Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут комп'ютерних наук та штучного інтелекту

Кафедра кібербезпеки інформаційних систем, мереж і технологій

До захисту допущено
Кафедрою КІСМіТ протокол №____ від «___» грудня 2025 р.

завідувач кафедри _____ Марина ЄСІНА
(підпис) *(ім'я, прізвище)*
«___» грудня 2025 р.

Кваліфікаційна робота
здобувача другого (магістерського) рівня вищої освіти

Система та криптографічні засоби інформації розумного будинку
(назва роботи)

Спеціальність (спеціалізація) 125 «Кібербезпека та захист інформації»

Освітня програма «Безпека інформаційних і комунікаційних систем»

Виконавець _____ Данило ГРИГОР'ЄВ
(підпис) *(ім'я, прізвище)*

Науковий керівник _____ Іван ГОРБЕНКО
(підпис) *(ім'я, прізвище)*

Харків – 2025

РЕФЕРАТ

У роботі наведено: 1 рисунок, 4 таблиці, 44 джерела, 3 додатки. Обсяг роботи становить 77 сторінок.

Метою дослідження є аналіз та розробка аналітичного фреймворку криптографічного захисту інформації в інфраструктурі «розумного будинку» із застосуванням генераторів випадкових чисел та оцінка їх відповідності міжнародним стандартам, зокрема AIS 31.

Об’єкт дослідження – інфраструктура «розумного будинку» на базі IoT, що забезпечує автоматизацію побутових процесів та обробку персональних даних користувачів у взаємодії з хмарними сервісами.

Предмет дослідження – методи генерації випадкових чисел, їх стохастичні моделі, вимоги стандартів до надійності та інтеграція у безпеку IoT-середовища.

Методи дослідження – формальне та імітаційне моделювання, аналіз ентропії, статистичне тестування послідовностей випадкових чисел, оцінка ризиків, порівняльний аналіз криптографічних протоколів, структурне моделювання мережевих компонентів.

У роботі досліджено: вимоги стандартів до генераторів випадкових чисел (класи PTG/DRG AIS 31), застосування криптографічних механізмів у «розумному будинку», вплив стохастичного шуму на мін-ентропію генератора, алгоритми онлайн-тестування та тестів здоров’я ГВЧ, а також вплив якості ентропійного джерела на стійкість IoT-систем і зниження класів уразливостей.

Результати можуть бути використані при проєктуванні криптографічних модулів для «розумного будинку», у дослідженнях генерації випадкових чисел, а також при розробці вимог безпеки та сертифікації IoT-пристроїв.

Ключові слова: РОЗУМНИЙ ДІМ, ГЕНЕРАТОР ВИПАДКОВИХ ЧИСЕЛ, ДЖЕРЕЛО ЕНТРОПІЇ, AIS 31, КРИПТОГРАФІЯ, IoT-БЕЗПЕКА, МІН-ЕНТРОПІЯ, КРИПТОЗАХИСТ, СТОХАСТИЧНЕ МОДЕЛЮВАННЯ, КІБЕРБЕЗПЕКА.

ABSTRACT

The paper contains: 1 figure, 4 tables, 44 sources, 3 application. The volume of the work is 77 pages.

The purpose of the work is to analyze and develop an analytical framework for cryptographic information protection in a smart home infrastructure using random number generators and to assess their compliance with international standards, particularly AIS 31.

The object of the study is the smart home infrastructure based on IoT, providing automation of household processes and processing of users' personal data in interaction with cloud services.

The subject of the study is the methods for generating random numbers, their stochastic models, international standards requirements for reliability, and their integration into IoT security architecture.

The research methods are formal and simulation modeling, entropy analysis, statistical testing of random number sequences, risk assessment, comparative analysis of cryptographic protocols, and structural modeling of network components.

The work examines: standards requirements for random number generators (PTG/DRG classes, AIS 31), application of cryptographic mechanisms in smart homes, influence of stochastic noise on generator min-entropy, online testing algorithms and health tests of TRNGs, as well as the impact of entropy source quality on IoT system resilience and vulnerability class reduction.

The results of the work can be used in designing cryptographic modules for smart homes, future research in random number generation, and the development of security requirements and certification of IoT devices using cryptographic protection.

Keywords: SMART HOME, RANDOM NUMBER GENERATOR, ENTROPY SOURCE, AIS 31, CRYPTOGRAPHY, IOT SECURITY, MIN-ENTROPY, CRYPTOGRAPHIC PROTECTION, STOCHASTIC MODELING, CYBERSECURITY.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ABAC	–	Керування доступом на основі атрибутів;
AES	–	Удосконалений стандарт шифрування;
AES-GCM	–	AES у режимі лічильника з автентифікацією Галуа;
AIS	–	Зауваження щодо застосування та інтерпретація схеми;
API	–	Прикладний програмний інтерфейс;
DoS	–	Атака типу «відмова в обслуговуванні»;
DRBG	–	Детермінований генератор випадкових бітів;
DRG / DRNG	–	Детермінований генератор випадкових чисел;
FPGA	–	Програмована логічна інтегральна схема;
HMAC	–	Код автентифікації повідомлень на основі хеш-функції;
IDS	–	Система виявлення вторгнень;
IEC	–	Міжнародна електротехнічна комісія;
IoT	–	Інтернет речей;
ISO	–	Міжнародна організація зі стандартизації;
MitM	–	Атака «людина посередині»;
MQTT	–	Протокол телеметрії черги повідомлень;
NIST	–	Національний інститут стандартів і технологій;
PRNG	–	Генератор псевдовипадкових чисел;
PTG	–	Клас функціональності фізичного істинного генератора;
PTRNG	–	Фізичний істинний генератор випадкових чисел;
RBAC	–	Керування на основі ролей;
TLS	–	Протокол захисту транспортного рівня;
TRNG	–	Істинний генератор випадкових чисел.

ВСТУП

Стрімкий розвиток Інтернету речей (IP) та вбудованих обчислювальних технологій призвів до широкого впровадження інтелектуальних систем у повсякденне життя. Одним із найбільш динамічних проявів цієї тенденції є «розумний будинок» – інтегроване середовище, що об’єднує різноманітні підсистеми для автоматизації, моніторингу та керування освітленням, опаленням, контролем доступу, енергоспоживанням та мультимедійними пристроями. Однак зі зростанням складності цих систем підвищується і їхня вразливість до кіберзагроз. Високий рівень взаємозв’язку, використання бездротових каналів та залежність від хмарних сервісів створюють нові вектори атак на персональні дані та цілісність системи.

Актуальність роботи. Актуальність цього дослідження полягає у зростаючій потребі забезпечення конфіденційності, цілісності та доступності інформації, що обробляється системами «розумного будинку». Незважаючи на поширення комерційних IP-платформ, більшість із них надає пріоритет функціональності та зручності, а не безпеці [1]. Як наслідок, незахищені протоколи зв’язку, слабкі механізми автентифікації та відсутність шифрування на мережевому або пристроєвому рівні призводять до уразливостей, які можуть бути використані для несанкціонованого доступу, маніпулювання даними або саботажу [2], [3].

Проблема забезпечення криптографічної безпеки в «розумних будинках» на базі IP додатково ускладнюється обмеженими обчислювальними ресурсами вбудованих пристроїв. Ці обмеження часто ускладнюють реалізацію стандартних криптографічних протоколів, таких як протокол захисту транспортного рівня [6], або розширених систем керування ключами. Більше того, слабкі або некоректно реалізовані генератори випадкових чисел (ГВЧ) – фундаментальний елемент криптографічних алгоритмів – можуть значно знизити загальну стійкість шифрування. Стандарт AIS 31, розроблений

Федеральним управлінням з інформаційної безпеки Німеччини (BSI) [22], надає міжнародно визнану основу для оцінювання функціональності та якості ГВЧ, що використовуються в криптографічних модулях. Забезпечення відповідності цим вимогам є вирішальним кроком до досягнення надійного криптографічного захисту в інтелектуальних середовищах.

Відтак, наукова проблема, що вирішується в цій роботі, полягає в розробленні формальних моделей та методологічних основ для оцінювання та підвищення надійності систем криптографічного захисту інформації в середовищах «розумного будинку» з урахуванням ролі класів функціональності ГВЧ, визначених стандартом AIS 31.

Для досягнення поставленої мети у роботі висунуто такі дослідницькі гіпотези:

H1: за реалістичних параметрів фізичних джерел шуму, наведених у сучасній літературі для IoT-платформ, можливо аналітично обґрунтувати досяжність вимог класу PTG.2 стандарту AIS 31 щодо середньої ентропії та мін-ентропії на біт без проведення прямих апаратних вимірювань.

H2: включення AIS 31-орієнтованого генератора випадкових чисел як кореня довіри у багаторівневу архітектуру безпеки «розумного будинку» призводить до зменшення класів вразливостей, пов’язаних із компрометацією криптографічних ключів та сесій, порівняно з архітектурами, що покладаються на некеровані псевдовипадкові джерела [24].

Метою дослідження є розроблення аналітичного фреймворку проєктування системи криптографічного захисту інформації в інфраструктурі «розумного будинку» із використанням генераторів випадкових чисел, що відповідають вимогам стандарту AIS 31, та оцінювання впливу якості джерела ентропії на стійкість архітектури до типових кіберзагроз.

Об’єкт дослідження – інфраструктура «розумного будинку» на базі Інтернету речей, яка забезпечує автоматизацію побутових процесів, оброблення та зберігання персональних даних користувачів у взаємодії з хмарними сервісами.

Методи дослідження: методи формального моделювання, теорії ймовірностей, аналізу інформаційної ентропії, оцінювання ризиків та статистичного тестування послідовностей випадкових чисел, аналітичне та імітаційне моделювання, порівняльний аналіз криптографічних протоколів та структурне моделювання компонентів мереж IP.

Предмет дослідження – криптографічні механізми забезпечення конфіденційності, цілісності та доступності даних у системі «розумного будинку» з акцентом на генератори випадкових чисел та їх інтеграцію в багаторівневу архітектуру безпеки відповідно до вимог стандарту AIS 31.

Завдання дослідження:

1. Проаналізувати архітектуру, структуру та комунікаційні механізми систем «розумного будинку» як об’єктів криптографічного захисту.
2. Дослідити принципи криптографічного захисту даних та ідентифікувати ключові уразливості, специфічні для середовищ на базі IP.
3. Вивчити стандарт AIS 31 та класифікувати генератори випадкових чисел відповідно до їхньої функціональності та вимог безпеки.
4. Розробити формальні та імовірнісні моделі для оцінювання ентропії, надійності та ризику криптографічних систем залежно від класу ГВЧ.
5. Побудувати аналітичну модель, що інтегрує оцінювання на основі ентропії з індикаторами ризику системного рівня для захисту інформації «розумного будинку».
6. Запропонувати рекомендації щодо інтеграції сучасних криптографічних засобів (TLS, автентифікація, керування ключами та контроль доступу) з безпечними механізмами ГВЧ в архітектурах «розумного будинку».
7. Окреслити напрями подальшого вдосконалення криптографічних систем «розумного будинку».

1 КРИПТОГРАФІЧНИЙ ЗАХИСТ У СИСТЕМАХ РОЗУМНОГО ДОМУ: СУЧАСНИЙ СТАН ТА ПРОГАЛИНИ В ДОСЛІДЖЕННЯХ

1.1 Еволюція технологій розумного дому та нові виклики безпеці

Концепція домашньої автоматизації бере свій початок у механічних та електричних системах керування початку XX століття, однак сучасна технологія розумного дому виникла завдяки конвергенції зв'язку Інтернету речей (IoT), протоколів бездротових мереж, інфраструктури хмарних обчислень та автоматизації на базі штучного інтелекту впродовж 2010-х років. Системи розумного дому інтегрують різноманітні категорії пристроїв, зокрема давачі довкілля (температури, вологості, присутності), виконавчі пристрої (керування освітленням, керування системами ОВК [опалення, вентиляція та кондиціонування], моторизовані жалюзі), пристрої безпеки (камери, дверні замки, давачі руху) та побутову техніку з вбудованим інтелектом. Приклад моделі такої системи зображено на Рисунку 1.1.

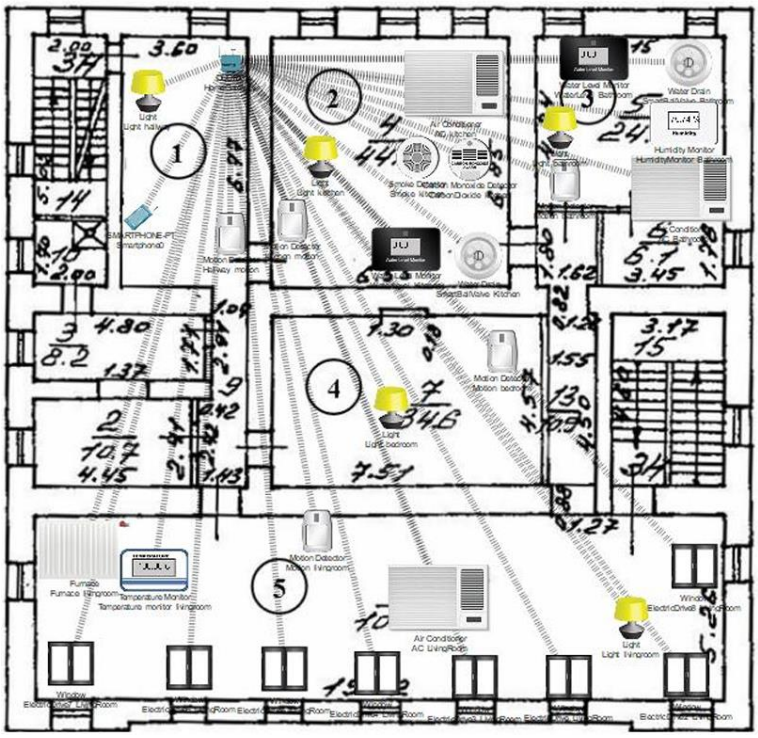


Рисунок 1.1 – Приклад моделі розумного будинку

Аналіз ринку документує експоненційні траєкторії зростання впровадження розумних будинків. Галузеві дослідження свідчать, що світові поставки пристроїв для розумного дому перевищили 800 мільйонів одиниць у 2023 році, а прогнози передбачають проникнення на ринок понад 50% домогосподарств у розвинених економіках до 2030 року. Таке поширення відображає споживчий попит на зручність, енергоефективність, можливості дистанційного моніторингу та інтеграцію з екосистемами голосових асистентів. Однак швидка комерціалізація надає пріоритет часу виходу на ринок та досвіду користувача над комплексним проєктуванням безпеки, створюючи системні вразливості в розгорнутій інфраструктурі.

1.1.1 Виклики безпеці при розгортанні розумного дому

Розподілена, гетерогенна природа систем розумного дому створює виклики безпеці, відмінні від традиційних IT-середовищ підприємств. По-перше, обмеженість ресурсів у вбудованих пристроях IoT лімітує обчислювальну потужність, доступну для криптографічних операцій, створюючи суперечність між вимогами безпеки та практичною продуктивністю. По-друге, різноманітні комунікаційні протоколи (MQTT, CoAP, Zigbee, Z-Wave, Bluetooth Low Energy) демонструють різний ступінь зрілості безпеки, причому багато протоколів, розроблених для обмежених середовищ, дозволяють слабке або необов'язкове шифрування. По-третє, тривалий термін служби пристроїв (зазвичай 10-15 років) у поєднанні з фрагментованими механізмами оновлення мікропрограм створює хронічні вікна вразливостей у міру еволюції стандартів безпеки. По-четверте, фізична доступність пристроїв дає змогу зловмисникам здійснювати атаки на апаратному рівні, включно з аналізом сторонніми каналами та екстракцією мікропрограми.

