УДК 355.40:004.056.5(477)

В. В. Корсак

КІБЕРАТАКА NOTPETYA ЯК ІНСТРУМЕНТ ГІБРИДНОЇ ВІЙНИ: ТЕХНІЧНІ ОСОБЛИВОСТІ ТА ІСТОРИЧНІ НАСЛІДКИ

Вінницький національний технічний університет

Анотація

У тезах досліджується кібератака NotPetya 2017 року як інструмент гібридної війни Росії проти України. Розглянуто технічні механізми атаки, її атрибуцію групі Sandworm ГРУ, глобальні економічні наслідки понад 10 млрд доларів та міжнародно-правові виміри інциденту. Зроблено висновок, що NotPetya є визначальним прецедентом застосування державної кіберзброї в сучасному збройному конфлікті.

Ключові слова: NotPetya, гібридна війна, Sandworm, кіберзброя, критична інфраструктура, Україна.

Abstract

Theses examine the 2017 NotPetya cyberattack as a tool of Russia's hybrid war against Ukraine. The technical mechanisms of the attack, its attribution to the Sandworm group of the GRU, the global economic consequences of more than $10 billion and the international legal dimensions of the incident are considered. It is concluded that NotPetya is a defining precedent for the use of state cyberweapons in a modern armed conflict.

Keywords: NotPetya, hybrid warfare, Sandworm, cyberweapons, critical infrastructure, Ukraine.

Вступ

Кібератака NotPetya, що відбулася 27 червня 2017 р., стала переломним моментом в еволюції гібридної війни. Вона ознаменувала нову еру кібервійни з підтримкою держав, де Україна стала мішенню кремлівських операцій, спрямованих на залякування тих, хто веде з нею бізнес [1]. Атака швидко вийшла за межі однієї країни і завдала безпрецедентної шкоди глобальній інфраструктурі, поставивши гострі питання щодо меж застосування кіберзброї та відповідальності держав у цифровому просторі [2]. Метою цих тез є комплексний аналіз технічних характеристик NotPetya, її місця в контексті гібридної агресії Росії проти України та довгострокових наслідків для міжнародної безпеки і кіберполітики.

Результати дослідження

NotPetya лише імітувала здирницьке програмне забезпечення. Попри шифрування файлів, зв'язку між ключем і ідентифікатором жертви не існувало – відновити дані навіть після сплати викупу було технічно неможливо, тому за своєю поведінкою це руйнівне шкідливе ПЗ, а не здирницьке [3]. В основі атаки лежав експлойт EternalBlue (CVE-2017-0144), що використовував уразливість протоколу SMB операційних систем Windows [4], а також інструмент Mimikatz для автоматизованої крадіжки паролів і подальшого lateral movement між вузлами мережі [5]. Велика українська банківська мережа була виведена з ладу за 45 с., а транзитний вузол країни – за 16 с. [6].

Вектором первинного зараження стало популярне українське бухгалтерське програмне забезпечення M.E.Doc. Зловмисники впровадили бекдор у середовище його розробки ще з квітня 2017 р., що дозволяло виконувати довільні команди та завантажувати шкідливі компоненти на уражені системи, а саме програмне забезпечення було вразливим з 2013 р. через незадовільне управління оновленнями та бекдорене тричі [7]. Такий підхід засвідчив витончений рівень підготовки операції та тривале попереднє планування.

Щодо атрибуції, ЦРУ США з «високим рівнем впевненості» встановило, що атаку здійснили хакери ГРУ Росії з метою дестабілізації фінансової системи України в умовах триваючої війни на Донбасі [8]. Велика Британія офіційно атрибутувала атаку підрозділу 74455 ГРУ, відомому як група Sandworm, у 2018 р. [9]. Мотив атаки був геополітичним: дестабілізувати Україну та сіяти

хаос, а не здійснювати фінансове вимагання [10], що вписує NotPetya в систематичний характер операцій Sandworm, включаючи знеструмлення електромереж України у 2015-2016 рр. [11].

Загальні збитки від атаки перевищили 10 млрд $: Maersk зазнала порушення операцій у 76 портах зі збитками 200–300 млн $, Merck – 870 млн $ [12]. Система радіаційного моніторингу Чорнобильської АЕС вийшла з ладу, постраждали українські міністерства, банки та метрополітен [13]. Радник Білого дому Том Боссерт охарактеризував атаку як «рівнозначну застосуванню ядерної бомби для досягнення незначної тактичної перемоги» [14]. Вірус вийшов з-під контролю і поширився назад на Росію, пошкодивши системи державної нафтової компанії «Роснефть», що унаочнило принципову некерованість подібної кіберзброї.

З міжнародно-правової точки зору NotPetya порушила суверенітет держав, оскільки серйозно заблокувала функціонування їхньої кіберінфраструктури у спосіб, що перевищував тимчасову відмову в обслуговуванні [15]. У лютому 2018 р. 7 країн спільно засудили Росію, що стало першим в історії прецедентом єдиної міжнародної атрибуції кібератаки [16]. Страхова компанія Zurich відмовила у виплаті 100 млн $, кваліфікувавши атаку як акт війни, однак суд відхилив це трактування [17]. Серед практичних уроків – необхідність ефективного управління вразливостями, актуального обліку мережевих активів та сегментації мережі для локалізації атак [18], адже законодавство у сфері кібербезпеки неухильно відстає від найновіших загроз, а суттєві заходи вживаються переважно лише після значних внутрішніх потрясінь [19].

