© Muzychenko K.M., Petryk V.M. Cyberwarfare Technologies on the Battlefield of the Russian-Ukrainian Conflict. // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 36-43. © This is an open access article under the CC BY 4.0 International license.*

DOI: 10.18372/2225-5036.32.21656

ТЕХНОЛОГІЇ СУЧАСНОЇ КІБЕРВІЙНИ НА ПОЛІ БОЮ РОСІЙСЬКО-УКРАЇНСЬКОГО КОНФЛІКТУ

Кирило Музиченко[1], Валентин Петрик[2]

[1] Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Україна
[2] Національний університет «Київський авіаційний інститут», Україна



МУЗИЧЕНКО Кирило Миколайович,
Рік та місце народження: 2003 рік, м. Київ, Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», 2025 рік.
Наукові інтереси: національна безпека, системи інформаційної зброї та технології інформаційної війни, інцидент-менеджмент у кіберпросторі, інформаційні війни
Публікації: більше 50 наукових публікацій, серед яких монографії, наукові статті, патент на корисну модель, тези доповідей на конференціях
E-mail: kirilmuzychenkho@gmail.com
Orcid: 0009-0004-0738-6273



ПЕТРИК Валентин Михайлович, к. н. з держ. управл., доцент
Рік та місце народження: 1968 рік, м. Київ, Україна.
Освіта: Київський національний університет ім. Тараса Шевченка, 1995 рік.
Посада: доцент кафедри кібербезпеки Державного університету КАІ.
Наукові інтереси: інформаційна безпека держави, кібергігієна, кіберпсихологія, інформаційні війни, спеціальні інформаційні операції та акції інформаційного впливу, духовно-релігійна складова національної безпеки
Публікації: більше 200 наукових публікацій, серед яких монографії, наукові статті, матеріали та тези доповідей на конференціях, підручники та навчальні посібники
E-mail: iszzi_open@ukr.net
Orcid: 0000-0003-2662-0876

Анотація. *У статті досліджуються технології сучасної кібервійни в контексті російсько-українського збройного конфлікту, що розпочався у повномасштабній фазі у лютому 2022 року. Проаналізовано основні категорії кіберзброї, що застосовуються на полі бою: деструктивне шкідливе програмне забезпечення (wiper-атаки), атаки на промислові системи управління, розподілені атаки на відмову в обслуговуванні (DDoS), операції злому і витоку даних, радіоелектронна боротьба, технології інформаційних операцій і дезінформації. Розглянуто специфіку інтеграції кіберзасобів із конвенційними військовими операціями, роль штучного інтелекту та великих мовних моделей в інформаційних операціях, а також застосування комерційних безпілотних авіаційних систем, підсилених кіберможливостями. Обґрунтовано наукову новизну дослідження, що полягає у комплексному системному аналізі кіберзасобів у контексті реального збройного конфлікту як полігону апробації технологій. Сформульовано прогноз щодо тенденцій розвитку технологій кібервійни на найближче десятиліття.*

Ключові слова: *кібервійна, інформаційна безпека, кіберзброя, wiper-атаки, DDoS, APT-групи, інформаційні операції, дезінформація, радіоелектронна боротьба, штучний інтелект у кібервійні, кіберрозвідка, захист критичної інфраструктури.*

Вступ

Російсько-український збройний конфлікт, що перейшов у повномасштабну фазу 24 лютого 2022 року, став першим у новітній історії прикладом масштабного поєднання конвенційних бойових операцій із систематичним застосуванням кіберзасобів на всьому спектрі збройного протистояння. На відміну від попередніх збройних конфліктів, у яких кібератаки виконували переважно допоміжну або демонстраційну роль, в даному протиборстві кіберзасоби виявляють ознаки повноцінного домену ведення бойових дій з притаманними йому принципами бойового застосування, організаційними структурами та технологічною базою.

Актуальність дослідження визначається кількома взаємопов'язаними чинниками. По-перше, наявний збройний конфлікт становить безпрецедентний за обсягом і тривалістю полігон реального бойового застосування технологій кібервійни, що дозволяє виявити закономірності їх ефективності й обмежень у реальних умовах — а не в контрольованих лабораторних або навчальних середовищах. По-друге, технологічна динаміка конфлікту охоплює весь спектр від традиційних шкідливих програм до генеративного штучного інтелекту, що визначає необхідність комплексного аналітичного підходу. По-третє, досвід цього конфлікту активно осмислюється провідними арміями та дослідними структурами світу й безпосередньо впливає на формування доктрин кібервійни наступного покоління.

Метою статті є комплексне технологічне та аналітичне дослідження кіберзасобів, що застосовуються у російсько-українському конфлікті, виявлення системних закономірностей їх використання, а також формулювання науково обґрунтованого прогнозу розвитку технологій кібервійни на найближче десятиліття.

Аналіз існуючих досліджень

Дослідницька спільнота накопичила значний масив робіт, присвячених окремим аспектам кібервоєнних операцій у контексті України. Зокрема, Devost, Houghton і Pollard у 2022 році встановили, що кібератаки, здійснені напередодні вторгнення, реалізовували принцип підготовки кібербоєвища, що узгоджується з доктриною Russian New Generation Warfare. Фундаментальний аналіз шкідливого програмного забезпечення типу wiper, застосованого проти України, виконано дослідниками компаній ESET, Mandiant та Microsoft, які задокументували принципово нові архітектурні рішення подібної зброї [1].

