

## НОВІТНІ ЗАСОБИ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА В УМОВАХ ТЕХНОГЕННОЇ ЦИВІЛІЗАЦІЇ

*Розглядаються характерні риси новітніх засобів інформаційного протиборства. Розкривається специфіка розрізнення їхнього застосування в семантичній війні та кіберпротистоянні. Наводиться перелік новітніх засобів інформаційного протиборства, до яких віднесено: фальсифікацію мови, хибну ідентифікацію, нав'язування ірраціоналізму, масові розсилки, віруси, логічні бомби тощо. Також охарактеризовані прийоми, які застосовуються на їхній основі: вкидання, тролінг, дискредитація, продукування віртуальних особистостей та ін.*

**Ключові слова:** новітні засоби інформаційного протиборства, інформація, семантична війна, кіберпротистояння, вкидання, дискредитація.

### **Kalinichenko Bogdan. The newest means of confrontation in the conditions of technogenic civilization**

*The article deals with the features of the newest means of information confrontation. The specifics of the distinction between their use in semantic war and cyber confrontation are revealed. Here is a list of the latest tools of information warfare, which include: falsification of speech, false identification, imposition of irrationalism, mass mailings, viruses, logic bombs, etc. Also described are the techniques that are used on their basis: throwing, trolling, discrediting, the production of virtual personalities, etc.*

**Key words:** newest means of information confrontation, information, semantic war, cyber confrontation, throw-in, discredit.

Прийнято вважати, що глобалізація кардинально змінила практично всі сфери суспільного життя. Різні частини світу почали зближатися, поступово виникають зразки уніфікованої культури, політика стає більш публічною, а на рівні конкретної держави складно вирізнити її зовнішній і внутрішній виміри. Історія людства стає єдиною, а не сумою історій конкретних суспільств. Водночас все це відбувається на тлі розвитку інфор-

маційної сфери, яка дедалі більше дає про себе знати як окрема складова соціального буття. Проте вона не існує як річ у собі, а виступає сполучною ланкою для інших сфер суспільного життя. Тому володіння, керування та розпоряджання інформацією стає визначальним атрибутом здійснення влади в XXI столітті. Контроль за інформаційними потоками перетворюється на основну мету будь-якого протистояння. Боротьба ведеться за вплив на громадську думку, що потім оформлюється у вигляді домінування у процесі формування порядку денного. Виникнення такого явища, як протистояння в інформаційній сфері, закономірно спричинило своєрідну «гонку озброєнь». З обмеженням традиційних каналів ведення інформаційної війни (газети, радіомовлення, телебачення, навіть окремі сегменти Інтернету) та створенням спеціальних органів з регулювання кіберпростору виникають більш складні засоби ведення протистояння. Це якісно змінює загальну картину інформаційного протиборства, що й зумовлює актуальність даного дослідження.

Питанню виникнення новітніх засобів інформаційного протиборства приділяється мало уваги у вітчизняних наукових джерелах. Така проблема зумовлюється декількома причинами. По-перше, зазначені засоби динамічно змінюються, що зумовлюється їхнім становленням як інструмента ведення інформаційної війни. По-друге, слід визнати той факт, що розвиток інформаційних технологій в Україні відбувається повільніше, ніж у країнах ЄС, США та Канаді. Відповідно це дістає відображення в необхідності осмислення більш сучасних засобів інформаційного протиборства. Водночас в Україні та сусідній Росії поступово відбувається теоретичне осмислення даного явища, оскільки, як уже зазначалося, універсальність глобалізації закономірно призводить до проникнення новітніх інформаційних технологій й на терени колишнього СРСР. Так, у даному контексті варто згадати напрацювання таких учених, як Г. Почепцов, К. Баранова, І. Нежданов, С. Черних та Н. Зуєва, Н. Єрофеева, В. Самохвалова. Свідоме абстрагування від імен західних дослідників зумовлюється прагненням розглянути розвиток новітніх інформаційних засобів саме у вітчизняних реаліях. Водночас з вищенаведених учених лише Г. Почепцов належить до українського політологічного дискурсу. Інші представляють Росію.

Але слід зауважити, що їхні напрацювання беруться до уваги не лише з огляду на певну інформативність, а й у контексті гібридного протистояння України та Росії. Відповідно метою даного дослідження є систематизація й визначення характерних ознак новітніх засобів інформаційного протиборства в умовах техногенної цивілізації.