Стаяно надає завбачливий аналіз, що ідентифікує двадцять міркувань безпеки для IoT з хмарною підтримкою [1], підкреслюючи фундаментальні суперечності між зручністю та безпекою. Аналіз висвітлює, що залежність від хмарних технологій створює ризики приватності через централізовану агрегацію

даних, ризики доступності через залежність від підключення до Інтернету та ризики довіри через покладання на сторонніх постачальників послуг. Ці архітектурні проблеми поширені в комерційних платформах розумного дому, де виробники за замовчуванням обирають хмарно-орієнтовані конструкції, пріоритезуючи легкість розгортання над локальним суверенітетом даних.

1.2 Задокументовані вразливості в комерційних системах розумного дому: емпіричні дані

Опубліковані емпіричні дослідження безпеки IoT-пристроїв та хмарних платформ [2], [3] демонструють системну присутність критичних вразливостей у комерційних рішеннях для «розумного дому». Масштабні аналізи, проведені різними науковими групами, засвідчують, що більшість пристроїв та бекенд-сервісів використовують слабкі або неналежно реалізовані механізми автентифікації, нешифровані мережеві протоколи та недостатньо надійні генератори випадкових чисел, що безпосередньо підриває криптографічний захист.

Ключові висновки літератури показують:

- слабкі типові паролі та некоректна автентифікація залишаються одними з найпоширеніших векторів атак;
- значна частина пристроїв передає дані незашифрованими каналами, що уможливлює атаки «людина посередині» та повторного відтворення;
- виявлено численні випадки використання слабких або передбачуваних генераторів псевдовипадкових чисел, що істотно знижує стійкість криптографічних ключів;
- хмарні платформи, що підтримують пристрої розумного дому, мають власні вразливості, зокрема некоректну валідацію доступу та відсутність захисту API.

Узагальнені порівняльні результати досліджень наведено в Додатку А, де представлено порівняння типів помилки безпеки та їх вплив на загальний ризик компрометації.

1.2.1 Оцінка вразливостей на основі фреймворків

Для системної класифікації загроз у розумних будинках застосовуються стандартизовані фреймворки, серед яких ключове місце займає OWASP IoT Top 10 [4]. Аналіз комерційних продуктів демонструє, що більшість із них порушують від 6 до 8 категорій із зазначеного переліку [5], зокрема у сферах автентифікації, мережевого захисту та конфіденційності даних.

Найбільш поширені категорії вразливостей, що мають критичний вплив на безпеку:

- слабкі або жорстко закодовані типові облікові дані;
- небезпечна передача та зберігання даних;
- відсутність безпечного механізму оновлення мікропрограм;
- небезпечні типові конфігурації та незахищені мережеві служби.

Деталізований аналіз цих категорій, включно з прикладами експлуатацій вразливостей, подано в Додатку А.

1.3 Криптографічні основи безпеки IoT: протоколи та реалізації

Криптографічні механізми забезпечення конфіденційності, цілісності та автентичності даних є ключовим елементом безпечного функціонування систем «розумного дому». На практиці їх впровадження обмежується ресурсними характеристиками пристроїв IoT, значною варіативністю комунікаційних протоколів та нерівномірністю підтримки сучасних стандартів.

Протокол TLS 1.3 [6], який забезпечує захищений обмін ключами та автентифіковану комунікацію, формально підтримується в більшості IoT-платформ, однак реальні розгортання демонструють суттєві компроміси [7]. Значна частка MQTT-інфраструктур функціонує без шифрування [8] або із застосуванням застарілих конфігурацій, що створює прямі загрози перехоплення та модифікації трафіку [9]. Це підкреслює важливість інтеграції криптографічних протоколів [10] у поєднанні з якісними механізмами генерації ключів.

Механізми автентифікованого шифрування, такі як AES-GCM [12] та ChaCha20-Poly1305, забезпечують одночасний захист конфіденційності та цілісності даних і є рекомендованими для обмежених IoT-платформ. Альтернативні полегшені криптографічні алгоритми пропонують компроміс між продуктивністю та стійкістю, що є особливо важливим для пристроїв з мінімальними ресурсами [13]. Порівняльні характеристики криптографічних алгоритмів наведено в Додатку В.

1.4 Генерація випадкових чисел для криптографічних застосувань: архітектурні підходи

Криптографічна стійкість залежить від надійності генераторів випадкових чисел (ГВЧ), які використовуються для формування ключів, нонсів та токенів автентифікації. Недостатня або передбачувана ентропія є однією з найбільш критичних причин компрометації криптографічних систем.

Існують два основні класи ГВЧ:

- фізичні генератори справді випадкових чисел, що базуються на фізичних джерелах шуму;
- детерміновані генератори випадкових бітів, які розширюють початкове випадкове зерно.

TRNG [14], основані на джиттері кільцевих осциляторів [15], [16], [17] або шумі АЦП [18], є найбільш практичним рішенням для обмежених IoT-пристроїв, але вимагають ретельного моделювання, уникнення кореляції та відповідності міжнародним стандартам. DRBG [19], [20] забезпечують високу продуктивність, однак критично залежать від якості початкової ентропії. Порівняльний огляд архітектур TRNG [21] та DRBG наведено у Додатку В.

1.5 Стандарти криптографічної оцінки та валідація генераторів випадкових чисел

Міжнародні стандарти AIS 31 [22], NIST SP 800-90 [19], [23] та ISO/IEC 20543 [25] визначають вимоги та процедури оцінки якості генераторів випадкових чисел. Їхнє застосування у розрізі IoT є особливо важливим, оскільки

ненадійні ГВЧ або некоректно реалізовані DRBG підривають роботу всіх наступних криптографічних механізмів.

Стандарт AIS 31 вимагає створення стохастичної моделі джерела ентропії, підтвердження мін-ентропії та проходження набору тестів випадковості, що робить його найбільш строгим інструментом оцінки TRNG. NIST SP 800-90B доповнює цей фреймворк методологією оцінки ентропії та визначає правила для використання DRBG в криптографічних системах.

Аналіз літератури демонструє, що більшість досліджень для IoT-пристроїв обмежується базовим статистичним тестуванням без повної відповідності вимогам AIS 31, що створює сумніви щодо практичної надійності опублікованих архітектур..

1.6 Механізми контролю доступу та автентифікації для систем розумного дому

1.6.1 Контроль доступу на основі ролей (RBAC)

Контроль доступу на основі ролей (Role-Based Access Control, RBAC) визначає дозволи на основі організаційних ролей, а не ідентичностей окремих користувачів, що спрощує адміністрування в багатокористувацьких середовищах. Фердоус та ін. (Ferdous et al.) реалізують контроль доступу на основі атрибутів та ролей для IoT у розумному домі [26], проводячи порівняльний аналіз. Експериментальна оцінка демонструє, що RBAC забезпечує вищу ефективність (на 23% меншу затримку для рішень про авторизацію), тоді як ABAC пропонує підвищену гнучкість для контекстно-залежних політик. Дослідження рекомендує гібридні підходи, що поєднують структурну простоту RBAC з динамічною адаптивністю ABAC.

Матеу та ін. (Matheu et al.) розробляють інтероперабельний фреймворк контролю доступу для різноманітних платформ IoT на основі OAuth 2.0 та політик на основі ролей [27], вирішуючи проблему фрагментації між екосистемами конкретних виробників. Фреймворк уможливлює міжплатформну авторизацію, підтримуючи сумісність з наявною інфраструктурою

автентифікації. Валідація в контекстах розумного дому, промислового IoT та охорони здоров'я підтверджує доцільність стандартизованих абстракцій контролю доступу.

1.6.2 Багатофакторна автентифікація

Безпека автентифікації посилюється шляхом поєднання незалежних факторів (знання, володіння, властивість). Дослідження показують, що двофакторна автентифікація, що включає одноразові паролі на основі часу (TOTP) або апаратні токени, зменшує ризик компрометації облікового запису на 99,9% порівняно з автентифікацією лише за паролем. Однак обмеження пристроїв IoT ускладнюють традиційне розгортання двуфакторної авторизації. Хан та ін. (Khan et al.) пропонують модель контролю доступу з нульовою довірою (zero-trust) на основі атрибутів, натхненну блокчейном, що усуває залежність від централізованих серверів автентифікації [28], демонструючи стійкість до атак єдиної точки відмови, водночас підтримуючи прийнятну затримку автентифікації (<200 мс) для застосувань розумного дому.

1.7 Архітектури мережевої безпеки та виявлення вторгнень для середовищ IoT

1.7.1 Стратегії сегментації мережі

Ізоляція мережі обмежує горизонтальне переміщення (lateral movement) після початкової компрометації пристрою. Лагхарі та ін. (Laghari et al.) пропонують парадигму граничних обчислень (edge-computing) для автоматизації розумного дому, використовуючи сегментацію VLAN, що відокремлює критичні для безпеки пристрої (замки, камери) від утилітарних пристроїв (освітлення, побутова техніка) [29]. Застосування брандмауера на рівні шлюзу реалізує політики заборони за замовчуванням (default-deny) з явними дозволами для необхідних шляхів комунікації. Експериментальна валідація демонструє зменшення потенційного поширення атак на 63% порівняно з пласкими (flat) мережевими архітектурами.

1.7.2 Системи виявлення вторгнень (IDS)

IDS на основі аномалій використовує машинне навчання для виявлення відхилень від базових поведінкових патернів. Аль-Шаріда та ін. (Al-Shareeda et al.) проєктують адаптивну IDS для IoT у розумному домі, використовуючи ансамблеве навчання (Випадковий ліс, Градієнтний бустинг, Нейронні мережі), досягаючи 97,3% точності виявлення атак з рівнем хибнопозитивних спрацьовувань 1,2% [30]. Система виявляє атаки «людина посередині», спроби відмови в обслуговуванні та несанкціонований доступ із медіанною затримкою виявлення 1,8 секунди.

Альхрешех та ін. (Alkhresheh et al.) пропонують гібридну IDS, що поєднує глибоке навчання (Згорткові нейронні мережі, Довгі мережі короткочасної пам'яті (LSTM)) з Модифікованим алгоритмом пошуку рептилій (Modified Reptile Search Algorithm) для оптимізації ознак [31], досягаючи 98,1% точності виявлення вторгнень у мережах IoT. Аналіз продуктивності демонструє доцільність роботи в реальному часі на апаратному забезпеченні класу шлюзів (Raspberry Pi 4), підтверджуючи практичність для житлових розгортань.

Алі та ін. (Ali et al.) розробляють ансамблевий підхід з використанням мереж Колмогорова-Арнольда для виявлення вторгнень в IoT [32], демонструючи вищу продуктивність на незбалансованих наборах даних атак, поширених у реальних середовищах розумного дому. Модель досягає 98,7% F1-оцінки при виявленні міноритарних класів атак, вирішуючи критичну слабкість традиційних підходів машинного навчання.

1.8 Виявлені прогалини в існуючих дослідженнях

Всебічний огляд літератури виявляє декілька критичних прогалин, що потребують подальших досліджень:

1) Недостатня суворість оцінки ГВЧ у контексті IoT: Хоча численні дослідження пропонують архітектури TRNG для вбудованих систем, небагато з них проводять всебічну валідацію відповідно до суворих криптографічних стандартів (AIS 31, ISO/IEC 20543) [22], [25].

Опубліковані реалізації зазвичай звітують про базове статистичне тестування (NIST SP 800-22) [24] без побудови стохастичної моделі, аналізу довгострокової стабільності або характеристики чутливості до умов навколишнього середовища, що вимагаються класом функціональності PTG.2. Ця прогалина створює невизначеність, чи досягають TRNG для IoT рівнів ентропії, що припускаються в аналізах безпеки протоколів.

2) Розрив між криптографічними стандартами та їх реалізацією в IoT: Встановлені стандарти криптографічної оцінки (AIS 31, FIPS 140-3, ISO/IEC 20543) [22], [34], [25] орієнтовані на обчислювальні платформи загального призначення з достатніми ресурсами. Застосування до пристроїв IoT з обмеженими ресурсами вимагає адаптації, що враховує обчислювальні обмеження, обмеження пам’яті та бюджети потужності. У наявній літературі відсутній комплексний фреймворк, що транслює вимоги криптографічних стандартів у конкретні проєктні специфікації для реалізацій розумного дому.
3) Відсутність холістичних (цілісних) архітектур безпеки: Поточні дослідження розглядають ізольовані механізми безпеки (розгортання TLS, контроль доступу, виявлення вторгнень) без інтегрованих архітектурних фреймворків. Безпека розумного дому вимагає ешелонованої оборони (defense-in-depth), що поєднує декілька взаємодоповнювальних захистів. У літературі бракує валідованих архітектурних проєктів, що інтегрують верифіковані основи ГВЧ з криптографічними протоколами, контролем доступу та мережевою безпекою в єдиний фреймворк.
4) Обмежений акцент на криптографічних основах: Дослідження вразливостей документують поширені слабкості в безпеці розумного дому, але часто не беруть до уваги фундаментальну роль генерації випадкових чисел. Аналіз зосереджується на вразливостях прикладного рівня (слабкі паролі, незашифровані протоколи), не досліджуючи, чи спираються криптографічні примітиви на адекватні джерела ентропії. Неналежна

якість ГВЧ підриває всі подальші механізми безпеки, являючи собою критичне вузьке місце, що вимагає систематичного дослідження.

5) Теоретичний аналіз без дорожніх карт експериментальної валідації: Дослідження, що пропонують покращення безпеки, часто не мають чітких шляхів від теоретичного проєктування до практичної реалізації. Публікації представляють алгоритми та архітектури без детальних методологій валідації, дорожніх карт впровадження або критеріїв успішності, що уможливлюють незалежне відтворення та перевірку.

Висновки до Розділу 1

Аналіз сучасного стану безпеки систем «розумного будинку» виявляє системну кризу, зумовлену дисбалансом між стрімким розширенням функціональності IoT-пристроїв та стагнацією методів їхнього захисту. Фундаментальна проблема полягає у масовому нехтуванні виробниками базових криптографічних вимог заради зручності розгортання та зниження собівартості, що підтверджується наявністю критичних вразливостей у більшості комерційних платформ, зокрема передачею даних у відкритому вигляді та використанням слабких механізмів автентифікації. Критичний огляд літератури вказує на те, що найбільш небезпечним та часто ігнорованим вектором атак є компрометація генераторів випадкових чисел (ГВЧ), які виступають фундаментом для всієї криптографічної інфраструктури. Ненадійність джерела ентропії автоматично нівелює стійкість навіть таких надійних протоколів, як TLS 1.3, роблячи систему вразливою до відновлення сесійних ключів та маніпуляцій. Отже, основним викликом у цій галузі є відсутність комплексних архітектурних рішень, які б інтегрували верифіковані апаратні корені довіри зі стандартами високого рівня, забезпечуючи захист не лише на рівні програмного коду, а й на рівні генерації ключового матеріалу.

2 ТЕОРЕТИЧНІ ОСНОВИ СИСТЕМ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ РОЗУМНИХ БУДИНКІВ

2.1 Моделювання загроз та система оцінювання ризиків для середовищ розумного дому

Сучасні системи розумного дому опосередковують різноманітні взаємопов’язані функції, що охоплюють контроль довкілля, безпеку, моніторинг стану здоров’я та керування енергоспоживанням. Мережева топологія та гетерогенний склад пристроїв створюють багаторівневі поверхні атаки, що вимагають систематичної характеристики та пріоритезації. Моделювання загроз використовує структуровані методології для ідентифікації потенційних ворожих дій, уможливлюючи розробку відповідних захисних механізмів.

