КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1190
УДК 004.056

Івкова Валерія Сергіївна
асистент кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID: 0000-0002-2370-1497
valeriia.s.ivkova@lpnu.ua

Леонов Андрій Володимирович
студент кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID: 0009-0008-1615-297X
andrii.leonov.kb.2023@lpnu.ua

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД OSINT-РОЗВІДКИ В УМОВАХ ВІЙНИ

Анотація. У статті вирішується актуальне науково-практичне завдання щодо підвищення рівня кіберстійкості та фізичної безпеки об’єктів критичної інфраструктури (КІ) України в умовах війни. Проаналізовано трансформацію розвідки на основі відкритих джерел (OSINT) з допоміжного аналітичного інструменту в ключовий елемент наведення високоточної зброї та планування деструктивних кібератак. На основі аналізу останніх інцидентів ідентифіковано та систематизовано критичні вектори загроз: технічну індексацію вразливостей промислових систем (ОТ) через пошукові системи IoT (Shodan, Censys), геопросторовий моніторинг змін інфраструктури за допомогою комерційних супутникових знімків та витоки чутливої інформації через соціальну інженерію (SOCMINT). Основна увага в роботі приділена розробці комплексної методики протидії, яка виходить за межі традиційного периметрального захисту. Обґрунтовано доцільність застосування стратегії мінімізації цифрового сліду (Digital Footprint Reduction) згідно зі стандартами NIST SP 800-82r3, що включає глибоку сегментацію мереж, використання діодів даних та обфускацію банерів обладнання. Детально розглянуто імплементацію технологій активного обману (Deception Technology) – впровадження ешелонованої системи пасток (Honeytokens, Honeypots) для дезорієнтації ворога та сповільнення процесу прийняття ним рішень (OODA loop). Запропоновано організаційні заходи щодо контррозвідувального моніторингу та регламентації публічної інформації, що дозволяє суттєво знизити ефективність ворожої розвідки ще на етапі збору даних. Практична цінність дослідження полягає у створенні адаптивного алгоритму захисту, який ускладнює верифікацію цілей агресором.

Ключові слова: критична інфраструктура, OSINT-розвідка, кібербезпека, SCADA-системи, Deception Technology, мінімізація цифрового сліду, Shodan, активний захист.

ВСТУП

З початком повномасштабного вторгнення РФ кіберпростір став повноцінним театром бойових дій. Сучасне протистояння характеризується не лише застосуванням конвенційної зброї, але й масовим використанням інформаційних технологій для розвідки, коригування вогню та дестабілізації об’єктів критичної інфраструктури (ОКІ). Як зазначають фахівці Національного координаційного центру кібербезпеки (НКЦК), у 2024 році російська кіберзагроза демонструє новий рівень агресії та маневреності, що дає підстави говорити про ведення «першої світової кібервійни» [1, с. 36].

Актуальність теми дослідження зумовлена тим, що в умовах війни розвідка на основі відкритих джерел перетворилася з допоміжного аналітичного інструменту на

потужну зброю, що використовується ворогом для підготовки ракетно-дронових ударів. Статистика свідчить про сталу тенденцію ескалації: за перше півріччя 2023 року кількість зареєстрованих кіберінцидентів в Україні зросла на 123% порівняно з аналогічним періодом 2022 року (з 342 до 762 випадків) [2, с. 7]. При цьому проглядається зміна вектору атак від хаотичного деструктиву до цілеспрямованого шпигунства та збору даних про критичні об'єкти, що підтверджується зростанням кількості операцій із прихованого збору інформації [2, с. 4].

Як зазначається у попередніх дослідженнях [3], ключова роль OSINT полягає у створенні цілісного інформаційного поля, що поєднує відкриті джерела з технічними (SIGINT) та геопросторовими (GEOINT) даними, що в умовах війни дозволяє ворогу формувати повний профіль цілі.

Особливу загрозу становить використання ворогом комерційних супутникових знімків, отриманих через третіх осіб, очевидно, для планування атак на інфраструктуру. Проаналізувавши 321 ракетний удар (в період з 24 лютого по 31 грудня 2022 року) ми виявили, що у 277 випадках (понад 86%) за кілька днів до атаки здійснювалось замовлення супутникових знімків відповідної локації через сервіси на кшталт Maxar або Planet [4]. Це підтверджує тезу, що відкриті дані стають елементом ланцюга ураження (kill chain) у сучасній війні.

Українська наукова спільнота та представники сектору безпеки наголошують на необхідності перегляду підходів щодо захисту інформації. Зокрема, заступник Секретаря РНБО України Сергій Демедюк акцентує увагу на тому, що інтеграція OSINT у систему національної безпеки є стратегічним завданням, оскільки цей інструмент виступає одночасно як засіб превентивного виявлення загроз, як канал витоку чутливої інформації [5, с. 58]. За таких умов, коли ворог використовує всі доступні цифрові сліди для завдання збитків, захист об'єктів критичної інфраструктури вимагає впровадження комплексних контр-розвідувальних заходів у відкритому інформаційному просторі.

Постановка проблеми. Суттєвою проблемою захисту об'єктів критичної інфраструктури в умовах сучасного конфлікту є парадокс доступності відомостей про архітектуру та конфігурацію систем у відкритому доступі. Традиційні системи захисту периметра (Firewalls, IDS/IPS) ефективно протидіють прямим вторгненням, але вони безсилі проти розвідки, що в загальному ведеться легальними методами через відкриті джерела. Велика кількість компонентів операційних технологій (OT) та систем диспетчерського контролю (SCADA), які забезпечують функціонування енергетики, водопостачання та транспорту, залишаються видимими для спеціалізованих пошукових систем.

Дослідження з використанням пошукової системи Shodan свідчать про масштабну видимість об'єктів критичної інфраструктури для зовнішніх користувачів. Тисячі контролерів (PLC) та інтерфейсів людино-машинної взаємодії доступні без належної автентифікації, що дозволяє зловмисникам збирати технічні метадані (версії прошивок, типи протоколів, IP-адреси) без значної затрати сил і ресурсів [6, с. 1]. Історична відсутність механізмів шифрування у промислових протоколах (Modus, Ethernet/IP) робить їх вразливими до зовнішнього сканування. Ситуація ускладнюється тактикою ворога щодо повторних ударів по раніше розвіданих цілях та експлуатацією вразливостей у ланцюгах постачання. Це зумовлює критичну необхідність переходу від пасивного захисту до стратегії Counter-OSINT із застосуваннях методик дезінформації.

