подолання супротиву. Підпорогові стимули.

Тема 2. Маніпуляція і маніпулятори: сутність. Моделювання маніпулятивного впливу. Маніпулювання інформацією. Маніпуляція дією. Мішені впливу. Принади у маніпулюванні. Спонукання цільової аудиторії (ЦА) до дій.

Змістовний модуль 2. Психологія мас

Тема 3.Поняття про маси. Людина в масі. Лідери мас. Масова свідомість. Лідери мас як об'єкт інформаційно-психологічного впливу (ІПсВ)

Тема 4. Природа масових настроїв. Механізми формування масових настроїв. Функції масових настроїв. Масові настрої як об'єкт ІПсВ.

Тема 5. Стихійна поведінка. Психологія натовпу. Психологія публіки. Масова паніка. Масова агресія. Врахування механізмів формування стихійної поведінки в ході організації ІПсВ на ЦА.

Тема 6.Масові комунікації та їх ефекти. Чутки та їх різновиди. Циркуляція чуток та боротьба з ними. Можливості засобів масової комунікації для виконання завдань ІПсВ.

Змістовний модуль 3. Політична психологія.

Тема 7. Політична свідомість і самосвідомість. Колективне безсвідоме в політиці. Три блоки психіки в політиці. Політичні установки і стереотипи. Політична поведінка. Врахування політичної свідомості ЦА в ході планування та проведення заходів ІПсВ.

Тема 8. Великі соціальні групи. Національний характер. Національна свідомість і самосвідомість. Рівні розвитку інтегративності великих груп. Психологія еліт як мішень ІПсВ.

Змістовний модуль 4. Психологія реклами.

Тема 9. Психологічні основи реклами як комунікації. Соціальні оцінки. Соціальні порівняння. Соціальна мода. Врахування даних категорій при підготовці продукції ІПсВ.

Тема 10. Реклама як інформаційний вплив: гіпноз, навіювання, наслідування, зараження, переконання, стереотип, імідж, ідентифікація, соціально-психологічна установка. Використання механізмів рекламного впливу при виконанні завдань ІПсВ

Тема 11. Психологія пропаганди і реклами у засобах масової інформації. Мета і завдання пропаганди. Пропаганда в умовах психологічної війни. Механізми впливу пропаганди на психіку людини. Вплив психологічних стереотипів на сприйняття змісту пропаганди. Умови використання закономірностей реклами для організації ІПсВ.

Тема 12. Експертиза реклами.

Техніки і технології визначення ефективності впливу інформаційних матеріалів. Оцінка ефективності інформаційних продуктів.

Змістовний модуль 5. Психологія російського націоналізму

Тема 13. Психологія етносів і народів російської федерації. Точки уразливості національної свідомості росіян. Етнічні конфлікти. Криміналітет в культурі та ідеології росіян. Конфлікти між етносами російської федерації на релігійному грунті.

Змістовний модуль 6. Оперативна діяльність та питання конспірації в діяльності персоналу підрозділів ПсО.

Тема 14. Рольова поведінка і поняття про оперативну діяльність. Інформатори, та способи їх залучення до співпраці. Організація зустрічей з потрібними людьми. Загальні вимоги до безпеки діяльності персоналу підрозділів ПсО. Загальні правила безпечної поведінки. Зовнішня та внутрішня безпека.

Когнітивно-смисловий підхід до формування необхідних компетенцій персоналу підрозділів ІПсО щодо створення продукції ІПсВ, на відміну від біхевіористського, забезпечить високий рівень їх професіоналізму та ефективність виконання завдань за призначенням.

Ринський І. М.
Скиданенко В. В.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

# ПРОБЛЕМИ ПІДГОТОВКИ КОМАНДИРІВ СИЛ ТЕРИТОРІАЛЬНОЇ ОБОРОНИ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА ПСИХОЛОГІЧНОЇ СТІЙКОСТІ ПІДРОЗДІЛІВ І НАСЕЛЕННЯ

Досвід війни України за Незалежність засвідчив суттєву зміну ролі командира у сучасному бою. В умовах повітряно-прозорої реальності, цифрової залежності управління, інформаційного перевантаження, психологічного виснаження особового складу командир дедалі більше виконує функцію не лише організатора бойових дій, а й елемента забезпечення інформаційної та психологічної стійкості підрозділу. Особливого значення зазначена проблема набуває для Сил територіальної оборони України. Підрозділи ТрО тривалий час виконують бойові завдання у складі угрупувань військ, одночасно зберігаючи тісний зв'язок із цивільним середовищем. Командир ТрО діє у військовому, інформаційному та соціально-психологічному середовищах одночасно. Соціальні мережі, Telegram-ресурси, цифрові платформи, відкриті інформаційні спільноти та безперервний потік негативної інформації формують умови психологічного напруження, емоційного виснаження та зниження критичності сприйняття інформації. У таких умовах навіть молодший командир стає одним із ключових елементів стабілізації внутрішнього інформаційного середовища. Саме від здатності сержанта своєчасно реагувати на панічні настрої, деструктивні чутки, конфлікти, маніпуляції залежить рівень керованості і ефективності підрозділу. Однак, більшість командирів не проходили спеціальної підготовки до дій в умовах когнітивного перевантаження війною. Їх навчали організації бою, управлінню підрозділом та застосуванню озброєння, але сучасна війна вимагає додаткових компетенцій: навичок кризової комунікації, інформаційної гігієни, розуміння механізмів інформаційно-психологічного впливу, протидії панічним настроям та підтримання внутрішньої інформаційної стійкості підрозділу. Окремою проблемою вбачається функціонування системи

територіальної оборони у повоєнний період. Після завершення активної фази війни рф не припинить інформаційного та психологічного тиску. Тоді саме командири Сил ТрО залишатимуться одним із базових елементів підтримання локальної стійкості громад, підготовки населення до національного спротиву та протидії інформаційно-психологічним операціям противника. Вбачається, що підготовка командирів Сил ТрО до забезпечення інформаційної та психологічної стійкості повинна розглядатись як складова загальної бойової підготовки, а не елемент психологічної підтримки персоналу. Командири повинні володіти навичками виявлення ознак психологічного виснаження, деструктивних інформаційних впливів, панічних настроїв та інформаційних маніпуляцій. Відтак, одним з напрямів має стати включення до системи підготовки офіцерів і сержантів базових елементів когнітивної безпеки та управління особовим складом в умовах інформаційного перевантаження. Важливого значення набуває розвиток навичок кризової комунікації. В умовах високої інформаційної турбулентності саме командир часто залишається основним джерелом довіри для особового складу. Його здатність оперативно доводити достовірну інформацію, пояснювати логіку рішень та знижувати рівень невизначеності безпосередньо впливає на керованість підрозділу. Окремим напрямом є формування у командирів практичних навичок роботи з цивільним середовищем. Специфіка ТрО полягає у постійному контакті з місцевими громадами та населенням, отже командир повинен бути готовим до функціонування не лише у військовому, а й у соціально-інформаційному середовищі. У повоєнний період саме підрозділи ТрО та їх командири можуть стати одним із ключових елементів підтримання локальної готовності до національного спротиву. Практична реалізація зазначених завдань можлива шляхом поєднання підготовки у вищих військових навчальних закладах, системи перепідготовки офіцерів і сержантів, а також залучення до роботи у військах штатних психологів, фахівців інформаційної безпеки та спеціалістів із кризових комунікацій. Таким чином, сучасна війна поступово змінює саму функціональну роль командира підрозділу Сил ТрО. В умовах цифровізації бойового простору, постійного інформаційного впливу та тривалого когнітивного виснаження особового складу командир дедалі більше виконує функцію оператора інформаційної та психологічної стійкості підрозділу.

