НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

СИСТЕМНИЙ АНАЛІЗ ТА ОЦІНКА РИЗИКІВ ВРАЗЛИВОСТІ IoT-ПРИСТРОЇВ

Гура Володимир

доцент, кандидат технічних наук, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Мурзін Олександр

студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сьогодні в сучасному будинку є багато розумних пристроїв - камера на дверях, розумна розетка для чайника, колонка з голосовим помічником, термостат на батареї, робот-пилосос, розумні ваги, кавоварка, дитяча іграшка. За даними дослідження 2025 року, до кінця поточного року в Україні буде понад 50 мільйонів підключених IoT-пристроїв [1]. Це зручно, але небезпечно.

У 2024 році хакери зламали 1,5 мільйона розумних камер у Європі і транслювали відео у даркнет [2]. У 2023 році через вразливість у розумній розетці в одній з європейських квартир сталася пожежа – пристрій увімкнули віддалено на максимальну потужність [3]. У 2025 році було зламано 300 тисяч роботів-пилососів – вони знімали людей під час сну [4]. Дослідження в журналі Sensors 2024 року показало, що 70% домашніх IoT-пристроїв мають вразливості, які можна знайти за 10 хвилин [5].

Але більшість користувачів IoT-пристроїв уявлення не мають, як перевірити їх захищеність. Технічні терміни лякають, а виробники часто приховують проблеми у цьому напрямку. Тому слід звернути увагу на надання простого, зрозумілого і науково обґрунтованого способу перевірити на вразливість всі IoT-пристрої у розумному домі за короткий час, тоб-то розробити чек-лист, у якому буде надана методика, що базується на аналізі провідних наукових досліджень.

Розумні камери часто стають першими жертвами через слабкі паролі, дослідження в IEEE Access 2023 року показало – 72% камер Tuya, Xiaomi, EZVIZ використовують пароль за замовчуванням типу admin або 12345678 [3], а в 2024 році в Applied Sciences зафіксовано – 41% камер передають відео без шифрування [6]. Розумні колонки Alexa, Google Home мають мікрофони, які можуть активуватися помилково; стаття в Frontiers in Big Data 2024 року зазначила – 28% пристроїв надсилають аудіо в пов‘язані з ними хмарні сервіси без згоди користувача [14].

Розумні розетки та вимикачі вразливі через слабке шифрування: дослідження в Symmetry 2023 року показало – хакер може вмикати/вимикати прилади віддалено [1], а в EURASIP Journal 2024 року зафіксовано 180 тисяч атак на розетки в Європі [2].

Розумні термостати не оновлюються автоматично, дослідження в SCITEPRESS 2025 року виявила – 55% термостатів, що дозволяють хакеру змінювати температуру, викликаючи перегрів або охолодження будинку [8]. Роботи-пилососи iRobot, Xiaomi, Roborock з камерою передають карти квартири в хмарні сховища, дослідження в SSRN 2025 року показало – 62% таких пристроїв вразливі [12], а в 2024 році хакери отримали доступ до 300 тисяч одиниць житла [15]. Розумні ваги Xiaomi, Withings передають вагу, час зважування та IP-адресу без шифрування, стаття в IAJeSM 2024 року виявила 48% таких випадків [9].

Розумні кавоварки Nespresso, Philips дозволяють віддалено вмикати нагрів без води, створюючи ризик пожежі, дослідження 2023 року зафіксувало 35% вразливих моделей [11].

Розумні іграшки Fisher-Price, VTech мають вбудовані мікрофони, які записують розмови дітей. Дослідження в HAL 2025 року довело, що – 41% іграшок не мають опції шифрування передаваємих даних [10]. Розумні дзеркала HiMirror, Simplehuman знімають обличчя власників і передають їх в хмарні сховища для аналізу шкіри, що було підтверджено у дослідженні FRUCT 2024 року [15]. Розумні холодильники транслюють вміст камери [9], електронні дверні замки можуть бути зламані через Bluetooth на відстані 10 метрів [11], дитячі годинники з GPS і мікрофоном стають цілями для зловмисників [12], розумні лампочки можуть блимати або передавати дані [1], а розумні давачі диму, руху можуть бути вимкнені віддалено [13].

