DOI: https://doi.org/10.26642/sas-2026-1(13)-46-51
УДК 004.3

Лукіна Катерина
молодший науковий співробітник
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
https://orcid.org/0000-0002-2803-7839

Інформаційна зброя в інформаційній війні

Анотація. Збройні конфлікти, що відбуваються в теперішній час, крім застосування безпосередньо зброї фізичного впливу, активно застосовують й інформаційні засоби впливу, тобто, крім збройної війни, в класичному розумінні цього визначення, одночасно відбувається й інформаційна війна. І в цій війні активно застосовуються передові інформаційні технології.

Засобом ведення інформаційної війни є інформаційна зброя, яку можна вважати самостійним та специфічним видом озброєння. Недооцінка потенціалу інформаційної зброї в умовах поточної інформаційної війни є критично небезпечним явищем і може мати фатальні наслідки при загостреннях і без того напруженої військово-політичної ситуації. Це підтверджується характером бойових дій, що нині ведуться в Україні. Особливістю інформаційної зброї є те, що її застосування дозволяє досягати політичні та військові цілі без традиційних бойових дій.

У статті розглянуто способи застосування інформаційної зброї, особливості, які відрізняють інформаційну зброю від традиційних видів озброєння. Однією з особливостей такої нетрадиційної зброї є те, що її вплив, зазвичай, спрямовується на ключові компоненти інформаційної сфери, такі як матеріальна інфраструктура, дані та люди. Метою впливу інформаційної зброї є спричинення шкоди інфраструктурі, поширення дезінформації, несанкціонований доступ до інформації для подальшого її використання, спотворення або знищення, вплив на людину. Також інформаційна зброя має такі особливості, як скритність, універсальність та масштабність, що робить її унікальним озброєнням. Потенціал інформаційної зброї в умовах інформаційної війни, що зараз триває, не можна недооцінювати. Тому класифікація інформаційної зброї є актуальним питанням для визначення подальших алгоритмів, механізмів та шляхів для зменшення або запобігання її впливу.

Ключові слова: інформаційна зброя; інформаційна війна; гібридна війна; скритність; дезінформація; несанкціонований доступ.

Актуальність теми дослідження обумовлена тим, що розгляд особливостей застосування інформаційної зброї, напрямків її застосування, класифікація за різними ознаками є необхідними етапами для подальшого створення правового поля щодо регулювання використання такої зброї. Також це необхідно для розробки стратегій кіберзахисту, для ідентифікації ризиків та відповідної оцінки загроз. Все це є актуальним для захисту національного інформаційного простору від зовнішнього впливу та маніпуляцій.

Аналіз останніх досліджень та публікацій. Основою статті стали роботи науковців, які досліджували інформаційну війну та інформаційну зброю. Серед робіт, що розглядали питання саме інформаційної війни, можна виокремити таких авторів, як: М.Лібікі [1], Г.Почепцов [2], О.Левченко [5], І.Гамова [6], Л.Шептицька [7] та інших, які досліджують інформаційну війну та її засоби ведення (інформаційну зброю) з різних ракурсів. У [8–10] виділено основні ознаки інформаційної зброї, а саме скритність, масштабність та універсальність. У [5, 11] розглянуто психологічні аспекти інформаційної зброї.

Метою статті є розкриття сутності інформаційної зброї, систематизація за різними напрямками класифікації, розгляд напрямку класифікації за об'єктом впливу, способи та прийоми застосування цього напрямку в сучасній війні.

Викладення основного матеріалу. Зброя – сукупність технічних пристроїв та засобів, що застосовується для ураження живої сили противника, його техніки, спорудження та інших цілей під час ведення бойових дій; озброєння [12].

Водночас у переносному значенні під зброєю розуміють будь-який засіб для збройної боротьби як з кимось, так і з чимось для досягнення певної мети. І зброя не обов'язково має бути призначена для безпосереднього вбивства, в неї можуть бути інші цілі, такі як:

- виведення людини з ладу (нелетальна зброя);

– виведення з ладу техніки, але при цьому не без впливу безпосередньо на людей (електромагнітний імпульс).