Відповідно, підготовка командирів Сил ТрО повинна охоплювати не лише класичні питання бойового управління, а й питання когнітивної безпеки, кризової комунікації, інформаційної гігієни та роботи з цивільним середовищем, оскільки від рівня їх готовності залежатиме не лише ефективність функціонування підрозділів ТрО у воєнний час, а й здатність системи національного спротиву України зберігати стійкість у довгостроковій перспективі.

Фараджов М. М.
Національний університет оборони України

## ПРОБЛЕМИ ТА АСПЕКТИ ПІДГОТОВКИ ФАХІВЦІВ У СФЕРІ ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ

Психологічні операції (далі - ПсО) є одними з най недооціненим напрямком ведення війни. Війна за незалежність України продемонструвала всю необхідність в їх ефективному застосуванні. Як показує практика підрозділи ПсО зробили великий крок у своєму розвитку з 2014 по 2022 рік (під час війни ще більше). Але не зважаючи на плюси є і мінуси.

Так в даній тезі хочу коротко розказати тільки про основні але дуже важливі проблеми:

Невідповідність програми підготовки навчання. У зв'язку з високим темпом розвитку технологій, навчальні програми в ВНЗ та навчальних центрах не встигають за розвитком сучасного поля бою в різних доменах. Основними проблемами відставання від сучасних тенденцій є саме не пріоритетність для підрозділів проводити аналіз проведених дій, що в свою чергу не дає можливість навчальним центрам та ВНЗ робити зміни в програмі навчань. Програма підготовки має бути гнучкою та адаптованою до сучасних реалій. Зараз на базі деяких навчальних центрів існують курси на яких курсантів та вже діючих військовослужбовців, фахівців своєї справи можуть навчити та направити в правильному напрямку розвитку. Основною умовою є бажання вчитися та розвиватися у цьому напрямку;

Гнучкість. Сучасне законодавство не сприяє розвитку проведенню підготовки ПсО в тому вигляді в якому б воно мало бути в умовах сучасної війни. Однією з основних проблем є закупівля тренажерів, які в країнах ЄС та

США можуть рахуватися, як товари подвійного призначення що ускладнює нашій країні навіть при наявності необхідної кількості грошей цих тренажерів та програмного забезпечення. Враховуючі що це війна за незалежність законодавці разом з військово-політичним керівництвом країни мають усіляко сприяти розвитку підготовку фахівців даного напрямку;

Матеріальна складова. Підготовка фахівців з ПсО потребують великих матеріальних вкладень та часу. Необхідність в закупці таких базових речей, як: доступи до більш розвинутих програм ШІ, відео- та фото-редактори, платформи розвідки відкритих джерел (OSINT), дата-майнінгу, системи моніторингу медіа, аналізу наративів, кіберполігони та необхідне програмне забезпечення;

Відсутність розуміння загальновійськових командирів щодо форм, способів та методів застосування фахівців ПсО. Це часто призводить до їх використання не за їх основним напрямком діяльності, закриваючі цим прогалини в інших місцях.

Основними предметами навчання є: планування психологічних акцій та заходів, розробка матеріалів впливу, інформаційно-комп'ютерні технології. В сучасній системі підготовки ПсО існує:

Порядок оцінки цільової аудиторії;

Інформаційний простір. Аналіз пропаганди;

Аналіз навколишнього середовища за методикою ASCOPE/PMESII

Основні технічні засоби для виконання завдань (ЗС-88, LRAD, гучномовець, БПЛА, агітснаряд, ТІАВ);

Комунікація (вербальна, невербальна, міжкультурна);

Репрезентація та підготовка до спілкування;

Теорія поставлення запитань в ході бесіди;

Аналіз поведінки співрозмовника;

Методика спілкування (переговорів);

Сучасні психологічні операції досягли безпрецедентного рівня технологічної складності. Вони більше не є кустарним процесом написання пропагандистських листівок; це математично вивірені інженерні кампанії, які керуються штучним інтелектом, спираються на аналіз великих даних та оперують у когнітивних і кібернетичних вимірах одночасно.

Таким чином, для того, щоб успішно протидіяти противнику в умовах сучасної війни, базових програм та звичайних тренажерів для підготовки фахівців ПсО вже категорично недостатньо. Країна має радикально

трансформувати підхід до їх навчання: забезпечити гнучкість навчальних програм, надати політичну та законодавчу підтримку для закупівлі передових технологій та інвестувати у створення високотехнологічних тренувальних центрів, основою яких стануть штучний інтелект, аналіз великих даних та сучасні кіберполігони. Тільки такий підхід дозволить готувати фахівців, здатних оперувати на безпрецедентному рівні технологічної складності.

Міхєєв Ю. І., канд. техн. наук, ст. досл.
Національний університет оборони України
Павленко М. М.
Житомирський військовий інститут імені С. П. Корольова

## АВТОМАТИЗАЦІЯ ПРОЦЕСІВ ПРОТИДІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОМУ ВПЛИВУ НА БАЗІ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

В умовах сучасних конфліктів противник активно реалізовує масштабні інформаційні кампанії, що спрямовані на дестабілізацію морально-психологічного стану військовослужбовців Сил оборони України та цивільного населення. Така ситуація зумовлює нагальну потребу у розробленні та впровадженні новітніх, стійких механізмів захисту власного інформаційного простору.

Традиційний алгоритм протидії ворожим наративам охоплює низку етапів: від безперервного моніторингу медіапростору та аналізу цільових аудиторій до розробки і безпосереднього розповсюдження контрконтенту. Проте сьогоднішнє комунікаційне середовище відзначається експоненційним зростанням обсягів даних (Big Data), розмаїттям каналів передачі інформації та постійним вдосконаленням маніпулятивних методів противника. Зазначені фактори вимагають переходу від ручного управління до автоматизованих систем реагування.

Найбільш перспективним напрямом модернізації контрзаходів є комплексна інтеграція інформаційних технологій штучного інтелекту (ШІ) на всіх етапах інформаційної боротьби. Зокрема, обробка природної мови (NLP) та аналіз тональності (Sentiment Analysis) дають змогу адаптивно розпізнавати прихований емоційний тиск і виявляти маніпуляції чи фейки у великих масивах неструктурованого тексту. Алгоритми глибокого навчання (Deep Learning) здатні

забезпечити автоматичну багатовимірну класифікацію контенту за ознаками дезінформації або ворожої пропаганди, ідентифікуючи складні патерни впливу.

Окремим критично важливим елементом проактивного захисту є застосування систем виявлення аномалій (Anomaly Detection), що допомагає фіксувати нетипові сплески комунікативної активності та розпізнавати початок нових інформаційно-психологічних операцій на ранніх стадіях. Крім того, інструментарій аналізу соціальних графів (Network Analysis) слугує дієвим засобом для ідентифікації скоординованих бот-мереж та ключових вузлів поширення деструктивного контенту, що дає можливість їх своєчасно ізолювати.

