

Яковюк Іван Васильович

*доктор юридичних наук, професор, професор кафедри
права Європейського Союзу Національного юридичного
університету імені Ярослава Мудрого,
завідувач сектором НДІ державного будівництва
та місцевого самоврядування НАПрН України
ORCID 0000-0002-8070-1645*

Новіков Євген Андрійович

*кандидат юридичних наук, науковий співробітник, НДІ правового
забезпечення інноваційного розвитку НАПрН України*

Купрійова Олександра Олегівна

*провідний фахівець науково-дослідницького сектору,
Національний юридичний університет імені Ярослава Мудрого*

**СУЧАСНІ ТЕХНОЛОГІЇ ТА ЇХ РОЛЬ У ЗАБЕЗПЕЧЕННІ
БЕЗПЕКИ УКРАЇНСЬКОЇ ДЕРЖАВИ І СУСПІЛЬСТВА
ПІД ЧАС РОСІЙСЬКОЇ АГРЕСІЇ**

Наукова робота присвячена вивченню проблем забезпечення національної безпеки в умовах російської агресії, зокрема ведення цифрових війн. Цифрові технології трансформують управління безпекою, створюючи нові ризики та можливості. Цифровізація пропонує суб'єктам безпеки нові джерела збору доказів злочинів, вчинених російською армією, інструменти для збору та аналізу даних, а також забезпечує ефективне та стабільне функціонування цифрового уряду, органів державної влади та безпеки, сприяє забезпеченню прав громадян в умовах воєнного стану та післявоєнний період.

Ключові слова: національна безпека, технологічна безпека, технології, цифрова держава, цифрова війна, «Дія», військовий стан, повоєнний період, Україна.

Yakoviyk Ivan

*Doctor of Law, Full Professor, Head of Department, Research Institute of State Building and Local Self-Government of the National Academy of Legal Sciences of Ukraine, Professor of the European Union Law Department,
Yaroslav Mudryi National Law University*

Novikov Eugene

PhD, Researcher of Scientific of the Scientific and Research Institute of Providing Legal Framework for the Innovative Development of NALS of Ukraine

Kupriiova Olexandra

*leading specialist of the scientific-research sector,
Yaroslav Mudryi National Law University*

**MODERN TECHNOLOGIES AND THEIR ROLE IN ENSURING THE
SECURITY OF THE UKRAINIAN STATE AND SOCIETY DURING
RUSSIAN AGGRESSION**

The research paper is devoted to the study of the problems of ensuring national security in the context of Russian aggression, in particular, the conduct of digital warfare. Digital technologies are transforming security management, creating new risks and opportunities. Digitalization offers security actors new sources of collecting evidence of crimes committed by the Russian army, tools for collecting and analyzing data, and ensures the effective and stable functioning of digital government, public authorities and security agencies, and contributes to the protection of citizens' rights under martial law and in the post-war period.

Keywords: national security, technological security, technology, digital state, digital warfare, Diia, martial law, post-war period, Ukraine.

Розв'язуючи агресію проти України країна-агресор покладалася на кількісні показники своєї переваги – в два рази більше чисельність армії та десятикратна різниця у воєнному бюджеті. Не дивно, що не тільки російське керівництво, але й спецслужби союзників України відводили від декілька днів

до кількох тижнів на завершення воєнної кампанії, яка мала завершитися поразкою Києва. Єдине, в чому Україна не поступалася, а навіть випереджала рф, це сучасні технології та ІТ-сфера¹⁰.

У перші дні свого президентства навесні 2019 р. В. Зеленський назвав цифровізацію національним пріоритетом та пообіцяв створити «країну у смартфоні». Вплив політики цифровізації став очевидним з перших днів війни. Одразу після початку агресії український уряд завершив процес завантаження найважливішої інформації в хмару з метою її захисту і забезпечення стабільного функціонування органів державної влади, безпекового сектору і держави в цілому на випадок, якщо внаслідок ракетних обстрілів будуть зруйновані відповідні будівлі¹¹, а в наслідок кібератак – порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем¹².