Аналіз останніх досліджень і публікацій. Проблематика протидії розвідці за відкритими джерелами набула критичного значення в умовах сучасних міждержавних

конфліктів [7]. Проаналізувавши останні дослідження, ми дійшли висновку про наявність суттєвого розриву між класичними підходами до кібербезпеки та реальними загрозами воєнного часу [8].

Зокрема, базові міжнародні стандарти захисту операційних технологій (ОТ), викладені в керівництві NIST SP 800-82r3, суттєво розширили парадигму безпеки. Цей документ інтегрує сучасні підходи, такі як концепція «нульової довіри» (Zero Trust) та управління ризиками ланцюгів постачання. Однак, незважаючи на актуальність, стандарт залишається інструкцією із забезпечення внутрішньої архітектурної стійкості та захисту від активних вторгнень [9]. Він практично не охоплює методи протидії пасивній розвідці та маскування цифрового сліду об’єкта в глобальній мережі, що є критичним для захисту від OSINT.

Це підтверджують дослідження Д. Канта та Р. Кройцбурга [6], які доводять, що навіть за умови дотримання технічних регламентів, значна кількість компонентів критичної інфраструктури (SCADA, контролери) залишається видимою для спеціалізованих пошукових систем (типу Shodan). Специфіка промислових протоколів, які історично розроблялися без функцій маскування, дозволяє агресору проводити ідентифікацію цілей без прямого контакту з ними.

Перспективним напрямом, що виходить за межі класичних стандартів, є впровадження технологій активної протидії. Дослідники С. Хан та Н. Хейр обґрунтовують ефективність застосування методів введення в оману – «Deception Technologies» [10]. Ці методи дозволяють не просто захищати периметр, а створювати хибні цілі для виснаження ресурсів ворожої розвідки, що ще мало інтегровано в українські практики [11].

Водночас у звітах Національного координаційного центру кібербезпеки [1] та наукових працях дослідників ЛьвДУВС під редакцією І. О. Ревака [5] акцентується увага на тому, що в умовах війни захист має включати елементи контррозвідки, так як Counter-OSINT. Оскільки ворог використовує відкриті дані та супутникові знімки для наведення кінетичної зброї, пасивний кіберзахист перестає бути достатнім заходом безпеки [12, с.170].

Таким чином, існує потреба в доповненні архітектурних вимог NIST r3 методами оперативного маскування та дезінформації.

Метою статті є розробка комплексної моделі захисту об’єктів критичної інфраструктури від розвідки за відкритими джерелами, яка, на відміну від класичних підходів периметрального захисту, базується на мінімізації цифрового сліду, впровадженні технологій дезінформування та алгоритмів контр-OSINT моніторингу.

Завдання дослідження:

1. Дослідити сучасний інструментарій OSINT як вектор критичної загрози для операційних систем та промислових технологій.
2. Обґрунтувати застосування технологій маскування та дезінформування для нейтралізації розвідувальних дій.
3. Розробити практичні рекомендації щодо мінімізації цифрових слідів об’єктів інфраструктури.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Класифікація та аналіз векторів OSINT-розвідки проти об'єктів критичної інфраструктури.

Дослідження сучасного інструментарію передбачає декомпозицію загроз, що формуються на основі відкритих даних. Проведений аналіз інцидентів на основі звітів CERT-UA та НКЦК [1, 2] дозволяє стверджувати, що сучасна розвідка проти об'єктів критичної інфраструктури трансформувалася в мультимодальну систему збору даних. На відміну від класичного шпигунства, вона не вимагає фізичного проникнення, а використовує цифрові сліди, які генерують технологічні мережі, персонал та фізичні об'єкти.

Систематизація виявлених загроз дозволяє виділити три критичні вектори, які формують поверхню атаки: технічний (Network Intelligence/TECHINT), геопросторовий (IMINT/GEOINT) та соціально-кадровий (SOCMINT).

Технічний вектор: індексація промислових протоколів та вразливостей.

Найбільш деструктивним вектором для операційних технологій є використання спеціалізованих пошукових систем (Shodan, Censys, ZoomEye), які автоматизують процес розвідки у глобальному масштабі. Згідно з дослідженнями Канта та ін. [6], механізм загрози полягає у пасивному зборі "банерів" – текстових метаданих, які повертають мережеві пристрої у відповідь на запит встановлення з'єднання (Handshake).

Аналіз архітектури SCADA-систем вказує на критичну вразливість протоколів прикладного рівня, які розроблялися без урахування вимог безпеки (Security-by-Design). Агрегація даних через Shodan дозволяє зловмиснику отримати специфічну інформацію без прямого сканування цільової мережі, що дозволяє обійти системи виявлення вторгнень (IDS).

Основні ідентифікатори компрометації (IoC), доступні через технічний OSINT:

1. Відкриті порти промислової автоматизації. Дослідження показує [6, с. 4], що наявність в індексі пошуковика порту 502 (Modbus TCP) або 102 (Siemens S7Comm) є прямим вектором для атаки типу Command Injection. Протокол Modbus у стандартній реалізації не має автентифікації, тому зловмисник, знайшовши IP-адресу через запит «port:502» в сервісах накшталт «Shodan», може віддалено надсилати команди на запис у регістри контролера, що призводить до аварійної зупинки технологічного процесу.

2. Деанонімізація обладнання через банери. Серверні відповіді часто містять точні версії прошивок. Наприклад, банер «Server: Moxa NPort 5110» дозволяє зловмиснику миттєво знайти відповідний експлойт у базі CVE ще до початку активної фази атаки.

3. Незахищені інтерфейси HMI (Human-Machine Interface). Виявлено, що значна частина панелей керування використовує VNC на порту «5900» без пароля або зі слабкими обліковими даними за замовчуванням. Як приклад, це надає зловмиснику візуальний доступ до мнемосхем управління енергооб'єктами.

