DOI: 10.25140/2411-5363-2025-1(39)-170-183
УДК 004.2

Юрій Іванович Підлісний

аспірант кафедри кібербезпеки та математичного моделювання
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: ypodlesny@ukr.net. **ORCID:** https://orcid.org/0009-0001-9783-3898. **ResearcherID:** LSL-1170-2024

АУДИТ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ: ОЦІНКА ВРАЗЛИВОСТЕЙ ТА ЗАХИСТ ВІД КІБЕРНАПАДІВ

У статті представлено результати дослідження питань безпеки Інтернету речей (IoT), аналізу ризиків та проведенню аудиту IoT-систем. Розглянуто ризики, пов'язані з використанням IoT-пристроїв, які виникають через недостатній рівень безпеки, відсутність єдиних стандартів та складність управління великими мережами. Особлива увага приділяється аудиту IoT-систем, який дозволяє ідентифікувати слабкі місця в інфраструктурі та мінімізувати можливі загрози. У статті запропоновано різні підходи до аудиту, зокрема проактивний, який спрямований на запобігання ризикам ще на етапі розробки та впровадження системи. Також проаналізовано можливі архітектури IoT (централізовані, децентралізовані, гібридні) та їхній вплив на загальну безпеку системи. Особлива увага приділена методології управління ризиками, яка може бути адаптована до потреб IoT. У статті наведено рекомендації щодо впровадження більш ефективних методів захисту, розробки нових стандартів та комплексного підходу до безпеки IoT-систем. Основна мета – створення надійної, безпечної та масштабованої екосистеми IoT, яка відповідає сучасним викликам.

Ключові слова: *Інтернет речей; безпека IoT; IT аудит систем; управління ризиками; архітектура IoT; захист даних; кіберзагрози, стандарти безпеки; вразливості мереж; протидія атакам; моніторинг; кібербезпека; проактивні методи.*

Рис.: 5. Бібл.: 12. Табл.: 1.

Актуальність теми дослідження. Відзначається стрімке зростання популярності технологій Інтернету речей (IoT), які стають невід'ємною частиною сучасного суспільства, охоплюючи різноманітні сфери – від побутових пристроїв до промислових систем. Разом із цим зростає кількість кіберзагроз, які ставлять під ризик конфіденційність, цілісність і доступність даних. Вразливості в архітектурі IoT мереж, обмеженість ресурсу пристроїв та недостатня адаптація стандартів безпеки роблять цю сферу критично важливою для досліджень. Забезпечення надійного захисту IoT мереж потребує розробки ефективних методів виявлення вразливостей та протидії кіберзагрозам, що є важливим для підтримки довіри користувачів та стабільності цифрової інфраструктури.

Постановка проблеми. У зв'язку з бурхливим розвитком Інтернету речей (IoT), безпека таких мереж стає однією з найважливіших проблем. Зростаюча кількість підключених пристроїв і взаємодія між ними створюють численні точки вразливості, що може призвести до різноманітних кіберзагроз. Аудит безпеки є необхідним інструментом для виявлення цих вразливостей і оцінки рівня загроз в IoT-мережах. Проблема полягає в тому, що традиційні методи аудиту безпеки не завжди ефективні для таких складних і динамічних мереж. Потрібні нові методики та підходи, що здатні враховувати специфіку IoT-середовища, зокрема різноманітність пристроїв, їхні обмежені ресурси, а також специфічні загрози, що виникають внаслідок їх взаємодії. Виявлення вразливостей і розробка заходів для протидії кіберзагрозам стають критично важливими для забезпечення належного рівня безпеки в таких мережах.

Таким чином, постає потреба в розробці ефективних методів аудиту, які дозволяють оперативно виявляти вразливості в мережах IoT, оцінювати рівень кіберзагроз та розробляти стратегії для їх нейтралізації, що дозволить забезпечити надійний захист і безпечну роботу таких технологій в умовах сучасних загроз.

Аналіз останніх досліджень і публікацій. Останні дослідження у сфері аудиту безпеки IoT зосереджуються на розробці нових методів для виявлення вразливостей у пристроях та мережах IoT. Вивчення зростаючої кількості кіберзагроз вимагає інтеграції сучасних технологій, таких як машинне навчання, штучний інтелект та аналіз великих даних для автоматичного виявлення аномалій та загроз. Багато робіт досліджують різні методи шифрування,

безпечну автентифікацію та протоколювання даних, щоб зменшити ймовірність атак. Окремо підкреслюється важливість безперервного моніторингу та аналізу мережевої активності для своєчасного виявлення та нейтралізації потенційних кіберзагроз.

Так, деякі автори [1] дають огляд безпекових проблем, з якими стикаються IoT-системи, зокрема, з погляду можливих загроз для приватності користувачів і конфіденційності даних. Авторами запропоновано кілька підходів для захисту IoT, включаючи використання блокчейн-технологій для створення безпечних і децентралізованих платформ для управління даними. У статті [2] автори зосереджуються на специфіці безпеки та конфіденційності в IoT-системах, які використовуються в "розумних містах". Вони розглядають загрози, які можуть виникнути через масове використання сенсорів, що підключаються до мереж. Пропонується кілька рішень для захисту таких мереж, зокрема, використання інтелектуальних методів для моніторингу та запобігання атак.

Загалом різні автори підкреслюють необхідність адаптації чинних стандартів безпеки до специфіки IoT, враховуючи обмеження пристроїв та високий рівень взаємодії між різними платформами. Безпека в IoT повинна охоплювати різні рівні: пристрої, мережі, хмарні системи та взаємодію між ними. Проблеми приватності [3] і довіри в IoT стають критичними, оскільки зростає кількість даних, які передаються між пристроями. Автори наголошують на необхідності створення політик довіри, які дозволяють забезпечити не лише технічний захист, а й соціальний контекст взаємодії користувачів з технологіями.

Однак більшість досліджень акцентують увагу на проблемах інтеграції безпеки в існуючі інфраструктури IoT, що включає забезпечення сумісності різних протоколів і платформ без шкоди для їхньої продуктивності та функціональності.