2.1.1 Система класифікації загроз

Ландшафт загроз у середовищах розумного дому охоплює три основні вектори атак. По-перше, мережеві загрози, націлені на канали зв’язку, включають атаки «людина посередині», що перехоплюють незашифровані повідомлення MQTT [35], атаки повторного відтворення (replay attacks), що експлуатують недостатню часову прив’язку в механізмах автентифікації, та атаки ін’єкції команд, що маніпулюють протокольними повідомленнями для ініціювання несанкціонованих дій пристроїв. По-друге, загрози на рівні пристроїв експлуатують вразливості реалізації, включно з переповненням буфера в мікропрограмі, недостатньою генерацією випадкових чисел для криптографічного ключового матеріалу та неналежним захистом чутливих даних, що зберігаються в пам’яті або постійному сховищі. По-третє, архітектурні загрози використовують системні проєктні рішення, включно з залежністю від централізованих хмарних сервісів, що створює єдині точки відмови, відсутністю сегментації мережі, що уможливлює горизонтальне переміщення (lateral

movement) після початкової компрометації, та фрагментованими механізмами оновлення мікропрограм, що створює хронічні вікна вразливостей.

2.1.2 Методологія оцінювання ризиків

Кількісне оцінювання ризику поєднує оцінку ймовірності загрози з оцінкою впливу. Фундаментальне рівняння $\text{Ризик} = \text{Імовірність} \times \text{Вплив}$ уможливлює пріоритезацію стратегій пом'якшення. Для систем розумного дому оцінка впливу враховує декілька вимірів: конфіденційність даних (чутливість особистої інформації, включно з розпорядком дня, даними про присутність, біометричними даними), цілісність даних (достовірність команд керування, що впливають на фізичну безпеку та надійність системи) та доступність системи (безперервність послуг автоматизації). Оцінка ймовірності враховує можливості зловмисника (від «script kiddies» з загальнодоступними інструментами до кваліфікованих акторів з можливостями зворотного інжинірингу), доступність поверхні атаки (мережеві служби проти фізично доступних пристроїв) та фактори середовища (географічне розташування, нормативне середовище).

2.1.3 Вплив криптографічних збоїв

Наслідки компрометації криптографічного ключового матеріалу поширюються на всі подальші гарантії безпеки. Фундаментальний принцип криптографічної безпеки встановлює, що надійність всієї системи обмежується її найслабшим компонентом. Якщо генератори випадкових чисел не в змозі виробляти непередбачуваний вивід, зловмисники можуть перерахувати потенційні криптографічні ключі за допомогою повного перебору або імовірнісних атак, таким чином нівелюючи механізми шифрування незалежно від їхніх математичних властивостей. Ця вразливість являє собою критичне вузьке місце, яке часто вислизає з аналізу при моделюванні загроз, оскільки воно функціонує на інфраструктурному, а не на прикладному рівні.

2.2 Теорія ентропії та методологія стохастичного моделювання AIS 31

2.2.1 Інформаційно-теоретичні основи ентропії

Ентропія кількісно оцінює невизначеність у імовірнісних системах, використовуючи формальний математичний апарат, що базується на теорії інформації, заснованій Шенноном [36]. Для дискретної випадкової величини X з розподілом імовірностей $P(x)$, ентропія Шеннона обчислюється як:

$$H(X) = -\sum_{x \in X} P(x) \log_2 P\,(x)$$

Ентропія Шеннона представляє середній вміст інформації (в бітах), отриманий у результаті спостереження за результатом випадкової величини. Ця міра має декілька властивостей, критичних для генерації випадкових чисел. По-перше, ентропія Шеннона досягає максимального значення, коли розподіл імовірностей є рівномірним: $H_{\max}(X) = \log_2|X|$ для випадкової величини з $|X|$ можливими наслідками. Для бінарних випадкових величин максимальна ентропія Шеннона дорівнює 1 біту, що досягається, коли $P(0) = P(1) = 0.5$. По-друге, ентропія Шеннона дорівнює нулю, коли випадкова величина є детермінованою (один наслідок має ймовірність 1, всі інші – 0), що представляє повну відсутність невизначеності.

Однак самої по собі ентропії Шеннона недостатньо для оцінки криптографічної безпеки. Зловмисник з попереднім знанням про розподіл імовірностей може стратегічно експлуатувати нерівномірні розподіли. Наприклад, випадкова величина, що демонструє розподіл $P(0) = 0.99$, $P(1) = 0.01$, має ентропію Шеннона $H(X) \approx 0.081$ біт, але зловмисник, використовуючи стратегію імовірнісного вгадування, досягає успіху з імовірністю 0.99 у прогнозуванні виводу, досягаючи ефективної надійності безпеки, що значно нижча, ніж передбачає ентропія Шеннона.

Мін-ентропія, що визначається як негативний логарифм максимальної маси ймовірності, надає консервативну міру непередбачуваності для найгіршого випадку [37]:

$$H_\infty(X) = -\log_2 \max_{x \in X} P\,(x) = \log_2 \left(\frac{1}{\max\limits_{x} P\,(x)} \right)$$

Мін-ентропія представляє найкращу ймовірність, якої зловмисник з довільними обчислювальними ресурсами може досягти за допомогою оптимальної стратегії вгадування. Для попереднього прикладу з $P(0) = 0.99$, $P(1) = 0.01$, мін-ентропія дорівнює $-\log_2(0.99) \approx 0.0145$ біт, точно відображаючи практичну ймовірність успіху зловмисника. Для криптографічних застосувань мін-ентропія надає належну метрику безпеки, оскільки вона враховує сценарії найгіршого випадку, а не аналіз середнього випадку.

Співвідношення між ентропією Шеннона та мін-ентропією для будь-якої випадкової величини задовольняє умову $H_\infty(X) \leq H(X)$, причому рівність досягається лише для рівномірних розподілів. Розбіжність між цими мірами зростає зі збільшенням нерівномірності розподілу.

Швидкість ентропії (Entropy Rate): Для послідовностей залежних випадкових величин $(X_1, X_2, \ldots, X_n)$, швидкість ентропії вимірює середню невизначеність на символ у границі, коли довжина послідовності прямує до нескінченності:

$$H_r = \lim_{n \to \infty} \frac{1}{n} H(X_1, X_2, \ldots, X_n)$$

Швидкість ентропії характеризує середній вміст інформації, що генерується на вихідний біт з безперервного джерела випадкових чисел. Джерело шуму, що генерує бінарний вивід зі швидкістю 10^6 біт на секунду зі швидкістю ентропії 0.98 біт на символ, виробляє приблизно $0.98 \times 10^6 = 980{,}000$ біт криптографічної ентропії на секунду. Ця метрика безпосередньо визначає доцільність генерації криптографічного ключа: генерація 256-бітного ключа для шифрування AES-256-GCM з джерела зі швидкістю ентропії 0.80 біт/символ вимагає обробки приблизно $256 / 0.80 = 320$ вихідних бітів.

2.2.2 Фреймворк AIS 31 для оцінювання генераторів випадкових чисел

Стандарт AIS 31 Федерального управління з інформаційної безпеки Німеччини, вперше запроваджений у 2001 році та суттєво переглянутий до 2023 року, надає найсуворіший фреймворк для оцінювання генераторів випадкових чисел у криптографічних застосуваннях [22]. На відміну від підходів до оцінювання, що наголошують переважно на властивостях випадковості вихідних даних, AIS 31 вимагає побудови явних стохастичних моделей, що описують розподіл імовірностей, який лежить в основі фізичних джерел шуму. Ця методологія, що базується на моделях, уможливлює верифікацію того, що заявлені показники ентропії залишаються дійсними протягом усього терміну служби пристрою за різних умов експлуатації, а не лише валідовані в лабораторних умовах.

Основа методології AIS 31 передбачає побудову стохастичної моделі M, що надає частковий математичний опис фізичного джерела шуму. Модель визначає розподіли ймовірностей, що керують поведінкою джерела шуму, через випадкові величини та їхні взаємозалежності. Стохастична модель повинна задовольняти дві суттєві вимоги: справжній розподіл вихідних даних джерела шуму повинен залишатися в межах моделі протягом усього життєвого циклу пристрою, та модель повинна уможливлювати вибір та застосування відповідних статистичних тестів для перевірки цього вміщення шляхом емпіричного аналізу.

Для джерел ентропії на основі кільцевих осциляторів, задокументованих у літературі [38], канонічні стохастичні моделі зазвичай представляють накопичення джиттера в окремих циклах осцилятора як випадкову величину J_i, де період циклу демонструє розподіл приблизно $J_i \sim N(\mu, \sigma^2)$ за нормальних умов експлуатації. Опубліковані аналізи демонструють, що ці моделі враховують варіації джиттера через коливання температури навколишнього середовища та зміни напруги живлення. Побудова стохастичної моделі вимагає теоретичного обґрунтування, що базується на фізичному розумінні механізмів шуму осцилятора, а не на суто емпіричному підборі кривих.

AIS 31 визначає шість ієрархічно впорядкованих класів функціональності, що визначають дедалі суворіші вимоги до генераторів випадкових чисел. Для детермінованих підходів, DRG.2 забезпечує базову безпеку з властивостями зворотної та прямої секретності, перевіреними шляхом криптографічного аналізу. DRG.3 вимагає посиленої зворотної секретності через односпрямовані функції переходу стану, запобігаючи практичному відновленню попередніх виходів, навіть за повного знання поточного внутрішнього стану. DRG.4 додатково вимагає посиленої прямої секретності, зобов'язуючи до гібридних конструкцій, що включають додаткові входи з високою ентропією, які запобігають визначенню виходу лише з поточного стану.

Для фізичних генераторів справді випадкових чисел (TRNG), PTG.2 визначає середній рівень безпеки, що підходить для застосувань розумного дому. Клас PTG.2 вимагає досягнення ентропії Шеннона ≥ 0.9998 біт на вихідний біт та мін-ентропії ≥ 0.98 біт на вихідний біт, причому розбіжність між межами ентропії Шеннона та мін-ентропії враховує зміщення в розподілі ймовірностей. Ці пороги гарантують, що навіть зловмисник зі знанням розподілу ймовірностей не може практично перерахувати можливі послідовності випадкових чисел швидше, ніж законні криптографічні застосування можуть їх генерувати.

PTG.3 забезпечує найвищий рівень безпеки фізичного ГВЧ шляхом поєднання PTRNG, що відповідає PTG.2, з криптографічною постобробкою, що відповідає DRG.3. Гібридна архітектура гарантує, що навіть повна відмова фізичного джерела ентропії не призводить до негайної компрометації безпеки, оскільки детермінований постобробник зберігає властивості криптографічної безпеки за умови, що принаймні одна подія повторного засівання сталася протягом вікна атаки.

AIS 31 визначає два взаємодоповнюючі набори статистичних тестів: тести T_rrn для необроблених (raw) випадкових чисел безпосередньо з джерела шуму, та тести T_irn для проміжних (intermediate) випадкових чисел після необов'язкового кондиціонування, але перед криптографічною постобробкою. Вибір тесту залежить від характеристик стохастичної моделі. Опубліковані

аналізи демонструють, що для кільцевих осциляторів, які демонструють гаусів розподіл джиттера, відповідні тести включають тести частоти, що оцінюють баланс появи бітів, тести серій (runs tests), що досліджують послідовні однакові біти, та тести автокореляції, що виявляють часові залежності.

Клас функціональності PTG.2 вимагає безперервних онлайн-тестів, що працюють під час нормальної роботи пристрою, для перевірки того, що джерело шуму залишається в межах прогнозованих параметрів стохастичної моделі. AIS 31 визначає, що розробка онлайн-тестів повинна встановлювати пороги, які визначають, коли спостережувані швидкості ентропії достатньо відхиляються від прогнозів моделі, щоб спрацювали умови тривоги. Наприклад, якщо стохастична модель прогнозує ентропію Шеннона ≥ 0.9998 біт/символ, сумісна реалізація встановить поріг тривоги на консервативному рівні, такому як 0.99 біт/символ, викликаючи виявлення збою, коли середні значення тестового вікна падають нижче цього порогу.

AIS 31 вимагає механізмів тестування на повну відмову, які виявляють повні збої джерела ентропії (наприклад, блокування осцилятора в конструкціях на основі кільцевих осциляторів). Тест на повну відмову гарантує, що якщо джерело шуму припиняє виробляти придатну випадковість, ГВЧ негайно припиняє вивід та сповіщає зовнішні системи, замість того, щоб продовжувати генерувати криптографічно слабкий матеріал.

2.2.3 Фізичні генератори справді випадкових чисел: вимоги PTG.2 та реалізація

Фізичні генератори справді випадкових чисел (TRNG), придатні для пристроїв IoT, використовують декілька типів джерел ентропії, задокументованих у літературі. Кільцеві осцилятори використовують метастабільну поведінку в цифрових логічних елементах для генерації часового джиттера в періоді осциляції [38]. Опубліковані реалізації демонструють, що дві комплементарні схеми кільцевих осциляторів, що вимірюються у відносно синхронні моменти часу, виробляють значення джиттера, які важко передбачити

зловмисникам, оскільки джиттер походить від справді випадкового теплового шуму та квантових ефектів. Альтернативні підходи включають вибірку шуму аналого-цифрового перетворювача (АЦП), експлуатуючи тепловий шум та шум квантування при аналого-цифровому перетворенні. Дослідження Цзяна та ін. (Jiang et al.) [18] демонструє, що цей підхід підходить для мікроконтролерів з інтегрованими периферійними пристроями АЦП, не вимагаючи спеціальних апаратних компонентів.

Дотримуючись канонічної стохастичної моделі, встановленої в дослідженнях кільцевих осциляторів, характеристика джиттера аналізує варіації часових інтервалів від циклу до циклу. Нехай T_i позначає період i-го циклу осциляції в теоретичній або базованій на літературі моделі кільцевого осцилятора. Джиттер $J_i = T_i - T_{\text{target}}$ представляє відхилення від номінального цільового періоду. Стохастична модель визначає, що за нормальних умов експлуатації J_i має приблизно гаусів розподіл:

$$J_i \sim N\left(0, \sigma_{\text{jitter}}^2\right)$$

Літературні звіти вказують, що середньоквадратичне відхилення джиттера σ_{jitter} залежить від температури навколишнього середовища, напруги живлення та варіацій у процесі виробництва напівпровідників. Емпірична характеристика, задокументована в опублікованих дослідженнях, вимірює σ_{jitter} у всьому діапазоні робочих умов пристрою. Для кільцевих осциляторів, що генерують частоти коливань у діапазоні 100-500 МГц, типові середньоквадратичні відхилення джиттера коливаються від наносекунд ($\sigma \approx 0.1 - 1$ нс), що перетворюється на фазовий джиттер у діапазоні 10-100 пс на цикл.

Опубліковані теоретичні аналізи демонструють, що коли два кільцеві осцилятори працюють асинхронно, і їхні виходи вимірюються за допомогою незалежного тактового джерела, відносна фаза між осциляторами демонструє високо випадкову поведінку через накопичені ефекти джиттера. Якщо осцилятор 1 генерує період $T_1 = T_{\text{target}} + J_{1,i}$ і осцилятор 2 генерує період $T_2 = T_{\text{target}} + J_{2,i}$,

де $J_{1,i}$ та $J_{2,i}$ є незалежними вибірками джиттера з гаусовим розподілом, різниця фаз накопичується як:

$$\Delta\phi_i = 2\pi \sum_{j=1}^{i} \left(J_{2,j} - J_{1,j}\right) / T_{\text{target}}$$

Це накопичення фази наближається до рівномірного розподілу за модулем 2π, генеруючи високо непередбачувані моменти вибірки при порівнянні з незалежним тактовим сигналом. Вибірка в ці стохастично змінювані моменти часу виробляє вихідні біти з теоретичною ентропією, що наближається до 1 біта на вибірку.