Первинний моніторинг проведений за допомогою пошукового сервісу «Shodan» за запитом «port:102 country:"UA"» (порт 102 – це стандартний порт протоколу Siemens S7Comm) демонструє значний масштаб проблеми.

Як зображено на Рис. 1, система ідентифікує 215 активних вузлів. Географічний розподіл вразливостей корелює з промисловими центрами та вузлами критичної інфраструктури у багатьох містах України, що підтверджує наявність значної поверхні атаки.

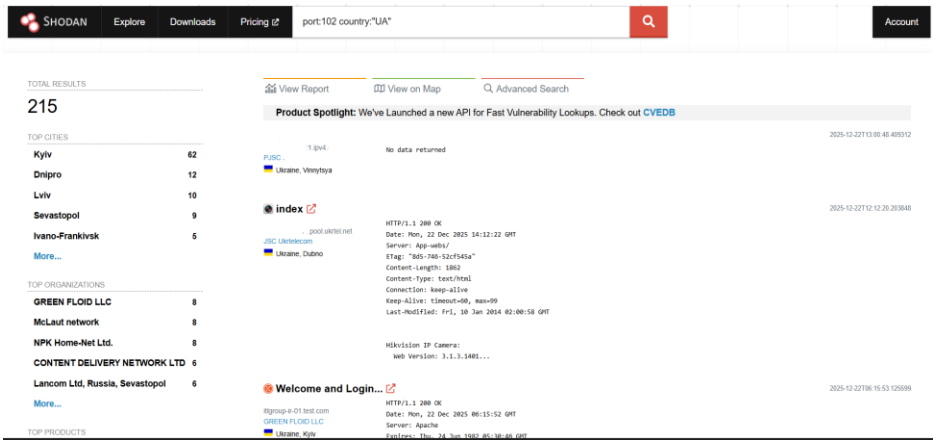

Рис.1. Статистичний звіт Shodan, що демонструє географічний розподіл та загальну кількість (215) вразливих вузлів за портом 102 в Україні

Однак, кількісні показники є лише верхівкою айсберга. Детальний аналіз банерів дозволяє здійснити точну ідентифікацію обладнання. На Рис.2 наведено результати вибірки, які підтверджують, що у відкритому доступі знаходяться не просто емулятори, а реальні промислові контролери серії Siemens SIMATIC S7-300.

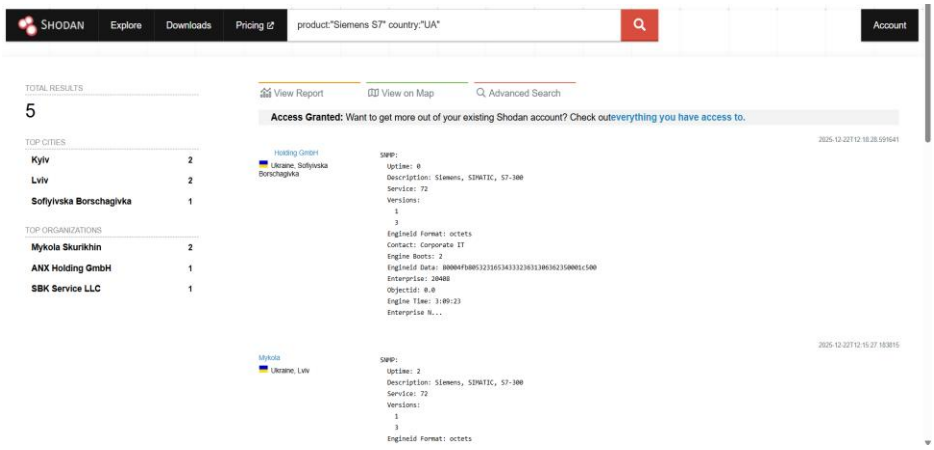

Рис. 2 Приклад деанонімізації промислових контролерів Siemens S7-300, що доступні у публічній мережі та розкривають системну інформацію

Таким чином, аналіз ступеня загроз для конфіденційної інформації підтверджує, що ідентифікація технічних параметрів обладнання через відкриті сервіси вимагає впровадження жорсткої чотирирівневої класифікації даних за рівнем критичності наслідків від їх витоку [13].

Геопросторовий вектор (IMINT/GEOINT). Супутникова розвідка та верифікація ударів. В умовах війни геопросторова розвідка на основі комерційних супутникових знімків стала ключовим елементом планування ракетно-дронових ударів по стаціонарних об'єктах критичної інфраструктури. Аналіз розслідувань [6] підтверджує пряму кореляцію між активністю запитів на супутникові знімки високої роздільної здатності (0.3-0.5 м/піксель) та подальшим вогневим ураженням об'єктів.

Механіка загрози реалізується за наступним алгоритмом:

1. Моніторинг змін: Ворог використовує автоматизовані алгоритми порівняння знімків (наприклад, від операторів Maxar або Planet Labs) для виявлення нових

інженерних споруд. Поява габіонів або бетонних укриттів навколо підстанцій є демаскуючою ознакою, що вказує на розташування критично важливого обладнання.

2. Оцінка результатів атаки: Після завдання удару повторний супутниковий знімок використовується для верифікації ступеня руйнування та прийняття рішення про повторний пуск ракет. Це дозволяє ворогу економити засоби ураження, атакуючи лише ті об'єкти, які не були виведені з ладу.

Особливістю цього вектору є його екстериторіальність: об'єкт критичної інфраструктури не може технічно заблокувати зйомку з орбіти, що вимагає застосування методів маскування, а не лише кіберзахисту.

Соціальний та кадровий вектор (SOCMINT). Третій вектор спрямований на експлуатацію людського фактору та витоків інформації через неконтрольовану активність персоналу. Як зазначають Лі та Парк, смартфони співробітників об'єктів КІ є постійними генераторами метаданих, які агрегуються ворожими OSINT-аналітиками [14, с. 2]. Аналіз загроз у цій площині виявляє такі критичні вразливості.

