Вісник ЛДУБЖД
Bulletin of Lviv State University of Life Safety
https://journal.ldubgd.edu.ua/index.php/Visnuk
ISSN 2078-4643 (print), ISSN 2708-1389 (online)

UDC 004.056.5:004.738.5
DOI: 10.32447/20784643.32.2025.10

В. І. Ящук, У. П. Пановик, С. А. Черкас, А. І. Івануса, Р. Л. Ткачук
Львівський державний університет безпеки життєдіяльності, м. Львів, Україна
ORCID: https://orcid.org/0000-0003-2651-4918 – В.І. Ящук
https://orcid.org/0000-0002-9663-4328 – У.П. Пановик
https://orcid.org/0009-0005-6362-6435 – С.А.Черкас
https://orcid.org/0000-0001-9141-8039 – А.І. Івануса
https://orcid.org/0000-0001-9137-1891 – Р.Л. Ткачук
Valentina.lender@gmail.com

КОМПЛЕКСНА МОДЕЛЬ ЗАХИСТУ IoT-ПРИСТРОЇВ У ПОБУТОВОМУ СЕРЕДОВИЩІ: ЗАГРОЗИ, ВРАЗЛИВОСТІ ТА МЕТОДИ НЕЙТРАЛІЗАЦІЇ

Постановка проблеми. Стрімкий розвиток технологій Інтернету речей (IoT) призвів до масового впровадження «розумних» пристроїв у побутове середовище, що суттєво підвищує комфорт, але водночас створює нові виклики для забезпечення інформаційної безпеки. Значна частина побутових IoT-пристроїв характеризується низьким рівнем захисту, відсутністю оновлень безпеки, слабкою аутентифікацією та незахищеними каналами передачі даних. Через це користувачі стають потенційними жертвами кіберзлочинів, зокрема несанкціонованого доступу, підміни даних, DDoS-атак чи перехоплення керування пристроями. Існуючі підходи до кіберзахисту часто не враховують специфіку побутового середовища, де ресурси обчислення та енергоспоживання є обмеженими. Наявні стандарти безпеки переважно орієнтовані на промислові або корпоративні системи, що ускладнює їхнє застосування для домашніх мереж. Відтак постає необхідність створення комплексної моделі захисту, яка б інтегрувала технічні, організаційні та поведінкові заходи, забезпечуючи адаптивну і багаторівневу протидію сучасним загрозам. Така модель має враховувати контекст побутового використання, динамічність підключень та взаємодію різних типів IoT-пристроїв. Формування єдиної системи моніторингу та нейтралізації вразливостей у домашньому середовищі є актуальним завданням сучасної кібербезпеки.

Мета. Мета дослідження полягає у розробленні комплексної моделі захисту IoT-пристроїв, що функціонують у побутовому середовищі, з урахуванням сучасних кіберзагроз, типових вразливостей та ефективних методів їх нейтралізації. Задля досягнення цієї мети проведено систематизацію існуючих підходів до безпеки Інтернету речей, проаналізовано основні ризики, характерні для домашніх IoT-мереж, та визначено напрями підвищення рівня їхньої інформаційної безпеки. Особлива увага приділяється створенню інтегрованого механізму моніторингу, виявлення та запобігання атакам, орієнтованого на доступні користувацькі середовища, а також впровадженню ефективних рішень у сфері автентифікації користувачів і пристроїв, що забезпечують запобігання несанкціонованому доступу до IoT-інфраструктури. Додатково розглядаються підходи до **захисту** даних IoT-систем, включно з їх шифруванням під час передавання та зберігання, перевіркою цілісності та забезпеченням стійкості до підміни чи несанкціонованої модифікації. В процесі дослідження авторами сформовано науково обґрунтовану та практично реалізовану модель, що забезпечить цілісність, конфіденційність і доступність даних у побутових IoT-системах.

Методи досліджень. У процесі дослідження застосовано системний підхід до аналізу безпеки побутових IoT-систем, що поєднує технічні, аналітичні та економічні методи. Використано методи загрозоорієнтованого моделювання для ідентифікації потенційних атак і вразливостей пристроїв різних класів. Для перевірки ефективності запропонованих заходів захисту розроблено реалістичні тестові стенди, які відтворюють типові конфігурації побутових мереж із підключенням смарт-пристроїв. Застосовано емпіричні методи тестування для оцінювання рівня стійкості до типових кіберзагроз, а також методи кількісного аналізу для визначення показників безпеки, відтворюваності результатів і порівняння альтернативних підходів. Для оцінювання економічної доцільності впровадження захисних рішень використано елементи моделювання життєвого циклу пристроїв. Узагальнення результатів здійснювалося із застосуванням методів порівняльного аналізу, класифікації та моделювання, що дозволило сформувати комплексну методологію оцінювання та підвищення кіберстійкості побутових IoT-систем.

Результати. У результаті проведеного дослідження сформовано та апробовано уніфіковану методологію оцінювання безпеки побутових IoT-екосистем, орієнтовану на кількісні показники та відтворювані метрики. Розроблено детальний план пілотного дослідження, що охоплює вибірку репрезентативних пристроїв, типові сценарії атак, чек-лист вимірювань, набір інструментів та стандартизовану процедуру проведення тестів.. Валідація запропонованої методології підтвердила її ефективність для кількісного оцінювання стійкості IoT-пристроїв до основних кіберзагроз, а також для порівняння різних моделей захисту. Розроблена модель дозволяє не лише ідентифікувати слабкі місця в архітектурі побутових систем, але й оцінити економічну доцільність впровадження конкретних контрзаходів. Крім того, підготовлено рекомендації для забезпечення етичності та безпеки експериментів, що забезпечує відповідність проведених тестів міжнародним стандартам відповідального розкриття (responsible disclosure). Отримані результати можуть бути використані для вдосконалення політик безпеки виробників, розроблення національних регламентів у сфері IoT-захисту та підвищення загальної кіберстійкості побутових мереж.

Ключові слова: Інтернет речей (IoT), кібербезпека, побутове середовище, побутова мережа, модель захисту, вразливості, кіберзагрози, автентифікація, безпека даних.

V. I. Yashchuk, U. P. Panovyk, S. A. Cherkas, A. I. Ivanusa, R. L. Tkachuk
Lviv State University of Life Safety, Lviv, Ukraine

COMPREHENSIVE PROTECTION MODEL OF IoT DEVICES IN THE HOME ENVIRONMENT: THREATS, VULNERABILITIES AND METHODS OF NEUTRALIZATION

Problem statement. The rapid development of Internet of Things (IoT) technologies has led to the mass introduction of “smart” devices into the home environment, which significantly increases comfort, but at the same time creates new challenges for ensuring information security. A significant part of household IoT devices is characterized by a low level of protection, a lack of security updates, weak authentication, and unprotected data transmission channels. Because of this, users become potential victims of cybercrimes, in particular unauthorized access, data substitution, DDoS attacks, or device control interception. Existing approaches to cyber protection often do not take into account the specifics of the home environment, where computing resources and energy consumption are limited. Existing security standards are mainly focused on industrial or corporate systems, which complicates their application for home networks. Therefore, there is a need to create a comprehensive protection model that integrates technical, organizational, and behavioral measures, providing adaptive and multi-level counteraction to modern threats. Such a model should take into account the context of domestic use, the dynamics of connections, and the interaction of different types of IoT devices. The formation of a unified system for monitoring and neutralizing vulnerabilities in the home environment is an urgent task of modern cybersecurity.

Purpose.

The purpose of the study is to develop a comprehensive model for protecting IoT devices operating in a domestic environment, taking into account modern cyber threats, typical vulnerabilities, and effective methods for neutralizing them. To achieve this goal, existing approaches to the security of the Internet of Things were systematized, the main risks characteristic of home IoT networks were analyzed, and directions for increasing their information security were identified. Particular attention is paid to the creation of an integrated mechanism for monitoring, detecting, and preventing attacks focused on accessible user environments, as well as the implementation of effective solutions in the field of user and device authentication that prevent unauthorized access to the IoT infrastructure. Additionally, approaches to protecting IoT system data are considered, including their encryption during transmission and storage, integrity checking, and ensuring resistance to substitution or unauthorized modification. In the process of research, the authors formed a scientifically sound and practically implemented model that will ensure the integrity, confidentiality, and availability of data in household IoT systems.

Research methods. In the process of research, a systematic approach to the analysis of the security of household IoT systems was applied, combining technical, analytical, and economic methods. Threat modeling methods were used to identify potential attacks and vulnerabilities of devices of different classes. To verify the effectiveness of the proposed protection measures, realistic testbeds were developed that reproduce typical configurations of household networks with smart device connections. Empirical testing methods were used to assess the level of resistance to typical cyber threats, as well as quantitative analysis methods to determine security indicators, reproducibility of results and comparison of alternative approaches. To assess the economic feasibility of implementing protective solutions, elements of device life cycle modeling were used. The results were summarized using comparative analysis, classification, and modeling methods, which allowed the formation of a comprehensive methodology for assessing and improving the cyber resilience of household IoT systems.

