Харківський національний університет радіоелектроніки
Кременчуцький національний університет імені Михайла Остроградського
Національний університет «Запорізька політехніка»
Національний університет «Львівська політехніка»
Державне підприємство «Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості»
Головне управління ДСНС України у Харківській області

II Всеукраїнська конференція «Інтелектуальні технології цивільної безпеки та робототехнічні системи аварійно-рятувальних робіт» (ICSTRO-2026)

II All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations” (ICSTRO-2026)

ЗМІСТ

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КІБЕРФІЗИЧНИХ СИСТЕМ ДО DDOS-АТАК ПІД ЧАС УПРАВЛІННЯ КРИТИЧНИМИ ОБ'ЄКТАМИ У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Б. І. Кислий, С. В. Сотник
Харківський національний університет радіоелектроніки
Україна, 61166, Харків, пр. Науки, 14
E-mail: bohdan.kyslyi@nure.ua, svetlana.sotnik@nure.ua

Анотація: У роботі розглянуто проблему забезпечення стійкості кіберфізичних систем до DDoS-атак під час функціонування критично важливих об'єктів у надзвичайних ситуаціях. Проаналізовано особливості сучасних DDoS-атак, їх вплив на доступність інформаційних ресурсів та безперервність роботи автоматизованих систем керування. Визначено основні ризики, що виникають під час порушення функціонування критичної інфраструктури, а також розглянуто сучасні підходи до підвищення кіберстійкості, зокрема використання резервування, сегментації мережі, моніторингу трафіку, систем виявлення вторгнень та інтелектуальних методів аналізу мережевої активності. Зроблено висновок, що комплексне впровадження сучасних засобів кіберзахисту дозволяє забезпечити безперервність роботи кіберфізичних систем навіть в умовах масштабних кібератак. Окрему увагу приділено особливостям забезпечення кіберстійкості критичної інфраструктури в умовах воєнних конфліктів, а також ролі регулярного тестування систем (навчальні тренування, моделювання атак, аудит безпеки) у виявленні вразливостей.

Ключові слова: кіберфізичні системи, DDoS-атаки, критична інфраструктура, кібербезпека, надзвичайні ситуації, мережевий захист.

ENSURING THE RESILIENCE OF CYBER-PHYSICAL SYSTEMS TO DDoS ATTACKS WHEN MANAGING CRITICAL INFRASTRUCTURE DURING EMERGENCIES

B. I. Kyslyi, S. V. Sotnik
Kharkiv National University of Radio Electronics
Ukraine, 61166, Kharkiv, Nauky Ave., 14
E-mail: bohdan.kyslyi@nure.ua, svetlana.sotnik@nure.ua

Annotation: This paper examines the problem of ensuring the resilience of cyber-physical systems to DDoS attacks during the operation of critical infrastructure in emergency situations. It analyzes the characteristics of modern DDoS attacks, their impact on the availability of information resources, and the continuity of automated control systems. The paper identifies the main risks arising from disruptions to critical infrastructure and examines modern approaches to enhancing cyber resilience, including the use of redundancy, network segmentation, traffic monitoring, intrusion detection systems, and intelligent methods for analyzing network activity. It is concluded that the comprehensive implementation of modern cyber defense measures ensures the continuity of cyber-physical systems even under conditions of large-scale cyberattacks. Special attention is paid to the challenges of ensuring cyber resilience of critical infrastructure under conditions of military conflict, as well as the role of regular system testing (training exercises, attack simulation, security audits) in identifying vulnerabilities.

Key words: cyber-physical systems, DDoS attacks, critical infrastructure, cybersecurity, emergencies, network security.