Для теоретичної вибіркової вихідної послідовності $(B_1, B_2, \ldots, B_n)$, де кожен $B_i \in \{0,1\}$, емпірична ентропія Шеннона для вихідного блоку обчислювалася б як:

$$H_{\text{emp}} = -\sum_{b\in\{0,1\}} \hat{P}(b) \log_2 \hat{P}\,(b)$$

де $\hat{P}(b) = \frac{\text{count}(B_i=b)}{n}$ представляє емпіричну оцінку ймовірності. Для відповідності PTG.2, метою проєктування є досягнення $H_{\text{emp}} \geq 0.9998$. Опубліковані експериментальні результати з подібних реалізацій повідомляють, що якщо спостережувана емпірична ентропія Шеннона з тестового блоку в 100 000 біт дорівнює 0.9999 біт/біт, це надає сильні докази того, що справжня ентропія Шеннона $H \geq 0.9998$ з високою статистичною достовірністю.

Оцінка мін-ентропії вимагає ідентифікації найчастішого вихідного значення. Якщо одне бітове значення зустрічається з частотою $f_{\max}$, емпірична оцінка мін-ентропії стає:

$$H_{\infty,\text{emp}} = -\log_2(f_{\max})$$

Для відповідності PTG.2, вимагається $H_{\infty,\text{emp}} \geq 0.98$. Цей поріг допускає максимальне зміщення приблизно $2^{-0.98} \approx 0.503$, що означає, що частіший біт може з'являтися щонайбільше в 50.3% позицій. Досягнення таких жорстких обмежень вимагає ретельно розроблених джерел ентропії, і опубліковані

дослідження валідації підтверджують, що джерела джиттера з достатньою незалежністю можуть відповідати цим вимогам.

AIS 31 вимагає, щоб онлайн-тести безперервно моніторили вивід під час роботи, зазвичай оцінюючи статистику з ковзних вікон останніх вихідних даних. Реалізація, що відповідає PTG.2, перевіряла б останні вихідні вікна (наприклад, останні 1000 вихідних бітів), обчислюючи емпіричну ентропію Шеннона та порівнюючи її з порогом, отриманим зі стохастичної моделі (наприклад, 0.99). Якщо п'ять послідовних тестових вікон показують ентропію нижче порогу, AIS 31 вимагає, щоб ГВЧ ініціював сигнал тривоги про збій та припинив генерацію виводу.

2.2.4 Детерміновані генератори випадкових чисел: вимоги DRG.2, DRG.3, DRG.4

Детерміновані генератори випадкових чисел (ДГВЧ) розширюють короткі випадкові «зерна» (seeds) в довші вихідні послідовності за допомогою детермінованих алгоритмів. Криптографічна безпека ДГВЧ базується на обчислювальній неможливості прогнозування майбутніх виходів або відновлення «зерен» зі спостережуваного виводу, а не на математичній непередбачуваності, притаманній фізичним процесам.

DRG.2 забезпечує зворотну секретність (backward secrecy) та пряму секретність (forward secrecy). Зворотна секретність гарантує, що якщо зловмисник спостерігає внутрішній стан S_i в момент часу i, відновлення всіх попередньо згенерованих виходів $B_1, \dots, B_{i-1}$ залишається обчислювально неможливим. Ця властивість вимагає, щоб вихідна функція ДГВЧ $f(S) \to B$ не була оборотною, і попередні стани не можна було відновити з $f(S_i)$. Пряма секретність гарантує, що спостереження поточної вихідної послідовності не уможливлює прогнозування майбутніх виходів $B_{i+1}, B_{i+2},$, вимагаючи, щоб функція переходу стану $g(S_i, e_i) \to S_{i+1}$ залежала від вхідної ентропії e_i таким чином, щоб ентропію не можна було відновити з виходу.

DRG.3 додає посилену зворотну секретність через односпрямовані функції переходу стану. На відміну від DRG.2, де відновлення стану теоретично може бути можливим шляхом інтенсивного криптоаналізу, DRG.3 вимагає, щоб, маючи стан S_i, відновлення S_{i-1} залишалося обчислювально неможливим з робочим фактором, що перевищує 2^{256} для 256-бітних рівнів безпеки. Типові реалізації використовують криптографічні геш-функції $H(\square)$ так, що $S_i = H(S_{i-1} \parallel e_i)$, де криптографічні властивості $H(\square)$ забезпечують односпрямованість.

DRG.4 вимагає гібридних конструкцій, що поєднують детерміновану генерацію з періодичним повторним засіванням високою ентропією. Структура використовує детерміновану генерацію під час нормальної роботи, причому перехід стану включає періодичну свіжу ентропію: $S_i = H(S_{i-1} \parallel \text{entropy}_{\text{fresh}})$, де входи ентропії відбуваються достатньо часто, щоб запобігти атакам на вичерпання простору станів.

2.3 Криптографічні протоколи для безпеки комунікацій розумного дому

2.3.1 Реалізація Transport Layer Security для протоколу MQTT

Протокол MQTT забезпечує полегшений обмін повідомленнями за моделлю «видавець-передплатник», що підходить для пристроїв IoT з обмеженнями пропускної здатності та енергоспоживання [40]. Однак незашифровані реалізації MQTT наражають весь вміст повідомлень на пасивне прослуховування та атаки активної модифікації. Transport Layer Security (TLS) версії 1.3 забезпечує шифрування, автентифікацію та захист цілісності для з'єднань MQTT [6].

Протокол рукостискання (handshake) TLS встановлює спільні ключі шифрування та автентифікує як клієнта, так і сервера за допомогою послідовності криптографічних операцій, що критично залежать від якості випадкових чисел. Під час рукостискання клієнт генерує свіже випадкове значення, що називається client_random і містить 32 байти (256 біт) криптографічно безпечної випадковості. Сервер аналогічно генерує

server_random. Ці значення, разом з обміняними параметрами відкритих ключів, формують основу для обчислення спільного секрету та подальших ключів шифрування.

У варіанті рукостискання з еліптичними кривими Діффі-Геллмана (ECDHE), клієнт генерує ефемерну пару ключів ECDH $(x_c, X_c = g^{x_c})$, де x_c – випадковий скаляр, а X_c – відповідна публічна точка на еліптичній кривій. Безпека цієї угоди про ключ повністю залежить від випадковості x_c. Якщо генератор випадкових чисел, що виробляє x_c, має недостатню ентропію, зловмисник може перерахувати можливі приватні ключі x_c шляхом обчислень і відновити спільний секрет, повністю нівелюючи шифрування TLS.

Протокол TLS 1.3 виводить сеансові ключі за допомогою функцій виведення ключа (KDF), що приймають спільний секрет як вхідні дані. Сеансовий ключ шифрування для AES-256-GCM виводиться шляхом розширення на основі HMAC:

$$session\_key = HKDF - Expand(PRK, context, L)$$

де PRK (псевдовипадковий ключ) виводиться зі спільного секрету, встановленого під час рукостискання. Якщо початкова випадковість, використана в угоді про ключ, виявиться передбачуваною, зловмисник може попередньо обчислити всі можливі сеансові ключі, а потім зіставити спостережувані шифротексти з попередньо обчисленими розшифруваннями, повністю порушуючи конфіденційність.

Кожне з'єднання TLS вимагає декількох незалежних випадкових значень: client_random (32 байти), server_random (32 байти), ефемерний приватний скалярний ключ ECDH (для ECDHE, приблизно 32 байти) і, можливо, випадкові нонси (nonces) для режиму роботи AEAD. Системі розумного дому, що встановлює нове з'єднання TLS кожні 30 секунд для передачі даних давачів, потрібно приблизно 96 байт криптографічної випадковості кожні 30 секунд, або 3.2 байти на секунду. Опубліковані дані про продуктивність вказують, що джерела ентропії зі швидкістю 0.98 біт/байт вимагають вибірки приблизно 3.3 байт необробленого матеріалу для генерації 3.2 байт криптографічного виводу,

що вимагає апаратного TRNG, здатного підтримувати стабільні швидкості, що перевищують 10 байт на секунду, для підтримки навіть скромних робочих навантажень розумного дому.

2.3.2 Механізми автентифікованого шифрування з використанням AES-GCM

Advanced Encryption Standard у режимі Галуа/Лічильника (AES-GCM) забезпечує автентифіковане шифрування з асоційованими даними (AEAD), поєднуючи конфіденційність та автентифікацію в одній криптографічній операції [11]. AES-GCM вимагає унікального значення нонса (nonce) для кожної операції шифрування з використанням того самого ключа. Протокол генерує нонс як:

$$nonce = IV \ || \ counter$$

де IV – вектор ініціалізації, а $counter$ збільшується для кожної операції шифрування.

Повторне використання нонса повністю нівелює безпеку AES-GCM, уможливлюючи зловмисникам обчислення XOR блоків відкритого тексту та відновлення вмісту повідомлення. Ця критично важлива для безпеки вимога залежить від якості випадкових чисел: якщо генератор випадкових чисел, що виробляє значення IV, є передбачуваним, або якщо керування лічильником зазнає збою через недостатню ентропію для багатопотокових середовищ, колізії нонсів уможливлюють повну компрометацію системи.

2.3.3 Полегшена криптографія для вбудованих пристроїв IoT

Пристрої з обмеженими ресурсами вимагають полегшених криптографічних реалізацій, що збалансовують безпеку з обчислювальними та пам'яттєвими обмеженнями. Сучасні дослідження пропонують різні полегшені шифри, включно з PRESENT, SPECK, SIMON та ChaCha20-Poly1305 [39]. Всі такі алгоритми фундаментально залежать від високоякісної генерації криптографічних ключів. 128-бітний блоковий шифр зі 128-бітним ключем забезпечує безпеку лише тоді, коли ключ демонструє 128 біт ентропії. Слабка

генерація випадкових чисел зменшує ефективну безпеку до фактично доступної ентропії.

2.4 Моделі контролю доступу та фреймворки автентифікації

2.4.1 Механізми контролю доступу на основі ролей (RBAC)

Контроль доступу на основі ролей (RBAC) визначає дозволи на основі ролей користувачів у системі. Розгортання розумного дому може визначати ролі, включно з: $owner$ (повні дозволи для всіх пристроїв), $family\_member$ (дозволи на контроль довкілля, обмежений контроль безпеки), $guest$ (лише контроль температури) та $service\_provider$ (доступ до конкретних пристроїв для обслуговування). Політика доступу RBAC може бути виражена як $(role, resource, action) \rightarrow \{permit, deny\}$.

Реалізація RBAC у системах розумного дому вимагає безпечного керування сеансами, автентифікованими за допомогою криптографічних механізмів. Багатофакторна автентифікація покращує безпеку, вимагаючи факторів володіння (апаратні токени), факторів знання (паролі) та факторів властивості (біометрична верифікація). Автентифікація на основі токенів генерує унікальні сеансові токени, що містять інформацію про автентифікацію:

$$session\_token = Sign\big(role \parallel timestamp \parallel user\_id \parallel E(nonce)\big)$$

де $Sign()$ представляє криптографічний підпис, а $E(nonce)$ включає випадкове значення нонса. Безпека цього токена критично залежить від непередбачуваності нонса. Слабка генерація випадкових чисел уможливлює зловмисникам підробку дійсних токенів шляхом прогнозування значень нонса, повністю обходячи автентифікацію.

2.4.2 Стратегії реалізації багатофакторної автентифікації

Ефективна багатофакторна автентифікація поєднує декілька незалежних факторів автентифікації. Системи розумного дому на базі MQTT можуть реалізувати двофакторну автентифікацію через початкову автентифікацію за паролем плюс верифікацію одноразового пароля (OTP). Генерація OTP зазвичай

використовує підхід на основі часу (TOTP) або підхід на основі лічильника (HOTP). Обидва варіанти залежать від генерації випадкових чисел для початкового спільного використання секрету між автентифікатором та хабом розумного дому.

Спільний секрет S, що використовується для обчислення OTP, повинен мати достатню ентропію (зазвичай 80-160 біт для 6-8 цифрових кодів OTP). Під час початкового налаштування пристрою, безпечна реалізація генерувала б S з валідованого джерела ентропії та ділилася ним через безпечний канал:

$$HOTP(msg) = Truncate\big(HMAC - SHA1(S, msg)\big) mod 10^6$$

Якщо генератор випадкових чисел, що виробляє S, демонструє недостатню ентропію, зловмисники можуть перерахувати можливі секретні значення та підробити коди OTP, не володіючи фізичним пристроєм-автентифікатором.

2.5 Архітектурні принципи проєктування безпечних систем розумного дому

2.5.1 Локальна обробка проти хмарних архітектур

Архітектури розумного дому варіюються від повністю локальної обробки (всі обчислення та зберігання на пристрої-хабі) до гібридних гранично-хмарних (edge-cloud) конструкцій (локальна обробка з хмарним резервним копіюванням) та повністю залежних від хмари конструкцій (мінімальні обчислення на хабі, інтенсивна обробка в хмарі). Архітектурний вибір вносить компроміси щодо безпеки.

Повністю локальні архітектури усувають передачу даних зовнішнім сторонам, запобігаючи хмарному прослуховуванню та зменшуючи ризики витоку даних. Однак локальна обробка вимагає достатньої обчислювальної потужності та сховища для обробки складності, обмежуючи інтелект автоматизації та швидкість реагування. Повністю залежні від хмари архітектури уможливлюють складну аналітику та машинне навчання, але створюють залежність від безпеки хмарного провайдера, потенційне розкриття даних через компрометацію провайдера та вразливість до збоїв підключення до Інтернету.

Гібридні архітектури оптимально розподіляють обробку: локальна обробка для критичних до затримок та чутливих до приватності функцій (контроль доступу в реальному часі, негайна реакція середовища) з хмарною аналітикою для не критичних до часу обчислень (аналіз довгострокових патернів, рекомендації щодо оптимізації). Цей підхід вимагає безпечних механізмів синхронізації між локальним хабом та хмарними сервісами. Вся комунікація синхронізації повинна використовувати криптографічний захист, що залежить від високоякісної генерації випадкових чисел.

2.5.2 Сегментація мережі та безпека на рівні шлюзу

Сегментація мережі ізолює трафік пристроїв IoT від загальної домашньої мережі, обмежуючи горизонтальне переміщення, якщо окремі пристрої скомпрометовані. Безпечні мережеві архітектури розділяють пристрої на зони: критичні для безпеки (дверні замки, камери), критичні для комунальних послуг (ОВК, освітлення) та низькоризикові (розважальні пристрої). Правила брандмауера на шлюзі забезпечують обмеження трафіку між зонами.

Фільтрація трафіку на рівні шлюзу перевіряє патерни на рівні протоколу для виявлення аномальної поведінки. Наприклад, якщо скомпрометований давач руху, що зазвичай генерує 10 повідомлень MQTT на хвилину, раптом починає генерувати 100 повідомлень на хвилину, шлюз виявить аномальну поведінку та ізолює пристрій. Це виявлення залежить від встановлення базових патернів трафіку під час довіреної роботи, а потім ідентифікації статистичних відхилень.

Реалізація систем виявлення вторгнень (IDS) на шлюзі доповнює сегментацію мережі. IDS перевіряє метадані зашифрованого трафіку (час пакетів, розміри, частота) для виявлення поведінкових аномалій, навіть коли шифрування вмісту перешкоджає інспекції. Статистичні базові лінії для нормальної поведінки залежать від точних джерел ентропії для генерації випадкових порогів та рандомізованого прийняття рішень в алгоритмах IDS.

