ГЛОБАЛЬНІ ВИКЛИКИ СУЧАСНОСТІ

ТА ШЛЯХИ ЇХ ВИРІШЕННЯ:

НАУКОВИЙ І ПРАКТИЧНИЙ ДИСКУРС

Збірник науково-практичної конференції

20 БЕРЕЗНЯ 2026

Вінниця

УДК 316.32:001.89:340.1

Г54 Глобальні виклики сучасності та шляхи їх вирішення: науковий і практичний дискурс: зб. матеріалів наук.практ.конф. (м. Вінниця, 20 березня. 2026 р.): Громадська Організація «Центр Науково-Дослідних Ініціатив., Вінниця: «ГО ЦНДІ» 2026.

Збірник містить наукові розробки науковців, представників практичних підрозділів Національної поліції та інших правоохоронних органів, докторантів, аспірантів та здобувачів вищої освіти, присвячені дослідженню теоретичних і прикладних аспектів розвитку взаємодії органів публічної влади та правоохоронних органів

Матеріали викладені в авторській редакції з незначними коректорськими правками.
Відповідальність за точність поданих фактів, цитат, цифр і прізвищ несуть автори.

Електронна копія матеріалів круглого столу безоплатно розміщується у відкритому доступі на сайті Громадської організації «Центр Наукового-Дослідних Ініціатив» у розділі «Архів наукових заходів», сторінка «Збірники наукових заходів» https://gocsri.com/index.php/index/uk/index

РЕДАКЦІЙНА КОЛЕГІЯ

СУДИН Андрій Андрійович,

львівський національний університет імені Івана Франка, аспірант

АНАЛІЗ КІБЕРЗАГРОЗ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Аналіз кіберзагроз об'єктів критичної інфраструктури є важливим для забезпечення національної безпеки. Ці об'єкти є основою функціонування держави та економіки, а їхній захист від кіберзагроз вимагає детального вивчення можливих атак [1]. Кіберзагрози можуть спричинити серйозні наслідки, такі як порушення роботи енергетичних, транспортних та комунікаційних систем, що викликає економічні та соціальні кризи [2]. Ураховуючи глобальну взаємозалежність, навіть незначні порушення можуть мати широкомасштабні наслідки.

Кіберзагрози, зокрема шкідливе програмне забезпечення, атаки на мережі, зломи та маніпуляції даними, стають все більш складними та невидимими для традиційних систем захисту. Технічні атаки, такі як DDoS-атаки, можуть паралізувати системи критичної інфраструктури на кілька годин або навіть днів, що спричиняє значні фінансові та репутаційні збитки. Сучасні методи кібербезпеки повинні включати не тільки технологічні інструменти, а й стратегії оперативного реагування на нові типи загроз.

З розвитком Інтернету речей (IoT) збільшується кількість вразливих точок доступу до критичних об'єктів інфраструктури. У разі атак на ці системи може виникнути серйозна загроза для фізичних об'єктів, таких як енергетичні станції чи водопостачальні мережі. Навіть незначний збій у роботі таких систем може призвести до великих економічних витрат, відновлення яких може зайняти багато часу, що впливає на стабільність усієї країни.

Аналіз кіберзагроз потребує впровадження інтелектуальних систем моніторингу, що здатні виявляти аномалії в реальному часі. Системи на основі машинного навчання можуть швидко адаптуватися до нових патернів атак,

покращуючи швидкість реагування. Вони забезпечують оперативне виявлення загроз на всіх етапах, що дає можливість миттєво зупинити атаки, перш ніж вони зможуть завдати серйозної шкоди критичним об’єктам інфраструктури.

Людський фактор є не менш важливим у забезпеченні кібербезпеки об’єктів критичної інфраструктури. Помилки, невиконання стандартів безпеки чи ненавмисне надання доступу до конфіденційної інформації можуть призвести до серйозних уразливостей у системах захисту, що підтверджують численні випадки, коли недбале поводження з даними або ігнорування протоколів безпеки ставало причиною успішних атак на великі організації.