Надзвичайно важливого значення в умовах війни набуло стабільне і ефективне функціонування цифрової держави та цифрового уряду України¹³. Важливу роль в цьому відіграє «Дія» – мобільний додаток та онлайн-портал, який допомагає українцям користуватися низкою державних служб за допомогою своїх смартфонів. «Дія» розроблена Міністерством цифрової трансформації України за підтримки USAID, яка інвестувала 8,5 млн. доларів у розширення послуг програми під час війни.

¹⁰ Так, за статистичними даними за 10 місяців 2022 р. експорт ІТ-послуг зріс на 9,9 % порівняно з минулим роком і приніс понад \$6 млрд. виручки, перевищивши показник 2021 р. на \$542 млн, хоча загальний експорт українських ІТ послуг знизився на 10,8 %. Експорт ІТ-послуг залишається однією з небагатьох сфер української економіки, яка продовжує процвітати навіть в умовах російської агресії.

¹¹ Уже в перші дні війни російська військова авіація здійснила ракетний обстріл і зруйнувала будівлі обласних державних адміністрацій, обласних управлінь Служби безпеки України і Міністерства внутрішніх справ України областей на Півночі, Сході і Півдні України, які вони намагалися захопити.

¹² За день до початку агресії росії проти України, кібератаки стали прелюдією до повномасштабної війни. Комп'ютерні системи українських міністерств, інших органів державної влади та банків стали об'єктами розподілених атак типу «відмова в обслуговуванні» (DDoS).

¹³ «Дія» була запущена в 2022 р. На кінець 2022 р. останню версію мобільного додатку «Дія» використали майже 18,5 млн осіб, а це більше половини дорослого населення України.

«Дія» – це додаток, який спочатку був розроблений для спрощення бюрократії¹⁴, після початку російської агресії український уряд перепрофілював для потреб воєнного часу. Успіх програми електронного управління «Дія», що використовується в Україні, став предметом обговорення на щорічній зустрічі Всесвітнього економічного форуму в Давосі (2023 р.). Слід зазначити, що в умовах російської агресії продовжується процес гармонізації України з Єдиним цифровим ринком ЄС (куратором проекту виступає Естонська Академія електронного управління¹⁵), що забезпечує реалізацію відповідних положень Угоди про асоціацію між Україною і ЄС. Європейський Союз зі свого боку використовує європейський проект під управлінням ФПАРР «Підтримка ЄС електронного уряду та цифрової економіки в Україні» EU4DigitalUA у співробітництві з Міністерством цифрової трансформації України продовжує сприяти розбудові цифрової держави для всіх українців.

Хоча розробники «Дія» роблять основний акцент на впровадженні нових функцій і подальший розвиток сервісів насамперед для українців, він представляє собою технологічний продукт, а насправді комплекс технологічних продуктів (Trembita, державні реєстри, цифрова ідентифікація, електронні послуги та ін.), зацікавленість в якому проявила низка держав Європи і Азії. В даний час USAID ініціює переговори з іншими країнами щодо потенційного використання аналогів «Дія» для розвитку систем електронного уряду, оскільки її тиражування в інших демократичних країнах буде корисним для модернізації доступу до послуг, економічного зростання та прозорості уряду.

Український технологічний продукт стає дедалі цікавішим для експорту. Вартість кожного окремого компонента «Дії» може досягати десятків мільйонів доларів. Варто зазначити, що продавати можна не тільки сам технологічний продукт, але і супроводжуючі його послуги (експертиза, консультації тощо). викликав зацікавленість в країнах Європи і Азії. Так, Естонське управління

¹⁴ «Дія» поєднує в собі мобільний додаток з доступом до цифрових документів та єдиний портал державних послуг як для населення, так і бізнесу. Його основна мета – зробити 100 % державних послуг доступними онлайн. У 2021 р. Україна стала першою країною з цифровим посвідченням особистості, яке можна використовувати на всій території країни.

¹⁵ Естонія та Україна підписали у Києві угоду про співпрацю для сприяння обміну досвідом у галузі цифрової трансформації.