З метою підвищення ефективності зворотного впливу, аналіз характеристик цільових аудиторій доцільно поєднувати з можливостями генеративних моделей ШІ для оперативного створення релевантних інформаційних матеріалів. Водночас, задля контролю якості та уникнення системних помилок, управління цими процесами має обов'язково базуватися на принципі «людина в контурі управління» (human-in-the-loop), де ШІ виконує функцію інтелектуальної системи підтримки прийняття рішень для оператора.

Комплексне застосування зазначених технологій дозволить здійснити перехід від фрагментарного моніторингу до функціонування цілісної, автоматизованої та проактивної системи виявлення інформаційно-психологічного впливу, що дозволить підвищити оперативність аналізу великих масивів даних та ефективність розгортання відповідних інформаційних контрзаходів.

Дзюбчук Р. В., канд. техн. наук, ст. наук. співроб.
Піонтківський П. М. канд. техн. наук, ст. наук. співроб.
Житомирський військовий інститут імені С. П. Корольова

## МЕТОД ПРОЄКТІВ ЯК ОСНОВА ПІДГОТОВКИ ФАХІВЦІВ У СФЕРІ ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ

Одним із основних завдань професійної діяльності фахівців у сфері психологічних операцій є створення високоякісного контенту, здатного вплинути на думки і свідомість як військовослужбовців противника, так і його цивільного населення. Досвід російсько-української війни показав достатньо високу дієвість російської пропаганди на власне населення та відносно високу

стійкість до психологічних операцій Сил оборони України.

За таких умов традиційні підходи до організації підготовки майбутніх офіцерів-фахівців психологічних операцій все частіше виявляються недостатньо ефективними. Фахівці за зазначеною спеціалізацією, що призначаються на відповідні первинні посади офіцерського складу у підрозділи психологічних операцій, повинні вміти ефективно діяти у нових або незнайомих середовищах за наявності неповної або обмеженої інформації, проводити дослідження, управляти робочими процесами, які є складними та непередбачуваними. Одним із шляхів набуття ними необхідних умінь та навичок є широке використання методу проєктів під час їхнього навчання у вищому військовому навчальному закладі.

Застосування методу проєктів у підготовці курсантів за напрямом інформаційно-психологічних операцій доцільно орієнтувати на виконання практично спрямованих завдань, пов'язаних із аналізом інформаційного середовища, плануванням інформаційного впливу, виявленням інформаційних загроз та розробленням заходів протидії деструктивним інформаційним кампаніям противника. У межах проєктної діяльності курсанти повинні працювати над моделюванням операцій, створенням сценаріїв інформаційного впливу, аналізом поведінки цільових аудиторій, а також оцінюванням ефективності застосованих комунікаційних засобів. Такий підхід забезпечує поєднання теоретичної підготовки з практичним опрацюванням реальних або наближених до реальних ситуацій сучасного інформаційного протиборства.

Реалізація методу проєктів передбачає самостійну або групову діяльність курсантів із поетапним аналізом поставленого завдання, збором та обробкою інформації, формуванням аналітичних висновків і представленням результатів роботи. Особливу увагу доцільно приділяти післяпроєктному аналізу, під час якого курсанти оцінюють ефективність власних рішень, виявляють помилки та визначають напрями вдосконалення інформаційно-аналітичної діяльності. Застосування такого підходу сприяє розвитку критичного мислення, навичок командної взаємодії, когнітивної стійкості та здатності приймати обґрунтовані рішення в умовах високої динаміки сучасного інформаційного середовища.

На думку провідних педагогів системи вищої військової освіти України, зокрема Вітченка А. О., Осьодла В. І. метод проєктів володіє значним розвивальним і виховним потенціалом для цілеспрямованого набуття

майбутніми військовими фахівцями як особистісно, так і професійно важливими якостями: аналітико-рефлексивними, проектувально-дослідницькими вміннями; самоосвітніми, управлінськими компетенціями; креативністю, імпровізацією; навичками співробітництва та роботи в команді тощо. Всі ці якості мають важливе значення для активізації навчально-пізнавальної діяльності курсантів (слухачів), які навчаються за напрямом психологічних операцій.

Таким чином, більш широке застосування методу проєктів під час підготовки фахівців психологічних операцій дозволить після випуску отримати фахівця, який вже має значний практичний досвід виконання спеціалізованих завдань, уміє працювати як в команді, так і самостійно, здатний критично оцінити результати як своєї власної роботи, так і своїх колег. В підсумку це сприятиме досягненню переваги над противником в умовах сучасного інформаційного суспільства.

Чумакевич В. О., канд. техн. наук, доц.
Бондаренко Ю. Л., канд. техн. наук
Іщенко І. А.
Житомирський військовий інститут імені С. П. Корольова

## ОСОБЛИВОСТІ ПІДГОТОВКИ ФАХІВЦІВ У СФЕРІ АНАЛІЗУ ТЕЛЕМЕТРИЧНИХ ДАНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Сучасний розвиток безпілотних авіаційних комплексів (БпАК) супроводжується постійним зростанням обсягів телеметричної інформації, що формується бортовими системами під час польоту. Дані телеметрії містять інформацію про режими роботи силової установки, параметри польоту, навігацію, стан бортових систем та керуючі сигнали автопілота. У сучасних умовах ефективне використання цієї інформації стає важливою складовою інформаційно-аналітичного забезпечення безпечної і ефективної експлуатації БпАК.

У зв’язку з цим особливої актуальності набуває питання підготовки фахівців, які здатні здійснювати аналіз телеметричних даних, виявляти ознаки нештатних режимів роботи та оцінювати ефективність функціонування безпілотних систем. При цьому підготовка повинна базуватись не лише на

теоретичному вивченні принципів роботи БпАК, а й на практичному аналізі реальних даних, отриманих у процесі експлуатації.

Однією з основних проблем підготовки фахівців у сфері інформаційних технологій є обмежене використання реальних телеметричних масивів під час навчання. У більшості випадків навчальний процес орієнтований на модельні або спрощені приклади, які не враховують характерних особливостей реальної експлуатації БпАК. Разом із тим реальні телеметричні дані характеризуються нерівномірною дискретизацією, наявністю шумів, пропусків значень, службових повідомлень та значною кількістю взаємопов'язаних параметрів, що суттєво ускладнює їх аналіз.

Важливим елементом підготовки є формування практичних навичок роботи з телеметричними файлами форматів MAVLink, TLOG та BIN, а також опанування методів попередньої обробки даних, фільтрації, часової синхронізації та аналізу режимів польоту. Використання реальних польотних даних дозволяє наблизити навчальний процес до умов практичної експлуатації та сформувати у фахівців навички інформаційно-аналітичної обробки даних БпАК.

Окремої уваги потребує підготовка фахівців до автоматизованого аналізу телеметрії із застосуванням сучасних інформаційних технологій. Зростання обсягів польотних даних ускладнює їх ручну обробку та потребує використання програмних засобів аналізу даних, елементів статистичної обробки та алгоритмів автоматизованого виявлення аномалій у роботі систем.