Серед останніх публікацій варто виділити доповідь Microsoft Digital Defense Report 2024, що містить найповнішу на сьогодні класифікацію APT-груп, пов'язаних із рф та Україною, а також аналіз динаміки їхньої активності протягом повномасштабного вторгнення. Дослідження Slayton і Kello (2023) поглиблює розуміння стратегічних обмежень кіберзброї та пояснює, чому очікування «кіберпотрясіння» не справдилися у повній мірі. Водночас аналітичні матеріали Belfer Center, RAND Corporation та CyberPeace Institute висвітлюють окремі кластери інцидентів.

Наукова новизна пропонованої статті полягає в: (1) системній класифікації всього спектру кіберзасобів за функціональними доменами застосування у рамках єдиної концептуальної моделі; (2) комплексному аналізі взаємодії кіберзасобів з конвенційними бойовими операціями (кібер-фізична конвергенція); (3) введенні в науковий обіг аналізу ролі комерційних технологій — великих мовних моделей та цивільних безпілотних авіаційних систем — у кіберзмаганнях конфлікту; (4) формулюванні прогнозу на основі виявлених закономірностей.

Основна частина дослідження

Wiper-програми — клас шкідливого програмного забезпечення, спеціально розробленого для незворотного знищення даних, — виявляють безпрецедентну різноманітність і технологічну складність у досліджуваному конфлікті. За даними ESET Research, лише протягом перших десяти місяців повномасштабного вторгнення в Україні задокументовано більше дванадцяти принципово різних різновидів wiper, що перевищує загальну кількість аналогічних зразків, зафіксованих у всіх попередніх збройних конфліктах разом [2].

HermeticWiper, розгорнутий за кілька годин до вторгнення 24 лютого 2022 року, застосовував легітимні компоненти EaseUS Partition Master для перезапису Master Boot Record та таблиць розділів. Паралельно HermeticWizard забезпечував латеральний рух мережею, а HermeticRansom маскував деструктивну природу атаки під вимогу викупу — класичний прийом «хибного прапора». Ця архітектура свідчить про заздалегідь сплановану, складну операцію зі значним ресурсом підготовки.

AcidRain, виявлений того самого дня і спрямований проти модемів Viasat KA-SAT, продемонстрував якісно новий вектор: компілятор під MIPS-архітектуру і рекурсивне знищення файлових систем та блочних пристроїв. Атака призвела до виведення з ладу тисяч комунікаційних терміналів в Україні та десяти країнах Європи, унаочнивши транскордонний ефект кіберзброї. CaddyWiper, FoxBlade (HydraWiper), DoubleZero, IsaacWiper та Industroyer2 доповнюють цей арсенал, кожен із яких демонструє еволюцію у виборі мішені та методах обходу засобів захисту [3].

Industroyer2, виявлений у квітні 2022 року і спрямований проти підстанції передачі електроенергії в Україні, є прямим нащадком Industroyer/Crashoverride — шкідливої програми, відповідальної за відключення електроенергії в Києві у грудні 2016 року. Принципова відмінність полягає у підтримці протоколу IEC 104, стандарту автоматизації підстанцій, що свідчить про ретельне вивчення атакуючим цільового обладнання та можливість завдання реальної фізичної шкоди енергетичній мережі.

Серед задокументованих атак на об'єкти критичної інфраструктури особливе місце посідають операції проти телекомунікаційного оператора «Київстар» у грудні 2023 року, приписувані групі Sandworm. Ця атака призвела до тривалого відключення послуг для понад 24 мільйонів абонентів і стала одним із найруйнівніших інцидентів проти телекомунікаційної інфраструктури. Атакуючі перебували в мережі оператора щонайменше з травня 2023 року, що демонструє стратегію довгострокового укорінення.

Постійні атаки на енергетичну інфраструктуру поєднуються з конвенційними ракетними ударами по об'єктах енергогенерації та розподілу, формуючи класичний приклад кібер-фізичної конвергенції: кіберзасоби і кінетичні засоби застосовуються синхронно для посилення сукупного деструктивного ефекту [4].

Розподілені атаки на відмову в обслуговуванні (DDoS) стали наймасовішим за кількістю інцидентів різновидом кіберактивності в обох сторін конфлікту. IT Army of Ukraine — неформальне об'єднання волонтерів та хакерських угруповань — координує атаки переважно через платформу Telegram, спрямовуючи їх проти урядових, фінансових і медійних ресурсів рф. Аналіз показує, що пікова активність IT Army корелює з ключовими подіями збройного конфлікту.

З боку рф масові DDoS-атаки здійснюються через координовані ботнети, а також прокремлівськими хактивістськими групами Killnet, XakNet та NoName057(16). Остання розробила автоматизований інструментарій

DDoSia, що дозволяє будь-якому добровольцю долучатися до атак без технічних знань, перетворюючи DDoS на інструмент масової мобілізації. Аналіз показує суттєву залежність між геополітичними рішеннями (постачання зброї, санкції, дипломатичні заяви) та сплесками DDoS-активності проти відповідних країн.

