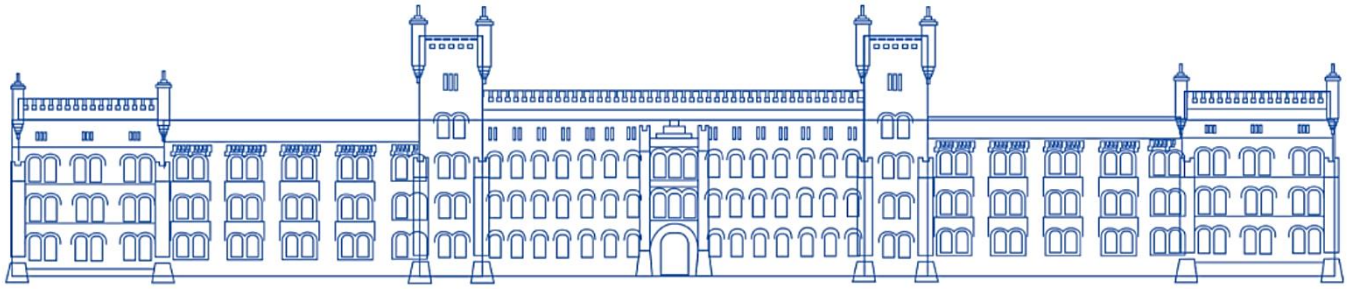
ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ



ЦИВІЛЬНИЙ ЗАХИСТ В УМОВАХ ВІЙНИ

Збірник тез доповідей
І Міжнародної науково-практичної конференції

17-18 квітня 2025 року

Цивільний захист в умовах війни : збірник тез доповідей І Міжнародної науково-практичної конференції, м. Львів, 17-18 квітня 2025 року. Львів: ЛДУ БЖД, 2025. 298 с.

У збірнику тез І Міжнародної науково-практичної конференції «Цивільний захист в умовах війни» висвітлено досвід сучасних тенденцій й викликів в організації цивільного захисту в умовах війни, а також формування основних напрямків вдосконалення та розвитку системи цивільного захисту.

Для наукових, науково-педагогічних та педагогічних працівників закладів освіти, працівників наукових, виробничих установ, підрозділів ДСНС України, представників державних та місцевих органів влади, громадських і професійних організацій та здобувачів освіти.

Автори несуть особисту відповідальність за зміст представлених публікацій, достовірність результатів і дотримання вимог академічної доброчесності. Оргкомітет не несе відповідальності за порушення правил правопису в друкованих авторських матеріалах.

розроблення та погодження паспорта безпеки на об'єкт критичної інфраструктури. Порядком передбачено вимоги до розроблення оператором критичної інфраструктури паспорта безпеки та його складових, а також механізм його погодження секторальними і функціональними органами у сфері захисту критичної інфраструктури.

Слід відзначити, що серед суб'єктів національної системи захисту критичної інфраструктури і Державна служба України з надзвичайних ситуацій – центральний орган виконавчої влади, який реалізує державну політику у сфері цивільного захисту. Національна система захисту критичної інфраструктури взаємодіє з єдиною державною системою цивільного захисту.

Впродовж останніх років питання захисту об'єктів критичної інфраструктури досліджували С. Азаров, Л. Арсенович, Д. Бірюков, Б. Богдан, О. Возненко, А. Гаврись, О. Герасименко, І. Гора, С. Єременко, Р. Іваненко, О. Калиновський, С. Кармазін, С. Кондратов, В. Крикун, С. Мельник, П. Підюков, М. Погребицький, П. Пригунов, А. Пруський, І. Рощина, В. Сидоренко, І. Соколовський, Я. Страхніцький, О. Суходоля, О. Тесленко, В. Тищенко, Н. Тур, В. Філіппова, В. Франчук, С. Чумаченко, О. Шпатакова, В. Юрченко, О. Яременко та інші.

Автором тез комплексно розглянуто питання державної політики та державного управління у сфері захисту критичної інфраструктури, зокрема в умовах дії воєнного стану, залучення до цієї діяльності ДСНС як суб'єкта національної системи захисту критичної інфраструктури [4].