Якщо використовується традиційна зброя, то поразка може досягатися за допомогою таких методів: придушення, виснаження та знищення. Під знищенням розуміємо завдання такої шкоди, після отримання якої повністю нейтралізується боєздатність противника. Придушення – це також завдання шкоди, але такої, після отримання якої противник тимчасово позбавляється боєздатності, можливості здійснювати маневри або керувати. Виснаження спрямоване на ведення по противнику тривалої вогневої або ударної атаки обмеженої сили для поступового його ослаблення.

У теперішній час збройні конфлікти, що відбуваються, показали, що стався перехід (зміщення) від збройних (силових) протистоянь до протистоянь у сфері інформації. І тепер у збройних конфліктах, крім застосування безпосередньо зброї фізичного впливу, активно застосовують і інформаційні засоби впливу, тобто, крім збройної війни в класичному розумінні цього визначення, одночасно відбувається й інформаційна війна. І в цій війні активно застосовуються передові інформаційні технології. При цьому варто зауважити, що певною мірою інформаційний вплив на суспільство, в тому чи іншому вигляді, відбувався з давніх часів.

Інформаційна війна – процес подання інформації таким чином, щоб сформувати у суспільстві чи певній групі людей бажану громадську точку зору, систему поглядів, хід думок з метою забезпечення сприятливого результату для організатора цієї інформаційної кампанії [4]. Поява поняття «інформаційна війна» обумовлена зростаючою значущістю та цінністю інформації в усіх сферах суспільного життя [6]. Цей вид війни є універсальним, він не обмежується лише військовою сферою, а може охоплювати широкий спектр життєдіяльності, в тому числі економіку, політику, дипломатію і, звісно ж, збройні конфлікти.

Інформаційна зброя є невід'ємним засобом ведення інформаційної (гібридної) війни та становить важливий елемент повномасштабного конфлікту [3, 4].

Важливість інформаційної зброї підтверджує і Президент України Володимир Зеленський у своєму зверненні до українського народу, наголошуючи на тому, що іноді інформаційна зброя може зробити більше, ніж зброя звичайна, і що єдність українського народу не зламати брехнею чи залякуванням, фейками чи теоріями змови [13].

Зазвичай, інформаційна зброя (ІЗ) застосовується не самостійно, а в інтеграції з іншими видами боротьби, такими як: радіоелектронна боротьба (РЕБ), розвідка, психологічні операції, фізичне знищення.

Застосування інформаційної зброї має низку специфічних особливостей. Одна з особливостей полягає в тому, що згідно з [14] її вплив може бути спрямований на будь-який з трьох ключових компонентів інформаційної сфери:

а) матеріальна інфраструктура: сюди входять засоби (наприклад, сервери, комунікаційне обладнання) та лінії зв'язку (наприклад, кабелі);

б) дані: вплив спрямований на інформацію в її первинному вигляді та на те, як вона передається (її потоки);

в) люди: ІЗ може бути використана для безпосереднього впливу на людину.

Наслідки використання ІЗ завжди негативні та мають руйнівний характер, що може виражатися в зазначеному далі:

- спричинення шкоди фізичним об'єктам інфраструктури (наприклад, виведення з ладу обладнання);
- псування інформації, а саме: знищення, спотворення, несанкціоновані зміни;
- вплив на людину: атаки на нервову систему, психіку та свідомість як окремої людини, так і цілих цільових груп.

Іншими особливостями ІЗ, які відрізняють її від традиційних видів озброєнь та роблять унікальним небезпечним інструментом, як визначається в [8], є скритність, масштабність та універсальність.

Скритність при застосуванні ІЗ означає можливість її використання таємно, непомітно, без очевидної підготовки та без попередження, досягаючи поставлених цілей ще до того, як жертва усвідомить сам факт нападу.

Масштабність полягає в можливостях ІЗ завдавати значної і часто непоправної шкоди у всіх сферах функціонування людини та суспільства (від економіки до інфраструктури) без врахування державних кордонів, суверенітету, без обмежень у просторі.

Універсальність ІЗ виражається у гнучкості в плані різноманіття сфер її застосування. ІЗ можна застосовувати як проти військових, так і проти цивільних структур як агресора, так і жертви. При цьому ефективність враження об'єктів впливу не залежить від їх реального фізичного розташування, географічного місцезнаходження.