Хакерські операції типу «злам і витік» (hack-and-leak) є ключовим інструментом інформаційних операцій в обох таборах. Принцип полягає в проникненні в мережі організації, викраденні конфіденційних даних і подальшому їх злитті через засоби масової інформації або Telegram-канали з метою дискредитації або дезінформації. Документування цих операцій свідчить про їх взаємозв'язок із новинним циклом: злиті матеріали з'являються у публічному просторі в моменти найвищої медійної уваги.

З боку рф подібні операції здійснюють угруповання Fancy Bear (APT28), Cozy Bear (APT29), Sandworm (APT44) та Gamaredon (ACTINIUM). ГРУ-пов'язаний Sandworm відповідає за найруйнівніші деструктивні операції, тоді як APT28 і APT29 спеціалізуються переважно на кібершпигунстві й операціях впливу. Україну з боку відповідного кіберугруповання представляють, зокрема, Ukrainian Cyber Alliance та IT Army, які задокументували злами систем управління дронами, залізничних систем та регіональних адміністрацій рф [5].

Одним із найбільш виразних технологічних феноменів конфлікту є масштабне застосування радіоелектронної боротьби (РЕБ) у поєднанні з кіберзасобами. Системи РЕБ рф — Krasukha-4, Zhitel, Borisoglebsk-2, Murmansk-BN та інші — активно застосовуються для придушення GPS-сигналу, виведення з ладу каналів управління безпілотними авіаційними системами та перехоплення комунікацій. Наслідком є масова відмова українських дронів у зонах активного застосування РЕБ.

Великогабаритні комплекси РЕБ, розгорнуті рф, функціонують на оперативному та стратегічному рівнях. Krasukha-4 призначена для придушення авіаційних радарів і деяких БПЛА на дальностях до 300 км. Borisoglebsk-2 є багатофункціональним комплексом, здатним одночасно придушувати декілька діапазонів: КВ, УКХ, транкінговий зв'язок і супутникові канали управління. Murmansk-BN — комплекс стратегічного рівня — здатний уражати КХ-канали зв'язку на дальностях до 5000 км, що дозволяє впливати на комунікації союзників України у Західній Європі. Zhitel орієнтований на придушення супутникових навігаційних систем GPS і ГЛОНАСС та стільникового зв'язку стандартів GSM/3G.

Поряд із великогабаритними комплексами у досліджуваному конфлікті сформувався принципово новий клас засобів РЕБ — так звані «окопні» або «польові», призначені для захисту окремих бойових позицій, транспортних засобів і підрозділів на тактичному рівні. Їх поява стала прямою відповіддю на масове застосування FPV-дронів і БПЛА, що несуть скидальні боєприпаси.

Окопні засоби РЕБ являють собою портативні або малогабаритні пристрої направленого чи кругового придушення у частотних діапазонах 433 МГц, 868 МГц, 900 МГц, 2,4 ГГц та 5,8 ГГц — тобто саме тих, що використовуються більшістю комерційних та військових БПЛА для передачі управляючих сигналів і відеопотоку. Фактично такий пристрій створює «купол мовчання» навколо позиції, у межах якого жоден дрон не може отримувати команди оператора або утримувати GPS-прив'язку.

Серед задокументованих зразків цього класу особливої уваги заслуговує розробка рф «Стриж-3», а також компактні носимі комплекси РЕБ, виконаний у форм-факторі, придатному для розміщення у рюкзаку військовослужбовця. «Стриж-3» забезпечує захист особового складу і техніки від FPV-дронів у радіусі до кількох сотень метрів, перекриваючи основні частотні канали управління. Натомість принциповою перевагою рюкзачного форм-фактора є мобільність: боєць зберігає захисний «купол» під час пересування, не прив'язуючись до стаціонарної позиції. Подібні рішення активно виробляються і вдосконалюються як державними підприємствами, так і волонтерськими технологічними спільнотами.

Паралельно розвивається клас бортових систем РЕБ, інтегрованих безпосередньо у броньовану техніку. Встановлення засобів придушення на танки, бойові машини піхоти та бронетранспортери дозволяє захищати техніку від дронів-камікадзе та скидальних боєприпасів безпосередньо у процесі руху та бою. Такі системи, на відміну від окопних глушників, живляться від бортової мережі машини і здатні перекривати більш широкий частотний спектр із більшою потужністю випромінювання. Документальні свідчення фіксують встановлення подібних комплексів на танки Т-72, Т-80 та Т-90 з обох сторін конфлікту, хоча конструктивні рішення суттєво різняться.

Показово, що значна частина окопних засобів РЕБ з обох сторін виготовляється в умовах, наближених до кустарних або дрібносерійних: на базі доступних SDR-модулів (Software Defined Radio), підсилювачів потужності та спрямованих антен. Це свідчить про демократизацію РЕБ як такої: технологія, що ще десятиліття тому була прерогативою провідних оборонних концернів, сьогодні відтворюється у гаражних майстернях і волонтерських лабораторіях.