Як висновок, питання подальшого розвитку національної системи захисту об'єктів критичної інфраструктури, її функціонування в умовах воєнного стану потребують подальшого проведення наукових досліджень, практичного впровадження їх результатів в діяльність суб'єктів національної системи захисту об'єктів критичної інфраструктури.

ЛІТЕРАТУРА

1. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882 - IX. Дата оновлення: 21.09.2024. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 08.04.2025)

2. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості»: Указ Президента України від 27.09.2021 р. № 479/2021. URL: https://zakon.rada.gov.ua/laws/show/n0065525-21#Text (дата звернення: 08.04.2025)

3. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної стійкості України: постанова Кабінету Міністрів України від 12.07.2022 р. № 787. URL: https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Textt (дата звернення: 08.04.2025)

4. Бойко О. Державна політика та державне управління у сфері захисту критичної інфраструктури. *Науковий вісник: Державне управління.* 2024. № 2 (16). С. 137–156. URL: https://doi.org/10.33269/2618-0065-2024-2(16)-137-156 (дата звернення: 08.04.2025).

УДК: 004.056.5:621.39(477)

КІБЕРБЕЗПЕКА: КОМПЛЕКС ЗАХОДІВ ЩОДО ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ СУЧАСНИХ ЗАГРОЗ

Р. Л. Ткачук, д.т.н., професор, А. М. Ткаченко
Львівський державний університет безпеки життєдіяльності

Критична інфраструктура виступає фундаментом функціонування та стабільності будь-якої держави, оскільки забезпечує безперервність надання життєво важливих послуг у таких

сферах, як енергетика, водопостачання, транспорт і телекомунікації. В умовах зростання масштабів кіберзагроз, зокрема в контексті збройної агресії російської федерації проти України, питання забезпечення кібербезпеки об'єктів критичної інфраструктури набуває особливого значення.

Кіберзлочинні дії, спрямовані на порушення функціонування інфраструктурних інформаційних систем, здатні спричинити не лише технічні збої, а й масштабні економічні, соціальні та гуманітарні наслідки. У цьому контексті особливу небезпеку становлять розподілені атаки типу відмови в обслуговуванні (DDoS), розповсюдження шкідливого програмного забезпечення, зокрема комп'ютерних вірусів, а також цілеспрямовані кібератаки на енергетичні системи, об'єкти військового призначення та інформаційні ресурси [1].

Досвід України, набутий у процесі збройного протистояння з державою-агресором, засвідчує суттєве зростання інтенсивності та масштабування кіберзагроз, спрямованих проти критичних секторів державної інфраструктури. Зокрема, у 2020 році Службою безпеки України було зафіксовано близько 800 спроб кібератак, а вже у 2021 році їх кількість зросла майже вдвічі — до приблизно двох тисяч. Після початку повномасштабного вторгнення у 2022 році кількість кібератак перевищила 4500 інцидентів. А станом на 18 лютого 2023 року СБУ нейтралізувала понад 550 цілеспрямованих атак, ініційованих хакерськими угрупованнями, що діють в інтересах держави-агресора. Незважаючи на високу інтенсивність та скоординованість цих загроз, значна їх частина була локалізована українськими фахівцями ще на початкових стадіях. Основними об'єктами атак виступають логістична та транспортна інфраструктура, підприємства паливно-енергетичного комплексу, а також об'єкти військового призначення [2].

Забезпечення належного рівня кібербезпеки критичної інформаційної інфраструктури потребує впровадження комплексу технічних та організаційних заходів. Одним із базових компонентів такої системи захисту, на нашу думку, виступає конфігурування міжмережевих екранів (фаєрволів) на всіх робочих станціях і серверах з метою запобігання несанкціонованому мережевому трафіку. У контексті використання різних операційних систем доцільним є застосування відповідних програмних рішень: зокрема, для систем на базі Linux ефективним інструментом є UFW (Uncomplicated Firewall), а для середовища Windows — SimpleWall, які забезпечують зручне керування правилами доступу та фільтрації трафіку на локальних вузлах [3].

