УДК 004.056:621.396.9:355.40

Д. І. Прокопович-Ткаченко, В. Т. Оленченко, М. П. Бондаренко

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: МЕТОДИ БОРОТЬБИ З ТАРГЕТОВАНИМИ АТАКАМИ НА ЕЛЕКТРОННІ КОМУНІКАЦІЙНІ СИСТЕМИ СИЛ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

У статті подано комплексний підхід до протидії таргетованим атакам, який охоплює методи кібербезпеки, фізичного захисту обладнання та вдосконалення протоколів електронних комунікації. Запропоновано багаторівневі стратегії захисту від атак типу DDoS, спроб радіоподавлення, фішингових атак та проникнення шкідливого програмного забезпечення. Показано, що запропоновані засоби дозволяють значно знизити ризики успішного проведення таргетованої атаки, підвищити безперебійність функціонування комунікацій та забезпечити належний рівень безпеки інформації. Окреслено напрямки майбутніх досліджень, зосереджених на інтеграції квантово-стійких алгоритмів шифрування, розвитку алгоритмів штучного інтелекту для пошуку прихованих загроз та вдосконаленні методів фізичного захисту електронник комунікаційних систем, зокрема супутникового обладнання Starlink.

Ключові слова: *таргетовані атаки, кібербезпека, сили безпеки і оборони України, криптографічний захист, стрибкоподібне перебудовування частоти, системи зв'язку.*

Постановка проблеми. Сучасні збройні конфлікти характеризуються значною роллю інформаційного та кібернетичного впливу, який охоплює як військову, так і цивільну інфраструктуру. У контексті гібридної війни російської федерації проти України особливе значення набувають таргетовані атаки на електронні комунікаційні системи сил безпеки і оборони України та комунікаційну супутникову мережу Starlink, яка дедалі частіше використовується як критичний канал передачі інформації у воєнний час.

Актуальність цієї теми зумовлена низкою факторів:

– щораз вищою складністю кібератак, що поєднують методи соціальної інженерії, радіоелектронної боротьби та проникнення в закриті мережі для зламу або виведення з ладу систем зв'язку;

– відсутністю уніфікованих стандартів захисту, які б враховували специфіку застосування військових комунікацій у польових умовах та під час бойових дій із застосуванням широкого спектра радіоелектронної боротьби (РЕБ);

– значним ризиком компрометації критичної інформації, яка передається через супутникові та наземні канали. Витік або порушення доступності такої інформації можуть мати стратегічні негативні наслідки.

Аналіз останніх досліджень і публікацій. У науковій літературі [1-4] значна увага приділяється методам криптографічного захисту та виявлення вторгнень, однак комплексні підходи, які синхронізують між собою технічні, організаційні та контррозвідувальні заходи, все ще залишаються недостатньо розробленими.

Порівняно з результатами інших робіт [5-9], у яких основний акцент робиться на суто криптографічних чи суто радіотехнічних аспектах, запропонований підхід передбачає багаторівневу стратегію, що може бути більш дієвою у складних бойових умовах.

Метою статті є формування методики захисту електронних комунікаційних систем сил безпеки і оборони України у контексті сучасних гібридних загроз та оцінка її ефективність.

Виклад основного матеріалу. За методологічну основу дослідження взято комплекс моделей і методів, що включають стохастичні підходи до оцінювання ризиків, адаптивні алгоритми стрибкоподібного перебудовування частоти для протидії радіоподавленню, а також автоматичні системи моніторингу мережі на базі систем керування подіями безпеки SIEM (Security Information and Event Management).

Для досягнення зазначеної мети

були поставлені такі завдання:

– аналіз наявних загроз, враховуючи специфіку DDoS, фішингових та радіоелектронних атак;

– розроблення методів і моделей, що поєднують криптографічний захист із динамічним перебудовуванням частоти та комплексним моніторингом за допомогою SIEM-систем;

– теоретичне й експериментальне оцінювання ефективності запропонованих методів, зокрема формулювання математичних моделей для кількісного вимірювання ризиків;

– обґрунтування практичної реалізації та масштабування розроблених підходів у реальних умовах бойових дій.