Також треба зазначити, що результати застосування ІЗ мають нематеріальний (віртуальний) та непередбачуваний (невизначений характер). Тобто, ІЗ використовує інформацію, яка є нефізичною

сутністю, що ускладнює її виявлення традиційними засобами. Наслідки застосування ІЗ складно точно спрогнозувати. Іноді великий обсяг інформації не дає досягти поставленої мети впливу, а якась достатньо незначна інформація призводить до кардинальних чи навіть катастрофічних наслідків. Отже, оцінити та точно спрогнозувати дію, кількість потрібної інформації практично неможливо.

Наслідки успішного застосування ІЗ можна порівняти з дією зброї масового ураження, особливо коли це спрямовано проти критичної інфраструктури або має масовий психологічний вплив.

Класифікація ІЗ може бути здійснена за різними напрямками, які розглянуті в багатьох дослідженнях. Для характеристики інформаційної зброї можуть застосовуватися такі показники, як масштабність та швидкість впливу, цілеспрямованість, вибірковість тощо. Узагальнені відомості щодо напрямків класифікації з коротким описом інформаційної зброї, що може належати до них, частково досліджені в [5, 8], наведено в таблиці 1.

Таблиця 1

Напрямки класифікації інформаційної зброї

Напрямок класифікації	Інформаційна зброя
За метою застосування та масштабом завдань, що вирішуються	Зброя для цілеспрямованого формування складових морально-семантичного фільтра соціальних об'єктів (системи цінностей, пріоритетів, системи інтересів тощо)
	Зброя для нав'язування стороні супротивника бажаних рішень і поведінки
	Зброя для ускладнення умов прийняття рішень стороною супротивника
	Зброя для зриву функціонування технічних та інших систем (автоматизованих систем управління; інформаційно-телекомунікаційних систем та ін.)
	Зброя для добування інформації про сторону супротивника
За об'єктами впливу (системи управління, свідомість населення, критична інфраструктура)	Зброя впливу на соціальні системи (людина, соціальні групи, суспільство, країни)
	Зброя впливу на соціально-технічні системи (автоматизовані системи управління, інформаційно-телекомунікаційні системи, Інтернет тощо) спрямована на виведення з ладу життєво важливих функцій держави та суспільства
	Зброя впливу на технічні системи (системи управління технологічними лініями, загальносистемне програмне забезпечення, перехоплення управління безпілотними засобами ураження та ін.)
	Зброя впливу на інші об'єкти інформаційної інфраструктури
За механізмами реалізації впливу: як саме реалізується вплив	Зброя, що базується на реалізації механізмів вербального впливу на людину та соціальні системи
	Зброя, що базується на реалізації механізмів невербального впливу на людину та соціальні системи
	Зброя, що базується на реалізації механізмів впливу на функціонування математично-програмного забезпечення ЕОМ
	Зброя, що базується на реалізації механізмів випромінювання енергії різної природи
За методами впливу, що реалізуються	Зброя, що базується на реалізації методів інтелектуального характеру (методи дезінформування, нейролінгвістичного програмування, рефлексивного управління та ін.), спрямована на те, щоб змусити об'єкт прийняти неправильне рішення
	Зброя, що базується на реалізації методів психологічного впливу на людину, суспільство, спрямована на зміну емоційного стану або морально-психологічної стійкості людини, або суспільства (пропаганда, розповсюдження чуток для створення паніки, підрив довіри до влади, армії, конкретної людини)
	Зброя, що базується на реалізації методів психофізіологічного впливу, в тому числі технічного характеру, на людину, суспільство (використання електромагнітного випромінювання для порушення роботи нервової системи або органів чуття, застосування акустичної зброї (ультразвук, інфразвук) для викликання паніки, дезорієнтації, погіршення стану здоров'я)
За характером впливу на інформацію та інформаційні процеси (спрямована на порушення цілісності, конфіденційності та достовірності)	Зброя руйнівного характеру (знищення наявної інформації чи обладнання)
	Зброя спотворювального характеру (зміна наявної інформації)
	Зброя модифікуючого характеру (впливає на інформаційні процеси)
За правовим статусом	Легальна (офіційні заяви)
	Нелегальна, прихована (хакерські атаки, підробки)
За масштабом вирішуваних бойових завдань	Стратегічна зброя
	Оперативно-тактична зброя
	Тактична зброя
За терміном (тривалістю) дії	Зброя короткострокової дії
	Зброя довгострокової дії
За часом застосування	Застосування у мирний час (прихований вплив, шпигунство)
	Застосування у воєнний час (пропаганда, знищення інфраструктури)

