УДК 623.4:004.056

В. О. Варишнюк, О. К. Басараб

НАПРЯМИ ВДОСКОНАЛЕННЯ ЗРАЗКІВ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ З ОГЛЯДУ НА РАДІОЕЛЕКТРОННУ, КІБЕРНЕТИЧНУ ТА ІНФОРМАЦІЙНУ СТІЙКОСТІ

Анотація. *Розглянуто вплив кібернетичних та інформаційних операцій противника на бойове застосування та експлуатацію зразків озброєння та військової техніки. На основі аналізу відкритих джерел і досвіду збройної агресії проти України визначено напрями вдосконалення озброєння та військової техніки, що знижують їхню вразливість до технічних і психологічних впливів: підвищення завадостійкості навігації, зв'язку й управління, зменшення електромагнітного та цифрового сліду, автентифікація команд і даних, підвищення ремонтопридатності, підготовка особового складу.*

Ключові слова: *озброєння та військова техніка; кібернетична стійкість, інформаційна стійкість; радіоелектронна стійкість; завадостійкість; ремонтопридатність.*

Annotation. *The influence of the adversary's cyber and information operations on the combat employment and operation of weapons and military equipment is examined. Based on an analysis of open sources and an assessment of the experience gained from the armed aggression against Ukraine, the main directions for improving weapons and military equipment to reduce their vulnerability to the adversary's technical and information-related effects are identified. These include enhancing the jamming resistance of navigation, communication, and control systems; reducing electromagnetic and digital footprints; ensuring the authentication of commands and data; improving maintainability; and enhancing personnel training.*

Keywords: *weapons and military equipment; cyber resilience; information resilience; electronic warfare resilience; jamming resistance; maintainability.*

Досвід збройної агресії проти України засвідчив, що боєздатність озброєння та військової техніки (далі – ОВТ) визначається не лише їхніми тактико-технічними характеристиками, а й здатністю зразків та їхніх екіпажів функціонувати в умовах активної протидії противника в електромагнітному, кібернетичному та інформаційному просторах. Захист особового складу від інформаційно впливу розглянуто в [1], водночас питання вдосконалення самих зразків ОВТ як складової забезпечення інформаційної та кібернетичної стійкості висвітлено недостатньо.

Мета роботи – визначити основні напрями вдосконалення ОВТ для зниження їхньої вразливості до кібернетичного та інформаційно впливу противника.

Вплив противника на ОВТ здійснюється у двох взаємопов'язаних площинах: технічній та інформаційній.

Технічна площина охоплює радіоелектронне придушення, підміну навігаційних сигналів, перехоплення та спотворення даних. Так, у 2019 р. представник Об'єднаного штабу Збройних Сил України полковник І. Павленко повідомив, що внаслідок підміни супутникових навігаційних сигналів було втрачено майже сотню безпілотників, а радіоретранслятор уражено комп'ютерним вірусом [2]. Згодом ця проблема торкнулася й західних боєприпасів. У квітні 2024 р. представник Пентагону визнав, що розроблений для України наземний варіант авіаційного керованого боєприпасу не забезпечив ураження цілей через застосування російських засобів радіоелектронної боротьби. Експерт Гудзонівського інституту (Hudson Institute) Б. Кларк пояснив такі збої підміною сигналів GPS, яку, за даними видання, Росія застосовує в Україні щонайменше з 2018 року [3]. За його словами, потужні станції радіоелектронної боротьби, призначені насамперед для придушення безпілотників, розміщені вздовж українського фронту з інтервалом 6–9 миль (приблизно 10–14 км) [3]. Подібних висновків дійшли й аналітики Королівського об'єднаного інституту оборонних досліджень (Royal United Services Institute for Defence and Security Studies, RUSI), які, досліджуючи наступальні операції 2022–2023 рр., зазначають, що програмно-визначені системи були критично важливими для забезпечення конкурентоспроможності сил, проте виявилися вразливими до цілеспрямованих

радіоелектронних завад. Зокрема, проти боєприпасів Excalibur і GMLRS противник з часом розробив ефективні контрзаходи [4].

Психологічна площина пов'язана з інформаційним впливом на особовий склад, сутність, форми та способи здійснення якого розкрито в [1].

На підставі аналізу відкритих джерел виокремлено п'ять основних напрямів удосконалення ОВТ.