Виділення недосліджених проблем. Однією з ключових проблем, яка залишається недослідженою, є розробка ефективних методів аудиту безпеки в реальному часі для мереж IoT. Існуючі методи здебільшого орієнтовані на постійне або періодичне сканування мережі, що не завжди забезпечує своєчасне виявлення нових загроз або вразливостей, особливо в умовах динамічного середовища IoT.

Недостатньо дослідженою залишається інтеграція різних стандартів безпеки для створення єдиної системи аудиту.

Відсутні ефективні методи для захисту від багатокрокових атак, які використовують кілька вразливостей.

Немає достатньо розроблених методів для автоматизації аудиту безпеки в IoT-мережах.

Мета статті. Створити тестову модель мережі IoT, вибрати методологію проведення аудиту й показати в рамках об’єму цієї статті, які конкретні етапи проведення аудиту були застосовані і які результати були отримані.

Виклад основного матеріалу. Поняттю Інтернет Речей (далі - IoT) вже 25 років, але найбільше розповсюдження він почав набувати останні 10 років. Термін IoT можна охарактеризувати як об’єднані за допомогою даних в одну мережу об’єктів, які контролюються іншими пристроями або серверами. Зв'язок між об’єктами, мережами або людьми включає як явні (свідомі) дії від одного пристрою IoT до іншого так і не неявні (несвідомі). Головна відмінність IoT в тому, що вплив людини на ці пристрої зменшений або відсутній.

На думку багатьох дослідників, IoT змінить кардинально суспільство, як і Інтернет [4]. IoT дозволяє еволюціонувати існуюче середовище з новими функціями, такими як створення «розумних» міст, мереж і різних автоматизованих середовищ. Використання IoT майже в усіх сферах людського буття створює багато переваг, але також і серйозних викликів, пов’язаних з безпекою та надійністю пристроїв, а також порушує серйозні етичні проблеми. Стрімка еволюція технологій, поширення автоматизації різноманітних процесів потребує дедалі більшого використання IoT, а їхнє операційне середовище стає

дедалі складнішим. Досить поширеними є ситуації, коли виробники підключають різноманітні пристрої IoT, прагнучи максимально автоматизувати процеси системи або середовища, але не приділяючи достатньої уваги безпеки цих пристроїв. Можна констатувати, що велике різноманіття розумних пристроїв робить складною задачу аудиту безпеки з поточними інструментами управління ризиками, а в деяких випадках серйозні ризики безпеки можуть бути невиявлені взагалі.

Так у [5] звернено увагу на проблеми, що виникають через відсутність захисту безпеки в системах Інтернету речей, а саме питання стандартизації, масштабування, конфіденційності, фізичної безпеки. У [6] зазначено, що при впровадженні нових екосистем (які використовують IoT) можливо не помітити наявних ризиків, які виникають через поглиблені зв'язки різних систем, різних стандартів передачі даних і різних стандартів шифрування. З іншого боку, для успішного аудиту системи й оцінки ризиків необхідно повне розуміння мережевого середовища системи, але, враховуючи вищезазначене, в мережах з використанням IoT деякі аспекти функціонування мережі часто невідомі або невизначені.

Взагалі інформаційна безпека систем, згідно з [4, с. 294], складається з таких проблемних аспектів що необхідні для керування ризиками (рис. 1): безпека програмного забезпечення, фізична безпека, контроль доступу, плани відновлення, аудит і моніторинг журналів, запобігання несанкціонованому доступу, безпека й конфіденційність даних.

Рис. 1. Безпека інформаційної системи

Джерело: розроблено автором.

Якщо аналізувати проблематику безпеки інформаційних систем з використанням пристроїв IoT, можна виділити наступне.

Наразі дедалі більше розповсюдження має так звана платформа IoT, коли за допомоги програмного забезпечення створюється спільна екосистема між пристроями і хмарними сервісами. Вона дозволяє передавати дані з різних пристроїв IoT безпосередньо на платформу сервісу для використання. Оскільки платформи IoT обробляють і містять величезну кількість даних, пристроїв та інформації про них, виникає багато питань, пов'язаних з безпекою та управлінням ризиками. З погляду обслуговування постійним викликом для хмарних сервісів IoT є підтримка належного рівня безпеки, наприклад, з позиції стандартизації, а також забезпечення конфіденційності, цілісності та доступності платформ. Кожна платформа IoT переважно має різноманітні розумні датчики, які виробляються різними виробниками і які контактують та взаємодіють між собою у міждоменний спосіб і звісно мають геть різні стандарти безпеки. У [7] автори зазначають, що платформи IoT також стикаються із загрозою різних типів дешевих датчиків. Платформи Інтернету речей зберігають, передають і розподіляють дані, що можуть включати конфіденційну інформацію, і коли йдеться про використання сотень або навіть тисяч IoT-пристроїв, важливо, щоб дані з датчиків можна було ефективно контролювати й управляти ними.

Великим викликом є також функціональні проблеми нестандартних гетерогенних інтерфейсів які використовуються для об’єднання пристроїв IoT з хмарними сервісами (тобто маємо різноманітні мережеві інтерфейси через які і взаємодіють розумні пристрої), деякі дослідники також зазначають що «Пристрої Інтернету речей не призначені для ефективної міжмашинної комунікації через мережеві накладні витрати, мережеві затримки та різні проблеми з обробкою даних» [8]. Іншою проблемою пристроїв IoT став їхній швидкий розвиток, який випереджає сумісні технології і виробники не в змозі створити загальні стандарти і правила безпеки.

На думку авторів [9] ризики життєвого циклу пристроїв Інтернету речей, пов'язані з мінімізацією кіберризиків, повинні регулярно переглядатися. Зменшення цих ризиків також вимагає інтеграції даних, процесів, пристроїв і систем у систему управління ризиками.

