1. Hautala T. New Managed Detection and Response System to Lower the Likelihood of Malicious Activities in IP Network. Master's Thesis, Metropolia University of Applied Sciences, Helsinki, 2022. 46 p.
2. Rajgopal P.R., Karanam L. MDR Service Design: Building Profitable 24/7 Threat Coverage for SMBs. International Journal of Applied Mathematics. – 2025. – V. 38, № 2s.
3. Fortinet. What Is Managed Detection and Response (MDR)? URL: https://www.fortinet.com/uk/resources/cyberglossary/managed-detection-and-response (application date: 30.04.2026).
4. MCK. The Role of AI in Managed Detection: How Artificial Intelligence Strengthens MDR Security. URL: https://www.mck.com/blog/role-of-ai-in-managed-detection (application date: 30.04.2026).
5. Rapid7. What Is MDR? Managed Detection and Response Security. URL: https://www.rapid7.com/fundamentals/what-is-managed-detection-and-response-mdr/ (application date: 30.04.2026).

Модель оцінювання кіберризиків IoT-інфраструктури розумного міста

УДК 004.056:004.738.5:004.77

Віталій Левицький[1], Олег Тотоськo[2]
Олександр Добруцький[3]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]levytskyylv@gmail.com, [2]totosko@gmail.com, [3]oleksandrdobruckij@gmail.com

Цифровізація міської інфраструктури передбачає впровадження IoT-пристроїв, сенсорних мереж, edge-вузлів, хмарних платформ і диспетчерських систем для моніторингу довкілля, транспорту, енергоресурсів, відеоспостереження та аварійного реагування. Зростання кількості підключених компонентів формує кіберфізичне середовище, у якому порушення безпеки даних має інформаційні, організаційні й технологічні наслідки. Традиційні підходи до управління ризиками орієнтовані переважно на корпоративні мережі й серверну інфраструктуру [1], тоді як міські IoT-системи мають малопотужні пристрої, неоднорідні протоколи, бездротові канали та залежність від хмарних сервісів. За NIST CSF 2.0 управління кіберризиками має охоплювати виявлення активів, захист, моніторинг, реагування й відновлення [2]. Метою роботи є розроблення моделі оцінювання кіберризиків IoT-інфраструктури розумного міста для пріоритезації захисту компонентів з урахуванням критичності, експозиції, вразливостей і зрілості захисних заходів. Новизна полягає в поєднанні логіки «загроза — вразливість — наслідок» із параметрами IoT-середовища: відкритістю, залежностями, сегментацією та рівнем захисту. Модель передбачає інвентаризацію активів, профіль загроз, оцінювання вразливостей, визначення впливу на сервіси, розрахунок інтегрального ризику та пріоритезацію заходів. До активів належать сенсори, виконавчі пристрої, шлюзи, edge-вузли, мережеве обладнання, API, бази даних, хмарні сервіси та операторські панелі.

Інтегральний показник ризику і-го компонента подається як $R_i = P_i \times I_i \times E_i \times D_i \times (1 - C_i)$, де P_i — імовірність загрози, I_i — вплив, E_i — експозиція, D_i — залежність від інших сервісів, C_i — зрілість захисту. P_i, I_i, E_i та D_i оцінюються за шкалою 1–5, C_i — у межах 0–1.

Таблиця 1

Складові оцінювання кіберризику IoT-компонента

Показник	Зміст оцінювання	Шкала
P_i	імовірність реалізації загрози з урахуванням вразливості та доступності атаки	1–5
I_i	вплив на конфіденційність, цілісність, доступність і безперервність сервісу	1–5
E_i	рівень відкритості компонента до мережевої або фізичної взаємодії	1–5
D_i	критичність залежностей від інших пристроїв, платформ і сервісів	1–5
C_i	зрілість захисних заходів: автентифікація, оновлення, сегментація, журналювання	0–1

Реалізація можлива як матриця ризиків або модуль муніципальної системи моніторингу кібербезпеки. Реєстр активів фіксує тип пристрою, місце розгортання, мережевий сегмент, відповідальний підрозділ і критичність сервісу. Профіль загроз охоплює несанкціонований доступ, компрометацію облікових даних, атаки на канал зв'язку, підміну телеметрії, відмову в обслуговуванні й незакриті вразливості, а також базові вимоги IoT-безпеки [3].