Розглянемо більш детальніше пропоновані програмні рішення для двох вище згаданих операційних систем:

1. UFW (Linux)

UFW є зручним інтерфейсом до iptables, що дозволяє легко налаштувати фаєрвол у Linux-системах.

Налаштування:

Встановлення (якщо не встановлено):

– sudo apt update;

– sudo apt install ufw.

Увімкнення фаєрвола:

– sudo ufw enable.

Налаштування політик за замовчуванням:

– sudo ufw default deny incoming;

– sudo ufw default allow outgoing.

Дозвіл доступу до необхідних сервісів (наприклад, SSH):

– sudo ufw allow ssh.

Перевірка статусу:

– sudo ufw status verbose.

Рекомендації:

– заборонити всі вхідні з'єднання, крім необхідних сервісів.

– використовувати лише дозволені порти.

– регулярно переглядати лог файли /var/log/ufw.log.

2. SimpleWall (Windows)

SimpleWall — це легкий, але ефективний фаєрвол-контролер для Windows, що працює поверх вбудованих фільтрів Windows Filtering Platform (WFP).

Налаштування:

– увімкнення фільтрації мережі;

– встановлення режиму "Whitelist" — дозволити лише затверджені додатки;

– додавання до списку дозволених тільки критично необхідних системних процесів та служб (наприклад, svchost.exe, explorer.exe);

– налаштування правил для конкретних IP-адрес або портів, якщо потрібно;

– увімкнення логування всіх спроб з'єднань.

Рекомендації:

– створити централізовану політику конфігурацій SimpleWall через шаблони;

– забезпечити захист від змін налаштувань користувачами;

– використовувати режим блокування за замовчуванням.

Загалом, налаштування локальних фаєрволів значно підвищує рівень безпеки мережевої взаємодії та знижує ризик зовнішніх атак. Усі зміни мають супроводжуватись документацією, резервним копіюванням конфігурацій та регулярним аудитом.

Таким чином, захист критичної інфраструктури потребує реалізації багаторівневої та цілісної стратегії, що охоплює формування національної політики кібербезпеки, інтеграцію заходів кіберзахисту до загальної системи національної безпеки, впровадження ефективних систем захисту інформаційно-чутливих ресурсів, систем раннього виявлення кіберзагроз, розробку дієвих механізмів оперативного реагування, а також створення резервних інструментів для відновлення функціонування інформаційно-комунікаційних систем після кібератак.

Ключовим чинником ефективної протидії кіберзагрозам виступає підготовка висококваліфікованих кадрів через впровадження спеціалізованих освітніх програм, тренінгів та систем сертифікації. Відповідно, формування надійного нормативно-правового поля у сфері кібербезпеки є необхідною умовою забезпечення стійкості критичної інфраструктури. У цьому контексті пріоритетом національної політики України має бути створення дієвої системи кіберзахисту, як складової загальної системи безпеки держави в умовах гібридної війни та постійного зростання цифрових загроз.

ЛІТЕРАТУРА

1. Боднар О., Ткачук Р. Л. Тактика моделей cyber kill chain і unified kill chain: розкриття анатомії кібератак. Інформаційна безпека та інформаційні технології : зб. тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів. (Львів, 30 листопада 2023 р.). Львів : ЛДУБЖД, 2023. С. 22–27.

2. Цього року СБУ уже нейтралізувала понад 500 російських кібератак. URL: https://www.slovoidilo.ua/2023/02/18/novyna/bezpeka/czoho-roku-sbu-uzhe-nejtralizuvala-500-rosijskyx-kiberatak

3. Ткачук Р. Л., Івануса А. І. Засоби захисту інформації у веб-системах. Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України : матеріали Науково-практичної конференції (Львів, 20 грудня 2024 р.). Львів : ЛьвДУВС, 2025. С. 119–123.

СЕКЦІЯ 3
ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