Таким чином, підготовка фахівців у сфері інформаційних технологій для експлуатації БпАК повинна враховувати реальні телеметричні дані, формування практичних навичок їх аналізу та розвиток інформаційно-інженерної складової підготовки. Це дозволить підвищити ефективність експлуатації безпілотних систем та якість прийняття рішень під час їх практичного застосування.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Нагорнюк А. В.
Житомирський військовий інститут імені С. П. Корольова

# ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРОТИДІЇ FPV-ДРОНАМ ШЛЯХОМ ЗАСТОСУВАННЯ АДАПТИВНОГО МОБІЛЬНОГО ЗАСОБУ РАДІОЕЛЕКТРОННОГО ПОДАВЛЕННЯ

Сучасний характер бойових дій в Україні характеризується стрімким розвитком і масовим застосуванням безпілотних літальних апаратів, серед яких особливе місце та ключове займають ударні дрони типу FPV (First Person View). Дані засоби ураження стали одним із ключових елементів ведення бойових дій на тактичному рівні завдяки своїй відносно низькій вартості, доступності компонентної бази, високій маневреності та можливості здійснювати точне наведення на ціль у режимі реального часу.

На відміну від класичних безпілотних систем, FPV-дрони керуються оператором безпосередньо через відеоканал, що забезпечує ефект «присутності» та дозволяє здійснювати високоточне наведення навіть у складних умовах місцевості.

Управління FPV-дронами здійснюється через радіоканали у визначених частотних діапазонах, найчастіше у межах 433 МГц 868–915 МГц, 2.4 ГГц та 5.8 ГГц.

У зв’язку з цим одним із найбільш перспективних напрямів протидії FPV-дронам є застосування мобільних пристроїв радіоелектронної боротьби, які здатні створювати радіоперешкоди та порушувати канали управління і передачі відеосигналу.

Важливою вимогою до таких систем є їх адаптивність. Це здатність до автоматичного визначати параметри сигналів противника, змінювати частотні діапазони роботи та ефективно формувати перешкоди та забезпечення своєчасного встановлення перешкоди в умовах змінної радіоелектронної обстановки. Адаптивність дозволяє значно підвищити ефективність радіоелектронного подавлення сигналів та зменшити енергоспоживання пристрою, що є критично важливим для мобільних систем.

Більшість сучасних засобів не мають адаптації, щодо створення радіоелектронних перешкод ворожим ударним дронам FPV. Саме із-за відсутності адаптації вони мають меншу ефективність роботи та час використання до повного розряду батареї.

Мною пропонується створення мобільного пристрою РЕБ для постановки адаптивних радіоперешкод ударним дронам типу FPV. Ідея роботи пристрою

полягає в тому, що він працюватиме постійно в режимі сканування (розвідки) радіочастотного спектру. При виявленні сигналу дрону він миттєво створює перешкоду на каналі управління дрону. Перешкода буде діяти по 10 секунд, після цього йде миттєве сканування спектру (дорозвідка). Якщо дорозвідка виявляє сигнал дрону то цикл миттєво повторюється і пристрій продовжує випромінювати перешкоду, а якщо сигнал відсутній він продовжує роботу в режимі сканування. Саме таким чином ми зможемо забезпечити адаптивність по часу, яка забезпечить максимально вчасну постановку радіоелектронної перешкоди. Також даний вид адаптивності забезпечить максимальний час роботи пристрою.

Даний пристрій зможе вирішити проблему адаптивності мобільних пристроїв РЕБ, та збільшити їх ефективність і час роботи.

Стрінада В. В., канд. техн. наук, доц.
Іщенко Д. А., канд. техн. наук, доц.
Житомирський військовий інститут імені С. П. Корольова

## РОЗВИТОК ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У КОНТЕКСТІ ЕВОЛЮЦІЇ БЕЗПІЛОТНИХ СИСТЕМ ЗА ДОСВІДОМ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Російсько-українська війна виступає каталізатором розвитку безпілотних систем (БпС) та інформаційних технологій (ІТ) військового призначення. У сучасних умовах бойові дії дедалі більше набувають ознак мережецентричної війни, у якій ключову роль відіграють швидкість збору, обробки, передачі та використання розвідувальної інформації. Саме ІТ визначають ефективність застосування безпілотних комплексів, роботизованих систем, систем зв'язку, розвідки та управління.

Досвід війни в Україні засвідчив, що БпС перетворилися з допоміжного засобу ведення бойових дій на один із головних інструментів досягнення оперативної та тактичної переваги. Їх розвиток став можливим завдяки інтеграції сучасних ІТ: штучного інтелекту, машинного навчання, супутникової навігації, цифрових систем зв'язку, хмарних платформ, автоматизованих систем управління та технологій аналізу великих масивів даних.

За таких умов актуальним є проведення дослідження щодо еволюції БпС та їх суттєвий вплив на розвиток ІТ за досвідом російсько-української війни.

До початку широкомасштабної війни БпС переважно використовувалися для ведення розвідки, коригування артилерійського вогню та спостереження. Однак бойові дії в Україні продемонстрували стрімке розширення функціональних можливостей безпілотних авіаційних комплексів (БпАК) та інших роботизованих платформ.

На початковому етапі війни основну роль відігравали тактичні розвідувальні безпілотники. Проте вже у 2022–2023 роках відбулося масове поширення FPV-дронів, ударних БпАК, баражуючих боєприпасів, морських безекіпажних платформ та наземних роботизованих систем. Це зумовило зміну підходів до управління військами, ведення розвідки та ураження противника.

Особливістю сучасного етапу бойових дій стало поєднання БпС із цифровими платформами управління боєм. Відтепер БпЛА функціонують не ізольовано, а як складові єдиної інформаційно-ударної системи, що забезпечує безперервний цикл: виявлення цілі; передачу даних; аналіз інформації; ухвалення рішення; вогневе ураження; оцінку результатів.

На основі аналізу досвіду війни в Україні визначені основні напрями подальшої еволюції ІТ у сфері БпС: автономізація безпілотних платформ; розвиток ройових технологій; інтеграція в єдині цифрові системи управління військами; підвищення стійкості до РЕБ; масове використання аналітики даних.

Важливим напрямом розвитку ІТ стало впровадження елементів штучного інтелекту в архітектуру БпС. Алгоритми машинного навчання застосовуються для: автоматичного розпізнавання цілей; класифікації озброєння та військової техніки противника; прогнозування маршрутів руху; автоматичного супроводження об’єктів; навігації в умовах радіоелектронної протидії. Особливого значення набувають технології автономного управління, які дозволяють безпілотним платформам виконувати бойові завдання навіть за умов втрати зв’язку з оператором.

Суттєвий вплив на розвиток БпС мають технології обробки великих масивів даних. У процесі бойових дій БпЛА генерують величезний обсяг відео-, фото- та телеметричної інформації.

Застосування хмарних платформ під час бойового застосування БпС дозволяє накопичувати інформацію з різних театрів бойових дій, здійснювати

оперативний аналіз розвідданих, формувати бази даних цілей, автоматизувати процес ухвалення рішень, забезпечувати взаємодію між підрозділами.

ІТ фактично формують нову архітектуру ведення сучасної війни, у якій перевага досягається не лише кількістю озброєння, а насамперед швидкістю інформаційного циклу.

Таким чином, досвід війни в Україні підтверджує формування нової моделі ведення бойових дій, у якій ІТ стають основою досягнення оперативної, тактичної та стратегічної переваги.