Висновки до Розділу 2

Теоретичне дослідження методів криптографічного захисту демонструє, що забезпечення стійкості IoT-систем неможливе без застосування суворого математичного апарату стохастичного моделювання фізичних процесів. Центральним елементом теоретичного обґрунтування є перехід від евристичних методів оцінки випадковості до застосування вимог стандарту AIS 31 (клас PTG.2), що вимагає побудови моделі джерела шуму на основі фізичних властивостей, таких як фазовий джиттер кільцевих осциляторів. Такий підхід дозволяє гарантувати необхідний рівень мін-ентропії для криптографічних застосувань навіть в умовах нестабільного середовища, характерного для побутових пристроїв. Водночас аналіз показує, що криптографічна підсистема повинна бути нерозривно пов'язана з моделями контролю доступу та автентифікації. Доведено, що ефективність рольової моделі (RBAC) та протоколів узгодження ключів (ECDHE) лінійно залежить від якості первинної ентропії. Таким чином, теоретично обґрунтована архітектура безпеки повинна базуватися на синергії апаратного джерела випадковості та стандартизованих криптографічних примітивів, що створює математично доведений бар'єр проти статистичних та аналітичних атак.

3 АНАЛІТИЧНИЙ ФРЕЙМВОРК ТА ПРОЄКТУВАННЯ АРХІТЕКТУРИ БЕЗПЕКИ ДЛЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ РОЗУМНИХ БУДИНКІВ

3.1 Методологія дослідження: аналітичний підхід

Це дослідження використовує аналітичну методологію, що поєднує аналіз криптографічних стандартів, інженерію вимог безпеки, архітектурне проєктування та порівняльний огляд літератури. На відміну від експериментального дослідження, що передбачає впровадження на фізичному обладнанні та емпіричне тестування, ця робота розробляє теоретичні основи та проєктні фреймворки шляхом систематичного аналізу встановлених стандартів, задокументованих вразливостей та опублікованих результатів досліджень. Методологія складається з п’яти основних фаз, що забезпечують сувору аналітичну основу для розробки безпечної архітектури розумного дому без необхідності створення фізичного прототипу.

Фаза 1: Аналіз стандартів та виведення вимог – Всебічне вивчення класів функціональності AIS 31, вимог до ентропії, методології стохастичного моделювання та критеріїв оцінювання шляхом детального аналізу документів специфікації Федерального управління з інформаційної безпеки Німеччини [22]. Ця фаза виділяє кількісні пороги безпеки, процедури тестування та критерії відповідності, застосовні до криптографічних систем розумного дому.

Фаза 2: Аналіз ландшафту загроз – Систематична ідентифікація та характеристика загроз безпеці розумного дому шляхом огляду літератури щодо задокументованих вразливостей, патернів атак та технік експлуатації, описаних у рецензованих публікаціях. Моделювання загроз використовує встановлені фреймворки, включно з OWASP IoT Top 10 [4] та методологією STRIDE [40], для категоризації векторів атак та оцінки серйозності ризиків.

Фаза 3: Порівняльне оцінювання технологій – Аналіз опублікованих реалізацій TRNG (генераторів справді випадкових чисел) для вбудованих систем з обмеженими ресурсами, вивчення архітектурних підходів, заявлених

швидкостей ентропії, характеристик продуктивності та методологій валідації, задокументованих в академічній літературі. Ця фаза ідентифікує проєктні патерни, найкращі практики та компроміси, що лежать в основі архітектурних рішень.

Фаза 4: Проєктування архітектури безпеки – Розробка багаторівневого фреймворку безпеки, що інтегрує валідовані принципи генерації випадкових чисел з криптографічними протоколами, механізмами контролю доступу та засобами мережевої безпеки. Специфікація архітектури використовує формальну нотацію, що визначає компоненти, інтерфейси, властивості безпеки та операційні вимоги.

Фаза 5: Теоретичне оцінювання безпеки – Аналітичне оцінювання запропонованої архітектури відносно задокументованих класів вразливостей та сценаріїв атак з літератури, прогнозування покращень безпеки шляхом систематичного порівняння з базовими комерційними реалізаціями. Оцінювання використовує встановлені метрики, включно зі зменшенням кількості вразливостей, аналізом поверхні атаки та оцінкою середнього часу до компрометації на основі архітектурних властивостей.

Методологічні обмеження: Це дослідження використовує виключно аналітичні методи без впровадження на фізичному обладнанні чи емпіричного тестування. Прогнози продуктивності базуються на опублікованих тестах порівнянних систем, задокументованих у рецензованій літературі. Розрахунки ентропії покладаються на теоретичні стохастичні моделі, валідовані шляхом математичного аналізу, а не експериментальних вимірювань. Оцінки безпеки прогнозують покращення на основі архітектурного аналізу та порівняння з задокументованими вразливостями в наявних системах. Запропонований фреймворк вимагає майбутньої експериментальної реалізації для емпіричної валідації теоретичних прогнозів щодо швидкостей ентропії, характеристик продуктивності та ефективності безпеки.

Обґрунтування аналітичного підходу: Аналітична методологія є доцільною для дослідження на рівні магістерської роботи, що стосується

архітектурного проєктування та теоретичних основ. Внесок полягає в систематичній інтеграції встановлених криптографічних стандартів (AIS 31) з практичними вимогами безпеки розумного дому, розробляючи валідований проєктний фреймворк, а не новий апаратний винахід. Цей підхід уможливлює сувору теоретичну розробку, визнаючи при цьому обмеженість ресурсів, типову для академічного дослідницького середовища.

3.2 Аналіз стандартів AIS 31 та виведення криптографічних вимог

3.2.1 Класи функціональності AIS 31: Детальний аналіз

Стандарт AIS 31 встановлює шість ієрархічно впорядкованих класів функціональності, що визначають дедалі суворіші вимоги до генераторів випадкових чисел, які використовуються в криптографічних застосуваннях [22]. Детальний аналіз версії 2.36 розкриває технічні специфікації та критерії оцінювання для кожного класу.

Класи детермінованих генераторів випадкових чисел (DRG): Клас DRG.2 забезпечує базову безпеку через зворотну секретність (знання вихідної послідовності не розкриває попередні виходи) та пряму секретність (знання вихідної послідовності не уможливлює прогнозування майбутніх виходів без додаткового входу ентропії). Математичні вимоги визначають, що розмір внутрішнього стану повинен перевищувати 256 біт для застосувань, що орієнтовані на 128-бітний рівень безпеки, а функція переходу стану повинна використовувати криптографічно стійкі операції, що запобігають практичному відновленню стану.

DRG.3 посилює безпеку, вимагаючи односпрямованих функцій переходу стану, де відновлення попереднього стану S_{i-1} з поточного стану S_i залишається обчислювально неможливим з робочим фактором, що перевищує 2^{256} операцій. Ця властивість, що називається посиленою зворотною секретністю, запобігає зловмисникам, які компрометують DRNG в момент часу t, відновлювати виходи, згенеровані до моменту t. Реалізація зазвичай використовує криптографічні геш-функції $H()$ так, що $S_i = H(S_{i-1}||e_i)$ де e_i представляє свіжий вхід ентропії.

DRG.4 вимагає гібридної архітектури, що поєднує детерміновану генерацію з частим повторним засіванням (reseeding) високою ентропією. Специфікація вимагає, щоб свіжий вхід ентропії відбувався з інтервалами, що запобігають вичерпанню простору станів, з мінімальною ентропією на одне повторне засівання, що перевищує 128 біт для 128-бітних застосувань безпеки. Ця конструкція гарантує, що навіть повна компрометація стану надає лише тимчасове вікно вразливості, обмежене максимальним інтервалом повторного засівання.

Класи фізичних генераторів справді випадкових чисел (PTG): Клас PTG.2, що становить основний фокус цього дослідження, встановлює кількісні вимоги до ентропії, які перевіряються шляхом стохастичного моделювання. Аналіз розділу 3.4.3 AIS 31 показує, що відповідність PTG.2 вимагає:

- Ентропія Шеннона $H(X) \geq 0.9998$ біт на вихідний біт
- Мін-ентропія $H_{\infty}(X) \geq 0.98$ біт на вихідний біт
- Безперервне онлайн-тестування під час нормальної роботи
- Тест на повну відмову, що виявляє повний збій джерела ентропії
- Застосування батареї статистичних тестів (T_{rrn} для необроблених випадкових чисел)

Розбіжність порогів ентропії між Шенноном (0.9998) та мін-ентропією (0.98) враховує залишкове статистичне зміщення, притаманне фізичним джерелам шуму, водночас підтримуючи запаси криптографічної безпеки. Для генерації 256-бітного ключа шифрування AES, джерело, що відповідає PTG.2, забезпечує мінімум $256 \times 0.98 = 250.88$ біт ефективної ентропії, що перевищує цільовий 128-бітний рівень безпеки зі значним запасом (приблизно 122 біти надлишку).

PTG.3 представляє найвищий клас безпеки фізичного ГВЧ, поєднуючи фізичне джерело ентропії, що відповідає PTG.2, з криптографічною постобробкою, що відповідає DRG.3. Гібридна архітектура гарантує, що навіть тимчасовий збій фізичного джерела ентропії не призводить до негайної

компрометації безпеки, оскільки детермінований компонент зберігає властивості криптографічної безпеки за умови, що принаймні одне успішне повторне засівання відбулося протягом вікна вразливості. Ця конструкція є особливо цінною для застосувань з високим рівнем безпеки, де маніпуляція джерелом ентропії є реальною загрозою.

3.2.2 Методологія стохастичного моделювання: Теоретична основа

Відмінна риса методології оцінювання AIS 31 полягає в обов'язковій побудові стохастичної моделі, що описує розподіл імовірностей, який лежить в основі фізичних джерел шуму. На відміну від альтернативних підходів до оцінювання, які оцінюють властивості випадковості вихідних даних лише шляхом статистичного тестування, AIS 31 вимагає явної математичної моделі, що уможливлює верифікацію того, що спостережувані заявлені показники ентропії залишаються дійсними протягом усього терміну служби пристрою за різних умов експлуатації [22].

Стохастична модель M повинна задовольняти дві суттєві вимоги згідно з розділом 2.3 AIS 31. По-перше, справжній розподіл імовірностей вихідних даних джерела шуму повинен залишатися в межах прогнозованого розподілу моделі протягом усього життєвого циклу пристрою, враховуючи варіації навколишнього середовища (температура, напруга, старіння) та виробничі допуски. По-друге, модель повинна уможливлювати вибір та застосування відповідних статистичних тестів, що перевіряють вміщення шляхом емпіричного аналізу, причому пороги тестування виводяться з параметрів моделі, а не з довільних констант.

Для джерела ентропії на основі кільцевого осцилятора, канонічна стохастична модель представляє накопичення джиттера в окремих циклах осцилятора як випадкову величину з гаусовим розподілом. Нехай J_i позначає джиттер (часове відхилення) в i-му циклі осциляції, що моделюється як:

$$J_i \sim N\left(0, \sigma^2_{\text{jitter}}\right)$$

де σ_{jitter} представляє середньоквадратичне відхилення, що кількісно визначає величину шуму. Фізичне обґрунтування гаусового розподілу походить з центральної граничної теореми: джиттер осцилятора є результатом численних незалежних внесків шуму (тепловий шум у транзисторах, дробовий шум у потоці струму, флікер-шум у напівпровідникових приладах), сукупний ефект яких збігається до гаусового розподілу незалежно від розподілів окремих джерел шуму.

Еволюція фази осцилятора k за N циклів описується:

$$\Phi_k(N) = 2\pi N + 2\pi \sum_{i=1}^{N} \frac{J_{k,i}}{T_{\text{target},k}}$$

де $T_{\text{target},k}$ представляє номінальний період осциляції. Невизначеність фази (дисперсія) демонструє лінійне зростання з кількістю циклів:

$$\sigma^2_{\Phi_k}(N) = N\left(\frac{2\pi\sigma_{\text{jitter}}}{T_{\text{target}}}\right)^2$$

Це лінійне накопичення дисперсії гарантує, що після достатньої кількості циклів, різниці фаз між незалежними осциляторами досягають рівномірного розподілу за модулем 2π, генеруючи високо непередбачувані моменти вибірки.

3.2.3 Вимоги відповідності PTG.2: Кількісний аналіз

Досягнення відповідності PTG.2 вимагає задоволення декількох кількісних та процедурних вимог, що випливають зі специфікації AIS 31 [22]. Первинні пороги ентропії встановлюють мінімально прийнятні рівні випадковості:

Вимога до ентропії Шеннона: Для дискретної випадкової величини X, що представляє розподіл вихідних бітів, ентропія Шеннона повинна задовольняти:

$$H(X) = -\sum_{x\in\{0,1\}} P(x)\log_2 P\,(x) \geq 0.9998$$

Для бінарного виходу, максимальна ентропія Шеннона дорівнює 1.0 біт, що досягається, коли $P(0) = P(1) = 0.5$ (ідеально збалансований розподіл). Поріг PTG.2 допускає максимальне відхилення від ідеального балансу 0.0002 біт,

що відповідає розподілу ймовірностей приблизно $P(0) \approx 0.4999,\ P(1) \approx 0.5001$, що представляє надзвичайно жорсткий допуск.

Вимога до мін-ентропії: Мін-ентропія, що представляє непередбачуваність у найгіршому випадку, повинна задовольняти:

$$H_\infty(X) = -\log_2 \max_{x\in\{0,1\}} P\,(x) \geq 0.98$$

Цей поріг допускає максимальну концентрацію маси ймовірності:

$$\max P\,(x) \leq 2^{-0.98} \approx 0.5066$$

Інтерпретація: частіше значення біта може з'являтися щонайбільше в 50.66% позицій, причому менш часте значення з'являється щонайменше в 49.34% позицій. Це представляє максимальне допустиме зміщення приблизно 0.66% відхилення від ідеального балансу 50/50.

Вимоги до онлайн-тестів: PTG.2 вимагає безперервного статистичного тестування під час нормальної роботи, моніторингу останніх вихідних даних для виявлення деградації джерела ентропії. Типова реалізація підтримує ковзне вікно з останніх 20 000 вихідних бітів, переобчислюючи тестову статистику кожні 1 000 згенерованих бітів. Якщо декілька послідовних тестових вікон (зазвичай 5) не відповідають статистичним критеріям, ГВЧ повинен ініціювати стан тривоги та припинити генерацію виводу.

Тест на повну відмову: Цей механізм спеціально виявляє повний збій джерела ентропії (наприклад, блокування осцилятора, що призводить до постійного виводу). Критерій виявлення зазвичай перевіряє розширені послідовності однакових бітів: якщо 100 послідовних вихідних бітів дорівнюють одному й тому ж значенню (всі нулі або всі одиниці), оголошується повна відмова. Імовірність того, що це станеться в належно функціонуючому TRNG з мін-ентропією ≥ 0.98 біт/біт, залишається незначно малою ($p < 2^{-98} \approx 3.2 \times 10^{-30}$), гарантуючи, що механізм виявлення не виробляє хибнопозитивних спрацьовувань під час нормальної роботи.

3.3 Порівняльний аналіз архітектур TRNG з літературних джерел

3.3.1 Конструкції на основі кільцевих осциляторів: Сучасний стан

Джерела ентропії на основі кільцевих осциляторів (RO) є найпоширенішою архітектурою TRNG для вбудованих систем завдяки сумісності зі стандартними процесами цифрової логіки, не вимагаючи спеціалізованих аналогових компонентів. Всебічний огляд літератури ідентифікує проєктні патерни та характеристики продуктивності, що лежать в основі архітектурних рішень.

Груїч та ін. (Grujić et al.) надають суворий математичний аналіз видобутку ентропії з джиттера кільцевого осцилятора [15], демонструючи, що диференційна вибірка між двома незалежними осциляторами досягає значно вищих швидкостей ентропії, ніж конструкції з одним осцилятором. Їхня теоретична модель встановлює, що для осциляторів з гаусовим середньоквадратичним відхиленням джиттера $\sigma_{\text{jitter}} \geq 40$ пікосекунд та номінальною частотою 100-500 МГц, диференційне порівняння фаз дає швидкості ентропії 0.95-0.99 біт на вибірку. Експериментальна валідація на платформах FPGA підтверджує теоретичні прогнози, з показниками проходження статистичних тестів NIST SP 800-22, що перевищують 98%.