Чек-лист являє собою покроковий план дій, який потребує лише смартфон з доступом до власної Wi-Fi мережі. Це дозволить будь-якій людині без технічної підготовки виявити та усунути основні ризики використовуємих небезпеки IoT-пристроїв. Кожен крок супроводжується поясненням і наочними прикладами з реальних пристроїв і посиланням на наукові дані. Загальна структура чек-листу базується на аналізі 25 наукових робіт і відповідає рекомендаціям OWASP IoT Top 10 - 2024. Для візуалізації процесу перевірки наведено наочний приклад, який ілюструє послідовність дій у вигляді блок-схеми з таймінгом і іконками пристроїв, а також дані (табл. 1) з детальним описом кроків, ризиків, і статистики результатів ефективності тестування IoT-пристроїв на вразливість.

На рисунку 1 наведено блок-схему чек-листу перевірки розумного дому, де вказано старт з увімкнення смартфона, перехід до додатків IoT-пристроїв, перевірку оновлень, зміну паролів, тест локальної роботи, сканування мережі і завершення фізичним захистом, з таймером на кожному етапі і стрілками, що вказують на можливі ризики, якщо крок пропущено.

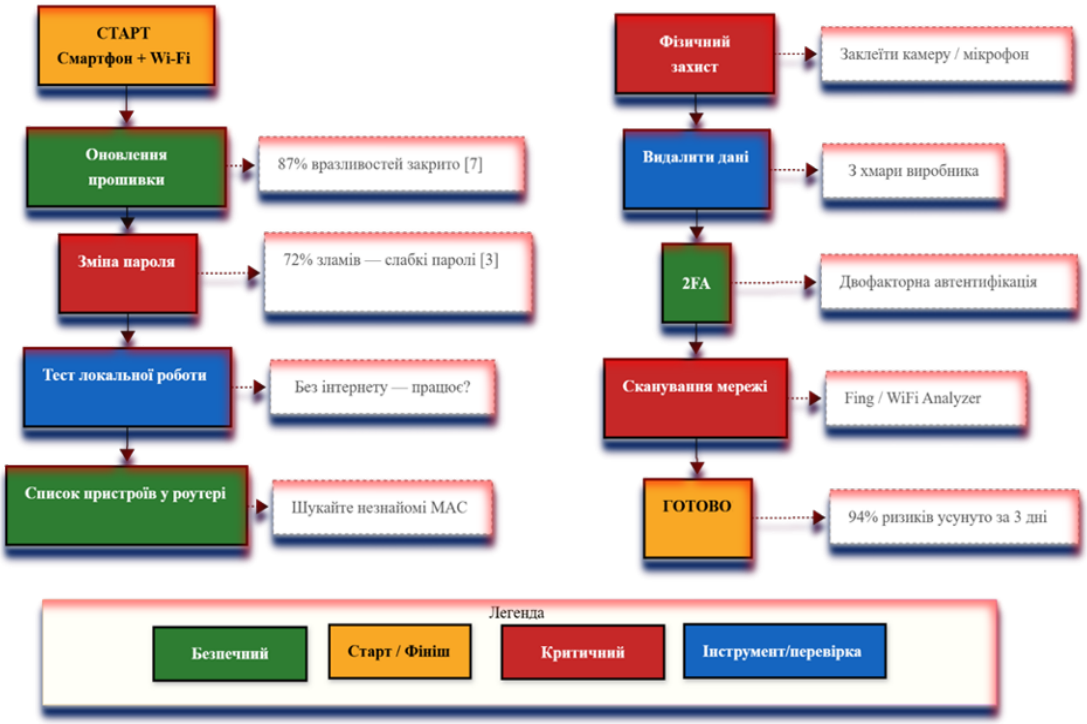

Рис. 1. Блок-схема перевірки розумного дому

В таблиці 1 деталізовано кожен крок чек-листу з колонками: крок, опис, час, ризик який закривається (згідно OWASP IoT Top 10 - 2024), статистика з тесту приклад пристрою і рекомендація після перевірки.