Перший напрям – підвищення завадостійкості засобів навігації, зв'язку та управління. RUSI наголошує на необхідності посилення електронного захисту військових систем. Своєю чергою, армія США в останні роки спрямувала значні кошти на розвиток засобів радіоелектронної боротьби та навігаційного обладнання, стійкого до завад, зокрема навігаційних приймачів із використанням М-коду GPS (контракт із BAE Systems на суму 318 млн дол. США) [4; 5]. За свідченнями Д. Патта, наданими під час слухань у Конгресі США, ефективність наведення боєприпасу Excalibur в Україні за кілька місяців знизилася із 70 до 6 відсотків [3]. Водночас засіб підміни навігаційного сигналу можна створити з використанням доступних і недорогих радіоелектронних компонентів та відкритого програмного забезпечення, тоді як ракета GMLRS коштує близько 160 тис. дол. США, а снаряд Excalibur – до 100 тис. дол. США [3]. Б. Кларк наголошує, що зазначені боєприпаси проєктувалися в умовах, коли доступних засобів підміни навігаційних сигналів ще не існувало. Мініатюрні та ефективні засоби підміни GPS з'явилися приблизно протягом останнього десятиліття [3]. Це підтверджує необхідність своєчасного перегляду вимог до зразків ОВТ з урахуванням появи нових засобів протидії. Практика засвідчує, що підвищення завадостійкості є цілком реальним. Так, за словами С. Бендетта з американського Державного дослідницького та аналітичного центру (Federally Funded Research and Development Center, FFRDC), представники української промисловості повідомляли про підвищення стійкості до радіоелектронного придушення окремих моделей безпілотників, виготовлених для війська, порівняно з попередніми зразками [2]. З огляду на це, для вітчизняних зразків ОВТ доцільно передбачати навігаційні приймачі із захистом від підміни сигналів, а також резервні канали зв'язку та навігації.

Другий напрям – зменшення електромагнітного та цифрового сліду. За даними видання Military Times, противник мав змогу придушувати мережі GSM на відстані до 20 миль (близько 32 км), визначати місцезнаходження смартфонів, а також використовував безпілотники, обладнані засобами радіопеленгації, для виявлення українських підрозділів. Крім того, російські війська успішно придушували роботу радіолокаційних станцій контрбатарейної боротьби, після чого завдавали ударів по їхніх «засліплених» позиціях [2]. З огляду на це, конструкція та програмне забезпечення ОВТ мають передбачати режими обмеженого випромінювання, засоби маскування радіосигналів, а також механізми контролю зберігання та передавання службової інформації. За оцінкою RUSI, взаємні радіоелектронні перешкоди між своїми підрозділами (фратрицидний вплив в електромагнітному спектрі) стали серйозною проблемою під час управління масштабними операціями. При цьому координація використання частот виключно на рівні військової частини або з'єднання виявилася недостатньо ефективною. Тому виникає потреба в упровадженні механізмів електромагнітного управління безпосередньо на рівні зразків ОВТ [4].

Третій напрям – забезпечення автентифікації команд і даних. Факт ураження радіоретранслятора комп'ютерним вірусом [2] свідчить про те, що канал управління сам може стати об'єктом кібернетичного впливу. Тому доцільно передбачати криптографічну автентифікацію наказів і критично важливих команд, а також перевірку достовірності джерел інформації. Реалізація таких заходів ускладнить підміну команд управління та знизить ризик виконання екіпажами хибних або несанкціонованих розпоряджень.

Четвертий напрям – підвищення ремонтопридатності та забезпечення можливості оперативного оновлення ОВТ. За даними О. Сампіра, під час проведення антитерористичної операції на сході України забезпечення військ озброєнням і військовою технікою в ході бойових дій здійснювалося переважно за рахунок відновлення техніки, що вийшла з ладу [6]. М. Шишанов і А. Веретнов пропонують оцінювати кількісні та якісні показники ремонтопридатності військової автомобільної техніки, а отримані результати використовувати для вдосконалення технологічності конструкції з погляду її ремонту [7]. На нашу думку, вимоги до модульності конструкції, уніфікації вузлів і агрегатів та зручності діагностування необхідно

закладати вже на етапі розроблення ОВТ. Такий підхід узгоджується з рішенням Міністерства оборони України у вересні 2024 р. щодо кодифікації та допуску до постачання рухомих модулів технічного обслуговування, призначених для ремонту озброєння та військової техніки в польових умовах [8]. Дослідження RUSI доповнює цей напрям ще однією важливою вимогою: збереження технологічної переваги передбачає можливість оперативного оновлення систем безпосередньо в польових умовах [4]. Важливим є також забезпечення зворотного зв'язку між військовими користувачами та розробниками ОВТ. Зокрема, директор міжфункціональної команди армії США з питань позиціонування, навігації та часу М. Монтелеоне розглядає досвід використання переданих Україні технологій як джерело інформації для подальшого вдосконалення відповідних систем [5].

