Системне вдосконалення підходів до забезпечення кібербезпеки об'єктів критичної інфраструктури

УДК 621.395.7 (043.2)

Юрій Якименко[1]

Державний університет інформаційно-комунікаційних технологій,
[1]yakum14@ukr.net

Системне вдосконалення кібербезпеки об'єктів критичної інфраструктури (ОКІ) в Україні є стратегічним пріоритетом в умовах постійних кібератак. Спрямованість кібератак здійснюються в основному на об'єкти енергетики,транспорту, фінансів, зв'язок (телеком), банківська система та державного управління (урядові портали), що є критично важливою складовою сучасних організацій, порушує їх функціонування і створює загрозу державі та суспільству. Кібератаки інтегровано поєднуються з військовими діями, а кіберзагрози стали системними та стратегічними, а не лише залишились як технічними. За сучасними дослідженнями по результатам комплексного аналізу кіберзагроз ОКІ в 2025 році та практикою кіберконфлікту в Україні основними ключовими загрозами визначені: цілеспрямовані атаки (apt); атаки на SCADA/ICS системи; DDOS-атаки на державні ресурси; шкідливе ПЗ (WIPER, RANSOMWARE); соціальна інженерія; AI-підсилені атаки. Як причина показано, що критична інфраструктура є особливо вразливою через застарілі системи та складність модернізації . [1] Класичні підходи щодо підвищення кібербезпеки ОКІ (з периметрового захисту- firewall, IDS/IPS; контролю доступу і антивірсного захисту) вже стали недостатньо ефективнми проти сучасних атак. Тому у 2025 році з'явилися інші- сучасні підходи: щодо перевірки кожного запиту (Zero Trust Architecture), щодо управління ризиками і пріоритезацією загроз (Risk-based Security), щодо моніторингу в 24/7 і реагування на інциденти SOC (Security Operations Center), щодо обміну інформацією про загрози (Threat Intelligence), щодо кіберстійкості, які спрямовані не тільки на захист, но і на відновлення ресурсів (Cyber Resilience). [1,2]

ІТ-інфраструктура об'єктів організацій включає в себе сервери, мережеве обладнання, програмне забезпечення, бази даних, хмарні сервіси та користувацькі пристрої. Її захист базується на класичній тріаді інформаційної безпеки — конфіденційність, цілісність та доступність. Саме закон України «Про основні засади забезпечення кібербезпеки України» встановлює загальні принципи побудови системи кіберзахисту та ролі її суб'єктів. Інший закон України «Про захист інформації в інформаційно-комунікаційних системах» визначає вимоги до захисту інформації і в державних інформаційних ресурсах. Відповідно до вимог цих законів захист ІТ-інфраструктури практично реалізується за принципом багаторівневого захисту. [2]

В 2025 році постановою КМУ затверджений оновлений перехід кіберзахисту ОКІ на ризик-орієнтовану модель, з урахуванням більш глибокого аналізу власних ризиків: шляхом проведення заходів з кіберзахисту та урахуванням отриманих результатів управління ризиками кібербезпеки в організації повинна бути побудована адаптивна система безпеки. Реалізація

нового підходу дозволить скоротити час реагування та відновлення функціонування ОКІ після кібератак, зменшити кількість значних кіберінцидентів, а також підвищити рівень кіберзахисту об'єкту. [3]