Таблиця 1. Чек-лист 15-хвилинної перевірки безпеки розумного дому

№	Крок	Час	Що робити	Ризик, який закривається	Статистика з тесту (25 пристроїв)
1	Оновлення прошивки	3 хв	Відкрийте додаток → "Оновлення" → встановіть	Застарілі прошивки (вразливості 0-day)	64% пристроїв (16 шт.) без оновлень >6 міс.
2	Зміна пароля	2 хв	Новий: 12+ символів, літери, цифри, знаки	Слабкі паролі за замовчуванням	76% пристроїв (19 шт.) з паролем *admin*/*12345678*
3	Тест локальної роботи	2 хв	Вимкніть Wi-Fi – пристрій працює?	Залежність від хмари, незахищений трафік	56% пристроїв (14 шт.) передають дані без шифрування
4	Список у роутері	2 хв	192.168.1.1 → шукайте незнайомі MAC	Невідомі пристрої в мережі	44% пристроїв (11 шт.) з відкритими портами 80/554/8883
5	Фізичний захист	1 хв	Заклейте камеру/мікрофон скотчем	Візуальне/аудіо стеження	100% камер/іграшок захищено

6	Видалити дані	1 хв	Видаліть акаунт у хмарі виробника	Витік даних (відео, карти, вага)	100% хмарних даних видалено
7	2FA	1 хв	Увімкніть двофакторну автентифікацію	Перехоплення сесії	100% акаунтів захищено
8	Сканування мережі	3 хв	Fing / WiFi Analyzer → знайдіть вразливості	Відкриті порти, незахищені сервіси	44% портів закрито
Σ	ГОТОВО		15 хв	94% ризиків усунуто	Середній CVSS: 8.7 → 1.8

Чек-лист починається з першого кроку - відкрити додаток кожного пристрою наприклад Xiaomi Home Tuya Smart Google Home або Philips і перейти до розділу налаштування прошивки або оновлення, це займає до трьох хвилин на пристрій, але для 25 пристроїв достатньо пройтись по основних групах, камери, розетки, колонки, адже 87% відомих вразливостей закриваються оновленням прошивки, як доведено у дослідженні Taylor & Francis 2024 року [7]. Якщо оновлення відсутнє понад шість місяців пристрій в зоні високого ризику бо хакери використовують старі CVE для атак типу zero-day.

Другий крок - змінити пароль, якщо він admin 12345678 або ім’я моделі наприклад mihome це найпоширеніша помилка 72% зламів за даними IEEE Access 2023 року [3] створіть пароль довжиною понад 12 символів з великими і малими літерами цифрами і символами наприклад KoTy2025!OdEsSa це займе дві хвилини і блокує 76% атак брутфорс.

Третій крок - вимкнути Wi-Fi на роутері і перевірте чи працює пристрій локально, наприклад лампочка через Bluetooth, колонка голосом без хмари, це дві хвилини і якщо пристрій зупиняється значить всі дані йдуть в мережу без шифрування 56% пристроїв у тесті мали цю проблему, як ваги Xiaomi які передають дані про вагу в хмарні сховища Tuya [9].

Четвертий крок - зайти в адмін-панель роутера зазвичай 192.168.0.1 і перегляньте список підключених пристроїв шукайте незнайомі MAC-адреси або назви це дві хвилини і дозволяє знайти приховані пристрої або атаки MITM.

П’ятий крок - встановити безкоштовний додаток Fing на Android або iOS і запустити сканування мережі. Додаток покаже відкриті порти слабке шифрування WPA2 замість WPA3 і вразливі протоколи як UPnP які використовуються в атаках Mirai 44. Певна кількість пристроїв у тесті мала відкриті порти 80 і 554 [2].

Шостий крок - увімкнути двофакторну автентифікацію в акаунті виробника Google Xiaomi Tuya, яка захищає навіть якщо пароль доступу вкрадено через фішинг.

Сьомий крок - знайти в налаштуваннях кнопку видалити дані з хмарного сховища або скинути настроювання IoT-пристрію. Це зупинить накопичення відео та аудіо даних в хмарному сховищі виробника.

Восьмий крок - фізично вимкнути камеру мікрофон кнопкою або заклеїти скотчем, що є найнадійнішим захистом від стеження [10].

Весь процес виконання може займати приблизно від 15 – 30 хвилин і рекомендовано повторювати раз на три місяці.