П'ятий напрям – удосконалення підготовки особового складу. Навчальні програми та тренажерні комплекси доцільно доповнити методами й прийомами протидії інформаційно-психологічному впливу противника. На необхідності навчання особового складу відповідним методам наголошують і автори дослідження [1]. При цьому підготовка екіпажів має охоплювати не лише технічні аспекти експлуатації ОВТ, а й формування навичок критичного оцінювання отриманої інформації, розпізнавання ознак маніпулятивного впливу та належного реагування на нього.

Отже, протидія кібернетичним та інформаційним операціям противника потребує комплексного підходу, що передбачає закладання вимог до електромагнітної та інформаційної стійкості ОВТ уже на етапах їх розроблення й модернізації, а також реалізацію відповідних організаційних заходів. Зокрема, пропонується включати до тактико-технічних завдань вимоги щодо захисту навігаційних систем від підміни сигналів, резервування каналів зв'язку, реалізації режимів обмеженого випромінювання, автентифікації команд, забезпечення модульності конструкції та можливості оновлення програмного забезпечення в польових умовах. Водночас програми підготовки екіпажів необхідно доповнити розділами, присвяченими протидії інформаційно-психологічному впливу противника. Подальші дослідження доцільно спрямувати на розроблення методик комплексного оцінювання кібернетичної, електромагнітної та інформаційної стійкості зразків ОВТ.

Список використаних джерел:

1. Юзова І. Ю., Пацек П. Інформаційно-психологічний вплив противника та протидія йому в умовах ведення гібридних війн. Наука і техніка Повітряних Сил Збройних Сил України. 2020. № 3 (40). С. 61-68. DOI: https://doi.org/10.30748/nitps.2020.40.07.

2. Snow S. US forces could learn from intense electronic war battle in Ukraine. Military Times. 2019. 30 Oct. URL: https://www.militarytimes.com/flashpoints/2019/10/30/us-forces-could-learn-from-intense-electronic-war-battle-in-ukraine/ (дата звернення: 02.11.2026).

3. Skove S. Another US precision-guided weapon falls prey to Russian electronic warfare, US says. Defense One. 2024. 28 Apr. URL: https://www.defenseone.com/threats/2024/04/another-us-precision-guided-weapon-falls-prey-russian-electronic-warfare-us-says/396141/ (дата звернення: 02.11.2026).

4. Watling J., Danylyuk O. V., Reynolds N. Preliminary lessons from Ukraine's offensive operations, 2022-23. Royal United Services Institute. 2024. 18 July. URL: https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-ukraines-offensive-operations-2022-23 (дата звернення: 02.11.2026).

5. Demarest C. Electronic warfare in Ukraine has lessons for US weapons, navigation. Defense News. 2024. 6 May. URL: https://www.defensenews.com/electronic-warfare/2024/05/06/electronic-warfare-in-ukraine-has-lessons-for-us-weapons-navigation/ (дата звернення: 02.11.2026).

6. Сампір О. Удосконалена методика оцінювання системи відновлення озброєння та військової техніки окремої механізованої бригади. Social Development & Security. 2021. Т. 11, № 5. С. 165-178. DOI: https://doi.org/10.33445/sds.2021.11.5.16.

7. Шишанов М. О., Веретнов А. О. Методичні основи оцінки ремонтопридатності військової автомобільної техніки. Озброєння та військова техніка. 2019. № 2 (22). С. 50-55. DOI: https://doi.org/10.34169/2414-0651.2019.2(22).50-55.

8. Міноборони допустило до експлуатації мобільні майстерні для ремонту озброєння. Міністерство оборони України. 2024. 14 верес. URL: https://mod.gov.ua/news/minoboroni-dopustilo-do-ekspluataczii-mobilni-majsterni (дата звернення: 02.11.2026).

Варишнюк Віталій Олександрович *– курсант Національної академії Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький, вул. Шевченка, 46, інд. 29000, e-mail: vitalijvarisnuk7@gmail.com, ORCID: https://orcid.org/0009-0009-7137-1750*

Басараб Олександр Корнійович *– кандидат технічних наук, доцент, професор кафедри безпілотних систем Національної академії Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький, вул. Шевченка, 46, інд. 29000, e-mail: alexander78.ua@gmail.com, ORCID: https://orcid.org/0000-0002-2852-9534*

Vitalii Varyshniuk *– Cadet, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, 46 Shevchenka St., Khmelnytskyi, 29000, e-mail: vitalijvarisnuk7@gmail.com, ORCID: https://orcid.org/0009-0009-7137-1750*

Oleksandr Basarab *– Candidate of Technical Sciences, Associate Professor, Professor of the Department of Unmanned Systems, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, 46 Shevchenka St., Khmelnytskyi, 29000, e-mail: alexander78.ua@gmail.com, ORCID: https://orcid.org/0000-0002-2852-9534*