інформаційних систем і українське агентство «Дія» повинні провести в Естонії розробку пілотного проекту з розробки національного мобільного додатка на основі додатка «Дія». Українські ІТ-фахівці вважають, що хоча Україна зараз залежить від технологічної допомоги США, до кінця війни ми вже продаватимемо програмне забезпечення для американської компанії Palantir. Це й не дивно, оскільки війна зазвичай дає поштовх суспільству до мобілізації зусиль, що згодом призводить до бурхливого розвитку технологій та інновацій.

Ще вторгнення росії в Україну в 2014 р. спровокувало появу військових інформаційних технологій як одного з найперспективніших напрямків. З того часу кількість військових ІТ-ініціатив в Україні поступово збільшується. Сьогодні Збройними Силами України використовується близько десятка найпоширеніших програм та додатків: Крапива, MilChat, Delta, ГісАрта, Термінал, ComBat Vision, Віраж Планшет та багато іншого. Експлуатаційні випробування у реальних бойових умовах роблять вказані українські розробки унікальними, цінними та затребуваними союзниками України.

Під час російської агресії, розв'язаної у 2022 р., українці продемонстрували неймовірну спритність, створюючи нові ефективні електронні послуги у найкоротші строки. Так, вже 1 березня 2022 р. у додатку з'явився eDocument – тимчасовий цифровий документ на період військового стану, який є посвідченням особи для тих, хто втратив фізичну версію паспорта. Того ж дня почав діяти додаток «Сигналізація повітряної тривоги» (за перший тиждень його завантажили понад 2 мільйони користувачів). Згодом з'явилася можливість через «Дію» зареєструвати факт майнових збитків від війни для отримання компенсації від держави. У квітні 2022 р. з'явилась можливість отримання одноразових виплат для підприємців із регіонів, які найбільше постраждали від вторгнення росії; згодом – подати заявку на набуття статусу внутрішньо переміщеної особи та фінансової допомоги онлайн; для мешканців тимчасово окупованих територій та регіонів з активними бойовими діями – оформити статус безробітного та отримувати щомісячну допомогу; проект eWork на гранти від держави на розвиток бізнесу.

Слід виділити військово-технічні системи, створені Україною самостійно. На особливу увагу заслуговує розроблений Центром інновацій та розвитку оборонних технологій Міністерства оборони України та Аеророзвідкою платформа і сервіси «Delta», яку розглядають як найпривабливішу сучасну українську інновацію. Вона побудована відповідно до стандартів НАТО, а тому є сумісною з аналогічними системами країн-членів Альянсу. Показово, що в експертній спільноті НАТО вона, як і раніше, вважається унікальною розробкою, яка пройшла апробацію у реальних бойових умовах. «Delta» представляє собою удосконалену цифрову мапу, що забезпечує військовим ситуаційну поінформованість. Протягом 2022 р. система «Delta» мала більше 30 релізів нових функцій для адаптації системи до поточних потреб ЗСУ. Сьогодні до неї також входять чат-боти eVorog¹⁶, розроблений Мінцифри, та STOP Russian War – СБУ, які є аналогами громадянської розвідки.

MilChat – це безпечний додаток для обміну повідомленнями, яким користуються близько 600 000 військових ЗСУ. Додаток також дозволяє обмінюватися даними тактичної обстановки, визначати координати, визначати азимут та передавати дані геолокації.

Слід також згадати чат-бот eEnemy Telegram, які дозволяє користувачам відправляти геолокацію, фото та відео ворожої техніки з можливістю опису побаченого у тексті. У квітні у бота eEnemy Telegram з'явилася функція повідомляти про окупантів, причетних до геноциду в Бучі, Ірпені та Гостомелі з можливістю надіслати фото чи відео військових злочинців та надати їх дані; в серпні було додано функцію повідомлення місцезнаходження вибухонебезпечних предметів, завдяки чому громадяни України змогли допомогти саперам у знешкодженні мін, снарядів та бомб, залишених окупантами. Перевагою цього бота є обов'язкова авторизація через «Дія», завдяки чому саботажники не зможуть спамити фейковими фото чи відео.

У комерційних постачальників були придбані системи: «Армія дронів» - для використання у повітряній розвідці, та система картографування поля бою

¹⁶ З моменту запуску чат-боту eVorog громадянами надано понад 453 000 звітів.