Управління ризиками має першорядне значення для культури безпеки, особливо коли мова іде про взаємозв'язок різних систем, а саме пристрої IoT утворюють великий набір різних зав’язків. Однак для підтримки зав’язків недостатньо лише протоколів і стандартів зв'язку, а необхідна багаторівнева співпраця між різними суб'єктами. Ця співпраця буде зосереджена на способах обробки та отримання даних.

Можна констатувати, що «без чітких керівних принципів для пристроїв і систем Інтернету речей, таких як нормативно-правові акти та загальні стандарти, неврегульовані питання негативно впливатимуть на промисловість» [10].

За останнє десятиліття Міжнародна організація стандартизації (ISO) провела багато досліджень, намагаючись визначити потенційні економічні вигоди від стандартизації для компаній, що використовують технології, які швидко розвиваються, але на разі стандартизація безпеки пристроїв IoT має фрагментарний характер.

Можливо припустити, що нові типи технологій створюють більше нових ризиків, які існуючі системи оцінки та управління не здатні передбачити. Деякі дослідники зазначають, що існуючі системи безпеки не підходять для регулярних оцінок безпеки, оскільки інтерфейси між різними системами, що містять пристрої Інтернету речей, невідомі під час оцінки безпеки систем [9].

Взагалі при проведенні аудиту пристроїв IoT, а саме перевірки системи на відповідність набору правил безпеки, виникає перша проблема навіть в визначенні «відповідність набору правил безпеки». Існуючі стандарти і навіть найновітніший ISO/IEC 27400, містять загальні положення для впровадження безпеки IoT і запроваджують ризик орієнтований підхід для проведення аудиту безпеки. Загалом можна констатувати, що стандарти охоплюють так званий високий рівень даних, але саме низкорівневі системні дані, отримані, наприклад, від скомпрометованого датчика диму, температури тощо можуть містити загрозу для всієї високорівневої системи.

Також при проведенні аудиту IoT систем треба бути готовим до відсутності так званого автономного аудиту (коли пристрої ведуть журнали самодіагностики або взагалі мають журнали з логуванням критичних подій), оскільки пристрої можуть не мати достатніх ресурсів для таких операцій. І не менш значущою проблемою є так звана вибірка даних для аудиту. Одні дослідники дають рекомендації для перевірки мобільного додатку (який управляє системою IoT), аналіз мережевого трафіку на предмет вторгнень, аналіз даних з різноманітних датчиків, що контролюють процеси аутентифікації та авторизації [11], але на практиці збір такої кількості різноманітної інформації і перевірки її на правила безпеки (також слід врахувати, що для різних підсистем IoT і навіть автономного пристроїв-різні стандарти безпеки), буде досить виснажливим процесом. На рис. 2 зображені основні проблеми проведення аудиту систем IoT.

Рис. 2. Основні проблеми проведення аудиту пристроїв IoT
Джерело: розроблено автором.

Сучасні методології аудиту безпеки можна розділити на ретроактивні, інкрементні та проактивні.

Ретроактивний підхід використовується для розслідування фактів зламу систем, аналізу їхніх причин і наслідків. Хоча він не здатен запобігти втраті даних або відмові в обслуговуванні, результати такого аналізу слугують основою для вдосконалення безпеки майбутніх систем.

Інкрементний підхід передбачає поетапне тестування або аудит системи з акцентом на ті компоненти, які зазнають змін або мають критичний вплив на цілісність, безпеку та ефективність. Цей підхід виявляється особливо ефективним у випадку динамічних систем із регулярними оновленнями, де базовим припущенням є стабільність поточної версії та відсутність критичних вразливостей перед впровадженням змін.

Проактивний підхід базується на запобіганні проблемам і ризикам до їх виникнення, а не на реагуванні на вже наявні загрози чи інциденти. У контексті інформаційної безпеки та IoT-мереж, він передбачає аналіз можливих слабких місць, прогнозування потенційних атак та впровадження попереджувальних заходів.

Для кращого розуміння методів аудиту IoT, необхідно представити архітектуру систем на базі IoT. Як зазначалось вище, пристрої IoT взаємодіють через гетерогенні системи, тому для забезпечення масштабованості, максимальної інтеграції і зниження вартості, використовується відкрита архітектура (тобто для проведення аудиту ми маємо доступ до інтерфейсів і компонентів).

У будь-якому разі, ці архітектури повинні відповідати вимогам безпеки, представленим на рис. 1, особливо цілісність, конфіденційність, доступність.

Найчастіше, на думку дослідників [12], використовуються три архітектури IoT:

- централізована архітектура, коли всі датчики, сенсори й інші пристрої IoT через шлюзи підключені до хмарної платформи, яка обробляє всі дані, керує пристроями й ухвалює рішення. Класичним прикладом є концепція «розумного дому» або навіть «розумного міста».

- децентралізована архітектура IoT, на відміну від вищезгаданої, обробка даних і ухвалення рішень розподілена між кількома вузлами.

- гібридна архітектура IoT поєднує особливості централізованої та децентралізованої архітектур для досягнення балансу між ефективністю обробки даних, масштабованістю та надійністю. У цій моделі частина функцій виконується централізовано (наприклад, обробка великих даних), тоді як інші функції розподіляються між пристроями (обробка локальних даних).

На рис. 3 зображена детальна гібридна архітектура пристроїв IoT, а саме хмарний сервер (який має декілька рівнів: додатки; файлове сховище; рівень керування зв'язком; канальний рівень, або протоколи зв'язку) та пристрої IoT, для яких передбачено такі рівні: додатки; проміжне ПЗ; протоколи керування (наприклад датчиками); операційна система (необов'язкова присутність); канальний рівень (представлений найбільш поширеними протоколами зв'язку для IoT.

Нині немає жодного документа, як провести аудит IoT систем і проаналізувати її безпечність, тому пропонується:

1. Застосувати проактивний підхід для проведення аудиту, спираючись на те, що ми, як правило маємо новітні системи, або які запроваджується вперше, тому важливо передбачити інциденти безпеки, провести так званий стрес-тест усієї системи і проаналізувати результати.

2. Будемо вважати, що на сьогодні більшість архітектур мають гібридну топологію, адже вона поєднує переваги інших.