- Геопросторова прив’язка за візуальними маркерами: фотографії, зроблені персоналом на робочих місцях, часто містять унікальні ідентифікатори приміщень (схеми евакуації, маркування кабельних трас, вид з вікна). Співставлення цих даних із супутниковими знімками дозволяє ворогу моделювати внутрішню топологію об'єкта та визначати розташування серверних кімнат та критично важливого устаткування.
- Експлуатація EXIF-даних: незважаючи на автоматичне очищення метаданих більшістю соціальних мереж, передача файлів через месенджери у форматі файлів (без компресії) або завантаження їх на спеціалізовані веб-ресурси та файлообмінники зберігає GPS-координати зйомки з точністю до кількох метрів [10, с. 3].
- Аналіз тендерної документації: публічні закупівлі є легальним джерелом розвідувальних даних. Технічні завдання на закупівлю засобів захисту інформації розкривають зловмиснику точну модель використовуваного фаєрволу та версію його програмного забезпечення, що дозволяє підібрати специфічні експлойти для обходу периметра.

Таким чином, сучасний OSINT-інструментарій дозволяє зловмиснику сформувати детальний "цифровий профіль" цілі, який включає IP-адреси вразливого обладнання, фізичні координати критичних вузлів та дані про використовувані засоби захисту, ще до початку активної фази кібероперації.

Методи мінімізації цифрового сліду. Враховуючи багатовекторний характер загроз, стратегія захисту об'єктів критичної інфраструктури не може обмежуватися лише налаштуванням міжмережевих екранів. Вона повинна базуватися на комплексному підході OPSEC, що охоплює кібернетичний, фізичний та адміністративний рівні.

Розроблена методика нейтралізації OSINT-розвідки включає три контури захисту, що відповідають ідентифікованим векторам загроз.

Контур №1. Мінімізація технічного сліду «Counter-TECHINT». Метою цього контуру є унеможливлення пасивного сканування технологічної мережі через пошукові системи накшталт Shodan, Censys та ін.. Згідно зі стандартом NIST SP 800-82r3, захист інформації про систему є критичним компонентом безпеки категорії «Protect» [15, с.96].

Реалізація захисту передбачає наступні кроки.

1. Глибока сегментація. Відповідно до моделі «Purdue», прямий доступ до рівня контролерів (L1) з Інтернету має бути фізично заблокований. Впровадження демілітаризованої зони (далі -DMZ) є обов'язковим: зовнішні запити термінуються на проксі-серверах у DMZ, які не мають прямої маршрутизації до SCADA-серверів. Для

критичних секторів рекомендовано використання діодів даних, що апаратно блокують будь-який вхідний трафік, пропускаючи лише вихідну телеметрію [15, с. 207].

2. Маскування банерів. Для протидії ідентифікації обладнання необхідно змінити стандартні налаштування відповідей серверів. Це включає:

– Перезапис заголовків «Server» та «User-Agent» на веб-інтерфейсах панелей керування.Наприклад, замість реального заголовку «Siemens/S7» система має видавати нейтральний «Unknown» або дезінформаційний заголовок.

– Налаштування режиму «Silent Drop» на фаєрволах, пакети сканування мають відкидатися, без відправки ICMP-повідомлення про недоступність порту, що робить хост "невидимим" для карт мережі.

Схематичне відображення описаної архітектури наведено на рис. 4. Вона демонструє дворівневий захист: зовнішній фаєрвол приховує присутність мережі в Інтернеті, а демілітаризована зона з проксі-сервером та приманкою у вигялід «HoneySpot» ізолює критичне обладнання. Використання діода даних перед OT-мережею забезпечує фізичне блокування вхідного трафіку до рівнів SCADA та PLC, що унеможливлює ідентифікацію технологічних процесів методами зовнішньої розвідки.

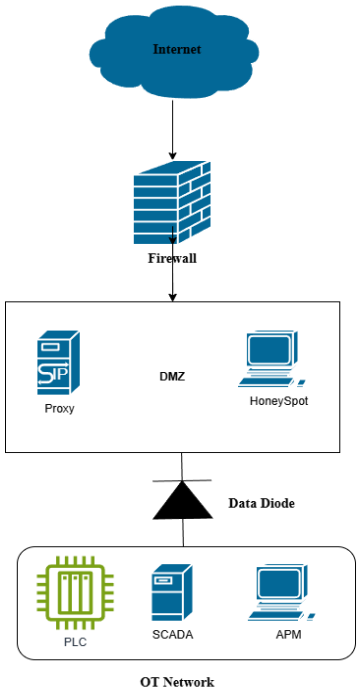

Рис.4 Архітектура захисту периметра OT-мережі з використанням DMZ та діодів даних

Для захисту об’єктів КІ доцільно інтегрувати метод компартменталізації, який дозволяє ізолювати цифрові середовища на рівні мережі та операційних систем. Доведено, що такий підхід знижує успішність OSINT-атак з 80% до 30% за рахунок ускладнення кореляції цифрових слідів об'єкта [16].

Контур № 2. Протидія геопросторовій розвідці «Counter-GEOINT». Як показав аналіз кейсу Molfar [4], супутниковий моніторинг є передумовою кінетичних ударів. Оскільки об'єкт критичної інфрастурктури не може технічно "збити" комерційний супутник або заблокувати його оптику, захист будується на принципах маскування та приховування змін. Рекомендовані заходи:

1. Маскування критичних вузлів. Встановлення захисних споруд (габіонів, антидронових сіток) має супроводжуватися візуальним маскуванням, що зливається з ландшафтом. Використання матеріалів, що поглинають теплове випромінювання, дозволяє знизити помітність трансформаторів в інфрачервоному спектрі, який використовується супутниками для оцінки активності обладнання.

2. Режимна дисципліна переміщень. Будь-які масштабні роботи (ремонт, підвезення обладнання) мають плануватися з урахуванням графіків прольоту супутників оптичної розвідки (які є прогнозованими). Мінімізація перебування техніки на відкритих майданчиках у "вікна" прольоту супутників знижує ймовірність фіксації змін.

3. Приховування наслідків. У разі ураження об'єкта, першочерговим завданням є візуальне приховування реального ступеня пошкоджень (наприклад, швидке накриття пошкоджених ділянок маскувальними елементами) аби позбавити ворога можливості провести якісну дорозвідку результатів удару та дезінформувати його.

