УДК 004.056

Д. О. Гнітецька
Т. Г. Кирилащук

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ В ОПЕРАЦІЙНО-ТЕХНОЛОГІЧНИХ МЕРЕЖАХ: ПРОБЛЕМИ АДАПТАЦІЇ IT-МЕТОДОЛОГІЙ ДО УМОВ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вінницький національний технічний університет

Анотація

Стаття присвячена дослідженню проблем адаптації методологій тестування на проникнення, розроблених для корпоративних IT-середовищ, до специфічних умов операційно-технологічних (OT) мереж, що забезпечують функціонування об'єктів критичної інфраструктури. Розглянуто ключові відмінності між IT- та OT-середовищами, проаналізовано існуючі стандарти та фреймворки пентестингу. Визначено основні виклики, пов'язані з проведенням тестування на проникнення в промислових мережах, та запропоновано підходи до їх вирішення.

Ключові слова: *операційно-технологічні мережі, тестування на проникнення, OT-пентестинг, критична інфраструктура, адаптація методологій, кіберзахист, промислові мережі.*

Abstract

The article is dedicated to the study of challenges in adapting penetration testing methodologies originally developed for corporate IT environments to the specific conditions of operational technology (OT) networks that ensure the functioning of critical infrastructure facilities. Key differences between IT and OT environments are examined, existing penetration testing standards and frameworks are analyzed. The main challenges associated with conducting penetration testing in industrial networks are identified, and approaches to addressing them are proposed.

Keywords: *operational technology networks, penetration testing, OT pentesting, critical infrastructure, methodology adaptation, cyber defense, industrial networks.*

Вступ

Цифровізація об’єктів критичної інфраструктури та інтеграція операційно-технологічних (OT) мереж із корпоративними IT-системами призвели до суттєвого зростання кіберзагроз для промислових систем керування (ICS/SCADA). Упродовж останніх років зафіксовано численні атаки на енергетичні та промислові об’єкти, зокрема із використанням спеціалізованого шкідливого програмного забезпечення та засобів віддаленого доступу, що підтверджує необхідність регулярної оцінки захищеності таких систем. Одним із ефективних методів оцінки безпеки є тестування на проникнення, однак застосування класичних IT-методологій у середовищах OT є ускладненим через високі вимоги до безперервності технологічних процесів, використання спеціалізованих протоколів та можливість виникнення фізичних наслідків у разі помилкового втручання [1,2].

Метою дослідження є аналіз проблем адаптації методологій тестування на проникнення до умов операційно-технологічних мереж та визначення підходів до безпечного проведення пентестингу в системах критичної інфраструктури.

Результати досліджень

Для розуміння проблематики проведення тестування на проникнення в операційно-технологічних мережах необхідно передусім окреслити принципові відмінності між IT- та OT-середовищами. У традиційних корпоративних IT-мережах пріоритетом є тріада конфіденційності, цілісності та доступності (CIA), де конфіденційність зазвичай займає провідне місце. В OT-середовищах ця пріоритетність змінюється: на першому місці знаходиться доступність і безперервність технологічного

процесу, оскільки будь-яке незаплановане втручання в роботу промислового обладнання може призвести до матеріальних збитків або створення загрози для життя і здоров'я людей [2].

Операційно-технологічні мережі функціонують на основі спеціалізованих протоколів, таких як Modbus, DNP3, IEC 60870-5-104, PROFINET та OPC, які розроблялися з акцентом на надійність і детермінованість передачі даних, а не на захист від кіберзагроз. Крім того, OT-системи часто містять застаріле обладнання з тривалим життєвим циклом, яке має обмежені можливості оновлення програмного забезпечення. У таких умовах активне сканування або навантажувальне тестування може призвести до відмови програмованих логічних контролерів або порушення технологічних процесів [3].

У корпоративних IT-мережах для оцінки захищеності широко використовуються методології тестування на проникнення, зокрема Penetration Testing Execution Standard (PTES), OWASP Testing Guide та рекомендації NIST SP 800-115, які передбачають активні фази розвідки, сканування, експлуатації вразливостей і постексплуатаційного аналізу. Проте застосування цих підходів у середовищах OT без відповідної адаптації є небезпечним, оскільки стандартні методи можуть спричинити нестабільну роботу обладнання або порушення виробничого процесу [4].

Активне сканування мережі за допомогою інструментів типу Nmap або Nessus здатне створювати аномальне навантаження на промислові контролери, що може призвести до їх зависання або аварійного відключення (як це неодноразово фіксувалося в практиці). Використання методів fuzzing щодо промислових протоколів також може викликати непередбачувану реакцію обладнання. Фаза постексплуатації, яка є стандартною для IT-пентестингу, у середовищі критичної інфраструктури пов'язана з ризиком ненавмисного впливу на керовані фізичні процеси [5].