3. Для полегшення аудиту проведемо декомпозицію системи та розіб'ємо архітектуру на складові:

- пристрій IoT (наприклад, датчик, привід, смартфон);
- мережа (наприклад, локальна мережа, Інтернет);
- хмара: платформа для зберігання, обробки та аналізу даних;.
- канали зв'язку: wi-fi, супутниковий зв'язок, ZiGbee, NFC, BT тощо.

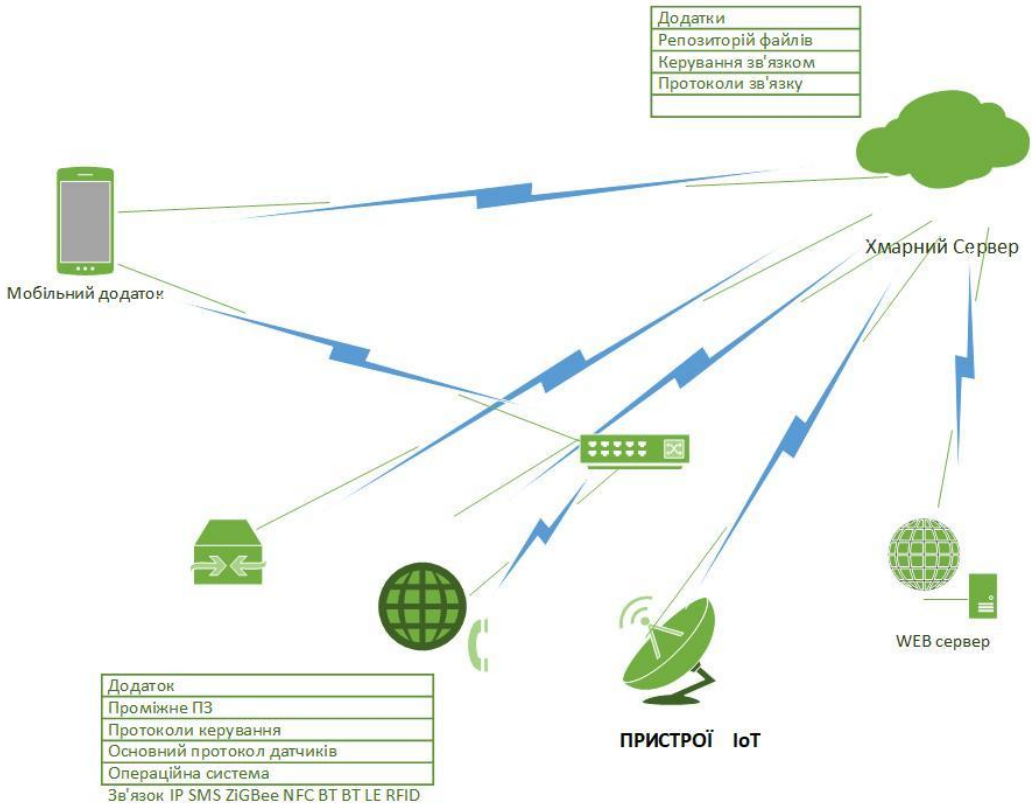

Рис. 3. Гібридна архітектура пристроїв IoT

Джерело: розроблено автором.

Наступним кроком після визначення проактивного підходу для проведення аудиту гібридної IoT системи необхідно визначити методологію управління ризиками, яка і допоможе знайти слабкі місця на всіх рівнях (пристрої, мережа, хмара), а головне дасть змогу зрозуміти, які ризики мають найбільший вплив на систему взагалі.

Наразі в контексті IoT можна використовувати такі стандарти:

1) **ISO/IEC 27005** – міжнародний стандарт, визначає процеси ідентифікації активів, оцінки загроз і вразливостей, аналізу ризиків і управління ними, він тісно інтегрується з ISO/IEC 27001. Головний недолік – його широке застосування для різноманітних систем, в контексті IoT не завжди враховує специфіку;

2) **NIST RMF** (Risk Management Framework) - рамкова методологія, створена Національним інститутом стандартів і технологій США, яка найбільш популярна для критичної інфраструктури і державних проєктів. Складається з шести ключових етапів, від категоризації системи до моніторингу контролів. Головні недоліки – значна ресурсозатратність і як і в стандарті ISO/IEC 27005 вимагає адаптації в контексті систем IoT;

3) **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation) - методологія, розроблена CERT, яка фокусується на оцінці ризиків та управлінні вразливостями. Це найбільш проста в провадженні методологія, оскільки вона фіксується на організаційних ризиках, але це і її головний недолік - відсутність технічних аспектів виявлення загроз;

4) **EBIOS** (Expression des Besoins et Identification des Objectifs de Sécurité) – це методологія управління ризиками, яка розроблена Агентством з кібербезпеки Франції (ANSSI). Її основна мета — ідентифікація, аналіз і оцінювання ризиків інформаційної системи з позиції її безпеки. Підходить для складних гібридних систем і зосереджується на практичності, а саме на реальних загрозах і методах їх вирішення. Недоліки, складність і ресурсозатратність;

5) **FAIR** (Factor Analysis of Information Risk) - методика, що дозволяє оцінювати фінансовий вплив ризиків. Головний недолік – кількісний аналіз на шкоду якісному;

6) **COBIT** (Control Objectives for Information and Related Technologies) - методологія, яка добре підходить для великих організацій через універсальність, але для систем IoT буде потрібна значна адаптація;

7) **CRAMM** (CCTA Risk Analysis and Management Method) - методика, розроблена британським урядом для аналізу ризиків інформаційної безпеки. Головна перевага – можливість проведення глибокого аудиту. Головні недоліки – складність впровадження і орієнтованість на «класичні» інформаційні системи.

З вищепредставлених стандартів, з погляду автора, найбільш підходить для IoT - **EBIOS, через його відповідність стандартам ISO/IEC 27005** та **ISO/IEC 31000 і можливості аналізувати ризики не тільки** на технічному рівні, а й на рівні організаційних процесів і зовнішнього середовища.