Для вирішення поставлених завдань застосовано комплексну методологію, що включає:

– моделі й алгоритми криптографічного захисту з використанням стійких симетричних (AES-256) та асиметричних (RSA, ECC) шифрів, а також із додатковим урахуванням квантово-стійких підходів (наприклад, NTRU) ;

– динамічне перебудовування частот, яке передбачає автоматичну зміну робочих частот передавача та приймача відповідно до псевдовипадкової послідовності. Це ускладнює завдання радіоперехоплення та радіоподавлення для противника;

– системи моніторингу мережевої безпеки на базі SIEM, які дозволяють у реальному часі відстежувати підозрілі активності та виявляти аномальні патерни даних або спроби несанкціонованого доступу;

– моделювання ризиків із використанням ймовірнісних та статистичних методів. Для кількісного оцінювання ефективності захисту застосовано формулу оцінки ризику:

$$Risk = \sum_{i=1}^{n} Pi \times Ii \tag{1}$$

де P_i - ймовірність реалізації конкретного типу i-ї атаки; I_i - потенційна критичність від i-ї атаки.

Зменшення ризику досягається як зниженням імовірності реалізації (через підвищення складності атаки), так і зменшенням критичності (через сегментацію мережі, резервування каналів).

– алгоритмічне забезпечення стрибкоподібного перебудовування частоти, яке можна описати формулою:

$$F(t) = F_0 + \Delta F \times (PRNG(t) \bmod M) \tag{2}$$

де F_0 – початкова частота; ΔF – крок частоти; PRNG(t) – псевдовипадковий генератор чисел (наприклад, на основі блочного шифру або лінійного конгруентного методу); M – кількість можливих частотних позицій.

Така перебудова ускладнює завдання перехоплення сигналу й забезпечує захист від навмисного радіоподавлення.

Крім того, було розроблено таблицю основних параметрів дослідження (див. табл. 1), що включає типи атак, застосовувані методи захисту та показники ефективності:

Таблиця 1 – Параметри дослідження

Параметр	Значення/Діапазон	Коментар
Типи атак	DDoS, фішинг, злам облікових даних, РЕБ	Розглянуті основнізагрози
Криптоалгоритми	AES-256, RSA-4096, NTRU	Посилена стійкість, у тому числі до квантових атак
Модуль SIEM	Splunk, QRadar, ArcSight	Використовуються для відстеження аномалій
Частотне перебудовування	50–500 стрибків/с	Вибір залежить відтипу операції
Резервні канали	HF/VHF/UHF, OneWeb, Iridium	Забезпечують безперервність зв’язку
Оцінка ефективності	Індекс безпеки (0-1)	Результат інтегрального аналізу

Методологічно дослідження спиралося на комп’ютерне моделювання атак і контрзаходів, а також на польові випробування у реальних умовах із використанням переносних терміналів Starlink та військових радіостанцій. Зокрема, проводився порівняльний аналіз функціонування каналів зв’язку у

двох режимах: звичайний (без захисту) та захищений (з частотним перебудовуванням і криптозахистом).

Під час випробувань фіксувалися:

– успішність проведення атаки (відсоток компрометованих/недоступних каналів);

– час відновлення зв'язку після виявлення атаки;

– споживання ресурсів (процесорного часу, пропускної здатності) для систем захисту.

Результати численних моделювань та експериментальних випробувань засвідчили високу ефективність комплексного підходу. Основні кількісні показники (див. табл. 2) дають змогу оцінити рівень безпеки та надійності мережі при застосування різних методів захисту.

Таблиця 2 – Основні результати порівняльного аналізу

Параметр	Без захисту	З комплексним захистом
Індекс безпеки (0-1)	0,42	0,82
Середній час відновлення після атаки, сек.	300	60
Ефективність радіоподавлення, %	70	25
Ймовірність зламу облікового запису	0,25	0,03
Середня успішність DDoS-атаки, %	75	18

Сучасні електронні комунікаційні системи є критичними для оперативного управління, передачі команд і забезпечення інформаційної безпеки. Проте в умовах гібридної війни вони піддаються численним загрозам, таким як DDoS-атаки, радіоподавлення, фішингові кампанії та компрометація облікових записів.

Таким чином, комплексний захист значно покращує показники безпеки, знижуючи успішність DDoS-атак з 75% до 18%, ймовірність зламу облікових записів з 0,25 до 0,03, вразливість до радіоподавлення з 70% до 25%, скорочуючи час відновлення зв'язку з 300 секунд до 60 секунд і підвищуючи загальний індекс безпеки з 0,42 до 0,82. Ці результати підтверджують, що комплексний підхід до кібербезпеки є критично важливим для забезпечення надійного зв'язку в умовах військових операцій.