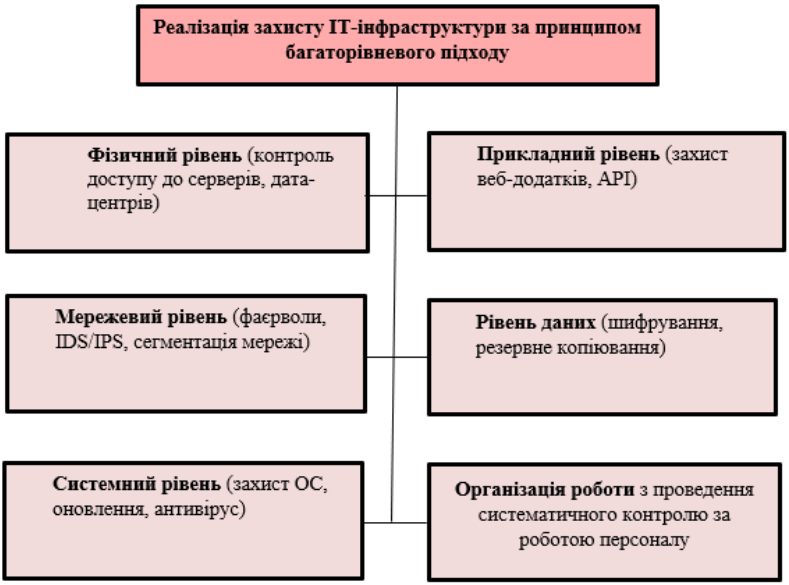

Рис.1. Реалізація захисту IT-інфраструктури за принципом багаторівневого підходу

В той же час відповідно до вимог міжнародного стандарту ISO/IEC 27001, організація, яка визначена як ОКІ, повинна впроваджувати систему управління інформаційною безпекою (ISMS), з основними функціональними завданнями оцінки ризиків, контролю доступу, управління інцидентами та аудитом. Саме вимоги цього стандарту і інших в сфері безпеки забезпечують системність, уніфікацію приємливих підходів в сучасних умовах діяльності і проведення оцінки рівней безпеки організацій. Завдяки функціонуванню ISMS повинно бути забезпечена безперервна готовність ОКІ до виконання своїх задач, визначених в документах політики безпеки.

Таким чином, системне вдосконалення кібербезпеки ОКІ повинно бути спрямовано на комплексне використання всіх можливостей ISMS в організаційному і технічному напрямках забезпечення багаторівневого захисту інформаційних ресурсів та в цілому - високого рівня ефективної діяльності організації. Безперервне вдосконалення треба проводити в послідовності дій: виявлення загроз, аналіз ризиків інформаційної безпеки, забезпечення захисту інформації, моніторингу процесів управління безпекою, реагування на інциденти інформаційної безпеки і відновлення до нормального стану діяльності ОКІ. Результати вдосконалення треба впроваджувати в побудовану

адаптивної системи безпеки організації. Більше можливостей демонструє впровадження інноваційних рішень, якими є використання штучного інтелекту у напрямах: виявлення аномалій, щоб відстежувати поведінку мережі та автоматично реагувати на загрози; прогнозування кібератак і використання сучасних технологій протидії різним кібератакам. Активно використовуються сучасні інноваційні технології: SOAR для автоматизації реагування, XDR для розширеного виявлення загроз, Digital Twins для оцінки інфраструктури, Cyber Range для використання як кіберполігонів у дослідженнях.

1. Звіт ДЦКЗ Держспецзв'язку про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (СВВ) за 2025 рік. URL:
2. https://cip.gov.ua/services/cm/api/attachment/download?id=73033
3. Ільєнко А.В, Телющенко В.А., Дубчак О.В. Сучасні кіберзагрози критичної інфраструктури України та світу № 3 (27), 2025 . DOI 10.28925/2663-4023.2025.27.719
4. Постанова КМУ від 13.11.2025 р. № 1470. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури (ОКІ) в новій редакції.

Трасування безпекових вимог у системах предиктивної аналітики

УДК 004.89:339.138 (043.2)

Дмитро Яценко[1], Володимир Садовенко[2]

Державний університет інформаційно-комунікаційних технологій,
[1]d.yatsenko@stud.duikt.edu.ua, [2]v.sadovenko@duikt.edu.ua

Системи предиктивної аналітики (СПА) у цифровому маркетингу обробляють масивні поведінкові, демографічні та транзакційні дані користувачів, що формують специфічну поверхню атаки. Поряд із класичними загрозами інформаційній безпеці такі системи зазнають впливу атак, специфічних для машинного навчання (МН): data poisoning, evasion, model extraction, membership inference, model inversion [1, 2, 3]. Чинні стандарти управління ризиками штучного інтелекту, зокрема ISO/IEC 23894:2023 [4] та NIST AI 100-2 E2025 [1], формулюють принципи високого рівня, проте не пропонують архітектурного інструментарію проєктування. Безпекові механізми впроваджуються на пізніх етапах життєвого циклу системи, що знижує стійкість і ускладнює верифікацію її властивостей.

Мета роботи — підвищення стійкості СПА до атак на МН шляхом розроблення методу трасування безпекових вимог до архітектурних компонентів, механізмів контролю та метрик верифікації, що враховує особливості маркетингових даних — відкритість каналів збору поведінкових сигналів та схильність навчальних вибірок до забруднення через клік-фрод.

Наукова новизна. Уперше для класу СПА у галузі цифрового маркетингу запропоновано метод трасування безпекових вимог за схемою «вимога — вектор загрози — архітектурний компонент — механізм контролю — метрика верифікації». На відміну від універсальних стандартів управління ризиками AI