З метою зменшення ризиків під час оцінки захищеності промислових мереж розроблено спеціалізовані стандарти та рекомендації, зокрема NIST SP 800-82 Rev. 3 (2023), IEC 62443, NERC CIP, а також рекомендації CISA та база знань MITRE ATT&CK for ICS. Ці документи визначають вимоги до проведення аналізу безпеки з урахуванням архітектури OT-мереж, зонування, рівнів безпеки (SL-2/SL-3) та можливих фізичних наслідків кіберінцидентів [2, 5, 6]. На початку 2026 року NIST розпочав роботу над pre-draft Rev. 4, яка враховує нові загрози та сучасні практики.

На основі аналізу сучасних стандартів і практик можна виокремити основні проблеми адаптації IT-методологій тестування на проникнення до умов OT-середовищ.

По-перше, відсутність ізольованих тестових середовищ. На відміну від корпоративних систем, де тестування може виконуватися на окремому стенді, у промислових мережах створення повноцінного тестового полігону, що відтворює реальне виробниче середовище, є складним і дорогим. Як альтернативу пропонується використання цифрових двійників, програмних емуляторів контролерів та спеціалізованих лабораторних середовищ [7].

По-друге, обмеження у часових вікнах для тестування. Перевірки в OT-мережах часто можуть проводитися лише під час планових зупинок або в періоди мінімального навантаження, що значно обмежує можливості повноцінного пентестингу порівняно з IT-інфраструктурою.

По-третє, підвищені вимоги до кваліфікації фахівців. Пентестер у сфері OT повинен мати знання не тільки з кібербезпеки, а й з автоматизації виробництва, архітектури ICS-систем і принципів роботи промислових протоколів, що ускладнює підготовку спеціалістів і створює дефіцит кадрів [3].

По-четверте, правові та регуляторні обмеження. Проведення тестування на проникнення на об'єктах критичної інфраструктури потребує погодження з експлуатаційним персоналом, чіткого визначення меж тестування та дотримання вимог галузевих стандартів і нормативних документів, що регламентують безпеку OT-систем [6].

Аналіз сучасних підходів до вирішення зазначених проблем показує доцільність використання пасивної розвідки на початкових етапах тестування, поетапного виконання перевірок із обов'язковим погодженням кожної фази, а також застосування спеціалізованих інструментів, адаптованих для OT-середовищ, зокрема Claroty, Dragos, Tenable.ot, Nozomi та інших рішень, розроблених для безпечного аналізу промислових мереж. Крім того, ефективним підходом є використання threat modeling з урахуванням типових сценаріїв атак, описаних у MITRE ATT&CK for ICS, що дозволяє зменшити ризик негативного впливу тестування на реальні технологічні процеси [5,7].

Висновки

Тестування на проникнення в операційно-технологічних мережах є важливим інструментом забезпечення кіберзахисту критичної інфраструктури, проте його проведення потребує суттєвої

адаптації класичних IT-методологій. Основні виклики пов’язані з пріоритетом доступності та безперервності, застарілим обладнанням, обмеженими можливостями активного тестування та високими кваліфікаційними вимогами.

Ефективне проведення OT-пентестингу можливе за умови використання спеціалізованих інструментів, поетапного тестування, пасивної розвідки, цифрових двійників, а також дотримання сучасних стандартів (IEC 62443, NIST SP 800-82 Rev. 3 (2023) та pre-draft Rev. 4 (2026), MITRE ATT&CK for ICS, CISA). Ці підходи дозволяють оцінити захищеність промислових систем без негативного впливу на виробничі процеси та підвищують безпеку критичної інфраструктури відповідно до вимог SL-2/SL-3.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Liang G. et al. URL: https://www.researchgate.net/publication/310739738_The_2015_Ukraine_Blackout_Implications_for_False_Data_Injection_Attacks (дата звернення: 23.03.2026).
2. NIST SP 800-82 Rev. 3. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf (дата звернення: 23.03.2026).
3. Ralston P. A. S. et al. URL: https://www.researchgate.net/publication/6214586_Cyber_security_risk_assessment_for_SCADA_and_DCS_networks (дата звернення: 23.03.2026).
4. PTES Technical Guidelines. URL: http://www.pentest-standard.org/index.php/Main_Page (дата звернення: 23.03.2026).
5. Hahn A. et al. URL: https://www.researchgate.net/publication/281358500_A_multi-layered_and_kill-chain_based_security_analysis_framework_for_cyber-physical_systems (дата звернення: 23.03.2026).
6. CISA. URL: https://www.cisa.gov/ics (дата звернення: 23.03.2026).
7. Ghaleb A. et al. URL: https://www.researchgate.net/publication/325700543_On_PLC_network_security (дата звернення: 23.03.2026).

Гнітецька Діана Олександрівна – студентка групи 1БКС-24б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: canisasjackal@gmail.com

Науковий керівник: ***Кирилащук Тетяна Геннадіївна*** - асистент кафедри захисту інформації факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: kgt0998@gmail.com

Diana Hnitetska – student, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: canisasjackal@gmail.com

Supervisor: ***Tetiana H. Kyrylashchuk*** – assistant of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com