Стрімкий розвиток ІТ і масове застосування БпС у російсько-українській війні суттєво трансформують вимоги до професійної підготовки офіцерського складу. Сучасний офіцер повинен володіти не лише традиційними військово-професійними компетентностями, а й знаннями у сфері цифрових технологій, автоматизованих систем управління, аналізу даних та застосування роботизованих комплексів. Тому інтенсивне застосування БпС сформувало новий клас ІТ, ефективність яких визначається ґрунтовним розумінням фізичних процесів, що насамперед потребує перегляду програм підготовки військових фахівців.

Cherkes O. P.
Olshansky M. A.
Korolov Zhytomyr Military Institute

## TRAINING OF MILITARY SPECIALISTS IN CONFIGURATION MANAGEMENT OF INFORMATION AND COMMUNICATION SYSTEMS UNDER THE CONDITIONS OF INNOVATIVE TECHNOLOGY IMPLEMENTATION

Under the conditions of contemporary armed conflict, Information and Communication Systems (ICS) have become one of the key enablers of command and control, intelligence processing, decision-making support, and combat coordination. In order to ensure the rapid capability enhancement of the Armed Forces, a critical task is the integration of advanced ICS solutions into the modern command and control architecture. Of particular importance is the implementation of Fast-Track procedures for the operational acceptance of defence-oriented software products, enabling the reduction of procurement timelines and the prompt satisfaction of urgent Defence Forces' requirements for advanced technological solutions.

At the same time, the deliberate reduction of testing procedures, shortened verification timelines, and the deployment of ICS based on Commercial Off-The-Shelf (COTS) components optimize financial and temporal expenditures but simultaneously create critical dependencies on external vendors and reduce the overall security posture of the information infrastructure. Such an approach generates direct threats to information confidentiality and integrity, limits the possibility of conducting a comprehensive independent security audit of commercial software products due to proprietary architectures and closed-source code, and, in the long-term perspective, may lead to the loss of full governmental control over ICS administration mechanisms. Furthermore, under conditions of continuous software updates and integration of new functional modules, the risk of Software Drift emerges, defined as the unauthorized deviation of the actual ICS state from the approved Configuration Baseline. This process may result in the loss of interoperability between information systems, critical failures of cryptographic protection mechanisms, and significant complications in data exchange management between military units. Under such conditions, information protection cannot be ensured without the strict integration of configuration management procedures, change control processes, and conformity assessment mechanisms for comprehensive information security systems.

Therefore, within the framework of Master-level military education programs, the focus of professional training is shifting toward the development of competencies in ICS configuration management in accordance with NATO standards and the national regulatory framework. Such an approach enables future military officers to make informed managerial and technical decisions aimed at maintaining an optimal balance between the rapid implementation of innovations and the security and resilience of military information systems.

Within the academic discipline “Fundamentals of Innovative Activity in the Security and Defence Sector”, the training of Master’s degree students is implemented through the study of three interconnected methodological approaches aimed at ensuring the operational and technologically secure integration of innovations into the security and defence domain.

The study of the life-cycle management methodology for armament and military equipment enables ICS to be considered as an integrated organizational and technical system throughout all stages of its existence — from capability requirement formulation, development, and testing to deployment, operation, modernization, and

disposal. This approach teaches future specialists to systematically assess the long-term implications of accelerated Fast-Track decisions within defence acquisition and operational environments.

This methodology is organically integrated with the DOTMLPFI framework, which provides an understanding that the implementation of advanced ICS is not limited to the procurement of software and hardware solutions, but also requires comprehensive transformation in the areas of doctrine development, organizational structure optimization, personnel training, technical support organization, and operational documentation development.

Simultaneously, in order to prevent technological failures at the early stages of innovative defence system design, future defence managers study the methodologies of Technology Readiness Level assessment, Technology Readiness Assessment, and identification of Critical Technology Elements. These approaches provide a clear understanding of how deficiencies in ICS architecture development or improperly formulated technical requirements may subsequently have a destructive impact on cyber resilience, interoperability, and operational reliability of the entire system.

Consequently, the training of Master's degree students within this academic discipline ensures a comprehensive understanding of the causal relationships between technical decisions, organizational procedures, security risks, and cybersecurity requirements throughout all stages of ICS operation under combat conditions.

Кригін О. О.
Житомирський військовий інститут імені С. П. Корольова

## ІДЕНТИФІКАЦІЯ РАДІОЕЛЕКТРОННИХ ЗАСОБІВ ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Сучасні воєнні конфлікти демонструють стрімку цифровізацію поля бою, де ключовим джерелом та споживачем інформації є безпілотні літальні апарати (БпЛА). У контексті інформаційної безпеки (ІБ), БпЛА є мобільними кіберфізичними системами, які здійснюють збір, обробку та передачу критично важливих даних. Своєчасне виявлення, розпізнавання та нейтралізація цих апаратів безпосередньо впливають на захищеність інформаційного простору

військ. Відтак, дослідження методів ідентифікації радіоелектронних засобів (РЕЗ) БпЛА стає однією з найактуальніших проблем сучасної ІБ.

Противник постійно вдосконалює технічні характеристики БпЛА (таких як «Орлан», «Lancet/ZALA», «Гранат», «Shahed», «Supercam»), створюючи нові загрози для цілісності та доступності даних радіотехнічної розвідки. Основними проблемами ідентифікації та протидії у сфері ІБ є:

Здатність БпЛА оперативно змінювати робочу частоту (псевдовипадкова перебудова робочої частоти — ППРЧ) та протоколи передачі даних (модифікація типу модуляції). Це унеможливлює класичний аналіз спектра та вимагає адаптивних алгоритмів розпізнавання образів сигналів.

Інформаційна комбінація та ретрансляція: Використання тактичних зв'язок (наприклад, розвідувальний ZALA як ретранслятор для ударного Lancet) утворює складні розподілені інформаційні мережі, які потребують комплексного потокового аналізу для виявлення керуючих вузлів.

Режим «радіомовчання» та автономність: Застосування інерційних навігаційних систем (INS) дозволяє БпЛА виконувати завдання без випромінювання радіосигналів. З погляду ІБ це створює проблему «інформаційної сліпоти» для стандартних засобів радіотехнічної розвідки, залишаючи кінетичне ураження єдиним виходом.

Для забезпечення ефективного захисту інформаційного периметра від загроз БпЛА недостатньо лише енергетичного придушення (РЕБ), оскільки фіксовані завади неефективні проти адаптивних сигналів. Необхідно задіяти щонайменше три різнодіапазонні комплекси та впроваджувати інтелектуальний підхід.

Успішна протидія вимагає чіткої ідентифікації інформаційних характеристик БпЛА: типу апарата, специфіки його сигнатур та протоколів логічного керування. Це дозволить здійснювати не просто засліплення каналів зв'язку, а цілеспрямоване інформаційне та протокольне блокування (кібер-РЕБ).

Осадчук М. В.
Житомирський військовий інститут імені С. П. Корольова

# ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

Стрімкий розвиток інформаційних технологій та зростання рівня цифровізації суспільства супроводжуються збільшенням кількості кіберзагроз, спрямованих на інформаційні системи державних установ, військових об'єктів, підприємств критичної інфраструктури та приватних користувачів. Традиційні методи виявлення атак, що базуються на сигнатурному аналізі та попередньо визначених правилах, не завжди здатні ефективно протидіяти сучасним кіберзагрозам, особливо атакам нульового дня та складним багатоетапним вторгненням. У зв'язку з цим актуальним напрямом розвитку систем кібербезпеки є впровадження технологій штучного інтелекту.