Україна розробила і впровадила ефективні контрзаходи: зміну частотних профілів каналів управління (ППРЧ— стрибкоподібну зміну частоти), застосування оптоволоконних ліній зв'язку для операторів FPV-дронів, а також алгоритми інерційної навігації та комп'ютерного зору, що дозволяють дрону зберігати траєкторію в умовах повного придушення GPS. Виникнення

протистояння РЕБ/контр-РЕБ сформувало самостійний технологічний цикл, у якому кожна інновація однієї сторони викликає адаптацію іншої впродовж тижнів, а не місяців, як це спостерігалося у попередніх конфліктах [6].

Оптоволоконні FPV-дрони заслуговують на окрему увагу як радикальне вирішення проблеми РЕБ. Замість радіоканалу управління — який може бути придушений — вони використовують тонкий волоконно-оптичний кабель, що розмотується у польоті. Оскільки оптоволокно є діелектриком і не випромінює електромагнітного сигналу, жоден засіб РЕБ традиційного типу не здатний перехопити або придушити канал управління. Ця технологія, раніше відома виключно у контексті протитанкових керованих ракет, була творчо адаптована для ударних дронів. Її поширення фактично знецінює значну частину інвестицій у традиційний РЕБ-захист, змушуючи шукати альтернативні методи протидії — зокрема, фізичне знищення оператора або кінетичний перехват дрона.

Принципово важливим є той факт, що GPS-придушення, технічно класифіковане як операція радіоелектронної боротьби, одночасно є кібератакою на навігаційний протокол і стає невід'ємною складовою загальновійськового бою. Цей феномен ілюструє розмивання меж між кіберпростором та фізичним бойовим середовищем — і є одним із ключових концептуальних уроків конфлікту для доктрини кібервійни.

Інформаційні операції (ІО) у досліджуваному конфлікті характеризуються безпрецедентним масштабом, технологічною складністю та тісним зв'язком із кінетичними бойовими діями. З боку рф реалізується комплексна система впливу, що охоплює: мережі фальшивих акаунтів у соціальних мережах (фабрики тролів); синтетичні медіа, зокрема deepfake-відео та аудіозаписи; штучне маніпулювання трендами алгоритмів соціальних платформ; поширення контенту через мережі підконтрольних ЗМІ.

Задокументовані інциденти включають deepfake-відео із зображенням президента України Зеленського, який нібито оголошує капітуляцію (березень 2022 року), а також численні синтетичні аудіозаписи з нібито перехопленими переговорами українського командування. Хоча ці матеріали були спростовані відносно швидко, вони демонструють потенціал синтетичних медіа як інструменту оперативного інформаційного впливу.

Застосування великих мовних моделей (LLM) в інформаційних операціях — тенденція, що посилилась із 2023 року, — дозволяє автоматизувати генерацію пропагандистського контенту адаптованого до лінгвістичних і культурних особливостей цільових аудиторій, масштабувати виробництво дезінформації та знижувати вартість операцій впливу. Генеративний ШІ становить загрозу якісного стрибка в ефективності ІО: за оцінками Belfer Center, вартість створення переконливого пропагандистського контенту знизилася у порядки між 2020 і 2024 роками [7].

У сучасних умовах російсько-українського конфлікту спостерігається активне впровадження штучного інтелекту як ключового інструменту ведення кібервійни, зокрема у сфері інформаційно-психологічних операцій. Штучний інтелект дозволяє автоматизувати процес створення, адаптації та масштабного поширення пропагандистських наративів, забезпечуючи високу персоналізацію впливу на цільову аудиторію. Для розуміння механізмів такого впливу пропонується концептуальна модель технологій кібервійни, яка відображає взаємозв’язок між даними навчання, архітектурою моделі, механізмами генерації контенту, системами контролю та результатами маніпулятивного впливу на поведінку користувачів.



Рис. 1. Концептуальна модель технологій кібервійни у російсько-українському конфлікті

Безпілотні авіаційні системи (БАС) відіграють ключову роль у досліджуваному конфлікті, реалізуючи перехрестя між конвенційним озброєнням та кіберзасобами. Їх застосування охоплює розвідку й цілевказання, ударні функції, ретрансляцію зв'язку, радіоелектронну розвідку та РЕБ. Характерною рисою конфлікту є масштабне використання комерційних споживчих квадрокоптерів (DJI Mavic, Autel) та їхніх модифікованих версій для бойових завдань.

Кіберзмагання навколо БАС формують окремий фронт протистояння. Захоплення українських БАС за допомогою глушіння та підміни GPS-сигналу (GPS spoofing) стало однією з перших задокументованих операцій цього роду в реальному конфлікті. Водночас Україна розробила інструментарій протидії: програмне забезпечення для виявлення та класифікації ворожих дронів за електромагнітними сигнатурами, системи перехоплення управління (так звані «кіберрушниці»), апаратні реалізації атак на протоколи управління (MAVLink, DJI OcuSync).