Отже, щодо новітніх засобів інформаційного протиборства слід насамперед відзначити Інтернет. Виникнення останнього призвело до своєрідної революції в інформаційній сфері. Як підкреслює російська дослідниця К. Баранова, принципи створення і розповсюдження продуктів ЗМІ сильно змінилися завдяки Інтернету<sup>1</sup>. Її колега В. Самохвалова поглиблює цю думку, акцентуючи увагу на новій атомізації суспільства, яка відбувається завдяки сучасним інформаційним технологіям<sup>2</sup>. Але якщо Інтернет на території України в середині 2000-х років, дійсно, сприймався як щось нове, то наразі ситуація абсолютно змінилася. В умовах неконтрольованої потужної експансії мережа Інтернет, по суті, була полігоном для створення та відточування різних засобів інформаційного впливу. Це, наприклад, інформаційні вкидання, неправдиві публікації, інформаційне зараження, перекручування фактів, виривання з контексту, підміна понять тощо. Але варто звернути увагу, що в даному випадку це продовжувало роботу традиційних друкованих або теле- і радіо ЗМІ. Власне на цьому й концентрує свою увагу К. Баранова, розглядаючи трансформацію ЗМІ з поширенням Інтернету.

Новітні засоби інформаційного протиборства криються в тих явищах, які з'явилися й можуть існувати виключно в мережі, — соціальні мережі, месенджери, форуми та платформи. Тобто все те, що може використовуватися для швидкого поширення інформації та утворення псевдомонілітних спільнот. Відповідно крізь призму вищеперерахованих елементів життя в Інтернеті доцільно аналізувати виникнення і подальший розвиток засобів інформаційного протиборства. При цьому можна розрізнити як інструменти, які застосовуються суто під час ведення кібервійни (новітні віруси, шкідливе програмне забезпечення, трояни та черв'яки), так і ті засоби, які спрямовані на створення й нав'язування нових «смислів».

К. Баранова виокремлює такі характеристики, які мають новітні засоби інформаційного протиборства: 1) швидкість розповсюдження інформації: ще з часів ведення класичної пропаганди такий параметр вважався чи не найважливішим, оскільки найголовніше — оперативно донести повідомлення до кінцевого споживача; 2) зрозумілість і доступність: в умовах інтенсифікації суспільного життя, коли в людини банально не вистачає часу читати довгі статті, записки чи замітки, повідомлення мають бути вкрай короткими, але інформативними і водночас простими<sup>3</sup>.

Її колега І. Нежданов доповнює важливі риси новітніх засобів інформаційного протиборства: 1) всеохопність — інформацію мають побачити якомога більше людей; 2) висока частотність — інформацію мають бачити часто (варто уточнити, що найбільший ефект спостерігається не від звичайного дублювання вже наявного повідомлення, а транслявання того ж самого змісту, але у зміненій формі); 3) довіра до джерела: в умовах техногенної цивілізації цей елемент класичної пропаганди набуває нового сенсу (слід розуміти, що при підвищенні інтенсивності ведення інформаційної війни часовий ресурс на створення та популяризацію певного каналу комунікації значно обмежений або його взагалі немає, тому в даному випадку довіра до джерела формується шляхом подачі повідомлення як суто інсайдерської інформації); 4) створення видимості масовості: реципієнт не лише повинен побачити інформацію, а й усвідомити, що до нього її вже багато хто побачив (для цього розміщуються коментарі, якщо це соціальна мережа, або «накручуються» перегляди, якщо це блог); 5) створення видимості значимості: як і в попередніх двох характеристиках, тут важливий належний рівень коментування та представлення самої інформації реципієнту (для цього інформація розміщується в топ-категоріях пошуку, з'являється у спливаючих вікнах, їй присвоюються популярні теги: розкритка тегу теж є новітнім засобом інформаційного протиборства)<sup>4</sup>.

До вищенаведеного В. Самохвалова додає: 1) фальсифікацію мови — інформація повинна не просто подаватися як така, а оперувати з навмисним неправильним використанням слів для подальшого викривлення змісту (тут варто зауважити, що підміна понять, яка вважається методом, переноситься в ранг харак-

теристик); 2) хибну ідентифікацію: інформація має нав'язувати реципієнту хибні критерії ідентичності, тобто заганяти його в рамки певної уявної спільноти (індивід починає жити у подвійній реальності, де співіснують взаємовиключні речі, явища та інтереси, що в подальшому поліпшує проведення міфологізації його свідомості); 3) нав'язування ірраціоналізму: інформація подається в гіперболізованій та химерній формі; це стосується як форми (шрифт, позиціонування, розміщення), так і змісту (емоційне навантаження, художні прийоми)<sup>5</sup>.