Results. As a result of the study, a unified methodology for assessing the security of household IoT ecosystems, focused on quantitative indicators and reproducible metrics, was formed and validated. A detailed plan for a pilot study was developed, covering a sample of representative devices, typical attack scenarios, a measurement checklist, a set of

tools, and a standardized testing procedure. Validation of the proposed methodology confirmed its effectiveness for quantitatively assessing the resilience of IoT devices to major cyberthreats, as well as for comparing different protection models. The developed model allows not only to identify weaknesses in the architecture of household systems, but also to assess the economic feasibility of implementing specific countermeasures. In addition, recommendations were prepared to ensure the ethics and security of experiments, which ensures that the tests conducted comply with international standards of responsible disclosure. The results obtained can be used to improve manufacturers' security policies, develop national regulations in the field of IoT security, and increase the overall cyber resilience of home networks.

Keywords: Internet of Things (IoT), cybersecurity, domestic environment, home network, protection model, vulnerabilities, cyber threats, authentication, data security.

Вступ. Стрімке зростання кількості «розумних» пристроїв, інтегрованих у побутові мережі створює нові вектори кіберзагроз. Вразливості IoT-систем часто пов'язані з відсутністю оновлень, слабкою автентифікацією та недостатнім рівнем шифрування даних, що відкриває можливості для несанкціонованого доступу та кібершпигунства. У сучасних умовах цифровізації побуту питання розроблення комплексних підходів до захисту таких систем набуває критичного значення для забезпечення конфіденційності, цілісності та доступності інформації користувачів.

Розвиток технологій Інтернету речей (Internet of Things, IoT) призвів до їхнього широкого впровадження у побутове середовище — від розумних телевізорів, термостатів і систем безпеки до побутової техніки, що здатна автономно приймати рішення та взаємодіяти з іншими пристроями. Така інтеграція цифрових технологій у повсякденне життя підвищує комфорт і ефективність побутових процесів, однак водночас створює нові виклики у сфері інформаційної безпеки. Кожен підключений пристрій є потенційною точкою входу для кібератак, які можуть призвести до несанкціонованого доступу, витоку персональних даних, збоїв у роботі систем або навіть фізичних наслідків.

Актуальність проблеми зумовлена тим, що більшість побутових IoT-пристроїв мають обмежені ресурси для реалізації складних механізмів захисту, а користувачі часто нехтують базовими правилами безпеки. Це сприяє зростанню кількості інцидентів, пов'язаних із зламом розумних пристроїв, створенням ботнетів та поширенням шкідливого програмного забезпечення, орієнтованого на IoT-середовище. Водночас існуючі підходи до захисту не забезпечують комплексного врахування різнорівневих загроз — від апаратних вразливостей до мережевих і поведінкових атак.

Отже, дослідження проблематики створення комплексної моделі захисту IoT-пристроїв у побутовому середовищі є вкрай актуальним. Така модель має поєднувати багаторівневий аналіз загроз, системну оцінку вразливостей та ефективні методи їх нейтралізації, що дозволить забезпечити стійкість і безпечне функціонування розумного дому в умовах зростаючих кіберзагроз.

Метою дослідження є розроблення комплексної моделі захисту IoT-пристроїв у побутовому середовищі, яка поєднує кількісну оцінку безпеки, моделювання реалістичного тестового середовища та економічну оцінку прийнятності захисних рішень, з метою підвищення ефективності механізмів захисту та визначення їх пріоритетності відповідно до реальних загроз і ресурсних обмежень.

Методи дослідження. Для формування сучасного бачення проблеми проведено систематичний огляд наукових публікацій, галузевих стандартів і рекомендацій провідних організацій у сфері кібербезпеки, таких як ENISA, NIST та OWASP [1-3]. Також враховано аналітичні звіти компаній Cisco щодо вразливостей і загроз у побутовому IoT-середовищі. Це дозволило ідентифікувати ключові ризики, актуальні загрози та існуючі практики їх нейтралізації. Для визначення кількісної оцінки стану захисту IoT-пристроїв запропоновано набір метрик, що охоплює три основні аспекти: конфіденційність, цілісність та доступність даних. Додатково враховано показники оновлення пристроїв і швидкості реагування на виявлені вразливості. Такі метрики дозволяють об'єктивно оцінювати ефективність існуючих і запропонованих механізмів захисту. Запропоновані захисні механізми перевірялися в імітованій домашній мережі з використанням honeypots, що дозволило моделювати реальні атаки на побутові IoT-пристрої. Реалізовано такі засоби безпеки: криптографія для ресурсозалежних пристроїв, механізми OTA-оновлення, контроль доступу RBAC та мережевий сегментатор. Експериментальна перевірка забезпечила валідацію практичної ефективності запропонованої моделі захисту. Для врахування економічних та організаційних аспектів дослідження використано опитування і структуровані інтерв'ю з виробниками побутових IoT-пристроїв та користувачами. Це дозволило оцінити бар'єри впровадження запропонованих рішень, їх прийнятність та можливі шляхи оптимізації з точки зору користувачів і бізнесу.

Наукова новизна роботи полягає у комплексному поєднанні кількісних метрик безпеки, моделювання реалістичного тестового середовища та економічної оцінки прийнятності пропонованих рішень. Такий інтегрований підхід дозволяє оцінювати ефективність механізмів захисту IoT-пристроїв у побутовому середовищі та визначати їх пріоритетність відповідно до реальних загроз і ресурсних обмежень.

Результати дослідження надають можливість розробляти конкретні стратегії захисту, що враховують технічні, організаційні та економічні аспекти безпеки IoT-пристроїв, сприяючи підвищенню рівня кіберстійкості побутових систем.

Інформаційний аналіз предметної області. Аналітичний огляд сучасних публікацій у сфері безпеки Інтернету речей демонструє поступову еволюцію наукових підходів — від ідентифікації базових технічних вразливостей до формування комплексних моделей захисту. Практичні рекомендації міжнародних організацій, зокрема ENISA та NIST, становлять фундамент для сучасних вимог до безпеки IoT-пристроїв: упровадження принципів security by design, безпечного життєвого циклу, керування оновленнями та постмаркетингового моніторингу [1, 2].

Подальший аналіз літератури підтверджує, що найбільш критичними проблемами залишаються слабкі або вбудовані паролі, відсутність механізмів безпечного оновлення, незахищені канали зв'язку та недоліки в управлінні життєвим циклом компонентів, включно з їх взаємодією з хмарними сервісами та мобільними застосунками [3].

У низці публікацій представлено дослідження загальних аспектів безпеки IoT-інфраструктур, класифікації вразливостей мережевих протоколів, недоліків прошивок та ризиків, пов'язаних із фізичним доступом до пристроїв [4, 5]. Окремий масив робіт присвячено управлінню життєвим циклом IoT-пристроїв, безпечним процедурам завантаження, оновлення мікропрограмного забезпечення, ротації та зберіганню криптографічних ключів, а також забезпеченню конфіденційності користувацьких даних [6, 7].

Питання організації надійних механізмів автентифікації та авторизації, особливо в контексті обмежених обчислювальних ресурсів побутових IoT-пристроїв, розглядаються у работах [8, 9, 10]. Значну увагу дослідники приділяють проблемам приватності персональних даних, де аналізуються моделі витоку інформації, ризики деанонімізації користувачів та підходи до мінімізації обсягів оброблюваних даних [11, 12, 13].

Паралельно активно досліджуються інциденти широкого масштабу, що включають ботнет-атаки, масове сканування вразливих IoT-вузлів та DDoS-атаки, які використовують компрометовані «розумні» пристрої як розподілені обчислювальні ресурси [14, 15, 16, 17, 18]. У цих роботах підкреслюється важливість інтеграції мережевих механізмів захисту — систем виявлення та запобігання вторгненням (IDS/IPS), сегментації домашніх мереж та аналізу поведінкових аномалій трафіка.

У цьому контексті особливе значення мають новітні рекомендації NIST, спрямовані на встановлення мінімальних вимог до безпеки споживчих IoT-пристроїв та домашніх маршрутизаторів; останні оновлення цих документів засвідчують тенденцію до стандартизації та уніфікації підходів до забезпечення кіберстійкості інтелектуальних пристроїв [19].

Аналітика комерційних звітів [20] (антивірусні компанії, постачальники мережевого моніторингу) демонструє зростання числа інцидентів і кількості подій на мільйони пристроїв; у 2024 році великі звіти виявляли масивні обсяги подій і повторювані класи вразливостей у побутовому IoT. Це підтверджує, що проблема є не лише академічною, а й практичною та масовою.

У праці [21] запропоновано багаторівневий підхід, який включає апаратну ізоляцію критичних ресурсів, безпечне завантаження і верифікацію прошивок, симетричне/асиметричне шифрування комунікацій, MFA для панелей управління, сегментацію домашньої мережі (VLAN, гостьові мережі), централізоване управління пристроями (MDM/IoT-платформи) і впровадження механізмів «псевдонімізації» даних. Академічні роботи також досліджують lightweight-криптографію та легкі протоколи автентифікації, придатні для ресурс-обмежених пристроїв.

Незважаючи на широку таксономію загроз і набори рекомендацій, сучасні публікації відзначають такі прогалини: відсутність універсальних метрик оцінки безпеки для побутового IoT; дефіцит реалістичних тестових середовищ і датасетів для верифікації захисних рішень; проблеми економічної мотивації виробників щодо оновлень і довготривалої підтримки пристроїв; питання приватності при використанні концентраторів і хмарних сервісів. Ці напрямки потребують подальших міждисциплінарних досліджень [22].