Якщо звернути увагу на напрямок класифікації за об'єктом впливу, то очевидно, що ІЗ, яка належить до цього напрямку, в своїй дії спрямована на людину та на техніку. Відповідно до цього інформаційна зброя поділяється на інформаційно-технічну та інформаційно-психологічну [15]. Вплив інформаційно-технічної зброї (ІТЗ) спрямований на інформаційні ресурси та інфраструктуру держави (в тому числі збройних сил). Дія інформаційно-психологічної зброї (ІПЗ) впливає на морально-психологічний стан людей, як окремих, так і груп, верств населення. Можна сказати, що ІТЗ атакує технології та дані, а ІПЗ – свідомість та психіку.

На сьогодні до інформаційно-технічної зброї належать засоби, інструменти, призначені для руйнівного впливу на інформаційні дані (знищення, викрадення, спотворення, викривлення), засоби, за допомогою яких можна отримати несанкціонований доступ до інформації зареєстрованих користувачів, заблокувати їх доступ та роботу. Також до ІТР зараховують засоби, здатні дезорганізувати роботу технічних пристроїв, вивести з ладу комп'ютерні системи, комунікаційні мережі та системи, які забезпечують функціонування держави й суспільства. ІТЗ, метою якої є несанкціонований збір інформації та здійснення кібератак, часто представлена спеціальним програмним забезпеченням і називається програмно-технічною інформаційною зброєю (ПТІЗ). Інструменти, які застосовує ПТІЗ, дозволяють здійснювати несанкціонований доступ до комп'ютерних систем, визначати коди доступу, ключі шифрування та іншу конфіденційну інформацію. Крім того, в арсеналі ПТІЗ є різні шкідливі програми: програмні закладки, комп'ютерні віруси та інші спеціалізовані засоби для здійснення кібератак.

Визначальною рисою ІПЗ є її прихований (латентний) характер. Ефективність дії ІПЗ базується на глибинному знанні цільової спільноти. Перед впливом на об'єкт (спільноту) організатори ретельно вивчають головні характеристики об'єкта, менталітет та психотип, для того, щоб в подальшому ефективно на нього вплинути, атакувати. Зазвичай об'єкт впливу не підозрює, не усвідомлює, що проти нього здійснюється атака. А якщо навіть усвідомлює, то не має можливості ефективно продіяти, що забезпечує домінування протиборчої сторони. Це робить ІПЗ надзвичайно потужним інструментом прихованої війни, що вимагає нових підходів до національної безпеки. До ІПЗ належать різні психологічні операції, а саме: пропаганда, де головним знаряддям є засоби масової комунікації, дезінформація, маніпуляції в ЗМІ та соціальних мережах для зміни громадської думки, підриву довіри до влади. ІПЗ діє таким чином, щоб противник (об'єкт впливу) змінював свою думку, ухвалював неправильні рішення, діяв із запізненням або діяв певним чином. Засоби впливу класичної ІПЗ – це медійний, пропагандистський та кіберпсихологічний впливи. Також є варіанти застосування ІПЗ у вигляді психотропних, нейролінгвістичних, психофізичних засобів тощо [5].

Інформаційна зброя і надалі залишатиметься багатогранним інструментом для кібервійни, дезінформації, шпигунства та руйнування інфраструктур. Акцент інформаційної зброї робиться на автономність, безконтактність та глибинне втручання у системи, що робить захист критично важливим та складним.

Якщо говорити про перспективи та напрямки розвитку й застосування інформаційної зброї, то, безсумнівно, вона надалі залишатиметься щонайменше рівноцінним зі звичайними видами озброєння засобом впливу і буде тільки вдосконалюватися.

Конкретний напрямок, який буде активно розвиватися, виділити складно, але однозначно, що вплив на будь-який об'єкт – чи то жива людина, система управління, чи база даних – буде здійснюватися переважно з використанням високих технологій, найсучасніших розробок, механізмів у сфері інформаційних технологій, оскільки це не потребує особистого спілкування і вплив може бути здійснений з будь-якого місця в будь-яку точку світу.