Особливістю моделі є врахування каскадних інцидентів: компрометація шлюзу може спричинити втрату телеметрії, помилкові управлінські рішення або недоступність суміжних сервісів. Тому D_i відображає роль компонента в цифровій екосистемі. Це важливо з огляду на атаки на доступність, програми-вимагачі, загрози даним та експлуатацію слабких місць цифрових сервісів [4].

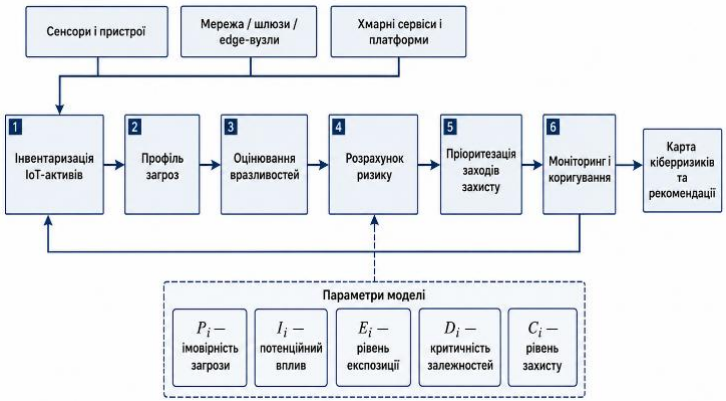

Рис.1. Модель оцінювання кіберризиків IoT-інфраструктури розумного міста

Результати можуть використовуватися для карти кіберризиків, сегментації мережі, посилення автентифікації, централізованого оновлення, резервування критичних сервісів і журналювання подій. Модель не замінює аудит, але є інструментом попереднього оцінювання та регулярного моніторингу. Подальші дослідження доцільно спрямувати на калібрування вагових коефіцієнтів, інтеграцію з SIEM/SOC-рішеннями та адаптацію до окремих міських сервісів..

1. Nurse J.R.C., Creese S., De Roure D. Security risk assessment in Internet of Things systems. IT Professional. 2017. Vol. 19(5). P. 20-26.
2. Kandasamy K. et al. IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP Journal on Information Security. 2020. Vol. 2020. Article 8.
3. Parsons E.K. et al. A survey on cyber risk management for the Internet of Things. Applied Sciences. 2023. Vol. 13(15). Article 9032.
4. Gharaibeh A. et al. Smart cities: A survey on data management, security, and enabling technologies. IEEE Communications Surveys & Tutorials. 2017. Vol. 19(4). P. 2456-2501.

Еволюція методів виявлення шкідливих URL: від евристик до трансформерних архітектур

УДК 519.6

Петро Венгерський[1], Володимир Лесик[2]

Львівський національний університет імені Івана Франка,
[1]petro.venherskyy@lnu.edu.ua, [2]volodymyr.lesyk@lnu.edu.ua

Стрімке зростання кількості вебресурсів та кіберзагроз зумовлює актуальність задачі виявлення шкідливих URL-адрес, що використовуються для фішингу, поширення шкідливого програмного забезпечення та координації бот-мереж. Традиційні підходи, засновані на чорних списках і сигнатурному аналізі, мають обмежену ефективність через нездатність виявляти нові або модифіковані атаки [1-3].

Метою роботи є систематизація еволюції методів виявлення шкідливих URL-адрес - від евристичних підходів до сучасних моделей машинного та глибокого навчання, а також визначення перспектив подальшого розвитку інтелектуальних систем захисту.

Еволюцію технологій детекції можна розділити на кілька послідовних етапів. Технологічний прогрес у цій галузі характеризується переходом від жорстких алгоритмів до гнучких нейромережевих архітектур [3] (рис. 1).

Початковий етап базувався на використанні ручних правил і статичних баз даних, що забезпечували швидку, але обмежену за узагальненням детекцію відомих аномалій [3].

Наступним кроком стало впровадження класичного машинного навчання (ML). Алгоритми логістичної регресії, SVM та ансамблеві методи (зокрема Random Forest) автоматизували класифікацію на основі видобутих ознак URL-адрес: лексичних, хостових, контентних та зовнішніх [1,3,4]. Лексичні ознаки дозволяють здійснювати швидку класифікацію без доступу до мережевих