Отже, в даному випадку були наведені та розкриті риси новітніх засобів інформаційного протиборства, спрямованих на ведення смислових воєн. Тепер перейдемо до виявлення характеристик, притаманних аналогічним інструментам, але у сфері кіберпротистояння. До них належать: 1) простота створення, передачі та розповсюдження: шкідливе програмне забезпечення, віруси тощо мають бути швидко відтворюваними, а також блискавично поширюватися об'єктом зараження і вдало закріплюватися в ньому; 2) стійкість до виявлення: шкідливе ПЗ повинне виконати поставлені цілі до того, як буде виявлене і знищене, а атаковані ресурси приведені до початкового стану або ж якомога довше залишати систему противника ураженою; 3) швидкість розгортання: дана ознака не є обов'язковою для всіх різновидів новітніх засобів інформаційного протиборства і фактично визначається закладеною метою, але у більшості випадків важливими є саме раптовість і швидкість досягнення конкретного результату; 4) здатність «замітати сліди»: віруси повинні не лише виконати поставлене завдання, а й не видати ворогу джерело свого походження, оскільки в такому разі підвищується загроза швидкого контрудару.

Розрізливши новітні засоби інформаційного протиборства за двома напрямками, а також окресливши найбільш притаманні їм риси, варто перейти до розкриття власне їх самих. Отже, до новітніх засобів інформаційного протиборства, які застосовуються в обох означених напрямках, слід віднести:

- акаунти, публічні сторінки та групи в соціальних мережах (наприклад, Facebook);
- масові розсилки, канали та групові чати в месенджерах (наприклад, Telegram);

- різноманітні онлайн-платформи та форуми (WarOnline);
  - експлойти – програми, спрямовані на пошук вразливості в інформаційній системі через її неправильну реакцію;
  - логічні бомби – програми відкладеної дії, яка спрацювуватиме за настання/виконання певних умов в атакованій інформаційній системі;
  - трояни – шкідливе ПЗ, що закріплюється разом з іншим файлом і допускається до інформаційної системи самим користувачем;
  - віруси – шкідливе ПЗ, основним завданням якого є «вшивання» в код інших програм задля подальшого розповсюдження й завдання шкоди;
  - формграбери – програми для зчитування паролів та кодів і їх подальшої передачі хакеру;
  - мережеві черв'яки – вкрай небезпечна шкідлива програма, яка самостійно здатна розповсюджуватися мережею Інтернет і завдавати значної шкоди інформаційним системам.
- Перші три пункти – це новітні засоби інформаційного протиборства, які використовуються у смислових війнах, а наступні – в кіберпротистояннях. На їх основі застосовуються наступні прийоми ведення інформаційної війни:
- вкидання – доведення до цільової аудиторії інформації, здатної викликати резонанс (зараз найбільш ефективними є вкидання через Telegram-канали);
  - посів – масове вкидання однотипної або ідентичної інформації (для цього прийому використовуються перші три наведені групи новітніх засобів інформаційного протиборства);
  - легалізація інформації – дія, спрямована на те, щоб домогтися відкритого використання певної інформації. Йдеться про розміщення незаконно добутої інформації від імені різного роду «хакерських груп», «пранкерів» тощо. У такий спосіб відбувається не лише уникнення юридичної відповідальності, а й опосередковано підвищується довіра до такої інформації (якщо йдеться про її вкидання через «пранкерів» або Telegram-канали);
  - зашумлення – масове вкидання інформації, покликане приховати або відволікти від важливої інформації;
  - тролінг – провокування гніву та конфлікту шляхом публікування контраверсійних повідомлень. Найбільший ефект від

використання даного прийому досягається в соціальних мережах, оскільки в такому випадку повідомлення «тролів» є доступними для широких мас людей;

– дискредитація – здійснюється через перебільшення слабостей об'єкта, вказування на його помилки або розповсюдження фейкової інформації. Зазвичай дискредитація поєднується з посівом, оскільки для її успішного використання потрібно якомога ширше запустити потрібне повідомлення;

– відволікання – найчастіше проводиться за допомогою публікації різного роду «сенсацій», емоційних новин;

– продукування віртуальних особистостей – створення фейкових акаунтів<sup>6</sup>.

Щодо прийомів застосування новітніх засобів інформаційного протиборства у сфері кібервійни варто зауважити, що тут немає цілого спектра різноманітних хитрощів. Шкідливе програмне забезпечення розповсюджується або на файлообмінниках, прикріплюючись до певних утилітарних програм, або через спам-розсилки, або за допомогою додатків та ігор, в які «вшиті» шпигунські програми на кшталт формграберів, або безпосередньо завантажуються в інформаційну систему самим хакером.