Для проведення більш конкретних досліджень побудуємо типову гібридну модель пристроїв IoT з базовими операціями, які дуже схожі на більшість існуючих платформ (рис. 4). Представимо таку архітектуру:

1) пристрої IoT: різноманітні розумні датчики (вологості, температури, руху, диму), які підключені через шлюзи;

2) шлюзи - обробка і передача даних до хмари;

3) хмара - забезпечує обробку даних, аналіз Big Data, машинне навчання;

4) локальний сервер - резервує дані, забезпечує доступ у разі втрати зв’язку з хмарою;

5) мобільний додаток - моніторинг і управляння IoT пристроями.

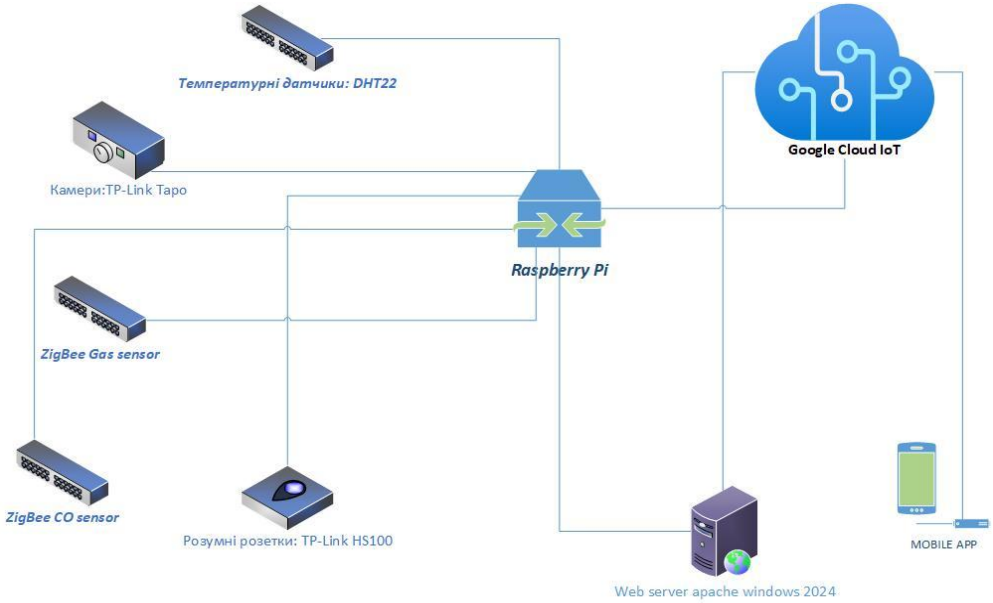

Рис. 4. Тестова гібридна модель IoT системи з реальними компонентами
Джерело: розроблено автором.

Для оцінки адекватності та точності запропонованої IoT-моделі порівняємо її з реальними IoT-платформами (Google Cloud IoT, AWS IoT) та вимогами ISO/IEC 30141:2024.

Таблиця 1 – Відповідність запропонованої IoT-моделі вимогам стандарту ISO/IEC 30141:2024 і провідним IoT-рішенням

Компонент	Наша IoT-модель	Вимоги ISO/IEC 30141:2024	Google Cloud IoT	Microsoft Azure IoT	AWS IoT	Відповідність
1	2	3	4	5	6	7
Рівень пристроїв (Perception Layer)	Zigbee-датчики (газ, CO, температура)	Використання сенсорів та актуаторів для збору даних	Підтримка різних сенсорів для збору даних через Bluetooth, Zigbee, LoRa	Підтримка сенсорів для різних типів даних, таких як температура, вологість, гази	Підтримка широкого спектра сенсорів для моніторингу навколишнього середовища	✔ Відповідає
Рівень мережі (Network Layer)	Wi-Fi, Ethernet, Zigbee,	Надійні мережеві протоколи з безпекою (наприклад, MQTT з TLS)	Використовує надійні протоколи для передачі даних через MQTT, HTTP, TLS	Використовує MQTT, HTTPS, AMQP для передачі даних, забезпечує високий рівень безпеки	Підтримка безпечних протоколів: MQTT, HTTPS, TLS для захисту даних	✔ Відповідає
Рівень шлюзів (Edge Layer)	Raspberry Pi для обробки даних	Використання периферійних обчислень для зменшення затримок	Використовує периферійні пристрої для обробки даних, такі як Google Edge TPU	Підтримка периферійних обчислень за допомогою Azure IoT Edge та спеціальних шлюзів	AWS IoT Greengrass для обробки даних на периферії	✔ Відповідає

Закінчення табл. 1

1	2	3	4	5	6	7
Рівень управління (Control Layer)	Центр. управління	Потрібно централізоване управління для моніторингу та контролю	Центральне управління через Google Cloud IoT Core для моніторингу пристроїв	Azure IoT Hub для централізованого управління пристроями та моніторингу	AWS IoT Core для централізованого управління пристроями	✔ Відповідає
Рівень хмари (Application Layer)	Google Cloud IoT для обробки даних	Використання хмарних платформ для аналітики	Використовує Google Cloud IoT для аналітики даних та їх збереж.	Azure IoT для аналітики даних, зберігання та інтеграції з іншими системами	AWS IoT для збору, зберігання, аналізу даних та інтеграції з іншими сервісами	✔ Відповідає
Безпека	Аутентифікація	Аутентифікація, контроль доступу, захист даних	Вбудована безпека через шифрування, аутентифікацію	Azure IoT забезпечує безпеку через шифрування та контроль доступу	Високий рівень безпеки за допомогою аутентифікації, шифрування та моніторингу	✔ Відповідає
Масштабованість	Локальна обробка на Raspberry Pi	Використання масштабованих рішень	Google Cloud IoT забезпечує масштабованість для обробки великих обсягів даних	Azure IoT забезпечує безперешкодну масштабованість для зростаючих обсягів даних	AWS IoT дозволяє легко масштабувати систему з додаванням нових пристроїв	⚠ Частково відповідає (рекомендується хмарна масштабованість)

Згідно з табл. 1 можна зробити висновок, що запропонована IoT-модель загалом відповідає стандарту *ISO/IEC 30141:2024* та має багато спільних рис із реальними комерційними IoT-рішеннями, такими як *Google Cloud IoT*, *Microsoft Azure IoT* та *AWS IoT*. Вона використовує ефективні сенсори для збору даних, периферійні обчислення для зменшення затримок та хмарні технології для обробки інформації, що є ключовими елементами сучасних IoT-систем. Модель є адекватною та точною, адже вона базується на сучасних принципах побудови IoT-систем і може бути вдосконалена відповідно до кращих практик без значних змін у своїй архітектурі.