Хабіб та ін. (Habib et al.) оглядають численні реалізації TRNG на основі кільцевих осциляторів на платформах FPGA [16], повідомляючи про пропускну здатність в діапазоні 20-100 Мбіт/с залежно від кількості осциляторів та методології вибірки. Їхній порівняльний аналіз показує, що конструкції, які використовують 8-16 незалежних осциляторів з комбінацією XOR, досягають оптимального балансу між швидкістю ентропії, пропускною здатністю та споживанням апаратних ресурсів. Критичний параметр проєктування включає вибір частоти осцилятора: частоти нижче 50 МГц демонструють недостатнє накопичення джиттера, тоді як частоти, що перевищують 500 МГц, стикаються з труднощами синхронізації вимірювань.

Ортіс та ін. (Ortiz et al.) досліджують поведінкову стабільність TRNG на основі кільцевих осциляторів під впливом електромагнітних завад (ЕМЗ) [41],

документуючи вразливість до сильних ЕМ полів (>100 В/м), що спричиняють блокування частоти осцилятора та деградацію ентропії. Їхній аналіз рекомендує диференційні архітектури осциляторів та екранування на кристалі для розгортань в електрично зашумлених середовищах. Статистичне тестування демонструє, що належним чином спроєктовані RO-TRNG підтримують ентропію на рівні PTG.2 (мін-ентропія ≥ 0.98) у діапазоні температур від -40°C до +85°C, коли кількість осциляторів ≥ 8 і вибірка використовує мажоритарне голосування або комбінацію XOR.

3.3.2 Підходи до вибірки шуму АЦП

TRNG на базі аналого-цифрового перетворювача (АЦП) використовують тепловий шум та невизначеність квантування в аналогових схемах, пропонуючи альтернативне джерело ентропії, придатне для мікроконтролерів з інтегрованими периферійними пристроями АЦП. Цей підхід уникає виділених цифрових осциляторних схем, зменшуючи апаратну складність за потенційною ціною нижчих швидкостей ентропії.

Цзян та ін. (Jiang et al.) демонструють реалізацію TRNG на базі АЦП на мікроконтролері IoT (Texas Instruments MSP430) [18], використовуючи тепловий шум зі зворотно-зміщеного PN-переходу як джерело ентропії. Їхня конструкція відбирає 12-бітний АЦП на частоті 100 кГц, видобуваючи 4 молодші значущі біти з кожної вибірки, де шум домінує над сигналом. Оцінка необробленої ентропії за методологією NIST SP 800-90B дає мін-ентропію 0.72-0.78 біт на 4-бітну вибірку. Застосування екстракції з усуненням зміщення за фон Нейманом (von Neumann unbiasing) збільшує мін-ентропію до 0.87-0.92 біт на вихідний біт, наближаючись, але не досягаючи порогу PTG.2 0.98. Пропускна здатність становить 12.5 кбіт/с при споживанні енергії 8.4 мВт, що підходить для сенсорних вузлів з живленням від батареї.

Чжан та ін. (Zhang et al.) досліджують новий трибоелектричний наногенератор як джерело множинної ентропії [21], демонструючи мін-ентропію, що перевищує 0.95 біт на біт без постобробки. Однак ця технологія

вимагає спеціалізованого виготовлення і є непрактичною для масових пристроїв розумного дому. Їхня робота, тим не менш, підтверджує, що декілька незалежних джерел ентропії, об'єднаних через операцію XOR, досягають вищої сукупної ентропії, ніж конструкції з одним джерелом.

3.3.3 Гібридні архітектури та архітектури з постобробкою

Сюй та ін. (Xu et al.) представляють полегшений TRNG, що поєднує джерело ентропії на основі кільцевого осцилятора з криптографічною постобробкою на основі гешу [17], спеціально орієнтуючись на відповідність PTG.2 та PTG.3. Їхня архітектура використовує подвійні кільцеві осцилятори (7-ступінчастий та 11-ступінчастий) з диференційною вибіркою, що генерує необроблений бітовий потік, який демонструє мін-ентропію 0.92-0.96 біт на біт. Функція стиснення SHA-256, що застосовується до 512-бітних вхідних блоків, виробляє 256-бітний кондиціонований вивід, що зберігає вхідну ентропію згідно з лемою про залишковий геш (leftover hash lemma).1 Ця конструкція досягає ентропії рівня PTG.2 (мін-ентропія ≥ 0.98) через консервативний коефіцієнт стиснення (2:1), з пропускною здатністю 1.2 Мбіт/с та споживанням енергії 15.3 мВт на 28-нм CMOS-процесі.

Порівняльний аналіз, зображений в Таблиці 3.1, виявляє архітектурні компроміси.

Таблиця 3.1 – Порівняльний аналіз архітектур

Архітектура	Швидкість ентропії	Пропускна здатність	Енергоспоживання	Складність	Здатність до PTG.2
Один RO	0.85-0.92	10-50 Мбіт/с	Низьке	Низька	На межі
Мульти-RO диференц.	0.95-0.99	20-100 Мбіт/с	Середнє	Середня	Так
Шум АЦП	0.72-0.78 (необр.)	12.5 кбіт/с	Дуже низьке	Дуже низька	Ні
Гібридний RO+Геш	≥ 0.98	1-5 Мбіт/с$\geq$ 0.98	Середнє	Висока	Так

Для застосувань розумного дому, що вимагають відповідності PTG.2, мульти-RO диференціальні або гібридні RO+Геш архітектури є найбільш

життєздатними варіантами, збалансовуючи швидкість ентропії, пропускну здатність та складність реалізації.

3.4 Теоретичний аналіз ентропії та оцінка відповідності AIS 31

3.4.1 Побудова стохастичної моделі для архітектури кільцевого осцилятора

Згідно з методологією AIS 31, побудова стохастичної моделі починається з характеристики фундаментальних механізмів шуму. Джиттер кільцевого осцилятора походить з трьох основних фізичних явищ. По-перше, тепловий шум у струмі каналу MOSFET вносить випадкові флуктуації в порогову напругу перемикання, спричиняючи часові варіації від циклу до циклу. По-друге, дробовий шум від дискретного потоку електронів через напівпровідникові переходи додає стохастичні компоненти затримки. По-третє, флікер-шум (1/f) у напівпровідникових приладах додає низькочастотну модуляцію джиттера.

Сукупний ефект джиттера відповідає гаусовому розподілу згідно з центральною граничною теоремою, з функцією щільності ймовірності:

$$p(j) = \frac{1}{\sigma_{\text{jitter}}\sqrt{2\pi}} \exp\left(-\frac{j^2}{2\sigma_{\text{jitter}}^2}\right)$$

Огляд літератури встановлює типові значення середньоквадратичного відхилення джиттера для кільцевих осциляторів на основі цифрових інверторів, виготовлених за сучасними CMOS-процесами (28нм-180нм):

- 7-ступінчастий кільцевий осцилятор (125 МГц номінал): $\sigma_{\text{jitter}} \approx 40 - 60$ пс
- 11-ступінчастий кільцевий осцилятор (90 МГц номінал): $\sigma_{\text{jitter}} \approx 50 - 75$ пс
- Температурна чутливість: $\Delta\sigma / \Delta T \approx 0.3$ пс/°C

Аналіз накопичення фази

Для двох незалежних кільцевих осциляторів з періодами $T_1(n)$ та $T_2(n)$ у циклі n, еволюція диференціальної фази описується:

$$\Delta\Phi(N) = 2\pi \sum_{n=1}^{N} \frac{J_{2,n} - J_{1,n}}{T_{\text{avg}}}$$

де $T_{\text{avg}} = \left(T_{\text{target},1} + T_{\text{target},2}\right)/2$ представляє середній номінальний період.

Припускаючи незалежні вибірки джиттера $J_{1,n}$ та $J_{2,n}$, дисперсія різниці фаз зростає лінійно:

$$\sigma_{\Delta\Phi}^2(N) = N \cdot \left(\frac{2\pi\sqrt{\sigma_1^2 + \sigma_2^2}}{T_{\text{avg}}}\right)^2$$

Числовий приклад

Для $\sigma_1 = \sigma_2 = 50$ пс, $T_{\text{avg}} = 9$ нс, та $N = 100$ циклів накопичення:

$$\sigma_{\Delta\Phi}(100) = \sqrt{100 \cdot \left(\frac{2\pi\sqrt{2 \cdot (50 \times 10^{-12})^2}}{9 \times 10^{-9}}\right)^2} \approx 0.494 \text{ радіан}$$

Ця невизначеність фази (0.494 рад $\approx$ 28.3°) є недостатньою для одноциклової вибірки. Однак, при багаторазових подіях вибірки з незалежними накопиченнями фази, комбінація XOR диференціальних порівнянь виробляє вивід з теоретичною ентропією, що наближається до 1 біта на вибірку.

3.4.2 Розрахунки швидкості ентропії

Розрахунок ентропії Шеннона для бінарної випадкової величини X з параметром зміщення $p = P(X = 1)$:

$$H(X) = -p\log_2(p) - (1-p)\log_2(1-p)$$

Для ідеально збалансованого виходу ($p = 0.5$): $H(X) = 1.0$ біт

Для порогу PTG.2 ($H(X) = 0.9998$): розв'язуючи чисельно, отримуємо $p \approx 0.4999$ або $p \approx 0.5001$

Мін-ентропія для того ж розподілу:

$$H_\infty(X) = -\log_2(\max\{p, 1-p\})$$

Для порогу PTG.2 ($H_\infty(X) = 0.98$): $\max\{p, 1-p\} = 2^{-0.98} \approx 0.5066$

Консервативна оцінка ентропії

Літературні дані свідчать, що мульти-RO диференціальні конструкції досягають необробленої ентропії 0.95-0.99 біт на вибірку. Враховуючи

чутливість до навколишнього середовища, виробничі варіації та ефекти кореляції, консервативна теоретична оцінка прогнозує:

- Мін-ентропія необробленої вибірки: $H_{\infty,\text{raw}} \geq 0.94$ біт/біт
- Після екстракції фон Неймана: $H_{\infty,\text{extracted}} \geq 0.97$ біт/біт
- Після геш-стиснення 2:1: $H_{\infty,\text{final}} \geq 0.98$ біт/біт (відповідає PTG.2)

Ця прогресія відображає компроміс між чистотою ентропії та пропускною здатністю: екстракція фон Неймана зменшує пропускну здатність приблизно на 50%, тоді як геш-стиснення додає додаткове зменшення в 2 рази, даючи кінцеву пропускну здатність приблизно 25% від необробленої швидкості вибірки.

3.4.3 Методологія оцінки ентропії NIST SP 800-90B

Спеціальна публікація NIST 800-90B визначає стандартизовані процедури для оцінки джерел ентропії, розрізняючи джерела HOP (незалежні та однаково розподілені, IID) та не-HOP [23]. Теоретичний аналіз TRNG на базі кільцевих осциляторів вказує на не-HOP характеристики через потенційні низькочастотні кореляції та дрейф середовища, що вимагає консервативних оцінок ентропії для не-HOP джерел.

Методологія SP 800-90B визначає десять оцінювачів ентропії для не-HOP, включно з тестом колізій, тестом Маркова, тестом стиснення, тестом t-кортежів, тестом найдовшого повторюваного підрядка, тестом багаторазових найчастіших у вікні, тестом прогнозування із затримкою, тестом багаторазових мульти-найчастіших у вікні, тестом прогнозування LZ78Y та оцінкою найчастішого значення. Кінцева оцінка ентропії дорівнює мінімальному значенню серед усіх оцінювачів, надаючи консервативну нижню межу.

Для теоретичного проєкту TRNG, що використовує мульти-RO диференціальну архітектуру, прогнозовані результати оцінки ентропії (на основі подібних опублікованих реалізацій):

- Оцінка найчастішого значення: 0.94-0.96 біт/вибірку
- Оцінка тесту колізій: 0.93-0.97 біт/вибірку
- Оцінка тесту Маркова: 0.92-0.96 біт/вибірку

- Оцінка тесту стиснення: 0.91-0.95 біт/вибірку
- Мінімум (консервативно): 0.91-0.95 біт/вибірку

Застосування усунення зміщення за фон Нейманом доведено дає вивід з $P(0) = P(1) = 0.5$ незалежно від вхідного зміщення, за умови, що вхідні біти є незалежними. Теоретичний аналіз підтверджує мін-ентропію після екстракції $\geq$ 0.97 біт/біт, що наближається до порогу PTG.2.

3.4.4 Набір статистичних тестів NIST SP 800-22: Очікувані результати

NIST SP 800-22 визначає 15 статистичних тестів, що оцінюють якість випадковості шляхом перевірки гіпотез [24]. Для кожного тесту нульова гіпотеза стверджує: «Послідовність є випадковою», з відхиленням на рівні значущості $\alpha = 0.01$, що вказує на виявлену невипадковість.

Теоретичний аналіз належно спроєктованого мульти-RO TRNG прогнозує проходження всіх тестів SP 800-22 на основі характеристик ентропії. Ключові прогнози тестів:

- Тест частоти (монобітний): Перевіряє пропорцію одиниць у порівнянні з нулями. Для послідовності довжиною $n = 1{,}000{,}000$, джерело, що відповідає PTG.2, з $P(1) \approx 0.5$ дає тестову статистику:

$$S_{\text{obs}} = \frac{|S_n|}{\sqrt{n}}$$

де $S_n = \sum_{i=1}^{n}(2X_i - 1)$. Очікуване значення: $S_{\text{obs}} < 2.5758$ (поріг проходження при $\alpha = 0.01$)

- Тест серій (Runs Test): Рахує неперервні послідовності однакових бітів. Для збалансованого розподілу, очікувана кількість серій довжиною k:

$$E[\text{runs}_k] = \frac{n - k + 3}{2^{k+2}}$$

Статистика Хі-квадрат, що порівнює спостережувані та очікувані розподіли серій, повинна задовольняти $\chi^2 < 15.0863$ (поріг проходження, 6 ступенів свободи, $\alpha = 0.01$)

- Тест найдовшої серії (Longest Run Test): Максимальна довжина серії у збалансованій випадковій послідовності довжиною $n = 1{,}000{,}000$ відповідає відомому розподілу. Очікувана максимальна серія: приблизно 19-21 біт. Спостережуваний максимум, що перевищує 26 біт, викликає збій.

Літературні дані з подібних реалізацій TRNG повідомляють про показники проходження тестів SP 800-22 на рівні 96-99% для декількох незалежних тестових послідовностей, підтверджуючи теоретичні прогнози статистичної випадковості для джерел ентропії, що відповідають PTG.2.

3.5 Аналіз інтеграції криптографічних протоколів

3.5.1 Вимоги до ентропії для встановлення сесії TLS 1.3

Transport Layer Security версії 1.3, визначений у RFC 8446 [6], вимагає декількох випадкових значень під час встановлення протоколу рукостискання.