Стрімка цифровізація управління критично важливими об'єктами (енергетика, транспорт, медицина, водопостачання) супроводжується зростанням кількості кіберзагроз, серед яких DDoS-атаки (Distributed Denial of Service) є одними з найнебезпечніших, оскільки спрямовані на порушення доступності інформаційних ресурсів [1-8]. Проблема набуває особливої

гостроти в умовах надзвичайних ситуацій та сучасних воєнних конфліктів, коли безперебійна робота критичної інфраструктури є визначальною для оперативного прийняття рішень і безпеки населення, а масштабні бот-мережі на основі IoT-пристроїв дозволяють досягати інтенсивності атак у сотні гігабіт і навіть терабіт за секунду, суттєво ускладнюючи їх виявлення та нейтралізацію. Це зумовлює необхідність не лише сучасних технічних засобів захисту, а й регулярного тестування стійкості систем, що робить дослідження методів забезпечення кіберстійкості CPS (Cyber-Physical Systems) до DDoS-атак актуальним завданням національної безпеки.

Стрімкий розвиток інформаційних технологій та цифрової трансформації сприяв широкому впровадженню кіберфізичних систем (Cyber-Physical Systems, CPS) у різні сфери людської діяльності. Сьогодні такі системи є невід'ємною складовою критичної інфраструктури держави, забезпечуючи автоматизоване управління енергетичними комплексами, транспортними мережами, промисловими підприємствами, медичними установами, системами водопостачання, зв'язку, цивільного захисту та іншими важливими об'єктами. Основною особливістю кіберфізичних систем є інтеграція фізичних процесів із програмними компонентами та засобами мережевого обміну даними, що дозволяє здійснювати оперативний контроль, моніторинг і дистанційне керування обладнанням.

Поряд із численними перевагами цифровізації зростає і кількість кіберзагроз, здатних негативно впливати на роботу критично важливих об'єктів. Однією з найпоширеніших загроз є DDoS-атаки (Distributed Denial of Service), метою яких є порушення доступності інформаційних ресурсів шляхом надсилання великої кількості мережевих запитів із великої кількості заражених пристроїв. У результаті перевантажуються сервери, мережеве обладнання або канали зв'язку, що призводить до значного погіршення продуктивності або повної недоступності інформаційних сервісів.

Особливо небезпечними DDoS-атаки стають під час виникнення надзвичайних ситуацій, коли швидкість отримання та обробки інформації є критично важливою. Під час ліквідації наслідків аварій, стихійних лих, техногенних катастроф або воєнних дій інформаційні системи повинні забезпечувати безперервний обмін даними між диспетчерськими центрами, оперативними службами, системами автоматичного керування та виконавчими механізмами. Будь-яке порушення роботи таких систем може суттєво ускладнити процес прийняття рішень, збільшити час реагування та створити додаткові ризики для життя і здоров'я людей.

Слід зазначити, що сучасні DDoS-атаки постійно вдосконалюються. Зловмисники використовують великі бот-мережі, до складу яких можуть входити сотні тисяч або навіть мільйони заражених комп'ютерів, серверів, маршрутизаторів та пристроїв Інтернету речей (IoT). Завдяки цьому інтенсивність атак може досягати сотень гігабіт або навіть терабіт за секунду, що значно ускладнює їх своєчасне виявлення та нейтралізацію. Крім класичних об'ємних атак, широкого поширення набули атаки на прикладному рівні, які імітують поведінку реальних користувачів і є складнішими для фільтрації [9].

Для кіберфізичних систем критично важливо забезпечити не лише конфіденційність і цілісність інформації, а й високу доступність усіх компонентів системи. Саме доступність є однією з основних цілей DDoS-атак. Навіть незначні затримки у передачі команд або отриманні телеметричних даних можуть негативно вплинути на функціонування автоматизованих систем керування технологічними процесами. Наприклад, порушення роботи систем електропостачання або диспетчерського керування транспортною інфраструктурою може призвести до масштабних технічних збоїв і значних економічних втрат.

Ефективний захист кіберфізичних систем повинен базуватися на принципі багаторівневої безпеки. Одним із найважливіших заходів є сегментація мережі, яка дозволяє ізолювати критично важливі компоненти від загальнодоступних інформаційних ресурсів. Крім того, широко застосовуються між мережеві екрани нового покоління, системи запобігання

вторгненням (IPS), системи виявлення вторгнень (IDS), засоби аналізу мережевого трафіку, механізми обмеження швидкості надходження запитів (Rate Limiting), балансування навантаження між серверами та використання спеціалізованих сервісів очищення трафіку від шкідливих пакетів [10]. Узагальнену структуру багаторівневого підходу до забезпечення стійкості кіберфізичної системи до DDoS-атак наведено на рис. 1.