Зменшення успішності DDoS-атак на 57% (з 75% до 18%) було досягнуто шляхом впровадження хмарних фільтрів трафіку, оркестрування контейнерів та резервування каналів, що перенаправляють легальний трафік під час пікових навантажень.

Ймовірність зламу облікового запису зменшилася майже на порядок (з 0,25 до 0,03), завдяки двофакторній автентифікації, регулярній зміні паролів та впровадженню системи continuous authentication, яка аналізує поведінкові фактори.

Ефективність радіоподавлення знизилася із 70% до 25% за рахунок застосування стрибкоподібного перебудовування частоти, додаткових наземних станцій Starlink та резервних вузлів HF/VHF/UHF.

Середній час відновлення після атаки скоротився з 300с до 60с завдяки автоматизованим скриптам перепідключення та активації резервних каналів.

Зростання інтегрального індексу безпеки з 0,42 до 0,82 свідчить про комплексний позитивний вплив впроваджених заходів, що підвищують захищеність та доступність каналів зв'язку.

Отримані результати підтверджують, що впровадження комплексного захисту на всіх рівнях електронних комунікацій (від організаційно-адміністративного до технічного) суттєво знижує ризик успішної таргетованої атаки.

Найбільш вагомий внесок у досягнення високої ефективності було досягнуто завдяки:

– поєднання криптографічного захисту і стрибкоподібного перебудовування частоти, яке синергійно ускладнює перехоплення й радіоподавлення сигналу [10-11].

– застосування SIEM-систем для моніторингу та аналізу подій у реальному часі, що дає змогу оперативно виявляти атаки та вживати заходів щодо їх локалізації [12-14].

– резервування каналів за рахунок розподіленої архітектури Starlink і застосування додаткових супутникових мереж (OneWeb, Iridium), а також військових систем супутникового зв'язку, що дало можливість маневрувати при виборі каналу передачі інформації в умовах радіоподавлення [15-16].

Крім того, застосування машинного навчання дозволяє прогнозувати атаки та визначати слабкі ланки системи зв'язку заздалегідь, що збільшує шанси на успішне відбиття атак на 10-15%.

Обмеження дослідження полягають у тому, що повномасштабні експерименти у бойових умовах вимагають додаткових ресурсів, узгодження з військовим командуванням та дотримання протоколів безпеки. Крім того, система Starlink перебуває у стані динамічного розвитку, що ускладнює створення повної моделі її вразливостей. Частина застосованих алгоритмів квантово-стійкого шифрування ще перебуває на стадії стандартизації [17], а отже їх ефективність та продуктивність можуть змінюватися.

Висновки

Проведене дослідження підтверджує, що застосування комплексного підходу до захисту електронних комунікацій сил безпеки і оборони України, який включає в себе криптографічний захист, стрибкоподібне перебудовування частоти, SIEM-системи та резервування каналів, значно підвищує рівень безпеки та зменшує ймовірність успішних таргетованих атак. Аналіз статистичних даних і результати моделювання засвідчили, що середня успішність DDoS-атак знизилася до мінімальних значень, а ймовірність зламу облікових записів становить лише 0,03, що свідчить про високу ефективність запропонованих контрзаходів. Запроваджені методи значно скорочують час відновлення зв'язку після атак до 60 секунд, що є критично важливим у бойовій обстановці, оскільки своєчасне прийняття рішень безпосередньо впливає на успіх військових операцій.

Дослідження також підтверджує, що ефективний захист комунікацій у сучасних гібридних війнах має базуватися на поєднанні технічних, організаційних і контррозвідувальних заходів, які повинні стати обов'язковим елементом військової стратегії. У зв'язку з цим рекомендується застосовувати системи стрибкоподібного перебудовування частоти та потужні методи шифрування, зокрема AES-256 та квантово-стійкі алгоритми, для забезпечення безпеки критично важливих каналів військового зв'язку.

Необхідно інтегрувати SIEM-платформи для автоматизованого моніторингу та аналізу мережевих подій, що дасть змогу оперативно виявляти аномалії та запобігати атакам. Важливим елементом забезпечення кібербезпеки є регулярне навчання особового складу щодо безпечної роботи у мережі, з застосуванням протидії фішинговим атакам та з дотриманням політики інформаційної безпеки.

Також доцільно розвивати резервні системи зв'язку, використовуючи не лише Starlink, а й альтернативні супутникові платформи, такі як OneWeb та Iridium, а також традиційні військові канали зв'язку, включаючи HF, VHF та UHF, що забезпечить неперервність комунікації навіть у разі масованих атак.