Region	Planet		Maxar		21AT		SIIS		SpaceWill		ISI		Satellogic		Capella		Total	
	before	after	before	after	before	after	before	after	before	after	before	after	before	after	before	after	before	after
Odesa	19	40	135	115	5	8	6	1	13	10	5	1	-	-	-	-	258	235
Kyiv	10	30	79	61	2	5	4	-	14	15	2	1	-	-	-	-	243	261
Dnipropetrovs'k	20	14	60	59	13	18	2	3	10	1	-	-	-	2	-	-	169	170
Zhytomyr	6	5	52	27	3	3	-	-	20	8	-	-	-	-	-	-	129	103
Zaporizhzhya	3	1	45	48	-	-	-	-	3	3	-	-	-	-	-	8	99	82
L'viv	7	11	18	30	3	2	-	-	9	4	1	-	-	-	-	-	82	89
Poltava	11	9	13	6	2	1	-	-	-	2	-	-	-	-	-	-	36	27
Khmel'nyts'kyy	9	5	2	4	-	-	-	-	-	-	-	-	-	-	-	-	23	15
Volyn	6	13	5	7	3	-	-	-	2	-	-	-	-	-	-	-	23	22
Kirovohrad	-	1	9	1	-	2	-	-	2	-	-	-	-	-	-	-	18	6
Chernihiv	2	5	1	7	-	-	-	-	9	1	-	-	-	-	-	-	16	17
Cherkasy	-	-	3	2	-	-	-	-	7	4	-	-	-	-	-	-	15	12
Ivano-Frankivs'k	1	8	4	1	-	-	-	-	1	3	-	-	-	-	-	-	15	23
Vinnytsya	4	2	6	11	3	-	-	-	-	3	-	-	-	-	-	-	14	22
Rivne	-	1	3	2	1	1	-	-	-	5	-	-	-	-	-	-	13	9
Sumy	-	-	2	1	-	-	-	-	-	-	-	-	-	-	-	-	10	13
Ternopil'	-	-	5	-	-	-	-	-	-	-	-	-	-	-	-	-	7	-
Transcarpathia	-	6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	6
Total	**98**	**151**	**442**	**382**	**35**	**40**	**12**	**4**	**90**	**59**	***8***	***2***	**-**	***2***	**-**	**8**	**1171**	**1112**

Рис.3 Статистичний розподіл замовлень комерційних супутникових знімків (Planet, Maxar та ін.) по регіонах України у прив'язці до ракетних обстрілів (до та після інцидентів) [4]

Контур № 3. Адміністративний та кадровий контроль «Counter-SOCMINT». Цей контур спрямований на перекриття каналів витоку інформації через персонал та документообіг. Базуючись на дослідженні Лі та Парк [14], людський фактор є найбільш вразливим елементом.

1. Політика "Очищення метаданих".

Впровадження автоматизованих DLP-систем, які примусово очищують метадані файлів перед їх відправкою за межі периметра. Видаленню підлягають:

- GPS-координати в EXIF-даних фотографій.
- Дані про автора, час редагування та версії програмного забезпечення у документах PDF/DOCX.
- Шляхи до мережевих принтерів та внутрішніх серверів, які часто зберігаються в колонтитулах документів.

2. Обмеження доступу до публічної інформації.

Використовуючи положення ст. 6 ч. 2 Закону України «Про доступ до публічної інформації», розпорядники інформації зобов'язані застосовувати «трискладовий тест» для обмеження доступу до даних, що можуть зашкодити національній безпеці [17, с.6].

Практична реалізація. У системі Prozorro та на офіційних сайтах заборонено публікувати детальні плани будівель, схеми кабельних мереж та точні специфікації систем кіберзахисту. Технічна документація має передаватися контрагентам виключно через захищені канали після підписання NDA, а в публічному доступі публікуються лише знеособлені вимоги, наприклад, "Мережеве обладнання з пропускною здатністю 10 Гбіт/с" замість "Cisco Catalyst 9300".

3. Зонування використання смартфонів.

Встановлення зон суворої заборони «No-Phone Zones» у приміщеннях диспетчерських, серверних та біля критичного обладнання. Це унеможливлює випадкову фотофіксацію екранів моніторів із мнемосхемами SCADA або створення "акустичних відбитків" роботи обладнання через мікрофони смартфонів [14, с. 6].

Реалізація цих трьох контурів дозволяє мінімізувати цифровий слід об'єкта, змушуючи противника витрачати непропорційно великі ресурси на верифікацію цілей, що підвищує ймовірність його виявлення на етапі розвідки.

Обґрунтування застосування технологій дезінформації для нейтралізації розвідувальних дій.

Аналіз методів маскування, проведений у попередньому підрозділі, демонструє їхню спрямованість на приховування об’єкта. Проте в умовах сучасного OSINT, коли цифрова інфраструктура вже могла бути частково скомпрометована або проіндексована пошуковими системами, виключно пасивного захисту недостатньо. Вирішенням цієї проблеми є перехід до концепції проактивного захисту, яка базується на впровадженні технологій дезінформації.

Згідно з дослідженнями Х. Хана, Н. Хейра та Д. Бальзаротті [10], застосування дезінформації дозволяє змінити асиметрію кіберпротистояння на користь захисника. Якщо класична парадигма вимагає від служби безпеки перекрити всі можливі вразливості, а нападнику достатньо знайти лише одну, то технології обману змушують агресора сумніватися у достовірності будь-якої отриманої інформації. Як зазначають Хан та ін., основною метою цього підходу є порушення когнітивного циклу прийняття рішень противником, в контексті циклу «OODA: Observe-Orient-Decide-Act», змушуючи його витрачати ресурси на атаку хибних цілей [10, с. 2].

В контексті захисту критичної інфраструктури а саме ОТ-мереж, найбільш ефективним є застосування багаторівневої системи пасток, які імітують реальні технологічні процеси. На першому рівні доцільно використовувати Honeytokens – цифрові маркери. Це штучно створені файли, облікові записи або записи в базах даних, які не мають легітимної цінності для виробничого процесу, але виглядають привабливо для зловмисника, наприклад, файли з назвами «SCADA_passwords.xlsx» або конфігураційні файли VPN. Особливістю цього методу є вкрай низький рівень хибних спрацьовувань: оскільки легітимний персонал не використовує ці об'єкти, будь-яке звернення до них є стовідсотковим індикатором інциденту [10, с. 5].