Сучасна література [4-20, 21, 22, 24-26] демонструє розуміння ключових векторів загроз і практичних заходів, але наголошує на необхідності уніфікації метрик, покращенні тестових платформ та стимулюванні виробників до довшої підтримки

пристроїв. Подальші дослідження мають поєднувати технічні інновації з соціально-економічними механізмами впровадження безпеки в масовий ринок споживчого IoT.

На основі огляду літератури доцільно: розробити стандартизовану методологію оцінки ризику для домашніх IoT-екосистем; інвестувати в реалістичні еталонні середовища (honeypots, тестові домашні мережі) для валідації захисних механізмів; досліджувати економічні моделі підтримки безпеки пристроїв (ліцензування, моделі життєвого циклу); (інтегрувати рекомендації ENISA/NIST/OWASP у практичні інструменти для виробників і користувачів.

Сьогодні існує багато рекомендацій (ENISA, NIST, OWASP) та емпіричних звітів про атаки [1-3, 20, 23], але відсутня уніфікована, кількісно-орієнтована методологія оцінки безпеки побутових IoT-екосистем із репрезентативними тестовими середовищами й економічними моделями підтримки життєвого циклу пристроїв. Не дослідженими залишаються багато питань, серед яких визначення метрики (кількісних та якісних), що найкраще відображають безпеку домашньої IoT-екосистеми, оптимальне поєднаннння lightweight-криптографії, оновлення firmware та мережевої сегментації для пристроїв із обмеженими ресурсами, визначення економічних та регуляторних механізмів стимулювання виробників до довготривалої підтримки безпеки.

Результати досліджень. Наведемо уніфіковану, кількісно-орієнтовану методологію оцінки безпеки побутових IoT-екосистем, яка поєднує стандартизовані метрики, репрезентативні тестові середовища і економічні моделі підтримки життєвого циклу пристроїв. Методологія призначена для дослідників, практиків і регуляторів та базується на міжнародних рекомендаціях (ENISA, NIST, OWASP) і сучасних підходах до метрик безпеки.

Метою розроблення методології є створення відтворювального, кількісного інструменту оцінювання безпеки домашньої IoT-екосистеми, що дозволяє порівняти класи пристроїв, верифікувати захисні заходи та оцінити економічну доцільність життєвого циклу підтримки.

На рисунку 1 наведено основні принципи пропонованої методології.

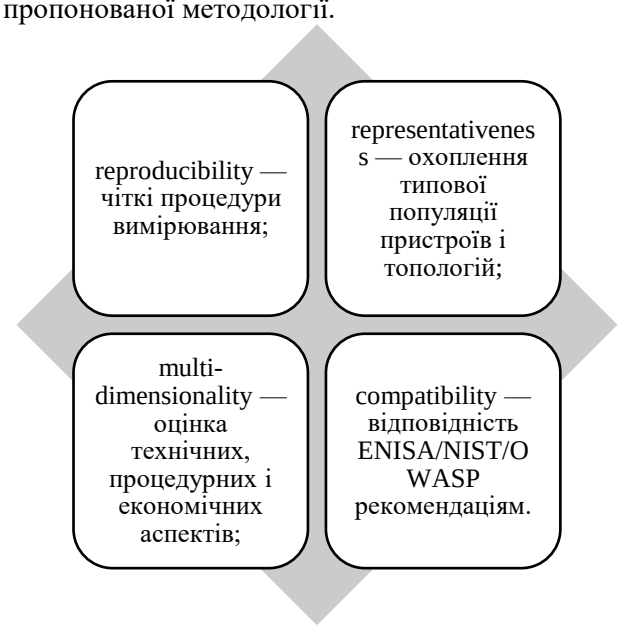


Рисунок 1 – Основні принципи методології

В таблиці 1 наведено метрики, які поділено на п’ять доменів, кожний домен містить набір індикаторів із вагою й формулою нормалізації (0–100).

Таблиця 1

Метрики оцінювання безпеки IoT-екосистеми

Назва домену	Назва індикаторів
Device Security (DS) — апаратна/прошивкова стійкість	наявність secure boot, механізмів оновлення (OTA), контроль цілісності прошивки, апаратне ізоляційне середовище.
Network Security (NS) — захист комунікацій	використання TLS/DTLS, протокол аутентифікації, сегментація мережі (гостьова VLAN), виявлення аномалій.
Lifecycle Management (LM) — процеси підтримки	політика оновлень (термін підтримки), доступність патчів, прозорість supply chain.
Privacy & Data Protection (PD)	мінімізація збору, шифрування даних at-rest/ in-transit, політика згоди користувача.
Operational Resilience (OR) — стійкість до атак	час відновлення (MTTR), детекція інцидентів, наявність журналювання й моніторингу.

Кожен індикатор оцінюється за шкалою 0–1 (формула тесту), комбінується по домену (зважене середнє) і перетворюється у відсоток. Для визначення агрегованої оцінки IoT-екосистеми застосовується зважене середнє доменів. При цьому доцільно параметри ваг можна налаштовувати під сценарій: безпека критичних пристроїв та/ або комфортні пристрої.

Запропоноване описове підґрунтя для репрезентативних тестових середовищ (testbeds)

(рис. 2), яке позиціонується як цілісна методологія для всебічного дослідження безпеки інтернету речей у побутових мережах. Передусім рекомендується провести системну класифікацію пристроїв, виділивши 4–6 функціональних класів — наприклад, розумні лампи та розетки, камери відеоспостереження, шлюзи/роутери, мультимедійні пристрої та бортові контролери HVAC — що забезпечить репрезентативність набору об’єктів дослідження та дозволить стандартизувати профілі поведінки й векторів загроз. Далі описуються типові домашні топології, які мають покривати спектр від мінімальної конфігурації (один роутер і три пристрої) через середню (роутер + шлюз + ≈10 пристроїв, мобільний контролер і хмарний сервіс) до розширеної інфраструктури з мульти-SSID, виділеною IoT-VLAN та NAS. Така стратифікація забезпечує коректне моделювання мережевих умов і потенційних вразливостей.

Класифікація пристроїв	виділити 4–6 класів (розумні лампи/розетки, камери, шлюзи/роутери, медіа-пристрої, бортові контролери HVAC).
Типові топології	мінімальна (одно-рутер + 3 пристрої), середня (роутер + шлюз + 10 пристроїв, мобільний контролер, хмара), розширена (мульти-SSID, IoT-VLAN, NAS).
Сценарії тестування	конфігураційні помилки, brute-force автентифікації, MITM, exploits відомих CVE, відновлення після компрометації. Використовувати як фізичні стенди, так і емульовані «digital twins».
Набори даних та інструменти	збір мережевого трафіка, логи пристроїв, артефакти прошивок; інтеграція з IDS/IPS і honeypot-середовищем. ENISA/NIST рекомендації використовуються для побудови сценаріїв і чек-листів.

Рисунок 2 – Репрезентативні тестові середовища (testbeds)

Сценарії тестування повинні включати симуляцію конфігураційних помилок, атаки методом перебору паролів (brute-force), MITM-атаки, експлуатацію відомих CVE та процедури відновлення після компрометацій; для підвищення достовірності слід застосовувати як фізичні стенди, так і емульовані «digital twins». Набори даних і інструментарій мають охоплювати збір мережевого трафіка, логів пристроїв та артефактів прошивок з подальшою інтеграцією з IDS/IPS та honeypot-середовищами для кореляції подій і виявлення аномалій. Методологія побудована на основі рекомендацій ENISA і NIST та передбачає використання їхніх чек-листів для формалізації сценаріїв, валідації результатів і забезпечення відтворюваності досліджень.

Процедура вимірювання безпеки в досліджуваних тестових середовищах реалізується як послідовний та відтворюваний набір етапів, що забезпечують системну оцінку технічного та функціонального стану пристроїв (рис. 3). На початковому етапі проводиться інвентаризація — детальна каталогізація апаратних компонентів, мережевих вузлів та встановлених версій програмного забезпечення; результати інвентаризації формують базу метаданих для подальшого порівняльного аналізу та трасування змін.

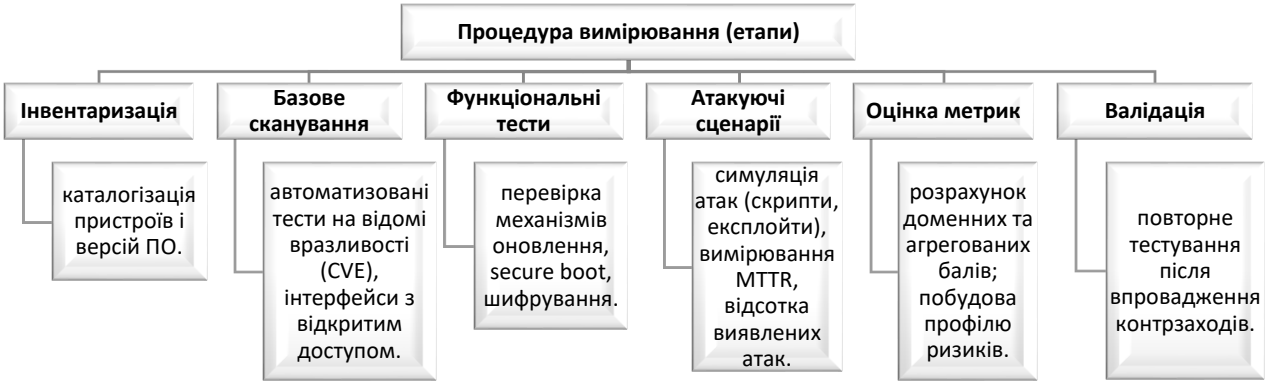


Рисунок 3 – Етапи процесу вимірювання в тестових середовищах

Наступний крок — базове сканування, яке включає автоматизовані сканери вразливостей для ідентифікації відомих CVE, перевірку відкритих сервісів та інтерфейсів з публічним доступом; цей етап дозволяє швидко виявити очевидні технічні прогалини та сформувати початковий набір ризиків. Функціональні тести спрямовані на перевірку захищених механізмів пристроїв: коректності реалізації процедур оновлення прошивки, наявності та працездатності secure boot, ефективності криптографічних механізмів шифрування даних та каналів зв'язку. Далі застосовуються сценарії атаки, які реплікують практичні вектори загроз шляхом виконання скриптів, брютфорс-атаки, MITM-імітацій та експлуатації доступних експлойтів; під час цих сценаріїв фіксуються показники виявлення та часу реагування — зокрема MTTR (mean time to recovery) та відсоток виявлених атак від загального числа спроб.

