УДК 355.4:004.7

Б. О. Верещак

КІБЕРВІЙНА ЯК НОВИЙ ВИМІР КОНФЛІКТУ. АТАКИ НА КРИТИЧНУ ЦИФРОВУ ІНФРАСТРУКТУРУ

Вінницький національний технічний університет

Анотація

Досліджено еволюцію кібератак на критичну цифрову інфраструктуру та зміну парадигми сучасних збройних конфліктів у бік системного ураження автоматизованих систем управління. Обґрунтовано необхідність переходу до децентралізованих архітектур та новітніх протоколів шифрування для забезпечення життєздатності національних мереж в умовах гібридних загроз.

Ключові слова: кібервійна, критична цифрова інфраструктура, автоматизовані системи управління, кібератаки, повітряний проміжок, постквантова криптографія.

Abstract

The evolution of cyberattacks on critical digital infrastructure and the changing paradigm of modern armed conflicts towards systemic damage to automated control systems are investigated. The necessity of transition to decentralized architectures and modern encryption protocols to ensure the viability of national networks in the context of hybrid threats is substantiated.

Keywords: cyber warfare, critical digital infrastructure, automated control systems, cyberattacks, air gap, post-quantum cryptography.

Вступ

Мілітаризація кіберпростору змістила фокус збройних конфліктів у площину цифрових систем управління. Якщо раніше кібероперації обмежувалися розвідкою, викраденням даних або DDoS-атаками, то сьогодні головною ціллю стають автоматизовані системи управління технологічними процесами та архітектури диспетчерського управління й збору даних (SCADA). Базовим прецедентом переходу кіберзброї у площину фізичного руйнування став вірус Stuxnet [1]. За таких умов кіберзброя інтегрується в ядро гібридної війни, розмиваючи юридичну та фактичну межу між мирним часом і збройною агресією [2].

Результати дослідження

Технічний розбір сучасних інцидентів виявляє критичну вразливість парадигми «повітряного проміжку» (air gap) – концепції повної фізичної ізоляції критичних систем від глобальної мережі Інтернет. Як показує практика, така ізоляція більше не гарантує безпеки промислових об'єктів, оскільки зловмисники системно експлуатують слабкі ланки у ланцюгах постачання або використовують побутові пристрої без належного кіберзахисту. Наприклад, під час ракетних обстрілів Києва у січні 2024 р. було зафіксовано злам звичайних роботизованих онлайн-камер зовнішнього спостереження, які використовувалися спецслужбами агресора для трансляції роботи української ППО та коригування ударів [3].

Вектор застосування шкідливого програмного забезпечення також змінився: фінансова вигода поступилася місцем максимізації деструктивного впливу з використанням вайперів (wipers) – софту, націленого виключно на безповоротне затирання даних. Яскравим прикладом є масштабна кібератака на ядро мережі телекомунікаційної компанії «Київстар» у грудні 2023 р., реалізована російським угрупованням Sandworm. Вона призвела до знищення віртуальних серверів та спровокувала каскадні збої: відсутність зв'язку у мільйонів абонентів, зупинку платіжних терміналів та локальні відключення систем оповіщення про повітряну тривогу [4].

Водночас кібероперації є ефективним інструментом асиметричної відповіді. Свідченням цього є успішна операція Головного управління розвідки Міноборони України у листопаді 2023 р. проти Федерального агентства повітряного транспорту рф («Росавіації»). Унаслідок зламу було здобуто великий масив закритої службової документації та завдано критичної шкоди серверам і базам даних відомства, що змусило його перейти на паперовий документообіг [5].

Аналіз актуальних захисних стратегій оголює проблему архітектури застарілих промислових систем. Більшість протоколів передачі даних проєктувалися десятиліття тому без урахування криптографічних стандартів. Накладання сучасних засобів захисту поверх старих протоколів створює затримки в передачі телеметрії, що є неприпустимим для систем реального часу. Окремим викликом є загроза квантового дешифрування у найближчій перспективі, що здатне долати класичні алгоритми захисту вузлів зв'язку [6].

Висновки

Зміщення вектору атак у бік критичної цифрової інфраструктури вимагає перегляду архітектурних рішень на рівні проєктування національних мереж. Централізовані системи управління довели свою неспроможність витримувати масовані кіберудари. Практична стійкість досягається лише через перехід до децентралізованих архітектур, розподіленої генерації та дублювання баз даних у хмарних середовищах з різною локалізацією. Подальша життєздатність критичної інфраструктури безпосередньо залежатиме від швидкості імплементації протоколів постквантової криптографії та впровадження систем автономного моніторингу аномалій на базі принципів «нульової довіри».

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Geers K. The Cyber Threat to National Critical Infrastructures: Beyond Theory. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). 2009. URL: https://ccdcoe.org/uploads/2018/10/Geers2009_The-Cyber-Threat-to-National-Critical-Infrastructures.pdf
2. State Service of Special Communications and Information Protection of Ukraine. War and Cyber: Three Years of Struggle and Lessons for Global Security. 2025. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=69131
3. СБУ заблокувала веб-камери, які знімали роботу систем ППО у Києві. РБК-Україна. 2024. URL: https://www.rbc.ua/rus/news/sbu-zablokuvala-veb-kameri-ki-znimali-robotu-1704206596.html
4. СБУ розкрила подробиці атаки російських хакерів на Київстар. UKR.NET. 2023. URL: https://www.ukr.net/news/details/technologies/101953173.html
5. ГУР провело кібероперацію проти "Росавіації": в мережу потрапили секретні дані. РБК-Україна. 2023. URL: https://www.rbc.ua/ukr/news/gur-provelo-kiberoperatsiyu-proti-rosaviatsiyi-1700721897.html
6. Ткаченко А., Левченко С. Vectors of ensuring economic security of energy enterprises in the context of quantum transformation. Економіка і регіон. 2025. URL: https://journals.nupp.edu.ua/eir/article/download/3771/3105

Верещак Богдана Олександрівна – студентка групи 4ПІ-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: ellae1419@gmail.com

Науковий керівник: ***Герасимов Тимофій Юрійович*** – доктор історичних наук, доцент кафедри суспільно-політичних наук, Вінницький національний технічний університет, м. Вінниця, e-mail: timger84@gmail.com

Bohdana O. Vereshchak – Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: ellae1419@gmail.com

Scientific Supervisor: ***Tymofii Yu. Gerasymov*** – Doctor of Historical Sciences, Associate Professor of the Department of Social and Political Sciences, Vinnytsia National Technical University, Vinnytsia, e-mail: timger84@gmail.com