Для протидії технічній розвідці через Shodan або Censys необхідно імплементувати емулятори промислових систем. Це програмні засоби, що імітують поведінку контролерів на мережевому рівні, відкриваючи стандартні порти, наприклад, 102 для S7Comm або 502 для Modbus та видаючи відповідні банери. Розміщення кількох десятків таких пасток у зовнішньому периметрі мережі призводить до «забруднення» видачі пошукових систем. Ворожий аналітик, базуючих на результатах сканування, де відображено значну кількість доступних вузлів, не може дистанційно відрізнити реальний контролер від емуляції. Це суттєво уповільнює процес розвідки та змушує нападника вдаватися до активного сканування, яке демаскує його присутність.

Більш складним рівнем захисту є розгортання пасток високої взаємодії «High-Interaction Honeypots» – повноцінних операційних систем або ізольованих сегментів мережі, які навмисно залишені вразливими. У випадку атаки на такий вузол система захисту не блокує зловмисника миттєво, а дозволяє йому завантажити шкідливе програмне забезпечення. Це дає можливість фахівцям SOC вивчити тактику ворога – TTPs, зібрати зразки шкідливого програмного забезпечення або інших засобів, та підготувати патчі для реальної інфраструктури до того, як атака сягне критичних активів [10, с. 16].

Таким чином, інтеграція Deception-технологій дозволяє не лише виявляти факт шпигунства на ранніх етапах, але й активно протидіяти йому шляхом дезінформації. Зловмисник отримує викривлену карту мережі, що призводить до помилок у плануванні кібератак та виснаження його ресурсів на взаємодію з фантомними об'єктами.

Таблиця 1

Порівняльна характеристика технологій дезінформації для захисту критичної інфраструктури

Тип засобу (Deception Type)	Принцип дії	Приклад реалізації в OT/SCADA	Рівень ризику для захисника
Honeytoken	Пасивний цифровий файл-маркер	Файл passwords.xlsx або vpn_config на робочому столі інженера	**Низький**. Не вимагає встановлення ПЗ.
Low-Interaction Honeypot	Емуляція мережевих сервісів та портів	Програма, що імітує відкритий порт 102 (S7Comm) та видає стандартний банер Siemens	**Низький**. Зловмисник не може зламати ОС, лише бачить сервіс.
High-Interaction Honeypot	Повноцінна вразлива операційна система	Реальний контролер або сервер в ізольованому VLAN, залишений без патчів	**Високий**. Є ризик використання як плацдарму, якщо ізоляція порушена.
Decoy (Хибна ціль)	Віртуальна мережева адреса	IP-адреса, що відповідає на ARP-запити, імітуючи активний хост	**Низький**. Використовується для виявлення сканування мережі.

Побудова комплексної системи Counter-OSINT моніторингу та реагування. Впровадження технічних засобів маскування та дезінформації, описаних у попередніх підрозділах, створює необхідний бар'єр проти зловмисника, проте не гарантує повної безпеки в динамічному середовищі. Завершальним елементом комплексної системи захисту об'єктів критичної інфраструктури є створення підсистеми постійного моніторингу власного цифрового сліду «Self-OSINT» та процедур реагування на інциденти витоку інформації.

Згідно з рекомендаціями NIST SP 800-82r3, ефективна стратегія кібербезпеки вимагає переходу від періодичних аудитів до безперервного моніторингу [15, с. 128]. В контексті протидії розвідці це означає, що служба безпеки об'єкта повинна бачити свою інфраструктуру очима ворога. Для цього пропонується впровадити регламент періодичного «самосканування», який включає автоматизований пошук згадок підприємства, IP-адрес його підмереж та прізвищ ключових співробітників у відкритих джерелах. Виявлення власного вразливого обладнання у базах накшталт «Shodan» раніше, ніж це зробить ворог, дозволяє усунути вразливість, наприклад, закрити порт або змінити банер, до моменту початку активної фази атаки.

Окремим напрямом є моніторинг інформаційного простору на предмет витоків чутливих даних через персонал. Як зазначають Лі та Парк, аналіз соціальних мереж дозволяє виявити несанкціоновані публікації фотоматеріалів з режимних зон [14,15]. Процедура реагування на такі інциденти повинна бути формалізована: при виявленні фотографії, що демаскує обладнання, необхідно не лише ініціювати її видалення, що часто неможливо оперативно зробити на зовнішніх ресурсах, але й терміново змінити конфігурацію засвіченого вузла або провести маскувальні заходи на місцевості, виходячи з припущення, що зловмисник вже зберіг цю інформацію.

Важливим елементом організаційної стійкості є взаємодія з національними центрами кібербезпеки. Згідно зі звітами НКЦК та CERT-UA, обмін індикаторами компрометації через платформи на кшталт MISP (Malware Information Sharing Platform) дозволяє оперативно дізнаватися про нові методики сканування, які використовують ворожі OSINT’ери. Якщо один об'єкт критичної інфраструктури фіксує специфічне сканування портів SCADA-систем з певних IP-адрес, ця інформація має бути миттєво передана іншим учасникам галузі для превентивного блокування зловмисника на рівні провайдерів.

Таким чином, система Counter-OSINT трансформує процес захисту з локальної ізольованої діяльності в екосистему колективної безпеки, де моніторинг відкритих джерел використовується для випередження дій противника.

ВИСНОВКИ

У статті вирішено актуальне науково-практичне завдання щодо підвищення рівня захищеності об'єктів критичної інфраструктури в умовах війни шляхом розробки комплексної методики протидії розвідці на основі відкритих джерел (OSINT).

Систематизовано вектори OSINT-загроз. На основі аналізу кіберінцидентів встановлено, що сучасна розвідка трансформувалася з пасивного збору даних у ключовий елемент наведення кібернетичної та кінетичної зброї. Визначено три критичні вектори вразливості для об'єктів КІ: технічний (ідентифікація протоколів SCADA через пошукові системи типу Shodan), геопросторовий (супутниковий моніторинг змін інфраструктури) та соціальний (витоки метаданих через персонал).