Сучасні бойові БПЛА еволюціонували від дистанційно керованих платформ із людиною в контурі управління до напівавтономних систем, у яких штучний інтелект виконує переважну частину когнітивної роботи, залишаючи оператору лише функцію кінцевого санкціонування удару. Ця архітектура отримала усталену назву «людина на контурі» (Human-on-the-Loop, HOTL) на противагу традиційній «людина в контурі» (Human-in-the-Loop, HITL). Принципова відмінність полягає у тому, що у HOTL-схемі система діє автономно, але оператор зберігає право втручання і підтвердження фінального рішення, тоді як у HITL людина санкціонує кожен окремий маневр.

Практична логіка переходу до HOTL-архітектури у бойових умовах продиктована фізичними обмеженнями: у середовищі активного РЕБ канал зв'язку між оператором і дроном може деградувати або повністю обриватися. Система, що повністю залежить від радіокоманд оператора, у такому середовищі стає недієздатною. Система з вбудованим ШІ здатна продовжувати виконання місії навіть при повній втраті зв'язку, повертаючись до оператора лише у вузловій точці підтвердження удару — якщо канал до того моменту відновиться, або ухвалюючи рішення автономно у крайньому випадку відповідно до заздалегідь заданих правил залучення.

Центральним компонентом ШІ-систем наведення є модуль комп'ютерного зору, що виконує в реальному часі сегментацію та класифікацію об'єктів у відеопотоці з камери дрона. Нейронні мережі архітектури YOLO (You Only Look Once) та їх похідні — YOLOv8, YOLOv9 — набули особливого поширення завдяки поєднанню високої швидкості обробки з прийнятною точністю розпізнавання. На сучасному апаратному забезпеченні (NVIDIA Jetson Orin, Hailo-8) такі мережі здатні обробляти відеопотік із частотою 30–60 кадрів на секунду безпосередньо на борту дрона без передачі даних на наземну станцію.

Навчання моделей розпізнавання цілей у контексті досліджуваного конфлікту здійснюється на масивах даних, сформованих із тисяч годин відеозаписів бойових вильотів FPV-дронів, оприлюднених у відкритих джерелах — Telegram-каналах, YouTube та спеціалізованих ресурсах. Цей масив є унікальним у своєму роді: жоден попередній збройний конфлікт не генерував настільки великого і публічно доступного корпусу анотованого відеоматеріалу бойових зіткнень. Зразки навчальної вибірки включають танки, бойові машини піхоти, бронетранспортери, вантажні автомобілі, польові укріплення, живу силу та артилерійські системи у різних умовах освітлення, пори року та кутах огляду.

Модель, навчена на подібному масиві, здатна з прийнятною точністю ідентифікувати клас цілі, оцінити її орієнтацію та спрогнозувати точку найбільш ефективного ураження — наприклад, моторний відсік танка або вентиляційну решітку бойового відділення. Деякі розробки йдуть далі, інтегруючи теплові сигнатури з інфрачервоних камер для виявлення техніки з працюючим двигуном у темряві або під маскувальними сітями.

Технологія автономного донаведення, відома у виробничих колах як «lock-on after launch» або «захоплення та супровід цілі», функціонує за таким принципом: оператор у ручному режимі виводить дрон у зону видимості цілі, після чого активує режим автономного захоплення. Система ШІ ідентифікує ціль у кадрі, оператор підтверджує вибір натисканням кнопки, і надалі дрон самостійно утримує ціль у центрі кадру та коригує траєкторію польоту для компенсації відносного руху цілі, власного дрейфу та впливу вітру. Оператор у цей момент може спостерігати за ситуацією і в будь-який момент перервати атаку або підтвердити удар.

Практична цінність цього підходу виняткова в умовах активного РЕБ: навіть якщо сигнал управління деградує до нуля після захоплення цілі, дрон продовжує наводитися автономно. Таким чином подавлення радіоканалу, що раніше гарантовано зривало атаку, може перестати бути ефективним контрзаходом. Системи донаведення цього класу задокументовані у використанні ЗСУ та вже стали предметом відкритих тендерів Міністерства оборони України.

Деякі реалізації ідуть ще далі, реалізуючи повністю автономний режим: дрон самостійно виявляє ціль заданого класу у полі зору, захоплює її і уражає без жодної взаємодії з оператором. Такі системи у доктринальному розумінні перетинають поріг летальних автономних систем озброєнь (LAWS), і їх застосування залишається предметом гострої міжнародно-правової дискусії.

Окрім розпізнавання цілей та донаведення, ШІ виконує функцію планування маршруту з урахуванням даних про зони РЕБ, розташування засобів ППО, рельєфу місцевості та часових вікон

зниженої активності систем виявлення. Алгоритми, засновані на методах навчання з підкріпленням (Reinforcement Learning), здатні генерувати оптимальні маршрути прольоту у реальному часі, адаптуючись до змін обстановки — наприклад, виявлення нового засобу ППО або активації глушника у певному секторі.

Роєві алгоритми, що координують одночасний політ групи БПЛА, є наступним рівнем складності. У роєвій атаці дрони розподіляють ролі між собою: одні виконують функцію розвідки та ретрансляції цілевказання, інші — удару по різних секторах цілі одночасно. Координація відбувається через mesh-мережу між вузлами рою з мінімальною залежністю від наземної станції. Задокументовані прецеденти роєвих атак у досліджуваному конфлікті свідчать про перехід від концепції до реального бойового застосування.