На етапі оцінки метрик робиться розрахунок доменних (наприклад, мережеві, апаратні, прикладні) та агрегованих балів ризику з подальшою побудовою профілю ризиків для кожного класу пристроїв і топології. Завершальним кроком є валідація — повторне тестування після впровадження контрзаходів для підтвердження їх ефективності та корекції моделей оцінювання; усі етапи супроводжуються детальною обробкою логів, документуванням методик і забезпеченням відтворюваності результатів у відповідності до прийнятих стандартів.

Валідність та масштабованість запропонованої методології оцінювання безпеки IoT-середовищ ґрунтуються на трьох взаємопов'язаних засадах: розширюваності, відтворюваності та відкритих полях для подальших досліджень (рис. 4). По-перше, архітектура метрик і модель вагування проєктуються як конфігуровані компоненти системи, що дозволяє адаптувати набір індикаторів та їхню значущість до локальних нормативно-правових вимог, специфіки прикладних сценаріїв та вимог зацікавлених сторін; така розширюваність забезпечує релевантність оцінок у різних юрисдикціях і контекстах застосування. По-друге, забезпечення відтворюваності досягається шляхом детального документування методик, публікації тестових сценаріїв, скриптів та образів середовища у відкритих репозиторіях. Це не лише сприяє незалежній валідації результатів, але й полегшує аудит методології та її інтеграцію в наукові й промислові процеси. Публічний доступ до артефактів експериментів дозволяє іншим дослідникам відтворювати експерименти, коригувати параметри та порівнювати отримані показники в уніфікованому середовищі.

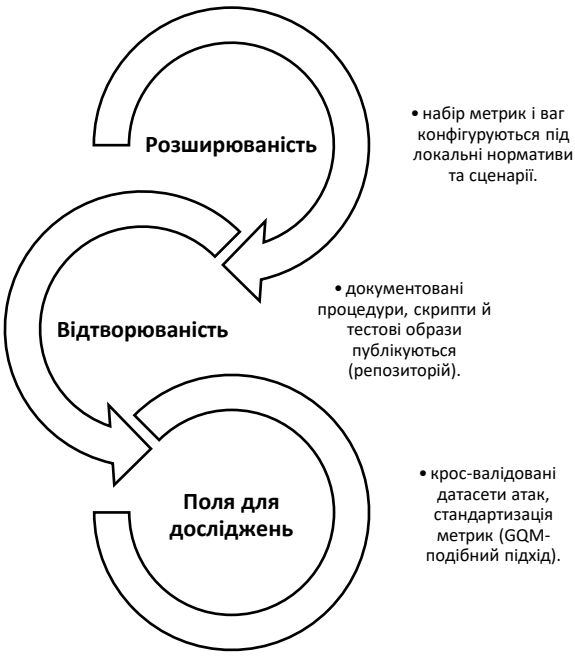


Рисунок 4 – Структурна схема забезпечення валідності та масштабованості методології оцінювання безпеки IoT-середовищ

Модель визначає низку перспективних полів для дослідницької діяльності: створення та крос-валідованих датасетів атак, стандартизація метрик через застосування підходів типу «Goal–Question–Metric» (GQM) та розробка уніфікованих профілів ризику. Такі напрями сприятимуть формуванню загальноприйнятих стандартів оцінки та дозволять використовувати накопичені дані для розвитку машинно-обчислюваних моделей виявлення аномалій.

Економічна модель підтримки життєвого циклу системи безпеки в IoT-екосистемах ґрунтується на поєднанні методів фінансового аналізу та підходів до управління ризиками. У центрі моделі перебуває концепція повної вартості володіння (Total Cost of Ownership, TCO), що охоплює всі етапи життєвого циклу продукту — від розроблення до експлуатації та зняття з підтримки. До структури витрат включаються інвестиції виробника або оператора у створення апаратно-програмних компонентів, підтримку інфраструктури для оновлень «over-the-air» (OTA), а також витрати на технічну підтримку користувачів на часових горизонтах 1, 3 та 5 років. Такий підхід дозволяє здійснювати прогнозування фінансової стійкості системи безпеки та оцінювати ефективність прийнятих управлінських рішень.

Другим компонентом виступає аналіз співвідношення витрат і вигод (Cost–Benefit Analysis), який застосовується для оцінки економічної доцільності впровадження заходів кіберзахисту. У межах цього підходу порівнюються очікувані фінансові втрати від можливих інцидентів (зокрема шкода репутації, компрометація персональних або конфіденційних даних, втрата користувачів чи клієнтів) із витратами на впровадження і підтримку засобів безпеки, включно з регулярними оновленнями та аудитами. Результати такого аналізу дозволяють кількісно оцінити доцільність інвестицій у безпеку та визначити оптимальний рівень фінансування відповідних заходів.

Третій аспект економічної моделі стосується інцентивів і ринкових механізмів підтримки безпеки. Передбачається впровадження моделі маркування («security label»), яка відображатиме рівень захищеності пристрою і може стати стимулом для виробників до пролонгації технічної підтримки. Додатковими механізмами можуть бути державні субсидії, сертифікаційні програми та моделі підписки, що гарантують користувачам доступ до оновлень безпеки протягом усього життєвого циклу пристрою. Як методологічну основу доцільно застосувати підхід NIST до маркування рівня безпеки, який поєднує вимірювані технічні критерії з ринковими стимулами, спрямованими на підвищення довіри користувачів та формування сталого ринку безпечних IoT-рішень.

Валідація запропонованої методології оцінювання безпеки IoT-пристроїв передбачає багаторівневий підхід, який поєднує експериментальне тестування, відкриту публікацію даних і створення практичного інструментарію для відтворення результатів. На першому етапі передбачається пілотне впровадження методології на репрезентативній вибірці, що включає від 20 до 50 пристроїв різних класів — від розумних ламп і камер спостереження до маршрутизаторів, шлюзів та мультимедійних систем. Під час випробувань збираються детальні дані про мережеву поведінку, конфігурації безпеки та реакцію систем на тестові атаки, після чого створюються відкриті набори даних (datasets) і скрипти для повторного використання науковою спільнотою. Такий підхід забезпечує прозорість і відтворюваність результатів, сприяючи формуванню бази для подальших досліджень і стандартизації процесів тестування.

Другий напрям зосереджено на розробленні відкритого інструментарію, зокрема комплексу «IoT Security Assessment Toolkit». Цей набір програмних засобів міститиме автоматизовані сканери вразливостей, шаблони сценаріїв атак, модулі для збору логів і генерації звітів, а також інтерактивну аналітичну панель (dashboard). Вона дозволятиме візуалізувати доменні та агреговані оцінки рівня безпеки, порівнювати результати між різними класами пристроїв і відстежувати динаміку змін після впровадження контрзаходів. Наявність відкритої екосистеми інструментів створює передумови для широкого впровадження методології в академічному, промисловому та нормативному контекстах.

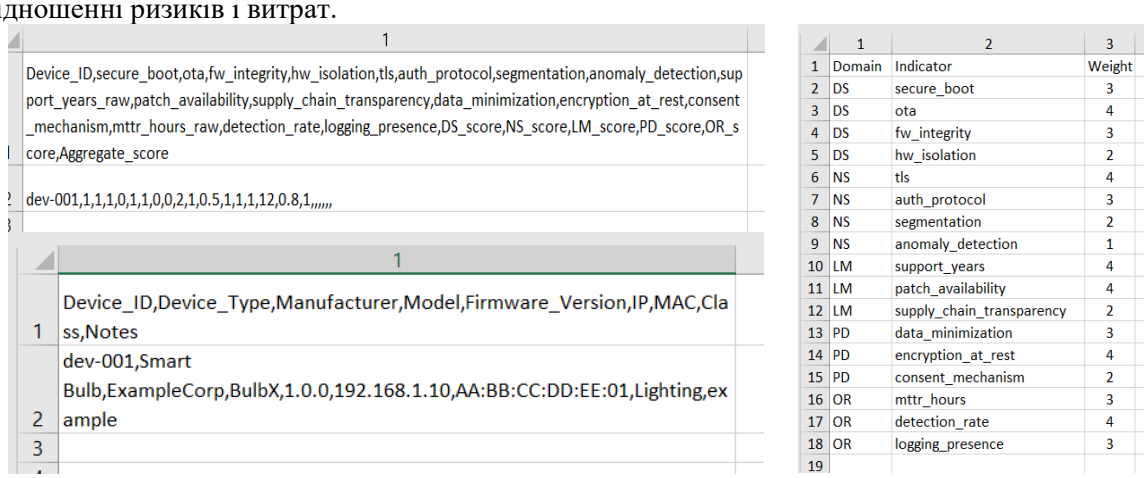
Кінцевим результатом запропонованого підходу є створення стандартизованого рейтингу безпеки IoT-пристроїв, який може стати основою для галузевих рекомендацій та регуляторних політик. На основі зібраних метрик і даних формуються об’єктивні рекомендації для виробників щодо мінімальних вимог підтримки, зокрема у межах політики часу підтримки (Time-Support Policy, TSP). Для органів влади та галузевих регуляторів цей рейтинг може слугувати орієнтиром при формуванні стандартів кібербезпеки споживчих пристроїв, а для користувачів — джерелом достовірної інформації щодо рівня довіри до продуктів на ринку.