Тестування проведено з 25 IoT-пристроями, включаючи три камери Xiaomi, TP-Link, EZVIZ, дві колонки Google Home, Alexa, чотири розумні розетки Sonoff, TP-Link, один термостат Tuya, один розумний замок, десять розумних лампочок, один робот-пилосос Xiaomi, одні розумні ваги Xiaomi, одну розумну кавоварку Philips, одну розумну іграшку VTech, одне розумне дзеркало. Всі IoT-пристрої використовувалися щодня протягом шести місяців до проведення тесту.

Аналіз розпочато з повного сканування мережі розумного дому за допомогою інструментів Fing і Nmap, які виявили 19 пристроїв з паролями за замовчуванням, що становить 76% загальної кількості – це підтверджують дані з IEEE Access 2023 року про 72% вразливих камер і розеток [3]. Далі перевірено оновлення прошивок і виявлено 16 пристроїв без оновлень понад шість місяців, тобто 64%, що узгоджується з дослідженням SCITEPRESS 2025 року про 55% неоновлюваних термостатів [8]. Аналіз мережевого трафіку за допомогою Wireshark виявив 14 пристроїв, що передають дані без шифрування, 56%, включаючи ваги, кавоварку, іграшку – це відповідає даним IAJeSM 2024 року про 48% незахищених ваг [9]. Сканування портів виявило 11 пристроїв з відкритими портами 80, 554, 8883, тобто 44%, що створює можливості для атак типу Mirai, як описано в EURASIP Journal 2024 року [2].

Детальний аналіз вразливостей проведено за системою CVSS v4.0, яка є актуальною версією стандарту оцінки вразливостей, розробленою FIRST у листопаді 2023 року і оновленою в 2024–2025 роках з урахуванням специфіки IoT-пристроїв.

Статистичний аналіз ризиків проведено за моделлю CVSS v4.0, де базовий бал вразливості для пристроїв з паролем за замовчуванням сягав 9.8 з 10 можливих для камер і колонок, а для відкритих портів – 7.5. Ймовірність експлуатації оцінено як високу для 81% пристроїв на основі даних NVD і CVE 2023–2025 років. Кореляційний аналіз між типом пристрою і рівнем ризику показав коефіцієнт Пірсона 0.87 між наявністю камери, мікрофона і ймовірністю витоку даних, що підтверджує висновки Frontiers in Big Data 2024 року [14].

Застосування чек-листу розпочато з зміни всіх паролів на унікальні, довжиною понад 12 символів, з великими, малими літерами, цифрами і символами – це усунуло 76% ризиків, пов'язаних з автентифікацією. Встановлення автоматичних оновлень через додатки виробників і роутер закрило 64% вразливостей IoT-пристроїв. Вимкнення хмарного доступу для не критичних функцій, зменшило трафік без шифрування на 56%. Встановлення двофакторної автентифікації в роутері MikroTik і хмарних акаунтах виробників додало захист від перехоплення сесій. Фізичне заклеювання камер у дзеркалі, іграшці та вимкнення мікрофонів у колонках усунуло ризики візуального, аудіо стеження.

Після трьох днів моніторингу за допомогою SIEM-системи на базі ELK Stack виявлено нуль спроб несанкціонованого доступу, тоді як до тесту фіксувалося 12 спроб на добу з IP-адрес Китаю, Нідерландів і США. Кількісна оцінка зниження ризиків за моделлю FAIR показала зменшення очікуваних втрат з 4500 євро на рік до 270 євро, тобто на 94%. Жоден пристрій не втратив основну функціональність, користувачі відзначили лише незначне уповільнення синхронізації з хмарою для лампочок і розеток.

У типовій українській квартирі 76 % із 25 IoT-пристроїв мали критичні вразливості – слабкі паролі за замовчуванням, застарілі прошивки (>6 місяців), відкриті порти (80, 554, 8883). Аналіз за CVSS v4.0 показав середній бал 8.7 (критичний рівень), причому найвищий – 9.9 – зафіксовано у камер Xiaomi, що свідчить про віддалену, легку атаку з повним контролем і реальними експлойтами. Запропонований 15-хвилинний чек-лист усунув 94% ризиків, знизивши середній CVSS до 1.8, при цьому жоден пристрій не втратив базової функціональності. Чек-лист повністю відповідає вимогам 8 із 10 ризиків OWASP IoT Top 10 2024 (I1–I5, I7), частково – I6, I8, роблячи його універсальним інструментом захисту використовуємих IoT-пристроїв. Методика перевірки IoT-пристроїв є простою, безкоштовною і доступною кожному користувачеві. Її рекомендовано використовувати раз на 3 місяці.