Проаналізуємо ризики моделі на рис. 4 за методологію EBIOS і створимо для тестування вказану модель в MATLAB. Хочемо зазначити, що мета цього аналізу показати конкретні етапи проведення аудиту IoT систем за вибраною методології і отримання загальних рекомендацій про усунення виявлених недоліків. Створення і тестування вказаною моделі в MATLAB, допомагає зрозуміти й отримати в реальному часі дані про вплив атак на пристрої, а також наскільки ефективні способи захисту.

Для створення моделі будемо використовувати Simulink і Communications Toolbox. *Simulink* буде використаний для моделювання динаміки системи, побудови моделі IoT мережі та взаємодії між пристроями, а також для аналізу поведінки в умовах кібернападів і захисту. *Communications Toolbox* буде застосований для моделювання комунікаційних протоколів в IoT мережах, а також для аналізу сигналів, шумів та інших аспектів передачі даних у цих мережах, що дозволяє детальніше оцінювати вплив кіберзагроз на зв'язок.

Етап 1: Контекст і цілі безпеки:

- ***Контекст:*** гібридна IoT-система для розумного будинку. **Розумні сенсори** збирають дані (наприклад, температура, вологість, відео зображення), **розумний шлюз** здійснює попередню обробку даних перед передачею до хмари, хмара обчислює великі дані, вебсервер відображає дані та забезпечує управління системою через вебінтерфейс, а кінцевий споживач отримує інформацію на смартфоні.

- ***Цілі:*** забезпечення конфіденційності даних, захист від зловмисників, стійкість до атак.
- ***Критичні активи:*** особисті дані користувачів, доступ до пристроїв, стабільність і цілісність системи.

<u>Етап 2:</u> Ідентифікація загроз

- **Потреби IoT системи:**

- ***Конфіденційність*****:** захист від перехоплення або підробки даних (наприклад, під час передачі через шлюз).
- ***Цілісність:*** дані повинні залишатися незмінними на всіх етапах обробки.
- ***Доступність:*** система має продовжувати роботу навіть під час загроз (DoS-атаки).

- **Загрози:**

- ***Загрози до сенсорів:*** підміна даних через фізичний доступ, некоректні вимірювання через зовнішні впливи (шум, саботаж).
- ***Загрози до шлюзу:*** атаки типу "чоловік посередині" (MitM), які порушують цілісність та конфіденційність даних (розрив з'єднання на дві частини, створюючи своє власне зашифроване з'єднання з Mobile APP й з сервером, до якого звертається користувач), затримки або втрати даних через перевантаження мережі.
- ***Загрози до хмари:*** відмова у наданні послуг (DDoS-атаки), несанкціонований доступ до збережених даних.
- ***Загрози до користувача:*** виведення некоректної інформації (помилки у виявленні аномалій), порушення приватності через злом додатків або вебсерверів.

<u>Етап 3:</u> Вразливості

Сенсори найбільш вразливі через відсутність фізичного захисту, а також через недостатнє калібрування.

Дані шлюзу можливо перехопити через недостатнє шифрування даних, а відсутність резервних маршрутів для даних може буди причиною великих затримок у передачі або повної її зупинки.

Несанкціонований доступ до хмари можливо отримати через слабку аутентифікації (відсутність двофакторної, слабкі паролі), а також через відсутність моніторингу аномалій.

<u>Етап 4:</u> Аналіз впливу

Некоректні рішення на основі змінених або підроблених даних (наприклад, зміна показників температури) напряму впливає на цілісність усієї системи.

Витік даних може нести конференційну інформацію про користувача (злом камери відеонагляду).

Проблеми зі шлюзом або хмарою призведуть до тимчасових затримок або повної втрати даних.

Якщо розглядати ці загрози, найбільш небезпечною є ймовірність ухвалення рішень на основі спотворених або недостовірних даних (наприклад, датчик дає неправильну інформацію про температуру і так не буду виявлена пожежа), а також витік конференційної інформації. Середня загроза або навіть низка-затримка в передачі інформації.

<u>Етап 5:</u> Контрзаходи (загальні рекомендації)

Цей етап формується на основі попередніх етапів.

Для сенсорів необхідно впровадити фізичну безпеку (розміщення у недоступних для саботажу місцях), а також можливість самодіагностики сенсорів (калібрування тощо).

Для шлюзу використовувати найбільш стійких протоколів шифрування передачі даних і резервування каналів передачі.

Хмара повинна мати мультифакторну автентифікацію та постійний моніторинг активності.

Користувач системи повинен дотримуватись політики паролів і регулярно проводити рекомендовані оновлення.