Аналіз кіберзагроз вимагає комплексного підходу до захисту, що включає ідентифікацію, оцінку ймовірності загроз, а також формування стратегій для зменшення ризиків. Моделювання можливих сценаріїв атак дозволяє ефективно передбачити розвиток ситуацій та визначити слабкі місця в існуючих системах безпеки, що дає змогу вчасно розробити та впровадити заходи для мінімізації потенційних втрат від кіберзагроз.

Методи захисту критичних інфраструктур повинні включати не тільки програмні рішення, але й організаційні заходи. Створення резервних каналів зв’язку, багаторазових систем резервування даних та багаторівневих систем доступу є важливими для забезпечення безперебійної роботи в разі кібернападів. Відсутність таких заходів може призвести до того, що навіть невелика атака на одну з точок доступу викличе системну кризу у всій інфраструктурі.

Міжнародна співпраця в боротьбі з кіберзагрозами є необхідною умовою для захисту критичних інфраструктур. Спільне обміну інформацією між державами та міжнародними організаціями допомагає швидко виявляти нові загрози та розробляти спільні стратегії для їх подолання, що особливо важливо у контексті глобалізації, де кіберзагрози можуть мати міжнародний характер і впливати на безпеку декількох країн одночасно.

Використання новітніх технологій, таких як квантове шифрування та блокчейн, має великий потенціал у забезпеченні безпеки критичних

інфраструктур. Зазначені технології можуть значно ускладнити можливість маніпулювання даними чи проникнення в системи через вразливості в старих алгоритмах шифрування, які відкривають нові горизонти для створення більш стійких та ефективних механізмів захисту від кіберзагроз.

Важливим етапом у забезпеченні кібербезпеки є постійне тестування систем захисту на стійкість до нових типів атак. Регулярне проведення стрес-тестів та аудиту кіберзахисту дозволяє виявити уразливі місця до того, як вони стануть ціллю для зловмисників. Оцінка ефективності систем має бути постійною, з урахуванням нових технологій та методів атаки.

Оцінка кіберризиків повинна бути невід'ємною частиною стратегічного планування для критичних інфраструктур. Врахування потенційних загроз і розробка на їх основі відповідних заходів зменшить ймовірність серйозних фінансових і соціальних втрат. Без ефективної оцінки ризиків неможливо створити надійний план захисту, який гарантуватиме стабільність і безпеку критичних об'єктів інфраструктури.

Захист об'єктів критичної інфраструктури в умовах швидко змінюваних кіберзагроз вимагає не тільки технологічних рішень, а й побудови стійких організаційних структур для забезпечення безпеки. Важливим етапом є інтеграція кібербезпеки в загальну стратегію розвитку та управління інфраструктурою. Наявність спеціалізованих команд з кіберзахисту, які працюють у тісній взаємодії з технічними, операційними та правовими відділами компанії, допомагає забезпечити системний підхід до боротьби з кіберзагрозами, що сприяє швидкому реагуванню на атаки та виявленню потенційних уразливостей на етапі їх формування.

Сучасні кіберзагрози мають не тільки технічний, але й психологічний компонент, оскільки вони можуть бути спрямовані на дестабілізацію психологічного стану персоналу критичних об'єктів інфраструктури. Вплив на людський фактор через фішинг, соціальні маніпуляції та дезінформацію може спричинити помилки, які дозволяють атакувати критично важливі системи. Для запобігання таким інцидентам необхідно впроваджувати комплексні

програми тренувань та навчання персоналу, які допомагають підвищити рівень обізнаності про потенційні кіберзагрози.

Особливу увагу необхідно приділяти питанням збереження конфіденційності даних, оскільки витік чи маніпуляції з чутливою інформацією можуть мати катастрофічні наслідки. Відповідно до міжнародних стандартів, всі дані, що зберігаються чи передаються через системи критичної інфраструктури, повинні бути надійно захищені шифруванням, а доступ до них—строго регламентований. Витік персональних даних чи інформації про інфраструктуру може не тільки знизити рівень довіри до інфраструктури, але й стати основою для подальших кіберзлочинів або атак.