Тобто, можна сказати, що тема розвитку інформаційної зброї є дуже перспективною та скоріш за все зосередженою на посиленні кібернетичних можливостей, штучного інтелекту, маніпулювання даними та психологічним впливом.

Стрімкий розвиток штучного інтелекту та машинного навчання вже сьогодні дозволяє людині, а також самому штучному інтелекту, самостійно виявляти вразливості супротивника, прогнозувати його дії, розробляти та здійснювати атаки, адаптуючись до системи захисту в реальному часі.

В той же час розвиток штучного інтелекту сприяє та надалі сприятиме створенню реалістичного фальшивого контенту (аудіо, відео, текст), за допомогою якого можна маніпулювати громадською думкою та пропагандою.

Вже в теперішній час використовується ІЗ для виведення з ладу енергетичних систем, атакуються інтернет-інфраструктури для блокування доступу до інформації, а також здійснюються атаки на пристрої Інтернету речей, який зараз активно розвивається. З часом такі атаки будуть тільки вдосконалюватися.

Інформаційна зброя як психологічний вплив на людей, груп людей, дезінформація як виклик до потрібних дій та рішень буде і надалі використовуватися. Перспективним напрямком її розвитку є більша персоналізація для більш влучного впливу.

Розвиток інформаційної зброї одночасно породжує проблеми вирішення (розв'язання, запобігання) наслідків її дії, тобто виникає необхідність у розробці певних механізмів захисту від впливів інформаційної зброї.

Це є складним завданням з кількох причин:

1. Нові методи загроз з'являються постійно, у зв'язку з цим не встигають розроблятися відповідні засоби захисту;
2. Складність виявлення здійснення атаки на початковому етапі;
3. Складність виявлення місця, звідки атака здійснюється, тому що це може бути будь-яка точка світу.

Висновки та перспективи подальших досліджень. Проведений огляд напрямків класифікації показав, що на сьогоднішній день інформаційна зброя є самостійним видом зброї в інформаційній війні, поряд з традиційною. При цьому інформаційна зброя має певний ряд особливостей, серед яких дуже важливими є скритність, універсальність та масштабність. Вплив та засоби впливу дуже різноманітні, їх потенціал критично небезпечно недооцінювати. Визнання будь-яких засобів інформаційною зброєю визначається за таким критерієм, як ефективність у досягненні цілей інформаційної боротьби.

Розгляд особливостей застосування інформаційної зброї, напрямків її застосування, класифікація за різними ознаками є необхідними етапами для подальшого створення правового поля щодо регулювання використання такої зброї, для розробки стратегій кіберзахисту, для ідентифікації ризиків та відповідної оцінки загроз, для визначення подальших алгоритмів, механізмів та шляхів для зменшення або запобігання її впливу. Все це є актуальним для захисту національного інформаційного простору від зовнішнього впливу та маніпуляцій.

Список використаної літератури:

1. *Лібікі М*. Що таке інформаційна війна / *М.Лібікі* // Військо України. – 2014. – № 04 (163). – С. 26–27 [Електронний ресурс]. – Режим доступу : https://shron3.chtyvo.org.ua/Viisko_Ukrainy/2014_N04_163.pdf.
2. Інформаційні війни: тенденції та шляхи розвитку / Детектор Медіа [Електронний ресурс]. – Режим доступу : https://ms.detector.media/manipulyatsii/post/6479/2012-08 12-informatsiyni-viyny-tendentsii-ta-shlyakhy-rozvytku/.
3. *Киричук Б.* Інформація як зброя: правовий аспект / *Б.Киричук, Т.Коберська* // III Міжнародна науково-практична конференція молодих учених та студентів «Філософські виміри техніки» (PDT-2022) [Електронний ресурс]. – Режим доступу : https://elartu.tntu.edu.ua/bitstream/lib/39689/2/PDT_2022_Kyrychuk_B-Information_as_a_weapon_52-54.pdf.
4. Інформаційна війна / Вікіпедія [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B2%D1%96%D0%B9%D0%BD%D0%B0.
5. *Левченко О.В.* Класифікація інформаційної зброї за засобами ведення інформаційної боротьби / *О.В. Левченко* //Сучасні інформаційні технології у сфері безпеки та оборони. – 2014. – № 2 (20). С. 142–145.
6. *Гамова І.В.* Інформаційні війни : підручник / *І.В. Гамова*. – Київ : Держ. торг.-екон. ун-т, 2022. – 184 с.
7. *Шептицька Л.* Досвід інформаційних війн в історії та сучасності як об'єкт досліджень сучасної науки та освіти. / *Л.Шептицька, О.Ременяк, Н.Захарчин* // Проблеми гуманітарних наук : збірник наукових праць Дрогобицького державного педагогічного університету імені Івана Франка. Серія : Історія. Спецвипуск. – 2024. – С. 35–43. DOI: 10.24919/2312-2595.spec.3.
8. *Хорошко В.* Особливості застосування сучасної інформаційної зброї / *В.Хорошко, Т.Козел, О.Ярошенко* // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2015. – Вип. 1. (29). – С. 9–15.
9. Інформаційна зброя – теорія і практика застосування в інформаційному протиборстві / Militarnyi [Електронний ресурс]. – Режим доступу : https://militarnyi.com/uk/news/informatsijna-zbroya-teoriya-i-praktyka-zastosuvannya-v-informatsijnomu-protyborstvi/.
10. Зброя інформаційна / Велика Українська Енциклопедія [Електронний ресурс]. – Режим доступу : https://vue.gov.ua/%D0%97%D0%B1%D1%80%D0%BE%D1%8F_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0.
11. *Алещенко В.* Психологічні аспекти інформаційної війни / *В.Алещенко* // Психологічний вісник Київського національного університету імені Тараса Шевченка. Серія : Військово-спеціальні науки. – 2022. – № 2 (50). – С. 27–31.
12. Зброя / Вікіпедія [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/%D0%97%D0%B1%D1%80%D0%BE%D1%8F.
13. Українцям потрібен своєрідний емоційний суверенітет / Укрінформ [Електронний ресурс]. – Режим доступу : https://www.ukrinform.ua/rubric-society/3530713-ukraincam-potriben-emocijnij-suverenitet-zelenskij.html.
14. *Лабенко Л.В.* Інформаційний тероризм: поняття та ознаки / *Л.В. Лабенко* // Міжнародні читання присвячені пам'яті професора Імператорського Новоросійського університету П.Є. Казанського : матеріали Міжнародної конференції, 22–23 жовтня. – Одеса : Фенікс, 2010. – С. 195–198.
15. Інформаційна зброя як інструмент інформаційної війни / *В.Хорошко, Ю.Хохлачова, Т.Пірцхалава, І.Іванченко* // Захист інформації. – 2022. – № 24 (2). – С. 50–58. DOI: 10.18372/2410-7840.24.16930.

References:

1. Libiki, M. (2014), «Shcho take informatsiina viina», *Viisko Ukrainy*, No. 04 (163), pp. 26–27, [Online], available at: https://shron3.chtyvo.org.ua/Viisko_Ukrainy/2014_N04_163.pdf
2. «Informatsiini viiny: tendentsii ta shliakhy rozvytku», *Detektor Media*, [Online], available at: https://ms.detector.media/manipulyatsii/post/6479/2012-08 12-informatsiyni-viyny-tendentsii-ta-shlyakhy-rozvytku/
3. Kyrychuk, B. and Koberska, T. (2022), «Informatsiia yak zbroia: pravovyi aspect», *III Mizhnarodna naukovo-praktychna konferentsiia molodykh uchenykh ta studentiv «Filosofski vymiry tekhniky» (PDT-2022)*, [Online], available at: //elartu.tntu.edu.ua/bitstream/lib/39689/2/PDT_2022_Kyrychuk_B-Information_as_a_weapon_52-54.pdf
4. «Informatsiina viina», Vikipediia, [Online], available at::://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B2%D1%96%D0%B9%D0%BD%D0%B0
5. Levchenko, O.V. (2014), «Klasyfikatsiia informatsiinoi zbroi za zasobamy vedennia informatsiinoi borotby», *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, No. 2 (20), pp. 142–145.
6. Hamova, I.V. (2022), *Informatsiini viiny*, pidruchnyk, Derzh. torh.-ekon. un-t, Kyiv, 184 p.
7. Sheptytska, L., Remeniak, O. and Zakharchyn, N. (2024), «Dosvid informatsiinykh viin v istorii ta suchasnosti yak obiekt doslidzhen suchasnoi nauky ta osvity», *Problemy humanitarnykh nauk*, zbirnyk naukovykh prats Drohobytskoho derzhavnoho pedahohichnoho universytetu imeni Ivana Franka. Seriia *Istoriia*, Spetsvypusk, pp. 35–43. doi: 10.24919/2312-2595.spec.3.
8. Khoroshko, V., Kozel, T. and Yaroshenko, O. (2015), «Osoblyvosti zastosuvannia suchasnoi informatsiinoi zbroi», *Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini*, No. 1 (29), pp. 9–15.
9. «Informatsiina zbroia – teoriia i praktyka zastosuvannia v informatsiinomu protyborstvi», *Militarnyi*, [Online], available at: https://militarnyi.com/uk/news/informatsijna-zbroya-teoriya-i-praktyka-zastosuvannya-v-informatsijnomu-protyborstvi/
10. «Zbroia informatsiina», *Velyka Ukrainska Entsyklopediia*, [Online], available at: https://vue.gov.ua/%D0%97%D0%B1%D1%80%D0%BE%D1%8F_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0
11. Aleshchenko, V. (2022), «Psykholohichni aspekty informatsiinoi viiny», *Psykholohichnyi visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka*. Seriia *Viiskovo-spetsialni nauky*, No. 2 (50), pp. 27–31.
12. «Zbroia», *Vikipediia*, [Online], available at: https://uk.wikipedia.org/wiki/%D0%97%D0%B1%D1%80%D0%BE%D1%8F
13. «Ukraintsiam potriben svoieridnyi emotsiinyi suverenitet», *Ukrinform*, [Online], available at: https://www.ukrinform.ua/rubric-society/3530713-ukraincam-potriben-emocijnij-suverenitet-zelenskij.html
14. Labenko, L.V. (2010), «Informatsiinyi teroryzm: poniattia ta oznaky», *Mizhnarodni chytannia prysviacheni pamiati profesora Imperatorskoho Novorosiiskoho universytetu P.Ye. Kazanskoho*, materialy Mizhnarodnoi konferentsii, 22–23 zhovtnia, Feniks, Odesa, pp. 195–198.
15. Khoroshko, V., Khokhlachova, Yu., Pirtskhalava, T. and Ivanchenko, I. (2022), «Informatsiina zbroia yak instrument informatsiinoi viiny», *Zakhyst informatsii*, No. 24 (2), pp. 50–58. doi: 10.18372/2410-7840.24.16930.

Lukina K.

Information Weapon in Information Warfare

Abstract. Contemporary armed conflicts, in addition to the direct use of conventional weapons, increasingly involve various informational means of influence. Thus, alongside armed warfare in the traditional sense, information warfare is simultaneously taking place, in which advanced information technologies play a crucial role.

Information weapons serve as a key instrument of information warfare and may be regarded as an independent and specific type of weaponry. Underestimating the potential of information weapons in the context of the ongoing information confrontation is critically dangerous and may lead to severe consequences in the event of further escalation of the already tense military and political situation. This is evidenced by the nature of the hostilities currently taking place in Ukraine. A distinctive feature of information weapons is that their use makes it possible to achieve political and military objectives without engaging in traditional combat operations.

The article examines the methods of employing information weapons and identifies the characteristics that distinguish them from conventional types of weaponry. One of the defining features of such non-traditional weapons is that their impact is typically directed at the key components of the information sphere, including physical infrastructure, data, and human actors. The objectives of information weapons include damaging infrastructure, spreading disinformation, gaining unauthorised access to information for further use, manipulation or destruction, and influencing individuals and public opinion. Information weapons are also characterised by such features as concealment, versatility, and scalability, which make them a unique form of weaponry. The potential of information weapons in the context of the ongoing information warfare should not be underestimated. Therefore, the classification of information weapons remains an important issue for developing effective algorithms, mechanisms, and strategies aimed at mitigating or preventing their impact.

Keywords: information weapons; information warfare; hybrid warfare; concealment; disinformation; unauthorised access.

Стаття надійшла до редакції 09.01.2025.