

**Кудрявський Іван Володимирович**  
*кандидат політичних наук, докторант,*  
*Приватне акціонерне товариство «Вищий навчальний заклад*  
*«Міжрегіональна Академія управління персоналом»*

DOI: <https://doi.org/10.36059/978-966-397-579-5-43>

## **АЛГОРИТМ ПІДТРИМКИ УПРАВЛІНСЬКИХ РІШЕНЬ У ДЕРЖАВНОМУ УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ**

Застосування багатофакторного аналізу для оптимізації систем, діяльність яких стосується безпеки, розглядалося дослідниками і раніше, зокрема у контексті кібербезпеки як складової інформаційної безпеки. Висока складність та масштабованість архітектури сучасних розподілених систем, різноманітність обладнання та інфраструктури, а також постійні зміни конфігурації та масштабування середовища породжують ряд проблем, пов'язаних зі збором та аналізом інформації для оцінки ризиків, необхідністю оперативної обробки великих масивів складних за структурою та гетерогенних за природою даних, що надходять із диференційованих систем безпеки та моніторингу, журналів подій, аудиторських звітів та інших джерел, а також відсутністю єдиного формату їх представлення [1]. Ця проблематика характерна і при формуванні підходів до реагування на інформаційні загрози, зокрема спрямований деструктивний інформаційно-психологічний вплив противника, не кажучи вже про становлення системи проактивної комунікації з урахування щонайменше короткострокового прогнозування сценаріїв розвитку ситуації.

Проблематика аналізу та оцінки інформації, поширеної у відкритому інформаційному просторі, характерна не лише для України, але навіть для провідних держав та армій, які стикаються з інтенсивним деструктивним інформаційно-психологічним впливом

у сучасних умовах. Так, американські дослідники говорять про відсутність в армії США інституціоналізованої програми розвитку освіти, призначеної для військовослужбовців, які навчаються виявляти, ретельно перевіряти та аналізувати шкідливу інформацію (тобто – дезінформацію, пропаганду тощо) у відкритому інформаційному середовищі [2]. Очевидна необхідність у формуванні такої програми та її ефективному застосуванні в умовах сучасної інформаційної та когнітивної війни, зокрема для забезпечення когнітивної переваги.

Тільки громадська організація «Детектор медіа», яка у режимі реального часу збирає та документує хроніки Кремлівської пропаганди навколо військового наступу на Україну, станом на 05 квітня 2025 року, 1136-й день широкомасштабного вторгнення, зафіксувала 2733 фейки, 817 маніпуляцій, 774 меседжі російської пропаганди та здійснила 559 викриттів [3]. Центр протидії дезінформації при Раді Національної безпеки і оборони України лише за один тиждень з 24.03.2025 р. по 30.03.2025 р., проаналізувавши 14 060 000 меседжів, виявив 20 472 інформаційні загрози [4]. База даних Оперативної групи Європейського союзу зі стратегічних комунікацій, яка є частиною дипломатичної служби ЄС, очолюваної Верховним представником ЄС, станом на 05 квітня 2025 року налічує 18 759 випадків поширення спрямованої дезінформації [5]. Наведені цифри характеризують здебільшого виявлені факти поширення дезінформації з метою реалізації деструктивного інформаційно-психологічного впливу, пов'язані з російською інформаційною агресією, яка ведеться не лише проти України, але й проти європейських країн та інших країн світу. Для хоча б приблизного розуміння масштабів інформаційної війни та власне когнітивної війни, яку розв'язав і веде наш ворог, необхідно враховувати, що до цих цифр входять лише опрацьовані, перевірені, доказані та описані випадки, причому, за кожним з них стоять різні версії інформаційного контенту, різні форми його подачі, не кажучи вже про десятки, сотні, а часто і тисячі каналів поширення такої інформації. Тобто, лише наведені цифри, якщо спробувати перевести

їх в кількість інформаційних повідомлень, які бачить суб'єкт моніторингу інформаційного простору, необхідно збільшувати в рази. І це без урахування інформаційних дій деструктивного характеру, які не були зафіксовані відповідними профільними організаціями і, відповідно, не увійшли в наведену статистику.

Якщо ж врахувати, що російська інформаційна агресія як супровід російської збройної широкомасштабної агресії є безумовно основною, але точно не єдиною проблемою захисту безпеки інформаційного простору України і в сучасних умовах, і щонайменше – у найближчому майбутньому, стає абсолютно зрозумілою неможливість навіть відстеження, не кажучи вже про адекватну оцінку і професійне реагування на повідомлення, які можуть становити реальну або потенційну інформаційну загрозу, без належної систематизації цієї роботи. За таких масштабів аналітичної діяльності, що вимагає величезної кількості достатньо складних та обґрунтованих рішень, жоден кадровий ресурс, фінансовий ресурс, і навіть ресурс спеціального програмно-технічного забезпечення, не дозволить ефективно виконувати завдання щодо управління у сфері захисту безпеки інформаційного простору без ефективного і водночас простого алгоритму, що дозволить прискорити прийняття рішень без збільшення різноманітних ресурсів та оцінити ефективність рішень у ретроспективі для формування порядку пріоритетності у виборі сценаріїв майбутніх дій.