Запропонована методологія являє собою інтегрований підхід до оцінювання рівня безпеки побутових екосистем Інтернету речей (IoT), який поєднує технічні метрики, реалістичні тестові стенди та економічні моделі підтримки життєвого циклу пристроїв. Її ключовою особливістю є орієнтація на кількісні, об’єктивно вимірювані показники, що дають змогу проводити відтворювану оцінку кіберстійкості пристроїв різних класів у стандартизованих умовах. Такий підхід забезпечує не лише технічну точність, а й можливість формування порівняльних рейтингів безпеки, релевантних для різних типів користувачів — від кінцевих споживачів до розробників і регуляторних органів.

Завдяки використанню реалістичних тестових стендів, які моделюють типові домашні топології та сценарії атак, методологія враховує динаміку реального середовища функціонування IoT-пристроїв, включно з факторами взаємодії, оновлень, конфігураційних помилок і можливих векторів компрометації. Це дозволяє отримати емпірично обґрунтовані результати, що мають високу практичну цінність для подальшого вдосконалення засобів кіберзахисту. Додатково, інтеграція економічних моделей, таких як Total Cost of Ownership (TCO) і Cost–Benefit Analysis, дає змогу оцінити ефективність заходів безпеки не лише з технічної, а й з фінансової точки зору. Таким чином, прийняття рішень про інвестиції в безпеку може базуватися на збалансованому співвідношенні ризиків і витрат.

Впровадження цієї методології підвищить прозорість ринку побутових IoT-пристроїв, сприятиме розробці обґрунтованих регуляторних рішень і створить мотиваційні механізми для виробників, орієнтовані на довготривалу підтримку програмного забезпечення та оновлень безпеки. У ширшому контексті її застосування сприятиме зміцненню загальної кіберстійкості домашніх мереж, формуванню культури відповідального споживання цифрових технологій і розвитку глобальних стандартів у сфері безпеки споживчого Інтернету речей.

Розрахунок доменних індексів пропонується здійснювати за формулами, наведеними в шаблоні на рисунку 5.



1

Device_ID,secure_boot,ota,fw_integrity,hw_isolation,tls,auth_protocol,segmentation,anomaly_detection,support_years_raw,patch_availability,supply_chain_transparency,data_minimization,encryption_at_rest,consent_mechanism,mttr_hours_raw,detection_rate,logging_presence,DS_score,NS_score,LM_score,PD_score,OR_score,Aggregate_score

dev-001,1,1,1,0,1,1,0,0,2,1,0.5,1,1,1,12,0.8,1,,,,,,

1

	Device_ID,Device_Type,Manufacturer,Model,Firmware_Version,IP,MAC,Class,Notes
1	
2	dev-001,Smart Bulb,ExampleCorp,BulbX,1.0.0,192.168.1.10,AA:BB:CC:DD:EE:01,Lighting,example
3	

	1	2	3
1	Domain	Indicator	Weight
2	DS	secure_boot	3
3	DS	ota	4
4	DS	fw_integrity	3
5	DS	hw_isolation	2
6	NS	tls	4
7	NS	auth_protocol	3
8	NS	segmentation	2
9	NS	anomaly_detection	1
10	LM	support_years	4
11	LM	patch_availability	4
12	LM	supply_chain_transparency	2
13	PD	data_minimization	3
14	PD	encryption_at_rest	4
15	PD	consent_mechanism	2
16	OR	mttr_hours	3
17	OR	detection_rate	4
18	OR	logging_presence	3
19			

де, Weights — таблиця ваг кожного індикатора; можна налаштувати під пріоритети.
Metrics_Definition — опис індикаторів і правила нормалізації (0–1).
Device_List — шаблон інвентаризації пристроїв.
Measurements — шаблон вимірювань; у рядку з прикладом вставлені формули для обчислення доменних оцінок (DS_score, NS_score, LM_score, PD_score, OR_score) та агрегованої оцінки (Aggregate_score). Формули використовують SUMPRODUCT із вагами у листі *Weights*; нормалізація для support_years і mttr_hours реалізована як MIN (value/5,1) та 1-MIN (value/72,1) відповідно.
Domain_Weights — ваги доменів, які використовуються для агрегованої оцінки (можна змінювати).

Рисунок 5 – Шаблон розрахунку доменних індексів

Рисунок 5 ілюструє шаблон розрахунку доменних індексів, який слугує основою для систематизованої оцінки рівня безпеки пристроїв у межах розробленої методології. Представлений набір електронних таблиць реалізовано у форматах Excel і CSV, що забезпечує сумісність із більшістю аналітичних платформ та інструментів обробки даних. Структура шаблону побудована за модульним принципом і включає три основні складові: головний файл з формулами розрахунку інтегральних і доменних показників безпеки, шаблон інвентаризації пристроїв (Device_List) та шаблон вимірювань (Measurements).

Основний Excel-файл містить набір формул для автоматизованого обчислення доменних індексів за визначеними групами метрик — наприклад, автентифікація, оновлення, шифрування, контроль доступу та реагування на інциденти. Формули побудовані так, щоб підтримувати вагові коефіцієнти та дозволяти динамічне оновлення результатів у разі зміни вхідних параметрів. Це забезпечує гнучкість у налаштуванні моделі відповідно до специфіки конкретного середовища тестування чи нормативних вимог. Файл Device_List.csv призначений для каталогізації пристроїв, що підлягають оцінюванню. Він містить поля для ідентифікації виробника, моделі, версії програмного забезпечення, типу пристрою та відповідних мережевих характеристик. Такий підхід дає змогу створити структурований реєстр досліджуваних об’єктів і забезпечує простоту інтеграції з іншими системами управління активами. Файл Measurements.csv містить стандартизовану форму для фіксації результатів вимірювань і спостережень, отриманих під час тестування. Дані з цього файлу

автоматично підключаються до основного Excel-шаблону, де здійснюється обчислення агрегованих показників і формування профілю безпеки кожного пристрою. Використання цих шаблонів дозволяє уніфікувати процес збору, аналізу та представлення даних, що, у свою чергу, підвищує точність оцінок і забезпечує відтворюваність результатів у межах наукових досліджень та практичних аудитів кібербезпеки IoT-пристроїв.

Запропонуємо план пілотного дослідження, який передбачає проведення експериментальної перевірки ефективності розробленої методології оцінювання безпеки побутових IoT-екосистем на основі кількісних метрик, структурованих сценаріїв атак та економічного аналізу впливу вразливостей. Основною метою пілоту є валідація запропонованої уніфікованої, кількісно-орієнтованої методики, що забезпечує відтворюваність результатів, їхню порівнянність у межах різних класів пристроїв та практичну застосовність у реальних умовах експлуатації.

У межах дослідження формується репрезентативна вибірка пристроїв, яка охоплює п’ять основних категорій побутових IoT-компонентів (табл. 2) розумні лампи та розетки, відеокамери, маршрутизатори та шлюзи, мультимедійні пристрої, а також елементи систем керування мікрокліматом (HVAC-контролери). Такий добір забезпечує різноманітність топологій (табл. 3), протоколів і рівнів ризику, що дозволяє комплексно оцінити стійкість системи до різних типів загроз.

Таблиця 2

Репрезентативна вибірка пристроїв (20–30 одиниць)

№ з/п	Назва пристрою	Кількість
1.	Розумні лампи/розетки	4-6
2.	Камери відеоспостереження (IP/Wi-Fi)	4-5
3.	Шлюзи / роутери з підтримкою IoT (домашні хаби)	3-4
4.	Медіапристрої / смарт-телевізори	3-4
5.	Датчики (температури, руху) та контролери (термостати)	3-4
6.	NAS/локальні сховища (як центральна точка даних)	1-2

Таблиця 3

Типові побутові топології (20–30 одиниць)

№ з/п	Розмір	Склад пристроїв
1.	Мінімальна	один роутер, 3 IoT-пристрої, 1 мобільний контролер.
2.	Середня	Роутер, IoT-шлюз, 10 пристроїв, хмарна інтеграція, NAS.
3.	Розширена	мульти-SSID (IoT VLAN + Guest + LAN), роутер з відкритим API, шлюз з локальним управлінням, зовнішній доступ через DDNS.