Реалізація описаних можливостей вимагає достатньої обчислювальної потужності при жорстких обмеженнях масогабаритних характеристик. Рішенням стало застосування спеціалізованих нейромережевих прискорювачів. NVIDIA Jetson Nano та Jetson Orin NX забезпечують продуктивність від 21 до 275 TOPS (трильйонів операцій за секунду) при споживанні від 5 до 25 Вт і масі менше 100 г. Модуль Hailo-8, ще компактніший, забезпечує 26 TOPS при споживанні близько 2,5 Вт, що дозволяє інтегрувати його навіть у дрони вагою менше кілограма.

Таким чином, технологічний бар'єр для розгортання бойового ШІ на малогабаритних платформах суттєво знизився: те, що декілька років тому було доступне лише у великих ударних БПЛА вартістю мільйони доларів, сьогодні реалізується у платформах вартістю кілька тисяч доларів. Це є фундаментальною зміною технологічного ландшафту кібер-фізичної зброї.

Збереження людини «на контурі» є не лише технічним, а й правовим і етичним вибором. Міжнародне гуманітарне право вимагає дотримання принципів розрізнення (розмежування комбатантів і цивільних), пропорційності та запобіжних заходів. Делегування рішення про летальний удар автономній системі ставить під сумнів можливість виконання цих вимог і встановлення правової відповідальності. Саме тому концепція HOTL, де людина-оператор зберігає право остаточного санкціонування, є спробою зберегти юридичну та моральну відповідальність за ударом при одночасному використанні всього спектра можливостей ШІ для підготовки цього рішення.

Проте на практиці межа між «людина підтверджує» і «людина лише не заперечує» розмивається під тиском бойових умов: висока швидкість розвитку ситуації, фізична та когнітивна втома оператора, скорочення часових вікон для прийняття рішення — усі ці фактори фактично делегують дедалі більше рішень автономній системі навіть там, де формально зберігається контроль людини. Цей феномен є одним із найгостріших концептуальних викликів, що порушує досліджуваний конфлікт для міжнародного права і доктрини кібервійни.

OSINT (Open Source Intelligence) — розвідка на основі відкритих джерел — у досліджуваному конфлікті набула ролі повноцінного інструменту стратегічного значення. Спільноти OSINT та сотні незалежних дослідників використовують методи геолокації фотографій і відеозаписів, аналізу супутникових знімків, відстеження рухів техніки за геотегами соціальних мереж та моніторингу радіоперехоплень для відновлення картини бойових дій у реальному часі.

Особливе значення мають комерційні супутникові системи спостереження: Planet Labs, Maxar та BlackSky забезпечують знімки з роздільною здатністю до 30 см, що дозволяє відстежувати переміщення бронеколон, виявляти позиції артилерії та документувати наслідки ударів. Доступність комерційних знімків суттєво демократизує стратегічну розвідку, традиційно монополізовану державними акторами.

На підставі виявлених закономірностей і темпів технологічного розвитку можна сформулювати обґрунтований прогноз щодо технологій кібервійни на горизонті 2025–2035 років.

Автономні кіберагенти стануть однією із технологій майбутнього, про яку варто збирати дані вже зараз. Перехід від статичного шкідливого програмного забезпечення до автономних агентів, здатних самостійно ухвалювати рішення щодо вибору мішені та методу атаки на основі моделей машинного навчання, є найбільш прогнозованою трансформацією. Прецедентом є вже задокументовані примітки ознаки автономної поведінки у Stuxnet та деяких wiper-програмах. На горизонті 5–7 років очікується поява автономних систем, здатних адаптуватися до захисних заходів у режимі реального часу [8].

Великі мовні моделі та мультимодальні системи штучного інтелекту радикально знизять вартість і підвищать якість продукції інформаційних операцій. Gartner прогнозує, що до 2027 року до 90% контенту в соціальних мережах на конфліктних тематиках генеруватиметься автоматизованими системами. Протидія цьому потребуватиме детекторів синтетичного контенту, криптографічної атрибуції та нових регуляторних режимів.

Квантові комп'ютери критичної потужності (понад 4000 логічних кубітів) можуть стати реальністю на горизонті 2030–2035 років, що поставить під загрозу значну частину сучасної PKI-інфраструктури. NIST вже завершив стандартизацію пост-квантових алгоритмів (CRYSTALS-Kyber, CRYSTALS-Dilithium), однак темпи оновлення інфраструктури суттєво відстають від прогнозованих темпів розвитку квантових обчислень.

Подальша конвергенція безпілотних авіаційних систем, наземних робототехнічних комплексів та морських платформ із кіберзасобами

призведе до формування єдиного кіберфізичного домену бойових дій, у якому розмежування між кіберопераціями і конвенційними бойовими діями стане умовним. Протидія засобам РЕБ і кіберстійкість автономних платформ стануть ключовими вимогами до систем озброєння.