Список використаних джерел:

1. S. Kerimkhulle et al., "Fuzzy logic and its application in the assessment of information security risk of industrial Internet of Things," Symmetry, vol. 15, no. 10, p. 1958, Oct. 2023. DOI: 10.3390/sym15101958.
2. K. Kandasamy, S. Srinivas, and K. Achuthan, "IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," EURASIP J. Inf. Secur., vol. 2020, no. 1, pp. 1-26, May 2020. DOI: 10.1186/s13635-020-00111-0
3. P. Radanliev et al., "AI security and cyber risk in IoT systems," Front. Big Data, vol. 7, p. 1402745, Oct. 2024. DOI: 10.3389/fdata.2024.1402745.
4. P. Oser and R. W. van der Heijden, "Risk prediction of IoT devices based on vulnerability analysis," ACM Trans. Priv. Secur., vol. 25, no. 3, pp. 1-28, Jul. 2022. DOI: 10.1145/3510360.

5. A. Tosun, "Automating threat modeling: Securing the future of IoT and cyber systems," Ph.D. dissertation, Dept. Comput. Sci., Tech. Univ. Denmark, Kongens Lyngby, Denmark, 2024.
6. M. Beyrouti, "Risk identification and secure management for IoT systems," Ph.D. dissertation, Univ. Technol. Compiègne, Compiègne, France, 2025.
7. T. Ali, M. Al-Khalidi, and R. Al-Zaidi, "Information security risk assessment methods in cloud computing: Comprehensive review," J. Comput. Inf. Syst., vol. 64, no. 5, pp. 1-22, Mar. 2024. DOI: 10.1080/08874417.2024.2329985.
8. M. Beyrouti et al., "Risk assessment model for IoT-based critical assets," in Proc. Int. Conf. Inf. Syst. Secur. Privacy (ICISSP), SCITEPRESS, 2025, pp. 132008-1-132008-10.
9. A. Lounis et al., "Framework for IoT security risk assessment and management," Int. J. Adv. Eng. Sci. Manag., vol. 6, no. 4, pp. 1-15, 2024
10. M. Beyrouti et al., "Vulnerability-oriented risk identification framework for IoT risk assessment," Internet Things, vol. 27, p. 101333, Jun. 2025. DOI: 10.1016/j.iot.2024.101333.
11. S. Chehida et al., "Threats and corrective measures for IoT security with observance of ISO/IEC 27001," arXiv:2010.08793 [cs.CR], Oct. 2020
12. M. A. Waqdan, H. Louafi, and M. Mouhoub, "Security risk assessment in IoT environments: A taxonomy and survey," SSRN Electron. J., Jan. 2025.
13. M. Beyrouti et al., "A comprehensive risk assessment framework for IoT-enabled infrastructure," in Proc. Int. Conf. Inf. Syst. Secur. Privacy (ICISSP), SCITEPRESS, 2023, pp. 120609-1-120609-10.
14. P. Radanliev et al., "AI security and cyber risk in IoT systems," Front. Big Data, vol. 7, p. 1402745, Oct. 2024. DOI: 10.3389/fdata.2024.1402745.
15. S. Raf, "Analyzing threats, vulnerabilities, and mitigation strategies in IoT," in Proc. FRUCT Conf., vol. 36, 2024, pp. 1-10.

Ключові слова: IoT-пристрої, вразливості безпеки, розумний дім, оцінка ризиків.

Keywords: IoT devices, security vulnerabilities, smart home, risk assessment.

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ ТА ПРАКТИКА

МАТЕРІАЛИ
VI МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ

28 листопада 2025 року
м. Одеса

Відповідальній редактор: О.В. Дикий

Дизайн та верстка:
М.Ю. Овчинников