Даний перелік не є повним, адже цифрові технології не стоять на місці, й з кожним днем модифікують засоби інформаційного протиборства. Наприклад, відбувається їхня специфікація та диференціація: наразі вже розрізняють типи фейкових акаунтів за спрямованістю, створюються онлайн-платформи та форуми під конкретну мету, модернізується шкідливе програмне забезпечення. Водночас не можна погодитися з думкою російської дослідниці Н. Єрофєєвої, яка вважає, що новітні засоби інформаційного протиборства (ті, що використовуються для ведення смислової війни), спрямовані на молодь, а традиційні ЗМІ більше охоплюють людей похилого віку<sup>7</sup>. Дійсно, певну кореляцію встановити можна, але, враховуючи швидкість розвитку інформаційних технологій і поширення самого Інтернету, він поступово витісняє друковані, теле- та радіо ЗМІ. Вони переміщують свою діяльність до мережі, тим самим підлаштовуючись під нові реалії.

Окремо слід наголосити на тому, що новітні засоби інформаційного протиборства, на відміну від нових та класичних, не

спрямовані на повну деструкцію людської свідомості та усталеної системи цінностей, як про це зазначають російські вчені С. Черних та Н. Зуєва<sup>8</sup>. Найбільш типовою метою інформаційного протиборства в умовах техногенної цивілізації є модифікація, ушкодження, зміна конфігурації, що дозволить у подальшому використовувати на свою користь отриману інформацію, контрольовану громадську думку, уражену інформаційну систему. Наразі не треба повністю зомбувати людей та знищувати ворожі інформаційні системи, оскільки їх можна поставити на службу собі. На цьому й акцентує увагу український дослідник Г. Почепцов, говорячи про управління протилежною стороною<sup>9</sup>. Парадоксально, але найбільш повно це розкривається у застосуванні новітніх засобів для ведення кібервійни. Дедалі частіше хакери використовують шкідливе програмне забезпечення не для знищення та повного паралізування інформаційних систем, а для налагодження їхньої неправильної роботи та крадіжок даних. Тому руйнівні черв'яки поступаються місцем вірусам та формграберам.

Таким чином, новітні засоби інформаційного протиборства не лише є атрибутом становлення техногенної цивілізації, а й відображають якісні зміни в інформаційному просторі. Поширення соціальних мереж та месенджерів спричинило виникнення вкрай атомізованих уявних спільнот, існування яких може обраховуватися днями, оскільки стрижнем їхньої єдності є той чи інший інформаційний привід. З інтенсифікацією суспільного життя та спрощенням подачі інформації підвищується кількість повідомлень, які може проглянути одна особа за добу. Люди фактично повністю занурюються в інформаційний простір, майже постійно тримаючи в руках смартфони. За логікою це мало б призвести до підвищення інформаційної грамотності та критичного мислення, але по факту, через перенавантаження повідомленнями та обмежений часовий ресурс, люди стають більш вразливими до вкидів, фейків, тролінгу та спам-розсилок у соціальних мережах та месенджерів. Незважаючи на те, що новітні засоби інформаційного протиборства запозичили деякі характерні риси класичної пропаганди, наразі гострою є проблема організації ефективної протидії їхньому впливу, оскільки традиційні заходи або не приносять бажаного результату, або,



навпаки, посилюють негативний ефект. Тому дане дослідження не вичерпує поставлених питань, а є спробою подальшого розгляду специфікації новітніх засобів інформаційного протиборства та розробки дієвих заходів нівелювання їхнього впливу.

1. Баранова Е. А. Мультимедийные технологии в средствах массовой информации как новый инструмент ведения информационной войны. *Вопросы теории и практики журналистики*. Иркутск: Байкальский государственный университет. 2016. Т. 5. №4. С. 621. 2. Самохвалова В. И. Специфика современной информационной войны: средства и цели поражения. *Философия и общество*. 2011. Вып. 3 (63). С. 61. 3. Баранова Е. А. Цит. работа. С. 622. 4. Нежданов И. Ю. Технологии информационных войн в интернете. URL: <http://bash.rosmu.ru/activity/attach/events/1283/01.pdf> (дата звернення: 17.11.2019). 5. Самохвалова В. И. Цит. работа. С. 63–65. 6. Нежданов И. Ю. Цит. работа. 7. Ерофеева Н. В. Современные информационные войны и их влияние на политическую стабильность государства. *PolitBook*. 2015. № 2. С. 81. 8. Черных С. Н., Зуева Н. А. Информационная война: традиционные методы, новые тенденции. *Контекст и рефлексия: философия о мире и человеке*. 2017. № 6. С. 192. 9. Почепцов Г. Г. Информационные войны: новые тенденции URL: [https://ms.detector.media/trends/1411978127/informatsionnye\\_voyny\\_novye\\_tendentsii/](https://ms.detector.media/trends/1411978127/informatsionnye_voyny_novye_tendentsii/).