«Delta», яка містить фактичні дані в режимі реального часу, завдяки чому військові можуть відповідно планувати свої дії.

Українська ІТ-армія¹⁷ блокують онлайн-ресурси країни-агресора, завдяки чому вдається розхитати важливі сфери життєдіяльності росії. Крім того, українська ІТ-армія протистоїть створеним у березні 2022 р. «Кібер фронту Z» та наприкінці січня 2023 р. – «Цифровій Армії Росії». Якщо основна форма діяльності ІТ-армії – це створення та розкрутка різноманітних петицій (наприклад, вимоги до транснаціональних корпорацій припинити ведення бізнесу в рф, заборона участі російських спортсменів до змагань тощо) спрямованих на міжнародну ізоляцію росії, то метою «Цифрової Армії Росії» є психологічний вплив на українське суспільство аби викликати демотивуючі емоції (зневіра, туга; паніка, страх; відчуття безсилля та усвідомлення, що ти нічого не можеш змінити; відчуття зради; відчуття марності та непотрібності), які змушують здатися.

29 березня 2022 р. волонтерський проект TacticMedAid запусив мобільний навчальний додаток, що містить базові рекомендації щодо надання першої допомоги, та працює в автономному режимі. Воно складається з двох розділів: цивільна частина спрямована на зупинку кровотечі; функція для військових включає пояснення алгоритмів різних поширених видів травм та поранень у бойових діях.

5 травня 2022р. президентом України В. Зеленським була запущена глобальна ініціатива United 24 зі збору коштів для підтримки України. Його першою частиною стала платформа для збору коштів, де одним кліком можна було пожертвувати кошти на три напрями допомоги (оборона та розмінування, гуманітарна та медична допомога та відновлення України). Таке державно-приватне партнерство є одним із ключів до успіху України під час війни.

¹⁷ ІТ-армія – це співтовариство ІТ-фахівців, створене наприкінці лютого 2022 р. з метою нейтралізації ворога в інформаційному та кіберпросторі. До її складу входять понад 300 тис. українських та іноземних волонтерів. Щоб вступити до її лав, фахівцям достатньо приєднатися до офіційного телеграм-каналу армії та дотримуватись інструкцій. До завдань учасників ІТ-армії входить мінімізація шкоди від кібер-атак ворогів на українські інтернет ресурси та протидія російській брехні у всесвітній мережі.

Таким чином в цілому українська комунікаційна інфраструктура під час агресії була не лише збережена, але й суттєво розвинута і зміцнена.

Крім того, слід зазначити, що українські військові виявилися здатними швидко опанувати зброю, надану західними союзниками, і яка була створена і функціонувала на передових інноваційних технологіях. Таким чином технологічні інновації допомогли Україні компенсувати військову перевагу росії у звичайних озброєннях. Російсько-українське протистояння наочно довело, що високотехнологічні системи озброєння суттєво збільшують воєнну могутність армії, нові платформи і стандарти, на яких вони засновані, забезпечують економічні важелі, а передові дослідження та технології не лише підвищують глобальну привабливість і конкурентоспроможність на ринку, але забезпечують ефективність.

Україна має перевагу, яка полягає у використанні можливостей Starlink. Росія намагалася створити власні електронні засоби бою, але безуспішно, оскільки прагнули використати комерційні супутникові дані та потокове відео з недорогих китайських дронів. При цьому у них виникли труднощі з координацією та обміном цими даними між підрозділами. Тоді як кожен український батальйон має свого розробника програмного забезпечення. З цього приводу слід зазначити, що в сучасному українському військовому ІТ-секторі переважають приватні та волонтерські ініціативи. Це забезпечує гнучкість, стимулює ринкову конкурентоспроможність, а тому стимулює подальший розвиток цієї галузі економіки. Але в цьому криються і певні ризики: використання у різних військових частинах різного програмного забезпечення може обернутися його несумісністю.

Отже, поєднання високого бойового духу із досконалим програмним забезпеченням для розвідки та управління боєм дають українським військовим вирішальну перевагу.