Наукова й практична цінність дослідження полягає в розробленні комплексних методів протидії таргетованим атакам, які охоплюють: захист від фішингових атак та зламів облікових записів військових; стійкість до радіоподавлення, радіоперехоплення і спотворення сигналу; інтеграцію криптографічних протоколів високого рівня безпеки; впровадження методів активної контррозвідки та моніторингу кібератак у реальному часі.

Перспективні напрями майбутніх досліджень охоплюють:

– розвиток квантово-стійких алгоритмів та їх інтеграцію у військові протоколи зв'язку;

– вдосконалення алгоритмів машинного навчання для більш точного виявлення складних таргетованих атак (APT-груп);

– покращення фізичного захисту супутникового обладнання та терміналів у польових умовах, зокрема протидію масованим радіоелектронним атакам та атакам дронів;

– розроблення єдиних стандартів та методичних рекомендацій щодо побудови комплексної системи кібербезпеки для військових комунікацій та критичної інфраструктури.

Перелік джерел посилання:

1. Kamien D. (Ed.). The McGraw-Hill Homeland Security Handbook. McGraw-Hill, 2017. URL: https://www.mheducation.com/ (дата звернення: 08.02.2025).

2. DiMaggio J., Peterson M. Threat Intelligence and Incident Response: *High-stakes Security. O'Reilly Media*, 2016. URL: https://www.oreilly.com/library/view/threat-intelligence-and/9781491935199/ (дата звернення: 08.02.2025).

3. Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. *NIST SP 800-160. National Institute of Standards and Technology*, 2018. DOI: 10.6028/NIST.SP.800-160. URL: https://doi.org/10.6028/NIST.SP.800-160 (дата звернення: 08.02.2025).

4. Kott A., Swami A. Cyber Defense and Situational Awareness. *Springer*, 2016. DOI: 10.1007/978-3-319-25107-5. URL: https://doi.org/10.1007/978-3-319-25107-5 (дата звернення: 08.02.2025).

5. Buchanan W. J., Macfarlane R., Smith D. Advanced Cryptographic Methods for Secure Military Communication. *Information Security Journal*, 2020, vol. 29, no. 3, pp. 202-214. DOI: 10.1080/19393555.2020.1767752. URL: https://doi.org/10.1080/19393555.2020.1767752 (дата звернення: 08.02.2025).

6. Koblitz N., Menezes A. A Survey of the Security of Elliptic Curve Cryptosystems. *SIAM Review*, 2017, vol. 59, no. 1, pp. 42-55. DOI: 10.1137/151003604. URL: https://doi.org/10.1137/151003604 (дата звернення: 08.02.2025).

7. Sharma G., Chen D. A Study on Post-Quantum Cryptography: RSA and ECC. *Journal of Cryptographic Engineering*, 2018, vol. 8, no. 4, pp. 275-286. DOI: 10.1007/s13389-018-0186-5. URL: https://doi.org/10.1007/s13389-018-0186-5 (дата звернення: 08.02.2025).

8. Bansal M., Kumar R. Radio Frequency Jamming Techniques and Their Countermeasures. *IEEE Communications Surveys & Tutorials*, 2017, vol. 19, no. 1, pp. 677-694. DOI: 10.1109/COMST.2016.2614462. URL: https://doi.org/10.1109/COMST.2016.2614462 (дата звернення: 08.02.2025).

9. Strobel D., Hess M. Satellite System Vulnerabilities, Security Issues, and Mitigation Techniques. *IEEE Aerospace and Electronic Systems Magazine*, 2018, vol. 33, no. 4, pp. 22-31. DOI: 10.1109/MAES.2018.160122. URL: https://doi.org/10.1109/MAES.2018.160122 (дата звернення: 08.02.2025).

10. Huber M., Kann V. Frequency Hopping for Military Communications: A Survey of Evolving Standards. *IEEE Communications Surveys & Tutorials*, 2020, vol. 22, no. 3, pp. 1345-1357. DOI: 10.1109/COMST.2020.
2987303. URL: https://doi.org/10.1109/COMST.2020.2987303 (дата звернення: 08.02.2025).