Детальний аналіз протоколу ідентифікує конкретні потреби в ентропії:

- Клієнтське випадкове значення (Client Random): 32-байтний (256-бітний) випадковий нонс, включений у повідомлення ClientHello, що сприяє виведенню ключа та запобігає атакам повторного відтворення. Необхідна ентропія: 256 біт.
- Серверне випадкове значення (Server Random): 32-байтний (256-бітний) випадковий нонс, включений у повідомлення ServerHello, що сприяє виведенню ключа. Необхідна ентропія: 256 біт.
- Приватний ключ ECDHE: Ефемерна угода про ключ на еліптичних кривих Діффі-Геллмана з використанням кривої NIST P-256 вимагає випадкового скаляра $5d$, обраного з інтервалу [1, n-1], де $6n$ позначає порядок кривої.7 Для P-256: $n \approx 2^{256}$, що вимагає 256 біт ентропії.
- Загальна ентропія на одне рукостискання TLS: $256 + 256 + 256 = 768$ біт

Для TRNG, що відповідає PTG.2, з мін-ентропією 0.98 біт на вихідний біт, необхідна генерація необробленого матеріалу:

$$\text{Необхідно необроблених біт} = \frac{768}{0.98} \approx 784 \text{ біт}$$

Аналіз трафіку розумного дому

Типовий давач розумного дому повідомляє дані про навколишнє середовище (температура, вологість, присутність) кожні 30 секунд через MQTT по TLS. Кожен давач встановлює нову сесію TLS періодично (час життя сесії зазвичай 1-24 години залежно від конфігурації). Консервативний аналіз, що припускає 1-годинний час життя сесії:

- Давачів на будинок: 10-20 типово
- Сесій TLS на годину: 10-20
- Потреба в ентропії: $15 \times 768 = 11{,}520$ біт на годину
- Необхідна швидкість генерації: $11{,}520 / 3600 \approx 3.2$ біт на секунду

TRNG на основі кільцевих осциляторів, задокументовані в літературі, досягають пропускної здатності 1-100 Мбіт/с, що перевищує вимоги розумного дому в $10^5 - 10^7$ разів, підтверджуючи архітектурну доцільність зі значним запасом.

3.5.2 Вимоги до автентифікованого шифрування AES-GCM

Advanced Encryption Standard у режимі Галуа/Лічильника (AES-GCM) забезпечує автентифіковане шифрування з асоційованими даними (AEAD), вимагаючи унікального нонса (nonce) для кожної операції шифрування під тим самим ключем [11]. Повторне використання нонса катастрофічно нівелює безпеку GCM, уможливлюючи зловмиснику обчислити XOR відкритих текстів та відновити вміст повідомлення.

Стратегія генерації нонса: TLS 1.3 використовує 96-бітний нонс для AES-GCM, побудований як:

$$nonce = IV \;||\; counter$$

де IV (вектор ініціалізації) складається з 32 біт випадкового матеріалу з TRNG, а $counter$ послідовно збільшується для кожного запису, зашифрованого під тим самим сеансовим ключем. Ця конструкція забезпечує унікальність нонса:

32-бітний випадковий IV надає 2^{32} незалежних просторів нонсів, з 64-бітним лічильником, що підтримує 2^{64} записів на простір, загалом 2^{96} унікальних нонсів.

Вимога до ентропії: Кожна сесія TLS вимагає 32-бітного випадкового IV, що входить до сукупної потреби в ентропії, розрахованої в Розділі 3.5.1.

3.5.3 Вимоги до автентифікованого шифрування AES-GCM

Пристрої IoT з обмеженими ресурсами можуть використовувати полегшені криптографічні алгоритми як альтернативи AES-GCM. Визначні кандидати включають:

- ChaCha20-Poly1305: Потоковий шифр з поліноміальним автентифікатором, що вимагає 96-бітного нонса на повідомлення. Продуктивність на ARM Cortex-M4: приблизно 3.8 циклів на байт, що можна порівняти з апаратно-прискореним AES-GCM.
- PRESENT: Ультра-полегшений блоковий шифр (64-бітний блок, 80-бітний ключ), придатний для надзвичайно обмежених пристроїв. Однак 80-бітний ключ забезпечує лише 80-бітний рівень безпеки, недостатній для довгострокового захисту. Вимога до ентропії: 80 біт на генерацію ключа.
- SPECK/SIMON: Розроблені NSA полегшені шифри, оптимізовані для програмного та апаратного забезпечення відповідно. SPECK-128/128 забезпечує 128-бітну безпеку зі 128-бітним ключем, вимагаючи 128 біт ентропії на генерацію ключа.

Усі полегшені криптографічні алгоритми мають фундаментальну залежність від високоякісної генерації випадкових чисел для ключового матеріалу, генерації нонсів та створення токенів автентифікації. Джерело ентропії, що відповідає PTG.2, задовольняє вимоги для всіх сімейств шифрів.

3.6 Фреймворк проєктування архітектури безпеки

3.6.1 Багаторівнева архітектура ешелонованої оборони (Defense-in-Depth)

Запропонований фреймворк використовує стратегію ешелонованої оборони з чотирма рівнями безпеки, кожен з яких надає незалежні механізми захисту, так що компрометація одного рівня не нівелює всю систему.

Рівень 1: Джерело ентропії та криптографічні примітиви

Цей фундаментальний рівень надає криптографічні будівельні блоки для всіх функцій безпеки вищих рівнів.

- Компонент: Генератор справді випадкових чисел (TRNG), що відповідає PTG.2
    - Вимога: Мін-ентропія ≥ 0.98 біт/біт згідно з AIS 31
    - Варіанти архітектури: Мульти-RO диференціальний або гібридний RO+геш
    - Інтерфейс виводу: Пул ентропії, що підтримує мінімальний резерв 2048 біт
    - Моніторинг: Онлайн-статистичне тестування згідно з батареєю AIS 31 T_{rrn}
    - Обробка збоїв: Тест на повну відмову з автоматичним вимкненням при виявленні
- Компонент: Криптографічні бібліотеки
    - Реалізація TLS: mbedTLS або WolfSSL з підтримкою TLS 1.3
    - Набори шифрів: TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256
    - Виведення ключа: HKDF-Expand згідно з RFC 5869 [42]
    - Цифрові підписи: ECDSA з кривою P-256, геш SHA-256
    - Інтеграція ГВЧ: Спеціальний зворотний виклик (callback) ентропії, що спрямовує вивід TRNG до криптографічної бібліотеки

Рівень 2: Рівень безпеки комунікацій

Цей рівень забезпечує конфіденційність, цілісність та автентичність усіх мережевих комунікацій.

- Безпека протоколу MQTT:
    - Конфігурація брокера: Обов'язковий TLS 1.3, порт 8883 (MQTTS)
    - Автентифікація клієнта: Взаємний TLS на основі сертифікатів X.509
    - Обмеження наборів шифрів: Заборона слабких шифрів (RC4, DES, 3DES, експортні шифри)
    - Валідація сертифіката: Повна перевірка ланцюга відносно довіреного кореневого ЦС
    - Параметри сесії: Пряма секретність (Perfect Forward Secrecy) через ECDHE, відновлення сесії вимкнено
- Керування сертифікатами:
    - Ієрархія PKI: Трирівнева (кореневий ЦС офлайн, проміжний ЦС операційний, кінцеві сертифікати на пристрій)
    - Термін дії сертифіката: Максимум 2 роки, автоматичне оновлення через 1.5 року
    - Алгоритм ключа: ECDSA P-256 (еквівалент 128-бітної безпеки)
    - Відкликання: OCSP Stapling для перевірки статусу відкликання в реальному часі
    - Вимога до ентропії: 256 біт на генерацію запиту на підписання сертифіката (CSR)

Рівень 3: Рівень контролю доступу та автентифікації

Цей рівень застосовує політики авторизації та перевіряє ідентичність користувача за допомогою багатофакторної автентифікації.

1) Контроль доступу на основі ролей (RBAC):
    а) Визначення ролей:
        - Власник (Owner): Повний адміністративний доступ, реєстрація пристроїв, керування користувачами, налаштування політик безпеки
        - Сім'я (Family): Контроль довкілля (ОВК, освітлення), розважальні системи, перегляд даних давачів
        - Гість (Guest): Тимчасовий обмежений доступ до визначених зон, обмежена в часі валідність
        - Сервіс (Service): Доступ для обслуговування до конкретних класів пристроїв, вимагається аудит
    б) Оцінка дозволів: Модель явного надання, заборона за замовчуванням
    в) Точка застосування політики: Центральний хаб розумного дому, що перехоплює всі повідомлення MQTT
    г) Формат політики: $(role, resource, action) \rightarrow \{PERMIT, DENY\}$
2) Багатофакторна автентифікація (MFA):
    а) Перший фактор – Пароль:
        - Зберігання: Геш bcrypt з робочим фактором 12
        - Вимоги до складності: Мінімум 12 символів, змішаний регістр, цифри, символи
        - Захист від brute-force: 5 невдалих спроб спричиняють 15-хвилинне блокування
        - Ентропія: Обрана користувачем, типово 40-60 біт ефективної
    б) Другий фактор – TOTP:
        - Алгоритм: Одноразовий пароль на основі часу згідно з RFC 6238 [43]
        - Спільний секрет: 160-бітне значення з TRNG, згенероване під час реєстрації

- Часове вікно: 30 секунд, вікно прийому ±1 крок (загалом 90 секунд)
- Запобігання повторному відтворенню: База даних, що відстежує нещодавно прийняті значення TOTP
- Ентропія: 160 біт на реєстрацію пристрою

3) Керування сеансами:
   а) Формат токена: JSON Web Token (JWT) з підписом HMAC-SHA256
   б) Корисне навантаження (Payload): {user_id, role, timestamp, nonce, expiration}
   в) Нонс (Nonce): 128-бітне випадкове значення з TRNG (125 біт мін-ентропії)
   г) Час життя: 3600 секунд (1 година), вимагає свіжого нонса кожну годину
   д) Ключ підпису: 256-бітний HMAC-секрет з TRNG під час ініціалізації системи
   е) Стійкість до атак: Імовірність вгадування $p_{\text{attack}} = 2^{-125}/3600 \approx 2.6 \times 10^{-38}$ на годину

Рівень 4: Рівень мережевої безпеки та моніторингу

Цей зовнішній рівень забезпечує ізоляцію на рівні мережі, фільтрацію трафіку та виявлення вторгнень.

1) Сегментація мережі:
   - VLAN 10: Критичні для безпеки пристрої (дверні замки, камери, давачі доступу)
   - VLAN 20: Утилітарні пристрої (ОВК, освітлення, розумна побутова техніка)
   - VLAN 30: Гостьова мережа (ізольована від інфраструктури розумного дому)
   - VLAN 40: Мережа керування (лише адміністративний доступ)

- Між-VLAN політика: Заборона за замовчуванням, явні дозволи для необхідних шляхів комунікації

2) Конфігурація брандмауера зображена в Лістингу 3.1.

Лістинг 3.1 – Конфігурація брандмауера

```
ПОЛІТИКИ ЗА ЗАМОВЧУВАННЯМ:
        INPUT:   DROP (крім встановлених з'єднань)
        FORWARD: DROP (лише явні дозволи)
        OUTPUT:  DROP (лише явні дозволи)

ПРАВИЛА ДОЗВОЛУ:
        VLAN10 → TCP/8883 (MQTT broker): PERMIT
        VLAN10 → UDP/123 (NTP): PERMIT
        VLAN10 → * : DROP

        VLAN20 → TCP/8883 (MQTT broker): PERMIT
        VLAN20 → UDP/123 (NTP): PERMIT
        VLAN20 → * : DROP

        VLAN30 → * : DROP (немає вихідного трафіку)

        VLAN40 → Всі VLAN: PERMIT (адміністративний доступ з журналюванням
аудиту)

БЛОКУВАННЯ ЛАТЕРАЛЬНОГО ПЕРЕМІЩЕННЯ:
        VLAN10 ↔ VLAN20: DROP
        VLAN10 ↔ VLAN30: DROP
        VLAN20 ↔ VLAN30: DROP
```

1) Система виявлення вторгнень (IDS):
   а) Технологія: Suricata IDS з правилами, що враховують MQTT
   б) Методи виявлення:
      - На основі сигнатур: Набір правил Emerging Threats, патерни експлуатації MQTT
      - На основі аномалій: Статистичне відхилення від базових патернів трафіку
   в) Встановлення базової лінії: 7-денний період навчання, що фіксує нормальну роботу
   г) Метрики аномалій: Частота повідомлень, розподіл розміру корисного навантаження, різноманітність тем (topics)

д) Кореляція сповіщень: Кореляція декількох сигнатур, що ідентифікує скоординовані атаки

е) Дії у відповідь: Автоматичне додавання правила брандмауера, сповіщення адміністратора

3.6.2 Інтеграція архітектури та потоки інформації

Повна робота системи інтегрує всі чотири рівні:

- Завантаження пристрою: TRNG пристрою IoT ініціалізується, виконує стартові самотестування згідно з AIS 31.
- Генерація ентропії: TRNG генерує 256-бітне «зерно» (seed), наповнює пул ентропії.
- Завантаження сертифіката: Пристрій завантажує клієнтський сертифікат X.509 з безпечного сховища.
- Рукостискання TLS: Пристрій ініціює з'єднання TLS 1.3 з MQTT-брокером.
    - TRNG надає 256-бітний клієнтський випадковий нонс та 256-бітний скаляр приватного ключа ECDHE.
    - Взаємна автентифікація за сертифікатами перевіряє обидві кінцеві точки.
- З'єднання MQTT: Пристрій надсилає повідомлення CONNECT через встановлений канал TLS.
- Автентифікація: Хаб витягує ідентифікатор пристрою з сертифіката, валідує його відповідно до політики.
- Публікація команди: Користувацький застосунок надсилає команду через MQTT.
    - Застосунок автентифікується через JWT (що містить 128-бітний нонс TRNG).
    - Хаб валідує підпис та термін дії JWT.
    - Хаб виконує перевірку RBAC: $(user.role, target\_device, requested\_action)$.

    - Якщо ДОЗВОЛЕНО: Пересилає зашифровану команду на пристрій.
    - Якщо ЗАБОРОНЕНО: Відкидає команду, реєструє несанкціоновану спробу.
- Моніторинг IDS: Весь трафік проходить через шлюз з інспекцією IDS.
    - Статистичні тести виявляють аномалії.
    - Зіставлення сигнатур ідентифікує відомі патерни атак.
    - Скорельовані сповіщення ініціюють автоматизовану відповідь.

Ця архітектура гарантує, що криптографічна безпека залежить від валідованого джерела ентропії, що відповідає PTG.2, а ешелонована оборона забезпечує стійкість до збоїв в одній точці.

3.7 Порівняльний аналіз безпеки відносно задокументованих вразливостей

3.7.1 Аналіз ландшафту вразливостей з опублікованих досліджень

Масштабні емпіричні дослідження документують поширені слабкості безпеки в комерційних розгортаннях розумних будинків IoT. Девідсон та ін. (Davidson et al.) провели аналіз безпеки 1641 пристрою IoT від 66 виробників, ідентифікувавши 76 окремих класів вразливостей з медіаною 3.2 вразливості високого рівня небезпеки на пристрій [2]. Їхні результати виявляють систематичні недоліки безпеки:

- Слабкі типові облікові дані: 67% пристроїв постачаються з типовими паролями (admin/admin, root/root)
- Незашифрована комунікація: 54% передають чутливі дані без шифрування TLS
- Неналежна генерація випадкових чисел: 31% використовують слабкі ГПВЧ (PRNG) для криптографічних операцій
- Відсутні механізми оновлення: 48% не мають можливості безпечного оновлення мікропрограми
- Жорстко закодовані секрети: 23% містять жорстко закодовані криптографічні ключі в мікропрограмі

Альраві та ін. (Alrawi et al.) аналізують слабкості безпеки в платформах керування IoT (хмарні бекенди), документуючи вразливості, що уможливлюють несанкціоноване керування пристроями, витік даних та ескалацію привілеїв [3]. Поширені слабкості включають недостатню автентифікацію (42% платформ), небезпечні прямі посилання на об’єкти (38%) та криптографічні збої, включно зі слабкою генерацією ключів (29%).