Сценарії атак розроблені на основі реалістичних векторів загроз і включають конфігураційні помилки, атаки типу brute-force на механізми автентифікації, атаки «людина посередині» (MITM), експлуатацію відомих уразливостей (CVE) та відновлення після компрометації (табл. 4) Для забезпечення достовірності експерименту передбачається використання як фізичних стендів, так і емульованих цифрових двійників («digital twins»), що дозволяє варіювати умови дослідження без шкоди для безпеки реальних систем.

Таблиця 4

Сценарії тестування (вектори нападу)

№ з/п	Назва вектора	Зміст тестування
1.	**Інвентаризаційні та інформаційні**	сканування відкритих портів, виявлення служб, fingerprinting.
2.	**Аутентифікація**	brute-force/credential stuffing на веб-інтерфейси та Telnet/SSH; перевірка слабких паролів.
3.	**Конфіденційність каналів**	MITM та SSL/TLS downgrade (перехоплення трафіка між пристроєм та сервером).
4.	**Експлуатація відомих вразливостей**	запуск експлойтів для CVE, які відповідають прошивкам у вибірці.

Продовження таблиці 4

№ з/п	Назва вектора	Зміст тестування
5.	**Оновлення прошивки**	перевірка механізмів OTA (підпис, валідація), можливість завантажити кастомний firmware.
6.	**Утилітарні атаки**	DDoS/ресурсне виснаження, створення ботнет-поведінки (у контрольованому середовищі).
7.	**Інтеграційні атаки**	зловживання мобільним додатком або хмарним API (неавторизований доступ до даних).
8.	**Відновлення після компрометації**	вимір MTTR, перевірка резервних процедур і журналювання.

Чек-лист вимірювань містить перелік технічних, організаційних і поведінкових показників, зокрема наявність механізмів шифрування, безпечного завантаження (secure boot), процедур оновлення, а також швидкість реакції системи на атаки (MTTR) та відсоток виявлених інцидентів (табл. 5). У процесі вимірювань фіксуються лог-файли, мережевий трафік, артефакти прошивок і журнали системних подій.

Таблиця 5

Чек-лист вимірювань

№ з/п	Назва	Характеристика
1.	Інвентарні дані	модель, версія прошивки, серійний/ідентифікатор.
2.	DS індикатори	secure_boot (0/1), OTA (0/0.5/1), fw_integrity (0/1), hw_isolation (0/1).
3.	NS індикатори	TLS (0/1), auth_protocol (0..1 шкала), segmentation (0/1), anomaly_detection (0/1).
4.	LM індикатори	support_years (роки), patch_availability (0..1), supply_chain_transparency (0..1).
5.	PD індикатори	data_minimization (0..1), encryption_at_rest (0..1), consent_mechanism (0..1).
6.	OR індикатори	mttr_hours (години), detection_rate (0..1), logging_presence (0..1).
7.	Кількість виявлених CVE; час до першого виявлення; успішність експлойтів (% сценаріїв).	
8.	Агреговані доменні та загальний рейтинг (за Excel-шаблоном).	

До складу інструментів входять системи сканування вразливостей (наприклад, Nmap, OpenVAS), засоби емуляції атак (Metasploit, Scapy), а також модулі збору даних і візуалізації результатів у межах розробленого «IoT Security Assessment Toolkit» (табл. 6).

Таблиця 6

Інструменти та ресурси

№ з/п	Назва інструменту	Приклад
1.	**Сканування та аналіз**	Nmap, Masscan, Shodan API (для порівняння), Nessus/OpenVAS (CVE-скан).
2.	**Трафік та MITM**	Wireshark, mitmproxy, Bettercap.
3.	**Експлуатація**	Metasploit, набір публічних PoC, custom скрипти (Python).
4.	**Тестове оточення**	ізольована лабораторна мережа з інтернет-шенкером/симуляцією хмарного сервера, VLAN-конфігурація.
5.	**Моніторинг і IDS**	Zeek (Bro), Suricata, прості honeypots (Cowrie, Dionaea) для побачення атак.
6.	**Автоматизація та звіти**	скрипти для наповнення CSV/Excel (Pandas), Kibana/Grafana для візуалізації результатів.
7.	**Файлове сховище артефактів**	зберегти логи, дампи, власні PoC в зашифрованому сховищі.

Процедура проведення пілотного дослідження реалізується як послідовність взаємопов'язаних етапів, наведених на рисунку 6, що забезпечують системність, відтворюваність і достовірність отриманих результатів. Першим етапом є планування, у межах якого здійснюється відбір пристроїв для тестування, визначення параметрів експериментальної мережі та конфігурації

тестового середовища. На цьому ж етапі узгоджуються етичні й юридичні аспекти дослідження, зокрема забезпечується відповідність процедур вимогам щодо конфіденційності, захисту даних і дотримання міжнародних норм, таких як Загальний регламент захисту даних (GDPR).

Рисунок 6 – Етапи алгоритму проведення дослідження комплексної моделі захисту IoT-пристроїв у побутовому середовищі

Другий етап — інвентаризація та базове сканування — передбачає створення структурованого переліку пристроїв у шаблоні Device_List (рис. 6), що містить основні технічні характеристики, версії програмного забезпечення, мережеві параметри та вразливості. Паралельно виконується початкове сканування на наявність відомих уразливостей (CVE), відкритих портів та неправильно налаштованих сервісів, що формує базову лінію безпеки для подальшого порівняння. На третьому етапі здійснюється функціональне тестування, спрямоване на перевірку наявності та коректності роботи ключових механізмів захисту: безпечного завантаження (secure boot), шифрування даних, механізмів оновлення «over-the-air» (OTA) та засобів контролю доступу. Ці показники формують ядро доменних індексів безпеки, що використовуються у подальшому аналізі.

Четвертий етап передбачає виконання сценаріїв атаки, які відтворюються у контрольованому, ізольованому середовищі. Для кожного пристрою по-черзі проводяться моделювання типових кіберзагроз, таких як brute-force-атаки на автентифікацію, атаки «людина посередині» (MITM), експлуатація вразливостей, виявлених у попередніх етапах. Це дозволяє оцінити реальну стійкість пристроїв до поширених векторів атак. П’ятий етап включає моніторинг усіх процесів тестування — запис логів, фіксацію подій безпеки, оцінювання середнього часу відновлення після атаки (MTTR) та відсотка виявлених інцидентів (detection rate). Зібрані дані інтегруються в шаблони вимірювань (Measurements.csv) (рис. 6) і слугують основою для кількісного аналізу. На шостому етапі відбувається впровадження контрзаходів, що базуються на виявлених недоліках. Серед основних заходів — мережева сегментація, встановлення оновлень, відключення зайвих інтерфейсів та посилення політик автентифікації. Мета цього етапу полягає у практичній перевірці ефективності запропонованих поліпшень. Сьомий етап передбачає повторне тестування після впровадження змін. Це дозволяє оцінити, наскільки запропоновані контрзаходи знизили рівень ризику та підвищили доменні показники безпеки. Завершальний, восьмий етап — аналіз і підготовка звітів — полягає у розрахунку доменних та агрегованих індексів безпеки, побудові профілю ризиків і проведенні економічної оцінки на основі моделей Total Cost of Ownership (TCO) та Cost–Benefit Analysis. Результати оформлюються у підсумковий звіт, що містить кількісні висновки, верифіковані дані та рекомендації для виробників, дослідників та регуляторних органів.

Економічна складова тесту передбачає комплексний аналіз вартості життєвого циклу пристрою та оцінку економічних наслідків від реалізації чи ігнорування заходів безпеки. На першому етапі здійснюється збір даних для розрахунку Total Cost of Ownership (TCO), що включає витрати на розробку та підтримку OTA-оновлень, технічну підтримку й інфраструктуру на горизонтах 1, 3 і 5 років. Далі проводиться оцінка потенційних втрат від інциденту безпеки, де враховуються прямі збитки (заміна пристроїв, відшкодування, штрафи) та непрямі (втрата репутації, падіння довіри користувачів). Аналіз Cost-Benefit дозволяє визначити економічну доцільність впровадження конкретних заходів,

наприклад, використання підписаних OTA, шляхом порівняння вартості їх реалізації зі зменшенням імовірності експлуатації у відсотковому вимірі. Окрему увагу приділено ринковим інцентивам, тобто економічним та організаційним факторам, що впливають на рішення виробників, операторів та користувачів щодо впровадження заходів безпеки IoT-пристроїв, які моделюють додану вартість сертифікатів безпеки або маркування «security label», що може забезпечити збільшення ринкової ціни та конкурентну перевагу. Таким чином, економічна складова дає змогу обґрунтувати інвестиції у безпеку як стратегічно вигідний напрям розвитку.

Очікувані результати дослідження включають створення узагальненого рейтингу безпеки пристроїв, визначення найвразливіших доменів та розробку рекомендацій для підвищення кіберстійкості. Крім того, пропонується набір стандартизованих сценаріїв і показників для подальшого використання в академічних і промислових дослідженнях. Критерії валідації охоплюють відтворюваність результатів, стабільність показників у повторних тестах та узгодженість із міжнародними рекомендаціями ENISA і NIST.