#### **References:**

1. Banova E. A. Multymedyyne tekhnolohyy v sredstvakh massovoi informatsyyu kak novyj instrument vedeniya informatsyonnoi voyny. *Voprosy teorii i praktiki zhurnalystyky*. Yrkutsk: Baikalskiy hosudarstvennyi unyversytet. 2016. T. 5. №4. S. 621. 2. Samokhvalova V. Y. Spetsyfyka sovremennoi informatsyonnoj vojny: sredstva y tsely porazheniya. *Filosofiya y obshchestvo*. 2011. Vыр. 3 (63). S. 61. 3. Baranova E. A. Tsyt. rabota. S. 622. 4. Nezhdanov Y. Yu. Tekhnolohyy ynformatsyonnykh voin v ynternete. URL: <http://bash.rosmu.ru/activity/attach/events/1283/01.pdf> (data zvernennia: 17.11.2019). 5. Samokhvalova V. Y. Tsyt. rabota. S. 63–65. 6. Nezhdanov Y. Yu. Tsyt. rabota. 7. Erofeeva N. V. Sovremennyye ynformatsyonnyye voyny y ykh vlyianye na polytycheskuiu stablynost hosudarstva. *PolitBook*. 2015. №2. S. 81. 8. Chernykh S. N., Zueva N. A. Ynformatsyonnaia voina: tradytsionnye metody, novye tendentsyy. *Kontekst y refleksyia: fylosofyia o mire y cheloveke*. 2017. № 6. S. 192. 9. Pocheptsov H. H. Ynformatsyonnye voyny: novye tendentsyy URL: [https://ms.detector.media/trends/1411978127/informatsionnye\\_voyny\\_novye\\_tendentsii/](https://ms.detector.media/trends/1411978127/informatsionnye_voyny_novye_tendentsii/).

***Kalinichenko Bogdan. The newest means of confrontation in the conditions of technogenic civilization***

The article deals with the features of the newest means of information confrontation. The specifics of the distinction between their use in semantic war and cyber confrontation are revealed. Here is a list of the latest tools of information warfare, which include: falsification of speech, false identification, imposition of irrationalism, mass mailings, viruses, logic bombs, etc. Also described are the techniques that are used on their basis: throwing, trolling, discrediting, the production of virtual personalities, etc.

It is accepted that globalization has fundamentally changed almost all spheres of public life. Different parts of the world have begun to converge, the patterns of a unified culture are gradually emerging, politics become more public, and at the level of a particular state it is difficult to distinguish its external and internal dimensions. The history of mankind becomes one, not the sum of the histories of particular societies. At the same time, all this is happening against the background of the development of the information sphere, which increasingly makes it known as a separate part of social life. However, it does not exist as a thing in itself, but acts as a link for other areas of public life.

Therefore, the possession, management and disposal of information has become a defining attribute of power in the 21st century. Control over information flows becomes the primary goal of any confrontation. The struggle is for influencing public opinion, which is then drawn up in the form of dominance in the process of agenda formation. The emergence of such a phenomenon as a confrontation in the information field naturally led to a kind of «arms race». With the restriction of traditional channels of information warfare (newspapers, radio, television, even certain segments of the Internet) and the creation of special bodies to regulate cyberspace, more sophisticated means of dealing with conflict are emerging.

The newest means of information warfare is not only an attribute of the emergence of technogenic civilization, but also reflects qualitative changes in the information space. The proliferation of social networks and messengers has led to the emergence of highly atomized imaginary communities. With the intensification of social life and the simplification of information flow, the number of messages, that one person can see per day, increases. In fact, people are completely immersed in the information space, almost constantly holding smart phones. Logically, this should lead to increased literacy and critical thinking, but in fact, due to message overloads and limited time resources, people become more vulnerable to social networking and messaging, trolling and spamming. This qualitatively changes the overall picture of information warfare, which determines the relevance of this study.

**Key words:** newest means of information confrontation, information, semantic war, cyber confrontation, throw-in, discredit.