Не менш важливим є резервування критичних компонентів інформаційної інфраструктури. Використання декількох центрів обробки даних, резервних серверів, альтернативних каналів зв'язку та дублювання мережевого обладнання дозволяє забезпечити безперервність функціонування навіть у випадку виходу окремих елементів із ладу. Додатково застосовується автоматичне перемикання на резервні вузли без втручання оператора, що суттєво скорочує час відновлення працездатності системи.

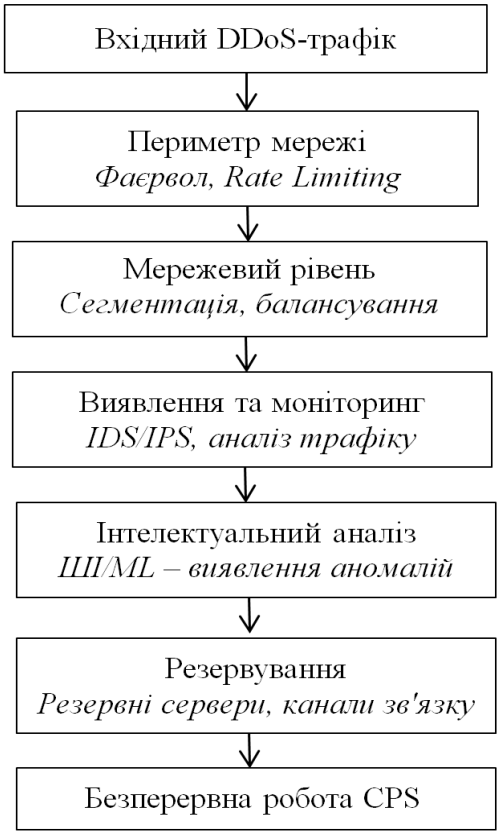

Рисунок 1 – Узагальнена схема забезпечення стійкості кіберфізичної системи до DDoS-атак

В останні роки дедалі більшої популярності набувають методи виявлення DDoS-атак із використанням технологій штучного інтелекту та машинного навчання. Такі алгоритми аналізують мережевий трафік у режимі реального часу, формують модель нормальної поведінки користувачів та здатні швидко виявляти аномальну активність. На відміну від традиційних сигнатурних методів, інтелектуальні алгоритми можуть ефективно виявляти навіть нові типи атак, що ще не були описані в базах сигнатур.

Важливу роль у забезпеченні стійкості відіграє постійний моніторинг технічного стану інформаційної інфраструктури. Системи моніторингу дозволяють контролювати завантаження процесорів, використання пам'яті, пропускну здатність мережі, кількість одночасних з'єднань, час відгуку серверів та інші параметри. Аналіз цих показників дає можливість своєчасно виявляти ознаки потенційної атаки та автоматично активувати засоби протидії.

Крім використання сучасних технічних засобів захисту, необхідно регулярно проводити тестування стійкості кіберфізичних систем до кіберінцидентів. Для цього застосовуються навчальні тренування, моделювання DDoS-атак, аудит інформаційної безпеки та оцінювання ризиків. Отримані результати дозволяють своєчасно виявляти слабкі місця інфраструктури та вдосконалювати механізми захисту.

Особливої актуальності питання кіберзахисту набувають в умовах сучасних воєнних конфліктів, коли інформаційна інфраструктура держави стає однією з першочергових цілей кібератак. Порушення роботи енергетичних об'єктів, транспортної системи, зв'язку або медичних установ може значно ускладнити ліквідацію наслідків надзвичайних ситуацій та негативно вплинути на безпеку населення. Саме тому забезпечення високої стійкості кіберфізичних систем є одним із ключових напрямів розвитку сучасної системи національної безпеки.