11. Zhang Y., Rayi V. K. Physical Layer Security in Frequency Hopping Systems. *Wireless Personal Communications*, 2018, vol. 101, no. 4, pp. 297-312. DOI: 10.1007/s11277-018-5745-9. URL: https://doi.org/10.1007/s11277-018-5745-9 (дата звернення: 08.02.2025).

12. Ciampa M. Security+ Guide to Network Security Fundamentals. *Cengage Learning*, 2018. URL: https://www.cengage.com/ (дата звернення: 08.02.2025).

13. Fulp E. W., Reeves D. S. A Multi-agent System for Network Intrusion Detection and Response. *Journal of Network and Systems Management*, 2015, vol. 23, no. 4, pp. 381-404. DOI: 10.1007/s10922-014-9325-2. URL: https://doi.org/10.1007/s10922-014-9325-2 (дата звернення: 08.02.2025).

14. Zuech R., Khoshgoftaar T. M., Wald R. Intrusion Detection and Big Heterogeneous Data: A Survey. *Journal of Big Data*, 2015, vol. 2, no. 1, p. 3. DOI: 10.1186/s40537-015-0013-4. URL: https://doi.org/10.1186/s40537-015-0013-4 (дата звернення: 08.02.2025).

15. Strohm M. Examining Resilience in Satellite Communications: Starlink, OneWeb, and Other LEO Constellations. *International Journal of Satellite Communications*, 2019, vol. 37, no. 2, pp. 97-105. DOI: 10.1002/sat.1301. URL: https://doi.org/10.1002/sat.1301 (дата звернення: 08.02.2025).

16. Trichakis G., Street M. Global Iridium-based Communication in Modern Military Operations. *Defense Technology Review*, 2021, vol. 29, no. 2, pp. 45-52. URL: https://www.defensetechnologyreview.com/ (дата звернення: 08.02.2025).

17. Commercial National Security Algorithm Suite 2.0. NSA/CSS, 2022. National Security Agency. URL: https://www.nsa.gov/ (дата звернення: 08.02.2025).

Стаття надійшла до редакції 26.11.2025 р.

UDC 004.056:621.396.9:355.40

D. Prokopovych-Tkachenko, V. Olenchenko, M. Bondarenko

PROTECTION OF CRITICAL INFRASTRUCTURE: METHODS OF COUNTERACTING TARGETED ATTACKS ON ELECTRONIC COMMUNICATION SYSTEMS OF THE SECURITY AND DEFENSE FORCES OF UKRAINE

The article examines the problem of ensuring the protection of electronic communication systems of the Security and Defense Forces of Ukraine under the conditions of modern hybrid warfare, which is accompanied by the growing impact of cyber and radio-electronic threats. It is demonstrated that traditional information security approaches focused exclusively on cryptographic methods or radio engineering solutions are insufficient given the complex multi-vector influence of the adversary. Particular attention is paid to a comprehensive approach to countering targeted attacks, which encompasses cybersecurity measures, physical protection of communication equipment, and improvement of electronic communication protocols. A multi-layer cyber protection model is proposed, combining cryptographic mechanisms (AES-256, RSA, NTRU), adaptive frequency-hopping techniques, the use of SIEM systems, and the reservation of HF/VHF/UHF and satellite communication channels. The results show that the proposed solutions significantly reduce the risk of successful targeted attacks, improve the continuity and reliability of communication processes, and ensure an adequate level of information security. The article outlines directions for future research related to the integration of quantum-resistant encryption algorithms, the development of artificial-intelligence-based threat detection technologies, the creation of unified standards and methodological recommendations for building comprehensive cybersecurity systems for military communications, and the improvement of physical protection measures for electronic communication infrastructure, including Starlink satellite equipment. The findings confirm the effectiveness of the integrated cybersecurity approach and its scalability for real combat conditions.

Keywords: *electronic communication systems, targeted attacks, cybersecurity, Security and Defense Forces of Ukraine, integrated protection, cryptography, frequency hopping, communication systems.*

Прокопович-Ткаченко Дмитро Ігорович – кандидат технічних наук, доцент, завідувач кафедри кібербезпеки, Університет митної справи та фінансів
https://orcid.org/0000-0002-6590-3898

Оленченко Віктор Тимофійович – кандидат технічних наук, доцент, начальник кафедри військового зв'язку та інформатизації, Національна академія Національної гвардії України
https://orcid.org/0000-0003-4220-4274

Бондаренко Максим Петрович – викладач кафедри забезпечення державної безпеки, Національна академія Національної гвардії України
https://orcid.org/0009-0002-7843-5103