Досвід атак на SolarWinds (2020) та Kaseya (2021) показав ефективність компрометації постачальників програмного забезпечення як вектора проникнення у захищені мережі. У воєнному контексті атаки на ланцюжки постачання програмного забезпечення, мікроелектроніки та вбудованих систем стануть стратегічним пріоритетом і вимагатимуть переосмислення концепцій управління ризиками ланцюжків постачання на рівні держав.

На рисунку 2 представлено концептуальну модель технологічної архітектури кібервійни у російсько-українському конфлікті, що відображає ієрархічну структуру та взаємозв'язки між основними доменами кіберпротистояння. Модель охоплює чотири функціональні домени першого рівня — деструктивні атаки, операції злому та DDoS, радіоелектронну боротьбу й інформаційні операції — кожен із яких деталізується конкретними інструментами та угрупованнями. Домени другого рівня відображають конвергентні технологічні платформи: безпілотні авіаційні системи з кіберможливостями та ШІ-системи наведення, що функціонують у взаємодії та спираються на дані кіберрозвідки й OSINT. Усі зазначені складові зрештою утворюють єдиний феномен кіберфізичної конвергенції — розмивання меж між кіберпростором і фізичним бойовим середовищем, — наслідком якого є системний вплив на об'єкти критичної інфраструктури. Нижній рівень моделі фіксує три прогнозовані вектори розвитку технологій кібервійни на горизонті 2025–2035 років, що випливають із закономірностей, виявлених у досліджуваному конфлікті.

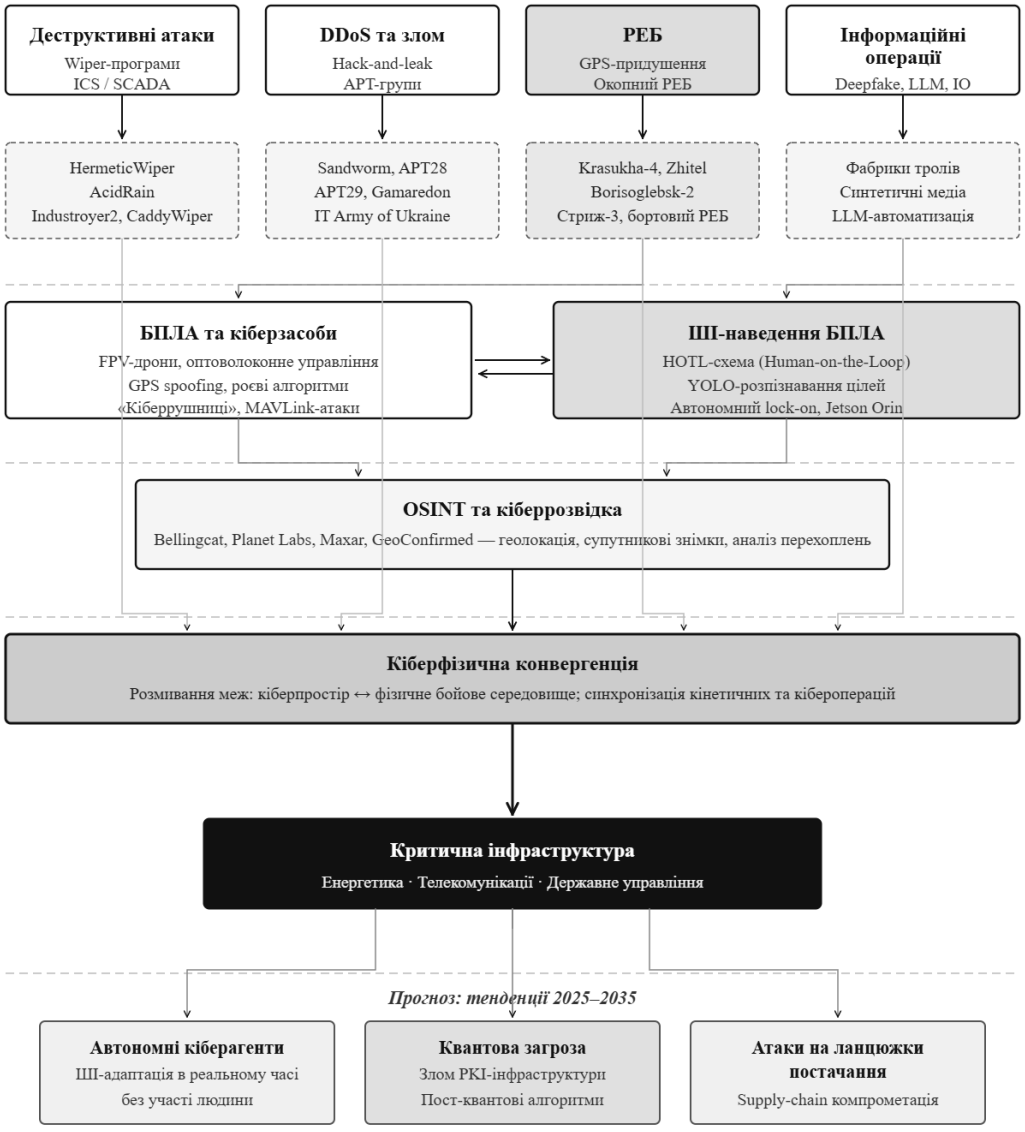


Рис. 2. Концептуальна модель технологій кібервійни у російсько-українському конфлікті

© Muzychenko K.M., Petryk V.M. Cyberwarfare Technologies on the Battlefield of the Russian-Ukrainian Conflict. // Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 36-43. © This is an open access article under the CC BY 4.0 International license.