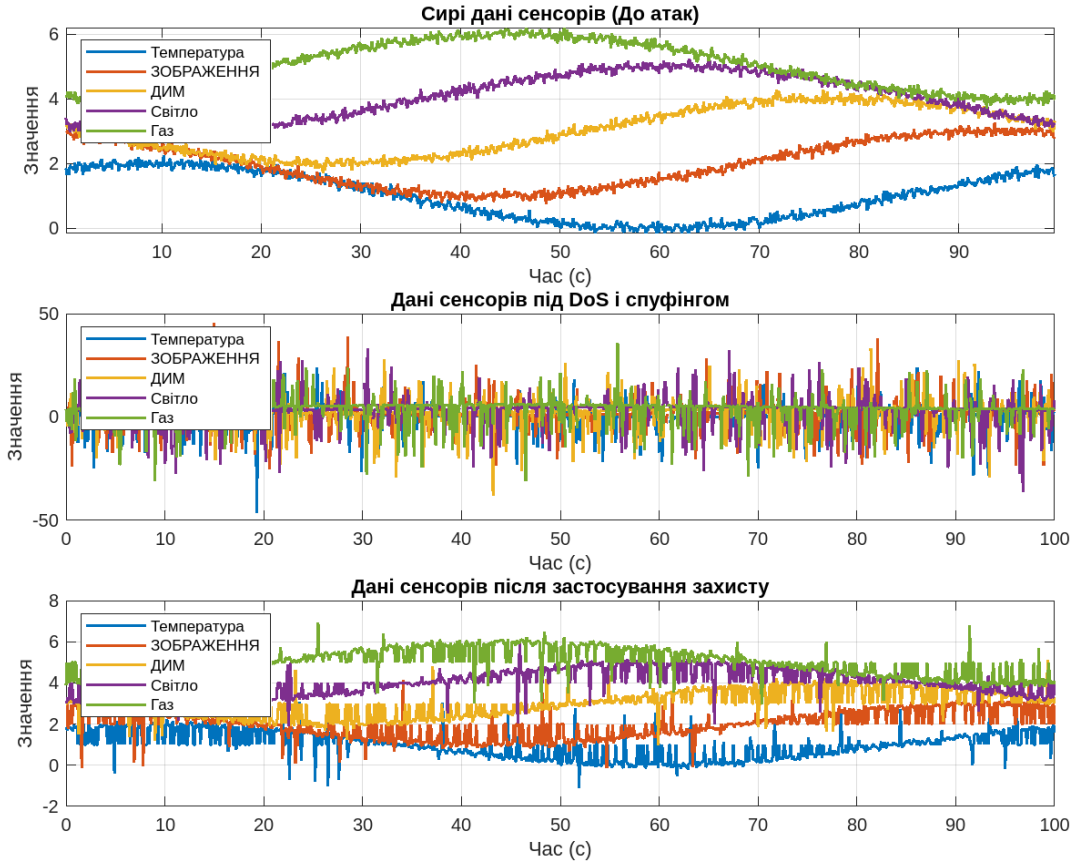

Рис. 5. Дані розумних датчиків під атакою с захистом і без посилання
Джерело: розроблено автором.

Наступним практичним кроком є створення тестової мережі IoT, яка була представлена на рис. 4, у програмному комплексі MATLAB. Проаналізувавши ризики по методології EBIOS, нам вже відомо, що розумні датчики найбільш незахищені перед DOS атаками і спуфінгом і через такі вторгнення виникають ризики втрати даних або їх підміни (фальсифікації). Як приклад, у нашій моделі відбувається симуляція DoS-атаки+спуфінг і для того щоб зрозуміти як впливають на наші розумні сенсори різноманітні аномалії, були створені відповідні графіки (рис. 5).

Перший графік демонструє сирі дані графіків, дані мають певну періодичність, згенеровано синусоїдальною функцією, що імітує нормальні показники сенсорів (наприклад, температура, рівень газу тощо), всі дані виглядають відносно стабільними, але з деяким флуктуаціями через шум.

Другий графік демонструє дані після атаки**,** маємо втрачені дані внаслідок DoS-атаки - пропуски або "пусті" ділянки на графіку, де дані відсутні. Це підтверджує, що система під час DoS-атаки втрачає важливу інформацію. Деякі дані будуть значно вищими або нижчими за очікувані значення, що вказує на підробку даних (спуфінг). Це може спричинити хибне інтерпретування інформації в реальній системі.

Третій графік показує дані датчиків після застосування захисних механізмів Після інтерполяції графіки виглядають більш гладкими і без пропусків, що свідчить про те, що система здатна "заповнювати" втрачені дані і захист від DoS-атаки дієвий. Аномальні зміни, викликані підробленими даними, замінені на значення, що більше відповідають очікуваному діапазону. Це зменшує ефект спуфінга, і графік набуває більш природного вигляду.

Підсумовуючи тести, можна зауважити, що був розглянутий приклад аудиту типової гібридної IoT системи за допомогою комбінації програмного комплексу MATLAB і методології для аналізу ризиків EBIOS. Ця синергія показала себе з найкращої сторони й виявила такі комбінації взаємодії одне з одним:

- за допомогою EBIOS створюються загрозові сценарії, які імплементуються в MATLAB для симуляції;
- MATLAB забезпечує візуалізацію наслідків атак, а EBIOS аналізує залишкові ризики й рекомендує покращення для безпеки;
- використовуючи моделі, створені в MATLAB і EBIOS, можна постійно покращувати IoT-систему, додаючи захисні механізми.

Узагальнюючи, така інтеграція дозволяє як аналітикам безпеки, так і інженерам ефективно тестувати, моделювати та вдосконалювати гібридні IoT-системи.

Висновки. У статті наведені і проаналізовані сучасні методології проведення аудиту IoT мереж. Наданий опис типової гібридної архітектури, обґрунтований вибір застосування проактивного підходу і методології управління ризиками. Створення тестової моделі, дозволило продемонструвати етапи проведення аудиту з практичного погляду, а також виявити й описати загрози, їхній вплив і контрзаходи. Результати, що були отримані й візуалізовані у графіках, демонструють, як кібератаки і захист від них, можуть впливати на дані, що генерують розумні пристрої.

Регулярне проведення аудиту та тестування IoT-мереж, надважливо, для запобігання кіберзагрозам і захисту критично важливих даних.

Список використаних джерел

1. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal, 4*(5), 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844.

2. Assiri, A., & Almagwashi, H. (2018). IoT security and privacy issues. U *1st international conference on computer applications & information security (ICCAIS)* (s. 1–5). https://doi.org/10.1109/CAIS.2018.8442002.

3. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146–164. https://doi.org/10.1016/ j.comnet.2014.11.008.