Штучний інтелект являє собою сукупність методів і алгоритмів, здатних виконувати аналіз великих обсягів даних, виявляти приховані закономірності та приймати рішення на основі накопиченого досвіду. У сфері кібербезпеки найбільшого поширення набули технології машинного навчання та глибокого навчання, які дозволяють автоматизувати процес аналізу мережевого трафіку, журналів подій та поведінки користувачів.

Однією з головних переваг використання штучного інтелекту є можливість виявлення аномалій у роботі інформаційних систем. На відміну від традиційних засобів захисту, інтелектуальні системи здатні формувати модель нормального функціонування мережі та виявляти відхилення від неї. Це дозволяє своєчасно виявляти спроби несанкціонованого доступу, шкідливу активність, розповсюдження шкідливого програмного забезпечення та інші прояви кіберзагроз.

Сучасні системи виявлення кіберзагроз на основі штучного інтелекту можуть аналізувати мережевий трафік у режимі реального часу, визначати підозрілі дії користувачів та автоматично класифікувати потенційні інциденти безпеки. Завдяки цьому суттєво скорочується навантаження на фахівців з кібербезпеки та підвищується швидкість реагування на загрози. Особливе значення такі технології мають для захисту великих корпоративних мереж та об'єктів критичної інфраструктури, де обсяги даних перевищують можливості їх ручного аналізу.

Разом із перевагами використання штучного інтелекту супроводжується низкою викликів. Ефективність роботи моделей машинного навчання значною мірою залежить від якості навчальних даних. Недостатня репрезентативність вибірки або навмисне спотворення даних можуть призвести до помилок класифікації та зниження ефективності системи. Крім того, кіберзлочинці також починають застосовувати технології штучного інтелекту для створення більш складних та адаптивних атак, що вимагає постійного вдосконалення засобів захисту.

Таким чином, використання штучного інтелекту є одним із найбільш перспективних напрямів розвитку сучасних систем виявлення кіберзагроз. Застосування алгоритмів машинного навчання дозволяє підвищити ефективність виявлення атак, скоротити час реагування на інциденти та забезпечити більш високий рівень захисту інформаційних ресурсів. Подальший розвиток даного напряму пов’язаний із підвищенням точності моделей, удосконаленням методів аналізу великих даних та створенням комплексних інтелектуальних систем кіберзахисту.

Панченко В. М.
Житомирський військовий інститут імені С. П. Корольова

## ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У ВІЙСЬКОВИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Стрімкий розвиток інформаційних технологій та цифровізація процесів управління військами призвели до суттєвого зростання ролі військових інформаційних систем у забезпеченні обороноздатності держави. Сучасні автоматизовані системи управління, засоби зв’язку та інформаційно-телекомунікаційні мережі забезпечують збір, обробку, передачу та зберігання значних обсягів даних, від своєчасності та достовірності яких залежить ефективність прийняття рішень на всіх рівнях військового управління. Одночасно з цим збільшується кількість та складність кіберзагроз, спрямованих на порушення функціонування інформаційних ресурсів, несанкціонований доступ до даних та дестабілізацію процесів управління військами.

Досвід сучасних збройних конфліктів свідчить про те, що кіберпростір став одним із ключових середовищ протиборства. Кібератаки все частіше

використовуються як складова комплексних операцій для отримання розвідувальної інформації, порушення роботи критично важливих систем та створення переваги над противником. Особливої актуальності набуває завдання своєчасного виявлення кіберзагроз, оскільки традиційні методи аналізу мережевого трафіку та моніторингу подій інформаційної безпеки не завжди здатні ефективно протидіяти сучасним складним і прихованим атакам.

Одним із перспективних напрямів підвищення ефективності кіберзахисту є використання технологій штучного інтелекту. Застосування алгоритмів машинного навчання дозволяє автоматизувати процес аналізу великих обсягів даних та виявляти приховані закономірності, які можуть свідчити про наявність кіберінцидентів. На відміну від традиційних сигнатурних методів, системи на основі штучного інтелекту здатні виявляти раніше невідомі загрози та адаптуватися до змін у характері дій порушника.

Перспективним підходом є використання алгоритмів класифікації та виявлення аномалій для аналізу мережевого трафіку військових інформаційних систем. У процесі функціонування такі системи формують модель нормальної поведінки мережі, після чого автоматично визначають відхилення від встановлених параметрів. Це дозволяє своєчасно виявляти ознаки несанкціонованого доступу, шкідливого програмного забезпечення, спроби витоку інформації або проведення мережевих атак.

Важливою перевагою технологій штучного інтелекту є можливість їх інтеграції з існуючими засобами моніторингу інформаційної безпеки. Завдяки автоматизованому аналізу подій скорочується навантаження на операторів центрів кібербезпеки та підвищується оперативність реагування на потенційні загрози. Крім того, використання адаптивних алгоритмів дозволяє підвищити точність виявлення атак та зменшити кількість хибних спрацювань, що є одним із важливих показників ефективності сучасних систем кіберзахисту.

Таким чином, використання технологій штучного інтелекту відкриває нові можливості для підвищення рівня захищеності військових інформаційних систем. Їх впровадження сприятиме своєчасному виявленню кіберзагроз, підвищенню стійкості інформаційної інфраструктури та забезпеченню безперервності процесів управління військами в умовах зростання кібернетичних загроз.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Чігінцев І. О.
Житомирський військовий інститут імені С. П. Корольова

# АКТУАЛЬНІ АСПЕКТИ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ ДЛЯ ПОТРЕБ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ УКРАЇНИ

У сучасних умовах гібридної війни кіберпростір набуває статусу окремого театру протистояння, де інформаційні атаки, кібершпигунство та деструктивні впливи становлять реальну загрозу національній безпеці. Сектор безпеки та оборони України стикається з постійно зростаючим рівнем складності кіберзагроз, що вимагає наявності висококваліфікованих фахівців з кібербезпеки, здатних діяти в умовах невизначеності та обмеженого часу на прийняття рішень.

Метою даного дослідження є аналіз актуальних аспектів підготовки фахівців з кібербезпеки та визначення ключових напрямів удосконалення освітнього процесу для потреб оборонного сектору.

Однією з основних проблем підготовки є розрив між теоретичною базою знань та практичними навичками, необхідними для роботи в реальних умовах кіберзагроз. Традиційні освітні програми часто не враховують швидку еволюцію методів атак, що використовуються в кіберпросторі, зокрема цільових атак, соціальної інженерії та атак на критичну інфраструктуру.

Важливим аспектом є впровадження практико-орієнтованого навчання, яке включає використання кіберполігонів, симуляцій реальних атак та відпрацювання сценаріїв реагування на інциденти інформаційної безпеки. Це дозволяє формувати у здобувачів освіти навички швидкого аналізу загроз та прийняття рішень у стресових умовах.

Окрему увагу слід приділяти міждисциплінарній підготовці, що поєднує знання з інформаційних технологій, криптографії, мережевої безпеки та основ оперативної діяльності. Для сектору безпеки та оборони особливо важливою є здатність фахівців працювати з критичною інформаційною інфраструктурою та забезпечувати її стійкість до кібератак.

Таким чином, підготовка фахівців з кібербезпеки для сектору безпеки та оборони України має базуватися на поєднанні теоретичної підготовки, практичних навичок та моделювання реальних загроз. Це дозволить сформувати кадровий потенціал, здатний ефективно протидіяти сучасним кіберзагрозам та забезпечувати кіберстійкість держави.