У зв'язку зі збільшенням кількості кіберзагроз важливим напрямком є розробка та впровадження процедур для відновлення критичних інфраструктур після кібернападів. Окреслені процедури повинні включати не тільки відновлення програмного забезпечення та апаратних засобів, але й план дій для швидкої реактивації функціонування об'єктів критичної інфраструктури. Для цього потрібна наявність резервних копій критичних даних, швидкий доступ до альтернативних систем управління та відповідні технічні ресурси, що забезпечують мінімізацію часу простою після атак.

Особливості сучасних кіберзагроз для критичної інфраструктури також включають адаптацію атак до нових технологічних змін. З розвитком 5G та інших комунікаційних технологій збільшується кількість можливих точок доступу до мереж, що створює нові ризики для безпеки. Атаки можуть бути спрямовані на викрадення або блокування даних, що передаються через нові мережі, а також на створення конфліктів між різними компонентами інфраструктури, що вимагає постійного оновлення стратегій кібербезпеки, інтеграції нових методів захисту та оцінки ризиків у процесі розвитку технологій.

Значення державного регулювання в сфері кібербезпеки не можна недооцінювати, оскільки державні установи виконують функцію контролю за

дотриманням стандартів безпеки на рівні національної інфраструктури. Законодавчі ініціативи, спрямовані на створення національних стандартів кібербезпеки, впровадження обов'язкових перевірок та аудитів інфраструктури, а також посилення відповідальності за кіберзлочини, значно підвищують ефективність захисту. Спільна робота урядів, бізнесу та міжнародних організацій є важливим кроком у створенні глобальної системи протидії кіберзагрозам.

Підвищення стійкості критичної інфраструктури до кіберзагроз потребує комплексного підходу до модернізації існуючих технологій. Оновлення програмного забезпечення та апаратних засобів має бути регулярним процесом, щоб захистити системи від нових уразливостей. Враховуючи постійний розвиток новітніх технологій та зміну типів загроз, оновлення базових інфраструктурних елементів має бути на постійному контролі, а зміни повинні впроваджуватися із врахуванням найновіших стандартів безпеки.

Таким чином, захист об'єктів критичної інфраструктури від кіберзагроз є складним і багатогранним завданням, що вимагає постійного вдосконалення як технологічних, так і організаційних заходів. Враховуючи зростання кількості і складності кібернападів, важливим є інтегрування сучасних методів моніторингу, аналізу загроз і постійного оновлення стратегій безпеки. Ключовими елементами ефективного захисту є технології шифрування, багаторівневий контроль доступу, а також комплексне навчання персоналу для підвищення обізнаності щодо потенційних кіберризиків.

Розвиток нових технологій, таких як Інтернет речей (IoT), 5G та квантові обчислення, відкриває нові можливості для атак, що вимагає адаптації існуючих систем безпеки до цих змін. Постійне вдосконалення національних та міжнародних стандартів кібербезпеки, а також активна співпраця між державами та приватним сектором, є необхідними для створення ефективної системи захисту критичних інфраструктур від кіберзагроз.

Список використаних джерел

1. Гаврись А. П., Філіппова В. В., Тур Н. Ю. Інформаційний аналіз систем захисту об’єктів критичної інфраструктури в період дії воєнного стану. *Вісник Львівського державного університету безпеки життєдіяльності*. 2024. № 30. С. 173–187. doi: 10.32447/20784643.30.2024.17.

2. Ільєнко А., Телющенко В., Дубчак О. Сучасні кіберзагрози критичної інфраструктури України та світу. *Кібербезпека: освіта, наука, техніка* : Електронне фахове наукове видання**.** 2025. № 3 (27). С. 150–164. doi: 10.28925/2663-4023.2023.27.719

ГЛОБАЛЬНІ ВИКЛИКИ СУЧАСНОСТІ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ: НАУКОВИЙ І ПРАКТИЧНИЙ ДИСКУРС

Збірник матеріалів

Науково-практичної конференції

(м. Кам'янське, 20 березня 2026 року)

Відповідальні за випуск: Л.П. ЗІНЧЕНКО

Комп'ютерне верстання: Н.М. ОСТАПОВА

Видавець і виготовлювач – Електронний формат збірнику

Громадська Організація «Центр Науково-Дослідних Ініціатив»

М. Вінниця