Висновки

Проведений аналіз дозволяє сформулювати ряд узагальнень, що мають наукове і прикладне значення. По-перше, російсько-український конфлікт підтверджує гіпотезу про формування кіберпростору як повноцінного домену збройної боротьби зі своєю операційною логікою, але спростовує ранні апокаліптичні прогнози щодо вирішальної ролі кіберзброї: кіберзасоби посилюють і підтримують конвенційні операції, але не замінюють їх.

По-друге, технологічна гнучкість обох сторін — і насамперед України — вражає. Асиметрична кіберпотенція долається через залучення глобальної спільноти, масове використання комерційних інструментів і технологій OSINT, а також через швидкі інноваційні цикли, стимульовані реальними бойовими умовами.

По-третє, конфлікт унаочнив, що кіберзахист критичної інформаційної інфраструктури є невід'ємною складовою обороноздатності держави. Успішна відбивна стратегія України — при суттєвій асиметрії наступальних кіберпотенціалів — свідчить про важливість заздалегідь підготовленої архітектури захисту, партнерства з технологічним сектором та оперативного обміну інформацією про загрози.

По-четверте, розмивання меж між кібервійною та інформаційними операціями, між кіберзасобами та радіоелектронною боротьбою вимагає перегляду традиційних класифікаційних схем і розробки нових концептуальних моделей для дослідження кіберконфліктів.

Практичне значення результатів дослідження полягає у їх застосуванні для вдосконалення доктринальних документів у сфері кібербезпеки та інформаційної безпеки, планування заходів із захисту критичної інфраструктури, а також для підготовки фахівців у відповідних галузях.

Література

[1] Devost M. Russian Cyber Operations in Ukraine: A Strategic Assessment / M. Devost // Journal of Cyber Policy. – 2022. – Vol. 7, No. 2. – P. 155–172.
[2] Cherepanov A. Industroyer2: Industroyer reloaded / A. Cherepanov, R. Lipovsky // ESET White Paper. – 2022. – 22 p.
[3] Polityuk P. Cyberattack on Kyivstar: Impact and Attribution / P. Polityuk // Reuters Investigates. – 2024. – 18 p.
[4] Slayton R. What Is the Cyber Offense-Defense Balance? / R. Slayton // International Security. – 2017. – Vol. 41, No. 3. – P. 72–109.
[5] Microsoft. Microsoft Digital Defense Report 2024. – Redmond: Microsoft Corporation, 2024. – 134 p.
[6] Watling J. The Ukrainian Art of War / J. Watling, N. Reynolds. – London: RUSI, 2023. – 48 p.
[7] Belfer Center. AI and the Future of Information Operations. – Cambridge: Harvard Kennedy School, 2024. – 62 p.
[8] Kello L. The Virtual Weapon and International Order / L. Kello. – New Haven: Yale University Press, 2017. – 336 p.
[9] RAND Corporation. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. – Santa Monica: RAND, 2023. – 210 p.
[10] CyberPeace Institute. Cyber Dimensions of the Armed Conflict in Ukraine. – Geneva: CyberPeace Institute, 2024. – 88 p.

УДК 355.4:004.7:623.4

Muzychenko K.M., Petryk V.M. **Cyberwarfare Technologies on the Battlefield of the Russian-Ukrainian Conflict.**

Abstract. The article examines cyberwarfare technologies in the context of the full-scale phase of the Russian-Ukrainian armed conflict. The study analyzes the main categories of cyber weapons employed: destructive wiper malware, attacks on industrial control systems, DDoS operations, hack-and-leak campaigns, electronic warfare, and information operations including AI-assisted disinformation. The article addresses the integration of cyber tools with conventional military operations (cyber-physical convergence), the role of large language models in information operations, and the weaponization of commercial unmanned aerial systems. Scientific novelty consists in a comprehensive systemic analysis of cyberwarfare tools as applied in a real armed conflict serving as a proving ground for next-generation warfare technologies. A forecast of cyberwarfare technology development trends for the coming decade is formulated.

Keywords: cyberwarfare, information security, cyber weapons, wiper attacks, DDoS, APT groups, information operations, disinformation, electronic warfare, artificial intelligence in cyberwarfare, cyber intelligence, critical infrastructure protection.

МУЗИЧЕНКО Кирило Миколайович*, Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації.*
MUZYCHENKO Kyrylo Mykolayovych*, State Scientific and Research Institute of Cybersecurity Technologies and Information Protection.*

ПЕТРИК Валентин Михайлович*, к. н. з держ. управл., доцент, кафедри кібербезпеки, Національний університет «Київський авіаційний інститут».*
PETRYK Valentyn Mykhailovych*, PhD in Public Administration, Associate Professor, Department of Cybersecurity, National university «Kyiv Aviation Institute».*

Дата надходження:	Дата прийняття:	Дата публікації:
14.07.2026	03.08.2026	21.08.2026