Обґрунтовано методику мінімізації цифрового сліду. Доведено, що традиційного захисту периметра недостатньо. Запропоновано імплементацію архітектурних рішень згідно зі стандартом NIST SP 800-82r3, зокрема, сегментація мережі, використання односпрямованих шлюзів, у поєднанні з техніками маскування банерів промислового обладнання, що унеможливлює його автоматизовану ідентифікацію.

Доведено ефективність технологій активної протидії. Аргументовано необхідність переходу від пасивної оборони до стратегії активного захисту (Active Defense). Запропоновано алгоритм розгортання системи пасток (Honeytokens, Honeypots), які імітують роботу реальних технологічних процесів. Це дозволяє порушити цикл прийняття рішень супротивником (OODA loop), змушуючи його витрачати ресурси на атаку хибних цілей, та забезпечує раннє виявлення загроз.

Сформульовано організаційні заходи протидії. Визначено, що технічні засоби мають бути підкріплені процедурами контр-OSINT моніторингу (Self-OSINT) та суворою політикою контролю публічної інформації (тендерна документація, візуальний контент), що дозволяє закрити канали витоку даних на адміністративному рівні.

Практична цінність роботи полягає у створенні уніфікованого підходу до захисту інформаційного периметра об'єктів КІ, який враховує специфіку воєнного часу та можливості сучасних засобів розвідки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. National Coordination Center for Cybersecurity. (2024). *Cyber digest: Review of cybersecurity events (May 2024)*. NCCS under the National Security and Defense Council of Ukraine.
2. State Service of Special Communications and Information Protection of Ukraine. (2023). *Russian cyber operations: Changes in tactics, goals, and capabilities of hacker groups of the Russian government and affiliated groups: Analytical report for the first half of 2023*. https://cip.gov.ua/ua/news/yak-zminyuyutsya-taktiki-cili-i-spromozhnosti-khakerskikh-grup-uryadu-rf-ta-kontrolovanikh-nim-ugrupovan-zvit
3. Ivkova, V., & Opirskyi, I. (2025). Research of existing tools and approaches to conducting OSINT in the context of information security of the individual and the state. *Computer Systems and Networks, 7*(1), 143–159. https://doi.org/10.23939/csn2025.01.131
4. Molfar Global. (n.d.). Satellite images and Russian missile strikes on Ukraine: Molfar analyzes *The Atlantic* investigation. https://www.molfar.institute/chy-kupuyut-rosiyany-v-maxar-i-planet-foto-shchob-obstrilyuvaty-ukrainu/
5. Revak, I. O. (Ed.). (2025). *Rol OSINT-doslidzhen u pidvyshchenni rivnia natsionalnoi bezpeky Ukrainy: Materialy kruhloho stolu (Lviv, May 7, 2025)* [The role of OSINT research in improving the level of national security of Ukraine: Roundtable proceedings]. Lviv State University of Internal Affairs. https://dspace.lvduvs.edu.ua/handle/1234567890/8875
6. Kant, D., Creutzburg, R., & Johannsen, A. (2018). Investigation of risks for critical infrastructures due to the exposure of SCADA systems and industrial controls on the internet based on the search engine Shodan. *Electronic Imaging, 2020*(3), 253-1–253-9. https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-253
7. Abouelnaga, Y., & El-Maghraby, A. (2025). Leveraging OSINT for advanced proactive cybersecurity: Strategies and solutions. *IEEE Access, 13*, 4521–4538. https://doi.org/10.1109/ACCESS.2025.3354123
8. Kulyk, O., & Skladannyi, P. (2025). Theoretical bases of methods of counteraction to modern forms of information warfare. *Applied Sciences, 15*(4), Article 1102. https://doi.org/10.3390/app15041102
9. Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability, 15*(18), Article 13369. https://doi.org/10.3390/su151813369
10. Han, X., Kheir, N., & Balzarotti, D. (2018). Deception techniques in computer security: A research perspective. *ACM Computing Surveys, 51*(4), 1–36. https://doi.org/10.1145/3214305
11. Mustak, M., Salminen, J., Mäntymäki, M., Rahman, A., & Dwivedi, Y. K. (2023). Deepfakes: Deceptions, mitigations, and opportunities. *Journal of Business Research, 154*, Article 113368. https://doi.org/10.1016/j.jbusres.2022.113368
12. Ivkova, V., & Opirskyi, I. (2025). OSINT technologies as a threat to the cybersecurity of the state. *Cybersecurity: Education, Science, Technique, 3*(27), 165–179. https://doi.org/10.28925/2663-4023.2025.27.749
13. Ivkova, V., & Opirskyi, I. (2024). Research of problems of ensuring the security of personal data and confidential information in the context of counteracting OSINT. *Cybersecurity: Education, Science, Technique, 2*(26), 189–199. https://doi.org/10.28925/2663-4023.2024.26.682
14. Lee, Y.-J., Park, S.-J., & Park, W.-H. (2022). Military information leak response technology through OSINT information analysis using SNSes. *Security and Communication Networks, 2022*, Article 9962029. https://doi.org/10.1155/2022/9962029
15. Stouffer, K., Pease, M., Tang, C., Lightman, R., & Zimmerman, T. (2023). *Guide to operational technology (OT) security* (NIST Special Publication 800-82 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3
16. Ivkova, V., & Opirskyi, I. (2025). Research of the possibility of integrating the compartmentalization method in protecting information in open sources. *Computer Systems and Networks, 7*(2), 71–83.
17. Verkhovna Rada of Ukraine. (2011). *Law of Ukraine "On access to public information" No. 2939-VI*. https://zakon.rada.gov.ua/laws/show/2939-17
18. Manuilova, Y. S. (2023). Ensuring cybersecurity of critical infrastructure facilities in conditions of cyber warfare. *Information and Law, 1*(44), 154–167. https://doi.org/10.37750/2616-6798.2023.1(44).287780

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Valeriia Ivkova
Postgraduate Student of Information Protection Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0002-2370-1497
valeriia.s.ivkova@lpnu.ua

Andrii Leonov
Student of Information Protection Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0008-1615-297X
andrii.leonov.kb.2023@lpnu.ua