ВИСНОВКИ. Отже, забезпечення стійкості кіберфізичних систем до DDoS-атак потребує комплексного підходу, який поєднує сучасні засоби мережевого захисту, резервування критичних ресурсів, безперервний моніторинг, використання технологій штучного інтелекту, регулярне тестування інформаційної інфраструктури та оцінювання ризиків кібербезпеки. Реалізація такого підходу дозволяє підвищити надійність функціонування критичних об'єктів, забезпечити безперервність їх роботи навіть за умов масштабних кібератак та мінімізувати можливі наслідки надзвичайних ситуацій. Використання резервних серверів, альтернативних каналів зв'язку та автоматичного перемикання на резервні вузли дозволяє зменшити залежність CPS від відмови окремих компонентів та скоротити час відновлення працездатності. Застосування методів штучного інтелекту та машинного навчання розширює можливості виявлення аномальної мережевої активності, зокрема атак, які складніше виявити традиційними сигнатурними методами. Таким чином, поєднання багаторівневого мережевого захисту, резервування, інтелектуального моніторингу та регулярного тестування створює основу для підвищення кіберстійкості критичних об'єктів, підтримання безперервності роботи CPS та мінімізації наслідків DDoS-атак в умовах надзвичайних ситуацій і воєнних конфліктів.

ЛІТЕРАТУРА

1. Nevliudov, I. & et al. (2026). Implementing Industry 5.0 technologies in civil safety emergency systems for intelligent management. Scientific Forum: Theory and Practice of Research: Collection of Scientific Papers «SCIENTIA» with Proceedings of the XII International Scientific and Theoretical Conference, July 17, 2026. San Francisco, USA: International Center of Scientific Resea, 2026, pp. 337-339

2. Sotnik, S. V. (2024). Analysis of Personal Information Security Issues in Peacetime and Wartime. International Journal of Academic Engineering Research (IJAER), 2024, Vol. 8 Issue 10, pp. 108-113

3. Ievtushenko, V. I., & et al. (2026). The development of information control systems for technological purposes. Computer-integrated technologies, automation and robotics 2026: Proceedings of III st All-Ukrainian Conference, Kharkiv, May 14-15, 2026: Thesises of Reports, 2026, pp. 39-43

4. Andreiev, A. S., & et al. (2025). Information technology in medicine. Information Technologies and Automation – 2025 / Proceedings of the XVIII International Scientific and Practical Conference. Odessa, October 30-31, 2025. – Odessa, ONUT Publishing House, 2025, pp. 1207-1209

5. Levenets, I. O., & et al. (2025). The role of artificial intelligence in optimizing information retrieval systems. Information Technologies and Automation – 2025 / Proceedings of the XVIII International Scientific and Practical Conference. Odessa, October 30-31, 2025. – Odessa, ONUT Publishing House, 2025, pp. 975-977

6. Sotnik, S. V. (2024). Features of using REST architecture for development of ARS for information systems. Міжнародна науково-практична конференція «Інформаційні системи в управлінні проєктами та програмами», Коблево, 9–13 вересня 2024 р. Збірник праць. – Харків: ХНУРЕ, 2024, pp. 42-45

7. Tverdokhlib, A., & et al. (2024). The Intelligent tools for optimizing information and search engines. Manufacturing & Mechatronic Systems 2024: Proceedings of VIII st International Conference, Kharkiv, October 25-26, 2024, pp. 28-31

8. Sotnik, S. V. (2025). Support systems for robotics: principles, algorithms and development prospects. Journal of natural sciences and technologies, 2025, 4(2), pp. 419-430. DOI: 10.5281/zenodo.18088674

9. Almeghlef, S. M., & et al. (2023). Application layer-based denial-of-service attacks detection against IoT-CoAP. Electronics, *12*(12), 2563.

10. Bouhdada, J. (2024). Securing Industrial Control Systems and Safety Instrumented Systems: A practical guide for safeguarding mission and safety critical systems. Packt Publishing Ltd., 256 p.