Висновки

NotPetya є визначальною подією в історії гібридної війни та розвитку кіберзброї. Атака заклала нову парадигму деструктивної кіберзброї, що маскується під здирницьке ПЗ і вражає через довірені канали оновлень. Вона підтвердила системний характер кіберагресії Росії проти України як складової гібридної війни. Збитки понад 10 млрд $ і ураження компаній у десятках країн довели некерованість кіберзброї в умовах глобальної цифрової взаємозалежності. Атака виявила критичні прогалини в міжнародному праві щодо кваліфікації кібератак і механізмів колективного реагування. Уроки NotPetya зберігають гостру актуальність в умовах повномасштабної війни та безперервного кіберпротистояння.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. HYPR. What is NotPetya? 5 Fast Facts // Security Encyclopedia. URL: https://www.hypr.com/security-encyclopedia/notpetya (дата звернення: 08.05.2026).
2. CCDCOE. NotPetya (2017) – International Cyber Law: Interactive Toolkit. URL: https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017) (дата звернення: 08.05.2026).
3. CISA. Petya Ransomware. Alert TA17-181A. – 2017. URL: https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware (дата звернення: 08.05.2026).
4. Armis. Reflecting on NotPetya: A Milestone in Cyberwarfare History. – 2023. URL: https://www.armis.com/blog/reflecting-on-notpetya-a-milestone-in-cyberwarfare-history/ (дата звернення: 08.05.2026).
5. Wikipedia. Petya and NotPetya. URL: https://en.wikipedia.org/wiki/Petya_and_NotPetya (дата звернення: 08.05.2026).
6. HYPR. What is NotPetya? 5 Fast Facts // Security Encyclopedia. URL: https://www.hypr.com/security-encyclopedia/notpetya (дата звернення: 08.05.2026).
7. Kerttunen M., Hemmelskamp J. MACI NotPetya // EURepoC. URL: https://eurepoc.eu/wp-content/uploads/2023/05/MACI_NotPetya.pdf (дата звернення: 08.05.2026).
8. Interfax Ukraine. CIA: Cyberattacks Against Ukraine Committed by Russian Military. URL: https://en.interfax.com.ua/news/general/476772-amp.html (дата звернення: 08.05.2026).
9. UK Government. Profile: GRU Cyber and Hybrid Threat Operations. URL: https://www.gov.uk/government/publications/profile-gru-cyber-and-hybrid-threat-operations/ (дата звернення: 08.05.2026).
10. Zoho Workplace. The NotPetya Catastrophe – Global Havoc in 2017. – 2023. URL: https://www.zoho.com/workplace/articles/notpetya-cyberattack.html (дата звернення: 08.05.2026).
11. Greenberg A. The Untold Story of NotPetya // Wired. – 2018. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (дата звернення: 08.05.2026).
12. CyberRanges. How Did NotPetya Cost Businesses Over $10 Billion? URL: https://cyberranges.com/how-did-notpetya-cost-businesses-over-10-billion-in-damages/ (дата звернення: 08.05.2026).
13. Zoho Workplace. The NotPetya Catastrophe – Global Havoc in 2017. – 2023. URL: https://www.zoho.com/workplace/articles/notpetya-cyberattack.html (дата звернення: 08.05.2026).
14. Control Engineering. How NotPetya Ransomware Took Down Maersk. URL: https://www.controleng.com/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/ (дата звернення: 08.05.2026).
15. Schmitt M. N. The NotPetya Cyber Operation as a Case Study of International Law // EJIL: Talk! – 2017. URL: https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/ (дата звернення: 08.05.2026).

16. Krasznay Cs. Case Study: The NotPetya Campaign // Academia.edu. – 2020. URL: https://www.academia.edu/49546003/Case_Study_The_NotPetya_Campaign (дата звернення: 08.05.2026).
17. CIAB. NotPetya: A War-Like Exclusion? – 2019. URL: https://www.ciab.com/resources/notpetya-a-war-like-exclusion/ (дата звернення: 08.05.2026).
18. Infosecurity Europe. What Have We Learned from NotPetya Six Years On? URL: https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/learnings-from-notpetya-cyberattack.html (дата звернення: 08.05.2026).
19. Cybrary. NotPetya: Its Consequences. – 2021. URL: https://www.cybrary.it/blog/notpetya-its-consequences (дата звернення: 08.05.2026).

Корсак Вікторія Валентинівна – студентка групи 4ПІ-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: vkorsak11@gmail.com
Герасимов Тимофій Юрійович – доктор історичних наук, доцент кафедри суспільно-політичних наук Вінницького національного технічного університету, м. Вінниця, e-mail: timger84@gmail.com

Korsak Viktoria V. – Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: vkorsak11@gmail.com
Gerasymov Tymophiy Y. – Doctor of Historical Sciences, Associate Professor department of society political sciences, Vinnytsia National Technical University, Vinnytsia. e-mail: timger84@gmail.com