Критерії успіху та валідації передбачають перевірку ефективності та надійності запропонованої методології оцінювання безпеки пристроїв на основі кількісних і якісних показників. Методологія має бути апробована на вибірці з 20–30 пристроїв із наданням повного набору метрик для кожного з них, що забезпечує репрезентативність результатів. Важливим індикатором достовірності є показник відтворюваності, відповідно до якого повторне проведення тестів не повинно перевищувати ±10% відхилення в агрегованих оцінках. Практична корекція результатів здійснюється шляхом впровадження рекомендованих контрзаходів, що мають забезпечити зниження кількості виявлених вразливостей щонайменше на 30% або підвищення агрегованого балу на попередньо узгоджену величину. Завершальним етапом є підготовка набору даних і скриптів для публікації в анонімізованому вигляді у відкритому репозиторії, що сприятиме науковій верифікації та подальшому відтворенню експерименту незалежними дослідниками.

Окрему увагу приділимо етичним і безпековим аспектам експерименту — тестування проводиться виключно в контрольованих середовищах без доступу до реальних користувацьких даних, із дотриманням принципів конфіденційності та мінімізації ризиків для інформаційних систем. Етичні та безпекові аспекти проведення пілотного дослідження є ключовим компонентом забезпечення його відповідності науковим і правовим нормам. Усі експериментальні випробування мають здійснюватися виключно в ізольованому лабораторному середовищі, повністю відокремленому від продуктивного інтернету, з метою уникнення можливих побічних наслідків або неконтрольованого поширення шкідливого впливу. Забороняється тестування пристроїв, що містять персональні дані третіх осіб, без попереднього отримання чітко задокументованої згоди їхніх власників. Усі прототипи експлойтів, доказів концепції (PoC) та технічна документація повинні зберігатися у захищеному сховищі з обмеженим доступом, що відповідає вимогам кібергігієни та інформаційної безпеки. Дотримання принципів відповідального розкриття вразливостей (responsible disclosure) є обов'язковим: будь-які критичні знахідки мають бути попередньо повідомлені виробнику до їхньої публікації. Крім того, у випадках, коли дослідження може впливати на конфіденційні дані або приватну власність, необхідно отримати офіційний етичний дозвіл відповідного комітету та погодити умови співпраці з виробниками або власниками досліджуваних пристроїв. Такий підхід забезпечує відповідність пілотного дослідження міжнародним науковим і правовим стандартам, зокрема вимогам GDPR щодо обробки персональних даних.

Очікувані результати дослідження передбачають отримання комплексного набору відтворюваних метрик і прикладів практичного застосування розробленої методології оцінювання безпеки пристроїв, представлених у вигляді таблиць, графіків та аналітичних звітів. На основі проведеного аналізу буде сформовано рекомендації для виробників, що включатимуть мінімальні вимоги до безпеки та політику підтримки часу життєвого циклу пристроїв (Time-Support Policy, TSP), а також орієнтири для користувачів і регуляторних органів. У межах відкритої наукової ініціативи планується створення open-source інструментарію, який міститиме скрипти, шаблони Excel/CSV і анонімізований датасет результатів тестування для подальшого використання у наукових і прикладних дослідженнях. Крім того, буде підготовлено статистичний звіт про типові вразливості, їх частотність та вплив на безпеку, а також економічну модель, що демонструє окупність заходів кіберзахисту з урахуванням зниження ризиків і втрат. Сукупність цих результатів сприятиме стандартизації підходів до оцінювання безпеки та підвищенню рівня захищеності сучасних IoT-рішень.

Організаційно-методичний план пілотного дослідження тривалістю три місяці передбачає послідовну реалізацію етапів підготовки, виконання експериментальних робіт та їх валідації (табл. 7).

Таблиця 7

Організаційно-методичний план пілотного дослідження

№ з/п	Тривалість	Перелік робіт
1.	Тиждень 1–2	• підготовка лабораторії, закуппівля/підбір пристроїв, документування
2.	Тиждень 3–4	• інвентаризація, базове сканування, напрацювання сценаріїв
3.	Тиждень 5–8	виконання атак і функціональних тестів, збір логів
4.	Тиждень 9	впровадження контрзаходів
5.	Тиждень 10–11	повторні тести, валідація
6.	Тиждень 12	аналіз, фінальний звіт, формування репозиторію

На першому етапі (тижні 1–2) здійснюються комплексні підготовчі заходи: облаштування лабораторного середовища, закупівля або відбір тестових пристроїв та формалізація супровідної документації. Упродовж другого етапу (тижні 3–4) проводиться інвентаризація наявних засобів, виконуються базове сканування та відпрацьовуються сценарії тестування із визначенням контрольних умов. Третій етап (тижні 5–8) передбачає практичну фазу — реалізацію атак та функціональних тестів з одночасним збором і централізацією логів і телеметрії для подальшого аналізу. На дев'ятому тижні відбувається впровадження рекомендованих контрзаходів, після чого у тижнях 10–11 виконуються повторні тести з метою валідації ефективності застосованих рішень. Завершальний етап (тиждень 12) включає системний аналіз отриманих даних, підготовку фінального звіту та формування анонімізованого репозиторію результатів і скриптів для подальшого оприлюднення та реплікації дослідження.

У результаті проведеного дослідження запропоновано комплексну модель захисту IoT-пристроїв у побутовому середовищі, яка враховує специфіку сучасних кіберзагроз, обмеженість обчислювальних ресурсів і потребу в економічно доцільних рішеннях. Запропонована методологія поєднує кількісні метрики оцінювання безпеки, експериментальну валідацію у реалістичних умовах функціонування домашніх мереж і аналіз економічної ефективності запропонованих контрзаходів. Це забезпечує системність і відтворюваність результатів оцінки, дозволяє порівнювати ефективність різних механізмів захисту та формувати рекомендації для виробників і користувачів IoT-пристроїв. Розроблена модель сприяє підвищенню рівня конфіденційності, цілісності та доступності даних у побутових IoT-екосистемах, а також може бути адаптована до різних класів пристроїв і середовищ експлуатації. Практичне значення одержаних результатів полягає у можливості їх застосування для розроблення національних політик безпеки, удосконалення стандартів виробників і підвищення загальної кіберстійкості побутових мереж.

Подальші наукові дослідження доцільно спрямувати на вдосконалення методів автоматизованого моніторингу стану безпеки IoT-пристроїв, розроблення алгоритмів самонавчальної адаптації систем захисту до нових типів атак і використання методів штучного інтелекту для прогнозування потенційних загроз. Перспективним напрямом є також створення відкритої бази даних вразливостей побутових IoT-пристроїв із дотриманням принципів відповідального розкриття, що сприятиме підвищенню прозорості та швидкості реагування на інциденти. Окремої уваги потребує дослідження соціально-економічних аспектів упровадження захисних технологій, зокрема оцінювання ринкових стимулів (інцентивів), які впливають на мотивацію виробників і користувачів до впровадження практик безпечного використання IoT-пристроїв.

Список літератури:

1. ENISA — Guidelines for Securing the Internet of Things (2020) doi: 10.2824/314452

2. NIST — Cybersecurity for IoT / Consumer IoT Cybersecurity (SP-серія, 2022 і суміжні документи). Електронне видання. Режим доступу: https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program

3. OWASP — Internet of Things Project / IoT Top 10 Електронне видання. Режим доступу: https://owasp.org/www-project-internet-of-things/

4. Kumar, V. Enhancing home IoT network security. Discov Appl Sci 7, 1085 (2025). https://doi.org/10.1007/s42452-025-07270-0

5. Zia, M. F., Siddiqua, M., Ouameur, M. A., Bagaa, M., Turjman, F. A. (2025). Securing the Future: A Survey on Smart Home Security in IoT-Integrated Smart Cities. Advances in Networks, 12(1), 1-18. https://doi.org/10.11648/j.net.20251201.11

6. Migwi D., Romaniuk R. S. Lightweight and scalable security for wireless IoT systems: challenges and research directions INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2025, VOL. 71, NO. 3, PP. 1–8 Manuscript received

June 2, 2025; revised June 2025. doi: 10.24425/ijet.2025.155451

7. Klimushyn P. S. Problematic aspects of IoT cybersecurity standardisation" (2025) Law and Safety, 96(1), pp. 53–66. doi:10.32631/pb.2025.1.05.