4. Atlam, H. F., & Wills, G. B. (2019). IoT security, privacy, safety and ethics. U *Internet of things* (s. 123–149). Springer International Publishing. https://doi.org/10.1007/978-3-030-18732-3_8.

5. Oracevic, A., Dilek, S., & Ozdemir, S. (2017). Security in Internet of things: A survey. U *2017 international symposium on networks, computers and communications (ISNCC)* (s. 1–6). https://doi.org/10.1109/ISNCC.2017.8072001.

6. Nurse, J. R. C., Creese, S., & De Roure, D. (2017). Security risk assessment in internet of things systems. *IT Professional, 19*(5), 20–26. https://doi.org/10.1109/mitp.2017.3680959.

7. DiMase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions*, *35*(2), 291–300. https://doi.org/10.1007/s10669-015-9540-y.

8. Botta, A., de Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: A survey. *Future Generation Computer Systems, 56,* 684–700. https://doi.org/10.1016/j.future.2015.09.021.

9. Radanliev, P., Roure, D. C. D., Nurse, J., Montalvo, R. M., & Burnap, P. (2019). Supply chain design for the industrial internet of things and the industry 4.0. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3346528.

10.Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., & Ande, R. (2018). IoT standardisation. U *ICFNDS'18: International conference on future networks and distributed systems*. ACM. https://doi.org/10.1145/3231053.3231103.

11.Salman, O., Elhajj, I., Chehab, A., & Kayssi, A. (2018). IoT survey: An SDN and fog computing perspective. *Computer Networks*, *143*, 221–246. https://doi.org/10.1016/ j.comnet.2018.07.020.

12.Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279. https://doi.org/10.1016 /j.comnet.2012.12.018.

References

1. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal*, *4*(5), 1250–1258. https://doi.org/10.1109/J IOT.2017.2694844.

2. Assiri, A., & Almagwashi, H. (2018). IoT security and privacy issues. U *1st international conference on computer applications & information security (ICCAIS)* (s. 1–5). https://doi.org/10.1109/ CAIS.2018.8442002.

3. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/ j.comnet.2014.11.008.

4. Atlam, H. F., & Wills, G. B. (2019). IoT security, privacy, safety and ethics. U *Internet of things* (s. 123–149). Springer International Publishing. https://doi.org/10.1007/978-3-030-18732-3_8.

5. Oracevic, A., Dilek, S., & Ozdemir, S. (2017). Security in Internet of things: A survey. U *2017 international symposium on networks, computers and communications (ISNCC)* (s. 1–6). https://doi.org/ 10.1109/ISNCC.2017.8072001.

6. Nurse, J. R. C., Creese, S., & De Roure, D. (2017). Security risk assessment in internet of things systems. *IT Professional*, *19*(5), 20–26. https://doi.org/10.1109/mitp.2017.3680959.

7. DiMase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions*, *35*(2), 291–300. https://doi.org/10.1007/s10669-015-9540-y.

8. Botta, A., de Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: A survey. *Future Generation Computer Systems*, *56*, 684–700. https://doi.org/ 10.1016/j.future.2015.09.021.

9. Radanliev, P., Roure, D. C. D., Nurse, J., Montalvo, R. M., & Burnap, P. (2019). Supply chain design for the industrial internet of things and the industry 4.0. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3346528.

10.Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., & Ande, R. (2018). IoT standardisation. U *ICFNDS'18: International conference on future networks and distributed systems*. ACM. https://doi.org/10.1145/3231053.3231103.

11.Salman, O., Elhajj, I., Chehab, A., & Kayssi, A. (2018). IoT survey: An SDN and fog computing perspective. *Computer Networks*, *143*, 221–246. https://doi.org/10.1016/ j.comnet.2018.07.020.

12.Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279. https://doi.org/10.1016 /j.comnet.2012.12.018.

Отримано 18.03.2025

UDC 004.2

Pidlisnyi Yuriy

PhD student, recipient of the Doctor of Philosophy degree in specialty 122
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: ypodlesny@ukr.net. **ORCID:** https://orcid.org/0009-0001-9783-3898. **ResearcherID:** LSL-1170-2024

AUDIT OF IOT NETWORKS: ASSESSING VULNERABILITIES AND PROTECTING AGAINST CYBER ATTACKS

This article addresses current challenges in ensuring security within the Internet of Things (IoT) networks, taking into account the modern challenges of the digital transformation era. The key risks associated with the use of IoT devices are outlined: the limitations of built-in security mechanisms, the lack of unified standards, hardware resource constraints, and the complexity of managing heterogeneous environments. Special attention is given to the role of security auditing as a tool for identifying vulnerabilities, assessing risks, and developing strategies to counter cyber threats. Existing auditing approaches, including reactive (retroactive), proactive, and incremental methods, are analyzed in the context of IoT environments. A comparative analysis of IoT system architectures—centralized, decentralized, and hybrid—is provided, highlighting their impact on security. A test model of an IoT network is proposed for practical threat modeling and auditing procedure verification. The article also focuses on modern risk management methodologies, including: ISO/IEC 27005, NIST RMF, OCTAVE, EBIOS, FAIR, COBIT, and CRAMM. The advantages and disadvantages of each are discussed in the context of IoT, emphasizing the suitability of the EBIOS methodology as the most adaptable for complex hybrid systems. The article also stresses the need for the improvement of security policies, adaptation of standards, and the development of auditing procedures that address both technical and organizational aspects of IoT operations. The main goal is to contribute to the creation of a reliable, scalable, and threat-resistant IoT ecosystem.

Keywords*: Internet of Things; IoT security; IT systems audit; risk management; IoT architecture; data protection; cyber threats; security standards; network vulnerabilities; attack counteraction; monitoring; cybersecurity; proactive methods.*

Fig.: 5. References: 12. Table: 1.

Підлісний Ю. І. Аудит мереж інтернету речей: оцінка вразливостей та захист від кібернападів. *Технічні науки та технології.* 2025. № 1(39). С. 170-183.