METHODS AND MEANS OF PROTECTING CRITICAL INFRASTRUCTURE FROM OSINT INTELLIGENCE IN WARTIME

Abstract. The article addresses the pressing scientific and practical issue of improving the cyber resilience and physical security of Ukraine's critical infrastructure (CI) in the context of warfare. It analyzes the transformation of open source intelligence (OSINT) from an auxiliary analytical tool into a key element in the targeting of high-precision weapons and the planning of destructive cyberattacks. Based on an analysis of recent incidents, critical threat vectors have been identified and systematized: technical indexing of industrial system (OT) vulnerabilities through IoT search engines (Shodan, Censys), geospatial monitoring of infrastructure changes using commercial satellite imagery, and leaks of sensitive information through social engineering (SOCMINT). The main focus of the work is on developing a comprehensive countermeasure methodology that goes beyond traditional perimeter protection. The feasibility of applying a digital footprint reduction strategy in accordance with NIST SP 800-82r3 standards, which includes deep network segmentation, the use of data diodes, and equipment banner obfuscation, is justified. The implementation of deception technology is considered in detail – the introduction of a layered system of traps (honeytokens, honeypots) to disrupt the enemy's cognitive decision-making cycle (OODA loop). Organizational measures for counterintelligence monitoring and regulation of public information are proposed, which can significantly reduce the effectiveness of enemy intelligence at the data collection stage. The practical value of the research lies in the creation of an adaptive protection algorithm that complicates the verification of targets by the aggressor.

Keywords: critical infrastructure, OSINT intelligence, cybersecurity, SCADA systems, Deception Technology, digital footprint minimization, Shodan, active defense.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. National Coordination Center for Cybersecurity. (2024). *Cyber digest: Review of cybersecurity events (May 2024)*. NCCS under the National Security and Defense Council of Ukraine.
2. State Service of Special Communications and Information Protection of Ukraine. (2023). *Russian cyber operations: Changes in tactics, goals, and capabilities of hacker groups of the Russian government and affiliated groups: Analytical report for the first half of 2023*. https://cip.gov.ua/ua/news/yak-zminyuyutsya-taktiki-cili-i-spromozhnosti-khakerskikh-grup-uryadu-rf-ta-kontrolovanikh-nim-ugrupovan-zvit
3. Ivkova, V., & Opirskyi, I. (2025). Research of existing tools and approaches to conducting OSINT in the context of information security of the individual and the state. *Computer Systems and Networks, 7*(1), 143–159. https://doi.org/10.23939/csn2025.01.131
4. Molfar Global. (n.d.). Satellite images and Russian missile strikes on Ukraine: Molfar analyzes *The Atlantic* investigation. https://www.molfar.institute/chy-kupuyut-rosiyany-v-maxar-i-planet-foto-shchob-obstrilyuvaty-ukrainu/
5. Revak, I. O. (Ed.). (2025). *Rol OSINT-doslidzhen u pidvyshchenni rivnia natsionalnoi bezpeky Ukrainy: Materialy kruhloho stolu (Lviv, May 7, 2025)* [The role of OSINT research in improving the level of national security of Ukraine: Roundtable proceedings]. Lviv State University of Internal Affairs. https://dspace.lvduvs.edu.ua/handle/1234567890/8875

6. Kant, D., Creutzburg, R., & Johannsen, A. (2018). Investigation of risks for critical infrastructures due to the exposure of SCADA systems and industrial controls on the internet based on the search engine Shodan. *Electronic Imaging, 2020*(3), 253-1–253-9. https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-253
7. Abouelnaga, Y., & El-Maghraby, A. (2025). Leveraging OSINT for advanced proactive cybersecurity: Strategies and solutions. *IEEE Access, 13*, 4521–4538. https://doi.org/10.1109/ACCESS.2025.3354123
8. Kulyk, O., & Skladannyi, P. (2025). Theoretical bases of methods of counteraction to modern forms of information warfare. *Applied Sciences, 15*(4), Article 1102. https://doi.org/10.3390/app15041102
9. Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability, 15*(18), Article 13369. https://doi.org/10.3390/su151813369
10. Han, X., Kheir, N., & Balzarotti, D. (2018). Deception techniques in computer security: A research perspective. *ACM Computing Surveys, 51*(4), 1–36. https://doi.org/10.1145/3214305
11. Mustak, M., Salminen, J., Mäntymäki, M., Rahman, A., & Dwivedi, Y. K. (2023). Deepfakes: Deceptions, mitigations, and opportunities. *Journal of Business Research, 154*, Article 113368. https://doi.org/10.1016/j.jbusres.2022.113368
12. Ivkova, V., & Opirskyi, I. (2025). OSINT technologies as a threat to the cybersecurity of the state. *Cybersecurity: Education, Science, Technique, 3*(27), 165–179. https://doi.org/10.28925/2663-4023.2025.27.749
13. Ivkova, V., & Opirskyi, I. (2024). Research of problems of ensuring the security of personal data and confidential information in the context of counteracting OSINT. *Cybersecurity: Education, Science, Technique, 2*(26), 189–199. https://doi.org/10.28925/2663-4023.2024.26.682
14. Lee, Y.-J., Park, S.-J., & Park, W.-H. (2022). Military information leak response technology through OSINT information analysis using SNSes. *Security and Communication Networks, 2022*, Article 9962029. https://doi.org/10.1155/2022/9962029
15. Stouffer, K., Pease, M., Tang, C., Lightman, R., & Zimmerman, T. (2023). *Guide to operational technology (OT) security* (NIST Special Publication 800-82 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3
16. Ivkova, V., & Opirskyi, I. (2025). Research of the possibility of integrating the compartmentalization method in protecting information in open sources. *Computer Systems and Networks, 7*(2), 71–83.
17. Verkhovna Rada of Ukraine. (2011). *Law of Ukraine "On access to public information" No. 2939-VI.* https://zakon.rada.gov.ua/laws/show/2939-17
18. Manuilova, Y. S. (2023). Ensuring cybersecurity of critical infrastructure facilities in conditions of cyber warfare. *Information and Law, 1*(44), 154–167. https://doi.org/10.37750/2616-6798.2023.1(44).287780

Отримано редакцією журналу / Received: 14.01.26
Прорецензовано / Revised: 30.01.26
Схвалено до друку / Accepted: 26.03.26