8. Tageldin, L. (2025) Internet of Things Security: Threats, Recent Trends, and Mitigation Approaches. Advances in Internet of Things, 15, 1-15. https://doi.org/10.4236/ait.2025.151001

9. Torres-Hernandez, C. M., Garduño-Aparicio, M., & Rodriguez-Resendiz, J. (2025). Smart Homes: A Meta-Study on Sense of Security and Home Automation. *Technologies*, *13*(8), 320. https://doi.org/10.3390/technologies13080320

10. Ouaissa, M., & Ouaissa, M. (2025). Analyzing and Mitigating Attacks in IoT Smart Home Using a Threat Modeling Approach-Based STRIDE. International Journal of Interactive Mobile Technologies (iJIM), 19(02), pp. 126–142. https://doi.org/10.3991/ijim.v19i02.52377

11. Palmese F., Mandalari A.M., Haddadi H., Redondi A.E.C. Intelligent Detection of Non-Essential IoT Traffic on the Home Gateway. (Apr 22, 2025) https://doi.org/10.48550/arXiv.2504.18571

12. Ezugwu A.E. Smart Homes of the Future. Wiley journal (2025) Transactions on Emerging Telecommunications Technologies, 2025; 36:e70041 https://doi.org/10.1002/ett.70041

13. Wenda Li , Tan Yigitcanlar, Alireza Nili, Will Browne, Fei Li Responsible smart home technology adoption: exploring public perceptions and key adoption factors. Internet of Things 32 (2025) 101622 https://doi.org/10.1016/j.iot.2025.101622

14. Raghavendra Mishra, Ankita Mishra Current research on Internet of Things (IoT) security protocols: A survey Computers & Security Volume 151, April 2025, 104310 https://doi.org/10.1016/j.cose.2024.104310

15. Inna Rozlomii, Andrii Yarmilko, Serhii Naumenko Innovative resource-saving security strategies for IoT devices Journal of Edge Computing, 2025, Vol.4, Iss. 1, pp. 35–56 /doi.org/10.55056/jec.748

16. Zhiyao Xu, Dan Zhao, Qingsong Zou, Jingyu Xiao, Yong Jiang, Zhenhui Yuan, Qing Li Synthetic User Behavior Sequence Generation with Large Language Models for Smart Homes https://doi.org/10.48550/arXiv.2501.19298

17. Muhammad Furqan Zia, & Maria Siddiqua. (2025). Integrated Security for Smart Homes in IoT-Enabled Cities: Trust,Privacy, and Resilience – A Survey. International Journal of Multidisciplinary Conference Proceedings (IJMCP), 2 (1). doi.org/10.61503/Ijmcp.v2i1.218

18. Sri Ramya Siraparapu , S.M.A.K. Azad Securing the IoT Landscape: A Comprehensive Review of Secure Systems in the Digital Era e-Prime - Advances in Electrical Engineering, Electronics and Energy Volume 10, December 2024, 100798 https://doi.org/10.1016/j.prime.2024.100798

19. Christina Skouloudi, Apostolos Malatras, Rossen Naydenov, Georgia Dede Guidelines for securing the internet of things. Secure supply chain for IoT, November 2020 Електронне видання. Режим доступу: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Guidelines%20for%20Securing%20the%20Internet%20of%20Things.pdf DOI: 10.2824/314452

20. THE 2024 IOT SECURITY LANDSCAPE REPORT Електронне видання. Режим доступу: https://blogapp.bitdefender.com/hotforsecurity/content/files/2024/06/2024-IoT-Security-Landscape-Report_consumer.pdf?utm_source=chatgpt.com blogapp.bitdefender.com+1

21. Raghavendra Mishra, Ankita Mishra Current research on Internet of Things (IoT) security protocols: A survey Computers & Security Volume 151, April 2025, 104310 https://doi.org/10.1016/j.cose.2024.104310.

22. Wen Fei, Hiroyuki Ohno, Srinivas Sampalli A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions ACM Computing Surveys, Volume 56, Issue 5 Article No.: 111, Pages 1 – 40 https://doi.org/10.1145/3625094

23. OWASP IoT Top 10 Vulnerabilities (2025 Updated) Електронне видання. Режим доступу: https://www.wattlecorp.com/owasp-iot-top-10

24. Amrita, Ekwueme, C. P., Adam, I. H., & Dwivedi, A. (2024). Lightweight Cryptography for Internet of Things: A Review. EAI Endorsed Transactions on Internet of Things, 10. doi.org/10.4108/eetiot.5565

25. Cisco Talos — Year in Review / Threat Reports (2024) Електронне видання. Режим доступу: https://blog.talosintelligence.com/content/files/2025/03/2024YiR-report.pdf

26. Sebestyen, H., Popescu, D. E., & Zmaranda, R. D. (2025). A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories. Computers, 14(2), 61. https://doi.org/10.3390/computers14020061.

References:

1. ENISA. (2020). *Guidelines for securing the Internet of Things*. https://doi.org/10.2824/314452

2. National Institute of Standards and Technology. (2022). *Cybersecurity for IoT / Consumer IoT cybersecurity*. https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program

3. OWASP. (2025). *Internet of Things Project / IoT Top 10*. https://owasp.org/www-project-internet-of-things/

4. Kumar, V. (2025). Enhancing home IoT network security. *Discover Applied Sciences*, *7*, 1085. https://doi.org/10.1007/s42452-025-07270-0

5. Zia, M. F., Siddiqua, M., Ouameur, M. A., Bagaa, M., & Turjman, F. A. (2025). Securing the future: A survey on smart home security in IoT-integrated smart cities. *Advances in Networks, 12*(1), 1–18. https://doi.org/10.11648/j.net.20251201.11

6. Migwi, D., & Romaniuk, R. S. (2025). Lightweight and scalable security for wireless IoT systems: Challenges and research directions. *International Journal of Electronics and Telecommunications, 71*(3), 1–8. https://doi.org/10.24425/ijet.2025.155451

7. Klimushyn, P. S. (2025). Problematic aspects of IoT cybersecurity standardisation. *Law and Safety, 96*(1), 53–66. https://doi.org/10.32631/pb.2025.1.05

8. Tageldin, L. (2025). Internet of Things security: Threats, recent trends, and mitigation approaches. *Advances in Internet of Things, 15*, 1–15. https://doi.org/10.4236/ait.2025.151001

9. Torres-Hernandez, C. M., Garduño-Aparicio, M., & Rodriguez-Resendiz, J. (2025). Smart homes: A meta-study on sense of security and home automation. *Technologies, 13*(8), 320. https://doi.org/10.3390/technologies13080320

10. Ouaissa, M., & Ouaissa, M. (2025). Analyzing and mitigating attacks in IoT smart home using a threat modeling approach-based STRIDE. *International Journal of Interactive Mobile Technologies, 19*(2), 126–142. https://doi.org/10.3991/ijim.v19i02.52377

11. Palmese, F., Mandalari, A. M., Haddadi, H., & Redondi, A. E. C. (2025). *Intelligent detection of non-essential IoT traffic on the home gateway*. https://doi.org/10.48550/arXiv.2504.18571

12. Ezugwu, A. E. (2025). Smart homes of the future. *Transactions on Emerging Telecommunications Technologies, 36*, e70041. https://doi.org/10.1002/ett.70041

13. Li, W., Yigitcanlar, T., Nili, A., Browne, W., & Li, F. (2025). Responsible smart home technology adoption: Exploring public perceptions and key adoption factors. *Internet of Things, 32*, 101622. https://doi.org/10.1016/j.iot.2025.101622

14. Mishra, R., & Mishra, A. (2025). Current research on Internet of Things (IoT) security protocols: A survey. *Computers & Security, 151*, 104310. https://doi.org/10.1016/j.cose.2024.104310

15. Rozlomii, I., Yarmilko, A., & Naumenko, S. (2025). Innovative resource-saving security strategies for IoT devices. *Journal of Edge Computing, 4*(1), 35–56. https://doi.org/10.55056/ jec.748

16. Xu, Z., Zhao, D., Zou, Q., Xiao, J., Jiang, Y., Yuan, Z., & Li, Q. (2025). *Synthetic user behavior sequence generation with large language models for smart homes*. https://doi.org/10.48550/arXiv.2501.19298

17. Zia, M. F., & Siddiqua, M. (2025). Integrated security for smart homes in IoT-enabled cities: Trust, privacy, and resilience – A survey. *International Journal of Multidisciplinary Conference Proceedings, 2*(1). https://doi.org/10.61503/ Ijmcp.v2i1.218

18. Siraparapu, S. R., & Azad, S. M. A. K. (2024). Securing the IoT landscape: A comprehensive review of secure systems in the digital era. *e-Prime – Advances in Electrical Engineering, Electronics and Energy, 10*, 100798. https://doi.org/10.1016/j.prime.2024.100798

19. Skouloudi, C., Malatras, A., Naydenov, R., & Dede, G. (2020). *Guidelines for securing the Internet of Things: Secure supply chain for IoT*. ENISA. https://doi.org/10.2824/314452

20. Bitdefender. (2024). *The 2024 IoT security landscape report*. https://blogapp.bitdefender.com/hotforsecurity/content/files/2024/06/2024-IoT-Security-Landscape-Report_consumer.pdf

21. Mishra, R., & Mishra, A. (2025). Current research on Internet of Things (IoT) security protocols: A survey. *Computers & Security, 151*. https://doi.org/10.1016/j.cose.2024.104310

22. Fei, W., Ohno, H., & Sampalli, S. (2025). A systematic review of IoT security: Research potential, challenges, and future directions. *ACM Computing Surveys, 56*(5), Article 111. https://doi.org/10.1145/3625094

23. OWASP. (2025). *OWASP IoT Top 10 vulnerabilities (2025 update)*. https://www.wattlecorp.com/owasp-iot-top-10

24. Amrita, E., Ekwueme, C. P., Adam, I. H., & Dwivedi, A. (2024). Lightweight cryptography for Internet of Things: A review. *EAI Endorsed Transactions on Internet of Things, 10*. https://doi.org/10.4108/eetiot.5565

25. Cisco Talos. (2024). *Year in review: Threat report*. https://blog.talosintelligence.com/content/files/2025/03/2024YiR-report.pdf

26. Sebestyen, H., Popescu, D. E., & Zmaranda, R. D. (2025). A literature review on security in the Internet of Things: Identifying and analysing critical categories. *Computers, 14*(2), 61. https://doi.org/10.3390/computers14020061.

Науково-методична стаття.
Надійшла до редакції 11.11.2025.
Прийнято до публікації 26.11.2025.