Указ Президента України «Про стратегію інформаційної безпеки» покладає моніторинг інформаційного простору, прогнозування та виявлення інформаційних загроз національній безпеці держави у воєнній сфері на Міністерство оборони України, а також сили оборони в межах їх компетенції [6]. Стаття 45 Стратегії національної безпеки України першим серед пріоритетних завдань правоохоронних, спеціальних, розвідувальних та інших державних органів, відповідно до їх компетенції, визначає активну та ефективну протидію розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам, російській та іншій підривній пропаганді [7]. Однак, зі зрозумілих причин, жоден зі

згаданих документів не описує та не визначає конкретних механізмів моніторингу й аналізу інформаційного простору, і тим більше – як повинна здійснюватися протидія російській та іншій «підривній пропаганді».

Доктрини зі стратегічних комунікацій Збройних Сил України та Національної гвардії України можуть розглядатися як цікавий, хоча і не зовсім вдалий приклад впровадження стандартів НАТО на рівні національних підзаконних актів у сфері стратегічних комунікацій та власне державного управління процесами захисту безпеки інформаційного простору. Попри те, що ці документи більш наближені до визначення порядку дій безпосередніх виконавців, аніж загальнодержавні стратегії, – вони теж не дають відповідей на запитання, яким чином має здійснюватися моніторинг інформаційного простору і реагування на інформаційні загрози чи недопущення виникнення інформаційних загроз [8; 9]. Чи не єдине суттєве досягнення документів – декларація необхідності проективної ініціативної позиції персоналу, який бере участь у процесах державного управління захистом безпеки інформаційного простору, та відхід від концепцій реагування за фактом, що в принципі виключає здобуття когнітивної переваги.

### Література:

1. Палко Д., Мирутенко Л. Метод комплексної оцінки ризиків кібербезпеки в розподілених інформаційних системах. *Кібербезпека: освіта, наука, техніка*. 2024. № 2. С. DOI: <https://doi.org/10.28925/2663-4023.2024.26.731> (дата звернення 05.04.2025).

2. Вайтсайд, Ремінгтон Д. Розгляд основ засобів масової інформації, інформації та даних армії США проти шкідливої інформації у відкритому інформаційному середовищі: якісне прикладне дослідження. Рукопис дисертації, поданий до Національного університету Санфордського педагогічного коледжу на здобуття наукового ступеня доктора педагогічних наук. Національний університет ProQuest. Дисертації та тези, 2024. URL: <https://www.proquest.com/openview/4bad2c7f9236292c9bcb14389acde41f/1?cbl=18750&diss=y&pq-origsite=gscholar> (дата звернення 05.04.2025).

3. Будь на сторожі якісної інформації – ставай частиною спільноти «Детектор медіа». URL: <https://disinfo.detector.media>. (дата звернення 05.04.2025).

4. Центр протидії дезінформації. URL: <https://cpd.gov.ua>. (дата звернення 05.04.2025).

5. База даних. URL: <https://euvsdisinfo.eu/disinformation-cases/>. (дата звернення 05.04.2025).

6. Про Стратегію інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021 / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/685/2021/print> (дата звернення – 05.04.2025).

7. Про Стратегію національної безпеки України: Указ президента України від 14 вересня 2020 р. № 392/220 / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text> (дата звернення – 05.04.2025).

8. Доктрина зі стратегічних комунікацій Збройних Сил України: наказ Головнокомандувача Збройних Сил України від 12.10.2020 року № ВКП 10-00(49).01. Сили територіальної оборони ЗСУ. URL: <https://sprotyvg7.com.ua/wp-content/uploads/2022/04/ВКП-10-0049.01-Доктрина-зі-стратегічних-комунікацій.pdf> (дата звернення – 05.04.2025).

9. Доктрина стратегічних комунікацій Національної гвардії України ВКП НГУ. Наказ командувача Національної гвардії України від 22.11.2021 № 541. / Національна гвардія України. URL: <https://ngu.gov.ua/wp-content/uploads/2022/12/vkp-11-0101.01-doktryna-strategichnyh-komunikaczij-ngu.pdf.pdf> (дата звернення – 05.04.2025).