Янюк Д. В.
Житомирський військовий інститут імені С. П. Корольова

# ФОРМУВАННЯ НАВИЧОК ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ У МАЙБУТНІХ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасний інформаційний простір характеризується стрімким поширенням інформаційних технологій та зростанням кількості інформаційних загроз. Однією з найбільш небезпечних загроз є дезінформація, яка використовується для маніпулювання громадською думкою, дестабілізації суспільно-політичної ситуації та впливу на процеси прийняття рішень. Особливо актуальною ця проблема є в умовах гібридних конфліктів, де інформаційний вплив виступає одним із ключових інструментів досягнення стратегічних цілей.

У зв'язку з цим важливого значення набуває підготовка майбутніх фахівців з інформаційної безпеки, здатних ефективно виявляти, аналізувати та нейтралізовувати дезінформаційні кампанії. Формування відповідних навичок повинно здійснюватися комплексно та охоплювати як теоретичну, так і практичну складову навчання.

Одним із ключових напрямів підготовки є розвиток критичного мислення, що дозволяє оцінювати достовірність інформації, визначати джерела її походження та виявляти ознаки маніпулятивного впливу. Майбутні фахівці повинні володіти методами фактчекінгу, аналізу медіаконтенту та оцінювання інформаційних ризиків. Особливої уваги потребує вивчення сучасних технологій створення дезінформації, зокрема використання штучного інтелекту для генерації фальшивих текстових, аудіо- та відеоматеріалів.

Важливою складовою професійної підготовки є практичне відпрацювання навичок виявлення інформаційних операцій у кіберпросторі. Для цього доцільно використовувати навчальні кейси, симуляційні моделі та спеціалізовані програмні засоби аналізу інформаційних потоків. Такий підхід сприяє формуванню у здобувачів освіти здатності оперативно реагувати на інформаційні загрози та приймати обґрунтовані рішення в умовах невизначеності.

Таким чином, формування навичок протидії дезінформації є важливою складовою професійної підготовки майбутніх фахівців з інформаційної безпеки. Ефективне поєднання теоретичних знань, практичної підготовки та сучасних інформаційних технологій дозволить підвищити готовність спеціалістів до протидії актуальним інформаційним загрозам і забезпечення інформаційної безпеки держави.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Староконь Є. Г., канд. психол. наук
Дедерко К. Е.
Житомирський військовий інститут імені С. П. Корольова

# ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА БЕЗПЕКА ОСОБИСТОСТІ ЯК ОБОВ'ЯЗКОВА ОСВІТНЯ КОМПОНЕНТА В ПРОФЕСІЙНІЙ ПІДГОТОВЦІ ВІЙСЬКОВИХ ЛІДЕРІВ

Було б дивним, якби після декількох повторів слово «цукор» ми відчули в роті солодкий смак. Однак, закликаючи розвивати критичне мислення, наголошуючи на його актуальності і важливості, ми продовжуємо тішити себе ілюзією, що розрізнені і різнопланові навчальні заходи приведуть до необхідного рівня володіння нашими випускниками інформаційними технологіями із захисту своєї психіки від негативного та деструктивного впливу інформації.

Сьогодні важливо зрозуміти, що формування інформаційно-психологічної безпеки особистості - це саме конкретний і цілеспрямований процес розвитку необхідних якостей людини: здатності критично сприймати інформацію, розпізнавати маніпуляції, зберігати емоційну стійкість і на цій основі ефективно діяти в умовах інформаційного впливу.

В умовах відбиття повномасштабної агресії російської федерації інформаційно-психологічна безпека стала одним із ключових чинників національної стійкості України. Ми є свідками, що за рахунок інформаційних процесів роздільна межа між війною і миром фактично зникла. Україна з моменту набуття незалежності постійно знаходиться в епіцентрі інформаційної війни з боку російської федерації. Бачимо, що сучасна війна ведеться не лише на полі бою, а й в інформаційному просторі, де росіяни активно використовують інформаційно-психологічні операції для впливу на свідомість військовослужбовців, населення нашої країни та міжнародну спільноту.

Для того, щоб процес формування інформаційно-психологічної безпеки у командирів-лідерів був результативним, необхідно зробити його цілеспрямованим, системним і систематичним, спираючись на закономірності функціонування інформаційної системи людини. Орієнтовний зміст майбутньої освітньої компоненти «Інформаційно-психологічна безпека особистості» може бути таким.

Тема 1. Людина як інформаційна система.

Тема 2. Свідомість людини як інформаційна мішень.

Тема 3. Базові напрямки створення інформаційно-психологічного впливу у воєнних цілях. Мішені та точки уразливості свідомості.

Тема 4. Комунікації в структурі інформаційного суспільства та їх застосування у воєнних цілях російською федерацією.

Тема 5. Комунікативна складова інформаційної війни російської федерації та її характеристика.

Тема 6. Маніпуляція російською федерацією індивідуальною та масовою свідомістю.

Тема 7. Вербальні засоби впливу на свідомість цільової аудиторії.

Тема 8. Технології організації російською федерацією інформаційно-психологічного впливу для зміни картини світу цільових аудиторій.

Тема 9. Механізми формування передумов для спрямованих соціальних вибухів та ситуацій "керованого хаосу".

Тема 10. Особливості застосування росіянами мережі Інтернет для передачі деструктивного контенту

Тема 14. Особливості пропаганди російської федерації в ході російсько-Української війни.

Тема 15. Прийоми роботи з інформацією для захисту психіки від негативного інформаційного впливу.

Знання та розуміння технологій та технік інформаційно-психологічного впливу на свідомість людини якраз і стане тим наріжним каменем, що дасть можливість і командиру-лідеру, і кожному військовослужбовцю забезпечити свою інформаційно-психологічну безпеку та безпеку підрозділу.

Тому, впровадження в освітній процес підготовки лідерів майбутньої Української Армії освітньої компоненти «Інформаційно-психологічна безпека особистості» - це негайна і сувора необхідність для зміцнення національної стійкості України сьогодні.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Залевський В. Й.
Житомирський військовий інститут імені С. П. Корольова

# НЕОБХІДНІСТЬ СТВОРЕННЯ АВТОМАТИЗОВАНИХ МОДЕЛЕЙ ВЕРИФІКАЦІЇ ІНФОРМАЦІЇ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИСТОСТІ ТА СУСПІЛЬСТВА

В епоху тотальної цифровізації смартфон перестав бути просто засобом зв'язку — він став основним каналом доступу до свідомості. Месенджери (Telegram, WhatsApp, Signal, Viber), завдяки своїй архітектурі та особливостям споживання контенту, створили ідеальне середовище для проведення інформаційно-психологічних операцій (ІПсО) на мікрорівні.

З огляду на швидкість поширення фейків, ручний фактчекінг програє інформаційним атакам: поки експерти-аналітики спростовують один наратив, він встигає охопити мільйони користувачів. Саме тому безпека суспільства сьогодні залежить від створення автоматизованих моделей верифікації на базі штучного інтелекту (ШІ) та обробки природної мови (Natural Language Processing –NLP).

Сучасна архітектура систем перевірки інформації зазвичай працює на трьох рівнях:

лінгвістичний – перевіряється емоційне забарвлення, токсичність тощо;

мережевий (графовий) – перевіряється швидкість поширення, джерела-патерни, зв'язки між каналами;

фактологічний – аналізуються співставлення тверджень у тексті з перевіреними базами даних та офіційними джерелами.

NLP в умовах війни перетворилася з суто академічної та комерційної технології на потужний інструмент розвідки, інформаційної безпеки та автоматизації управління.

Українське NLP сьогодні швидко розвивається, і його архітектура та застосування мають чітко виражений оборонний характер. Агресор генерує колосальні обсяги інформаційного шуму — як у радіоефірі, так і в кіберпросторі. Людина фізично не здатна обробити такі масиви даних. Саме тут NLP стає критичною перевагою.

Розпізнавання лінгвістичних аномалій (контрзаходи ІПсО) де російські ботоферми масово генерують контент українською мовою за допомогою

автоперекладачів. NLP-моделі натреновані виявляти структурні калькування та семантичні помилки, невидимі на перший погляд.

Автоматизація OSINT та розвідки відкритих джерел здійснюються за рахунок навчених NLP-моделей які безупинно «парсять» тисячі ворожих каналів, форумів та місцевих пабліків. Алгоритми проводять аналіз тональності, виявляючи панічні настрої після ударів, а також ідентифікація об'єктної сутності — автоматично витягують з тексту назви населених пунктів, номери військових частин, імена командирів та прив'язують їх до географічних координат.

Обробка радіоперехоплень (SIGINT/COMINT) здійснюється розпізнаванням мовлення на NLP. Програма автоматично переводить російські розмови в текст, фільтрує нецензурну лексику та шум, і миттєво підсвічує ключові слова: позивні, назви техніки, частоти, накази про переміщення.

Інтеграція з системами ситуаційної обізнаності дозволяє надавати звіти, повідомлення в месенджерах та доповіді у неструктурованому текстовому вигляді. Алгоритми NLP здатні виділити з хаотичного текстового повідомлення тип виявленої цілі (наприклад, БпЛА, комплекс РЕБ або ППО, влучання), її координати та час, і автоматично нанести цей маркер на цифрову мапу бою, пришвидшуючи процес прийняття рішень.

Сьогодні інформаційний простір у персональних терміналах є повноцінним доменом збройної боротьби. Сучасні ІПсО адаптовані до паттернів споживання новин, експлуатуючи когнітивні вразливості (втому, тривожність) для дестабілізації суспільства. Оскільки алгоритми ШІ схильні до «галюцинацій», а тактика зловмисників постійно еволюціонує, найбільш ефективною парадигмою інформаційної безпеки є синергія машинного аналізу (здатний фільтрувати до 90% інформаційного «шуму») та фінальної експертної верифікації людиною.

Отже, ефективність вітчизняних NLP-рішень полягає у здатності швидко трансформувати масиви неструктурованих ворожих комунікацій у формалізовані розвідувальні дані, що мінімізує вплив людського фактору, оптимізує час реакції та забезпечує інформаційну перевагу.

*Житомирський військовий інститут імені С. П. Корольова*
*11 червня 2026 року*

Даник Ю. Г., д-р техн. наук, проф.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Шестаков В. І., д-р техн. наук, доц.
Ширшов Р. А.
Національна академія Служби безпеки України

# МЕТОДИКА ОЦІНЮВАННЯ ВИНИКНЕННЯ, РОЗМНОЖЕННЯ ТА ПОШИРЕННЯ ПОМИЛОК У СИСТЕМАХ ШТУЧНОГО ІНТЕЛЕКТУ У ХОДІ OSINT

Сучасна розвідка на основі відкритих джерел (Open Source Intelligence, OSINT) дедалі більше спирається на технології штучного інтелекту (ШІ). Системи на основі великих мовних моделей та інших архітектур машинного навчання застосовуються на всіх етапах OSINT-циклу: для збирання й попереднього оброблення великих масивів відкритих даних, автоматизованого вилучення сутностей (осіб, організацій, локацій) та зв’язків між ними, реверсивного пошуку зображень, геопросторового аналізу, аналізу соціальних мереж, побудови профілів і складання аналітичних висновків. Інтеграція ШІ суттєво підвищує продуктивність аналітика, скорочує час оброблення інформації та дає змогу опрацьовувати обсяги даних, недосяжні для ручного аналізу. Водночас залучення ШІ привносить у процес OSINT нові, раніше відсутні джерела ризиків, пов’язані з надійністю самих інтелектуальних систем.

На відміну від поширеного уявлення про ШІ як про об’єктивний інструмент, сучасні дослідження свідчать, що помилки є невід’ємною властивістю самої природи навчання моделей ШІ, а не лише наслідком технічних дефектів чи неякісних даних.

Попри ґрунтовну формалізацію механізмів виникнення, накопичення та масштабування помилок ШІ загалом, питання їх конкретного впливу на результати OSINT-досліджень залишається недостатньо вивченим. Бракує як математичного опису трансформації помилок ШІ у похибки аналітичних висновків OSINT, так і кількісного оцінювання цього впливу та обґрунтованих рекомендацій щодо його мінімізації.

Метою доповіді є доведення до наукової спільноти результатів дослідження впливу систематичного зміщення в навчальних даних, помилки

генерації (галюцинації), та помилки втрати контексту на результати OSINT та розроблення рекомендацій щодо його мінімізації.

У ході дослідження: здійснено математичний опис зазначених помилок; розглянуто стійкі причинно-наслідкові та статистичні зв'язки; формалізовані ланцюги помилок «навчальні дані → галюцинація», «навчальні дані → втрата контексту» та «втрата контексту → галюцинація». Доведено, що помилки здатні накопичуватися, відтворюватися та масштабуватися: за довгих ланцюгів міркувань і слабкої зовнішньої верифікації їх вплив зростає надекспоненційно, а в системах із самонавчанням можливе «розмноження» помилок за вірусним сценарієм, сумарна помилка не є простою сумою складових.

У доповіді розкриваються способи та алгоритми оцінювання швидкості накопичення та розмноження помилок в ШІ-системах, сформульовані практичні рекомендації, щодо виявлення, контролю та мінімізації впливу помилок на результат OSINT.

Запропоновані алгоритми та методика дають змогу формально оцінювати надійність застосування інструментів ШІ в OSINT, виявляти «точки розриву» аналітичних ланцюгів і завчасно нейтралізувати негативні впливи помилок ШІ.

**ЗМІСТ**

**Н А У К О В Е  В И Д А Н Н Я**

МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

# “ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНІ ТА ПСИХОЛОГІЧНІ ОПЕРАЦІЇ В УМОВАХ ПОВНОМАСШТАБНОЇ ЗБРОЙНОЇ АГРЕСІЇ рф ПРОТИ УКРАЇНИ”

**Тези доповідей**

Видавничий оригінал виготовлений
у науково-організаційному відділі ЖВІ

Відповідальний за випуск
**Федорчук Дмитро Леонідович**

Комп’ютерна верстка та макетування – **І. В. Голуб**
Дизайн і макет обкладинки – **О. Ю. Тофанчук**

Свідоцтво про реєстрацію серія ДК № 7355 від 9 червня 2021 року
Підписано до друку 03.06.2026. Формат 60 × 84 / 16
Ум. друк. арк. 14,2. Зам. 409 опер.

Друкарня ЖВІ

Просп. Миру, 22, м. Житомир, 10004