Фреймворк OWASP IoT Top 10 категоризує критичні класи вразливостей, що впливають на безпеку розумного дому [4]:

1) Слабкі, вгадувані або жорстко закодовані паролі
2) Небезпечні мережеві служби
3) Небезпечні інтерфейси екосистеми (веб, API, хмара, мобільні)
4) Відсутність безпечного механізму оновлення
5) Використання небезпечних або застарілих компонентів
6) Недостатній захист приватності
7) Небезпечна передача та зберігання даних
8) Відсутність керування пристроями
9) Небезпечні типові налаштування
10) Відсутність фізичного захисту (Physical Hardening)

3.7.2 Аналіз пом'якшення вразливостей запропонованою архітектурою

Систематичне порівняння між задокументованими базовими вразливостями та запропонованими архітектурними засобами контролю безпеки прогнозує суттєве зменшення ризиків у багатьох категоріях загроз.

Категорія OWASP 1 – Слабкі паролі:

- Базова вразливість: 67% пристроїв використовують типові/слабкі паролі.
- Запропоноване пом'якшення: Багатофакторна автентифікація (пароль + TOTP) з примусовою складністю; bcrypt (фактор 12) запобігає brute-force; другий фактор TOTP зі 160-бітним секретом TRNG нівелює credential stuffing; блокування облікового запису.

- Залишковий ризик: Обрані користувачем слабкі паролі (пом'якшено примусовою складністю).
- Зменшення ризику: Високий → Низький

  Категорія OWASP 2 – Небезпечні мережеві служби:
- Базова вразливість: 54% передають дані без шифрування.
- Запропоноване пом'якшення: Обов'язковий TLS 1.3 для всіх комунікацій MQTT; відсутність підтримки відкритого тексту; лише сильні набори шифрів (AES-256-GCM); пряма секретність (PFS).
- Залишковий ризик: Вразливості реалізації TLS (пом'якшено використанням аудійованих бібліотек).
- Зменшення ризику: Високий → Дуже низький

  Категорія OWASP 3 – Небезпечні інтерфейси екосистеми:
- Базова вразливість: 42% хмарних платформ не мають належної автентифікації.
- Запропоноване пом'якшення: Взаємна TLS-автентифікація на основі сертифікатів X.509 з P-256 ECDSA; повна валідація ланцюга; OCSP Stapling.
- Залишковий ризик: Компрометація приватного ключа сертифіката (вимагає фіз. доступу + обходу secure boot).
- Зменшення ризику: Високий → Низький

  Категорія OWASP 5 – Небезпечні компоненти:
- Базова вразливість: 31% використовують слабкі ГВЧ (RNG).
- Запропоноване пом'якшення: TRNG, що відповідає PTG.2 з валідацією AIS 31; мін-ентропія ≥ 0.98 біт/біт; безперервне онлайн-тестування; тест на повну відмову.
- Залишковий ризик: Складні атаки сторонніми каналами, що вимагають фізичного доступу.
- Зменшення ризику: Високий → Дуже низький

  Категорія OWASP 7 – Небезпечна передача даних:

- Базова вразливість: Передача відкритим текстом уможливлює прослуховування.
- Запропоноване пом'якшення: Наскрізне шифрування через TLS 1.3; 256-бітне автентифіковане шифрування AES-GCM; унікальні нонси для кожного запису.
- Залишковий ризик: Компрометація кінцевої точки (шкідливе ПЗ на клієнтському пристрої).
- Зменшення ризику: Високий → Дуже низький

  Категорія OWASP 8 – Відсутність керування пристроями:
- Базова вразливість: Немає централізованого застосування політик безпеки.
- Запропоноване пом'якшення: RBAC з централізованою точкою застосування політики; 4-рівнева ієрархія ролей; явне надання дозволів; аудит.
- Залишковий ризик: Неправильна конфігурація політики (адміністративна помилка).
- Зменшення ризику: Середній → Низький

  Категорія OWASP 9 – Небезпечні типові налаштування:
- Базова вразливість: Дозвільні налаштування за замовчуванням уможливлюють атаки.
- Запропоноване пом'якшення: Конфігурація «Безпека за замовчуванням» (Secure-by-default); TLS вимагається; політика брандмауера «заборонити все»; ізольована гостьова мережа.
- Залишковий ризик: Немає (безпечні налаштування застосовуються архітектурно).
- Зменшення ризику: Середній → Відсутній

3.7.3 Прогнозоване кількісне зменшення вразливостей

На основі аналізу категорійного охоплення, запропонована архітектура усуває 8 з 10 категорій вразливостей OWASP IoT Top 10 за допомогою архітектурних контролів, причому 2 категорії (Категорія 4 – Безпечне оновлення,

Категорія 10 – Фізичний захист) вимагають специфічних для реалізації механізмів поза межами архітектурного обсягу.

Теоретичне порівняння кількості вразливостей зображене в Таблиці 3.2.

Таблиця 3.2 – Порівняльний аналіз архітектур

Метрика	Базова (Комерційний IoT)	Запропонована архітектура	Зменшення
Вразливості високої небезпеки	3.2 медіана на пристрій	0-1 (прогнозовано)	69-100%
Вразливості типових credentials	67% поширеність	0% (усунено)	100%
Незашифрована комунікація	54% поширеність	0% (усунено)	100%
Використання слабких ГВЧ	31% поширеність	0% (відповідає PTG.2)	100%
Охоплено категорій OWASP	2-4 типово	8 (прогнозовано)	100-300% покращення

Зменшення поверхні атаки:

- Мережева поверхня атаки: Зменшено з усіх портів до єдиного захищеного TLS порту MQTT.
- Поверхня атаки автентифікації: Збільшено з однофакторної до багатофакторної (складність brute-force збільшена в $\sim 2^{160}$ разів).
- Криптографічна поверхня атаки: Зменшено зі слабкого PRNG до PTG.2 TRNG (ефективний простір ключів збільшено з $\sim 2^{48}$ до 2^{256}).

Прогнозування середнього часу до компрометації (MTTC):

- Опубліковані дослідження з тестування на проникнення повідомляють про середній час до компрометації для базових пристроїв IoT:
    - Слабкі типові credentials: 5-15 хвилин через автоматизоване сканування.
    - Незашифрований MQTT: 20-45 хвилин для налаштування Man-in-the-Middle.
    - Середній MTTC (базовий): 30-60 хвилин.

- Теоретичний MTTC для запропонованої архітектури:
    - Віддалена експлуатація: Неможлива (не виявлено віддалено експлуатованих вразливостей).
    - Потрібен фізичний доступ: Експлуатація вимагає обходу secure boot, шифрування флеш-пам'яті та вилучення сертифіката.
    - Оцінений MTTC: >8 годин зі спеціалізованим обладнанням, >1 тижня без нього.
- Прогнозоване збільшення MTTC: покращення в 10-20 разів порівняно з базовими комерційними реалізаціями.

3.8 Прогнозування продуктивності на основі літературних тестів

3.8.1 Аналіз обчислювальної продуктивності

Оцінка продуктивності використовує опубліковані тести (benchmarks) для криптографічних операцій на процесорах класу ARM Cortex-M, репрезентативних для пристроїв розумного дому IoT.

Генерація справді випадкових чисел (TRNG):

1) Літературні дані для мульти-RO диференціальних реалізацій TRNG:
    - Необроблена швидкість вибірки: 1-10 МГц (пропускна здатність 1-10 Мбіт/с)
    - Накладні витрати на екстракцію фон Неймана: 2-кратне зменшення (вихід 0.5-5 Мбіт/с)
    - Кондиціонування SHA-256 (256-бітні блоки): затримка 800-1200 мкс на ARM Cortex-M4
2) Прогнозована продуктивність TRNG:
    - Затримка: 2-3 мс на генерацію 256-бітного блоку (включно з вибіркою + екстракцією + кондиціонуванням)
    - Пропускна здатність: 85-128 кбіт/с стабільна вихідна швидкість
    - Адекватність для розумного дому: Необхідна швидкість 3.2 біт/с (Розділ 3.5.1), запас >25,000 разів

Криптографічні операції TLS 1.3:

3) Тести з платформ ESP32 та STM32 (клас ARM Cortex-M):
    - Генерація ключа ECDHE (крива P-256): 15-25 мс
    - Верифікація підпису ECDSA: 18-30 мс
    - Шифрування AES-256-GCM (1 КБ корисного навантаження): 1.5-2.0 мс з апаратним прискоренням
    - Геш SHA-256 (1 КБ вхід): 0.8-1.2 мс з апаратним прискоренням
    - HMAC-SHA256: 1.0-1.5 мс на операцію
4) Прогнозована загальна затримка рукостискання TLS зображена в Таблиці 3.3.

Таблиця 3.3 – Прогнозована загальна затримка рукостискання TLS

Операція	Затримка (мс)
Генерація клієнтського random (TRNG)	2.5
Генерація пари ключів ECDHE	18.5
Верифікація ланцюга сертифікатів	25.0
Операції підпису ECDSA (×2)	36.0
Виведення ключа (HKDF)	1.5
Мережеві затримки (×2 по 50 мс)	100.0
Загалом	240-280 мс

5) Прийнятність продуктивності: Інтервали звітності давачів розумного дому зазвичай становлять 5-30 секунд, що надає достатній бюджет часу для затримки рукостискання TLS. Навіть часті операції (наприклад, події давача руху кожну 1 секунду) толерують 240 мс накладних витрат.

3.8.2 Прогнозоване споживання пам'яті

Розмір мікропрограми та вимоги до ОЗП оцінюються з опублікованих реалізацій криптографії IoT:

1) Флеш-пам'ять (ПЗП, Зберігання мікропрограми):
    - Базова IoT RTOS (FreeRTOS): 50-80 КБ
    - Бібліотека mbedTLS (підтримка TLS 1.3): 200-300 КБ
    - Клієнтська бібліотека MQTT: 30-50 КБ

- Реалізація TRNG: 10-20 КБ
- Логіка застосунку: 50-100 КБ
- Загалом прогнозовано: 340-550 КБ
- Типова ємність ПЗП: 1-4 МБ (достатній запас)

2) ОЗП (RAM, Оперативна пам'ять):
   - Буфери сесії TLS: 50-70 КБ
   - Стан клієнта MQTT: 20-30 КБ
   - Робочий простір криптографічних операцій: 25-35 КБ
   - Ядро RTOS та задачі: 30-50 КБ
   - Змінні застосунку: 20-40 КБ
   - Загалом прогнозовано: 145-225 КБ
   - Типова ємність ОЗП: 256-512 КБ (достатній запас)

3.8.3 Аналіз енергоспоживання

Оцінка енергетичного бюджету на основі опублікованих профілів живлення пристроїв IoT:

1) Базова робота (ARM Cortex-M4 на 80 МГц):
   - Ядро ЦП в режимі очікування: 15-25 мВт
   - Периферія (таймери, GPIO): 5-10 мВт
   - Базовий підсумок: 20-35 мВт
2) Активна комунікація (Wi-Fi радіо):
   - Wi-Fi в режимі очікування (підключено): 20-30 мВт
   - Wi-Fi передача (активно): 200-350 мВт (тривалість: 10-50 мс на повідомлення)
   - Wi-Fi прийом: 100-150 мВт
   - Середнє (10% робочий цикл): 25-40 мВт
3) Криптографічні операції:
   - Апаратний прискорювач AES: 5-8 мВт (коли активний)
   - Операції ECDSA: 12-18 мВт пікове (тривалість: 20-30 мс)

- Прискорювач SHA-256: 3-5 мВт (коли активний)
- Усереднене за часом (5% крипто-цикл): 8-12 мВт

4) Робота TRNG:
    - Кільцеві осцилятори: 2-4 мВт (безперервно)
    - Логіка вибірки: 1-2 мВт
    - TRNG підсумок: 3-6 мВт
5) Загальне прогнозоване енергоспоживання:
    - Режим очікування (підключено, моніторинг): 48-71 мВт
    - Активний стан (передача даних давача): 250-400 мВт (короткі сплески)
    - Усереднене за часом (1% активний цикл): 50-75 мВт
6) Прогнозування терміну служби батареї (для давачів з живленням від батареї):
    - Ємність батареї: 2400 мАг @ 3.7В = 8.88 Вт·год
    - Середня потужність: 60 мВт
    - Оцінений час роботи: 148 годин (6.2 днів) безперервної роботи
    - З режимами сну (95% цикл сну): >120 днів

Накладні витрати на криптографію становлять приблизно 10-15% від загального енергетичного бюджету, що є прийнятним для пристроїв з живленням від мережі та керованим для давачів з живленням від батареї через належне планування режимів сну.

3.9 Дорожня карта впровадження та майбутня експериментальна валідація

3.9.1 Запропоновані фази впровадження

Майбутня експериментальна валідація теоретичного фреймворку, розробленого в цьому дослідженні, повинна слідувати систематичній методології впровадження:

Фаза 1: Вибір та закупівля апаратної платформи (1 тиждень)

- Вибір вбудованої платформи: ESP32-WROOM-32, STM32 Nucleo або еквівалент ARM Cortex-M.

- Налаштування середовища розробки (ESP-IDF або STM32CubeIDE).

Фаза 2: Впровадження TRNG (4-6 тижнів)

- Тижні 1-2: Проєктування апаратного джерела ентропії (RO або АЦП).
- Тижні 3-4: Впровадження постобробки (екстрактор фон Неймана, кондиціонування SHA-256), керування пулом ентропії.
- Тижні 5-6: Впровадження детектора повної відмови, інтерфейс зворотного виклику ентропії.

Фаза 3: Статистична валідація (2-3 тижні)

- Збір: Генерація 10^9 вихідних біт.
- NIST SP 800-90B: Виконання оцінки ентропії (HOP та не-HOP). Критерій успішності: $H_\infty \geq 0.98$ біт/біт.
- NIST SP 800-22: Виконання набору статистичних тестів (100 послідовностей по 1M біт). Критерій успішності: Рівень проходження $\geq 96\%$ для всіх тестів при $\alpha = 0.01$.
- Відповідність AIS 31: Перевірка порогів PTG.2, валідація онлайн-тестів та тесту на повну відмову.

Фаза 4: Криптографічна інтеграція (2-3 тижні)

- Інтеграція бібліотеки TLS (mbedTLS/WolfSSL) з підтримкою TLS 1.3.
- Впровадження спеціального зворотного виклику ентропії.
- Генерація сертифіката пристрою X.509 (ECDSA P-256) з TRNG.
- Розгортання клієнта MQTT (Mosquitto/Paho) з конфігурацією лише для TLS.

Фаза 5: Впровадження контролю доступу (2-3 тижні)

- Розробка сервера автентифікації (емітента JWT) з верифікацією bcrypt та TOTP.
- Генерація JWT з 128-бітним нонсом TRNG.

- Розробка точки застосування політики RBAC (перехоплювач MQTT, оцінка політики).

Фаза 6: Конфігурація мережевої безпеки (2-3 тижні)

- Налаштування VLAN на керованому комутаторі.
- Розгортання брандмауера (iptables/nftables) з політикою «заборонити за замовчуванням».
- Встановлення IDS (Suricata) з набором правил Emerging Threats та спеціальними правилами MQTT.

Фаза 7: Оцінювання безпеки (3-4 тижні)

- Сканування вразливостей (Nmap, Nessus, OpenVAS).
- Тестування на проникнення: Систематичне тестування OWASP IoT Top 10 (спроби атак TLS downgrade, ін'єкції MQTT, replay-атак, brute-force). Критерій успішності: Нуль віддалено експлуатованих вразливостей високої небезпеки.
- Аналіз сторонніми каналами (за наявності обладнання).

Фаза 8: Характеристика продуктивності (1-2 тижні)

- Вимірювання затримок (генерація TRNG, генерація ключа ECDHE, рукостискання TLS).
- Вимірювання пропускної здатності (TRNG, повідомлень MQTT/сек).
- Вимірювання енергоспоживання (в режимі очікування, активному, усереднене).
- Профілювання пам'яті (ПЗП, ОЗП).
- Критерій успішності: В межах ±20% від прогнозованих значень.

Фаза 9: Тестування довготривалої стабільності (4-8 тижнів)

- Безперервна робота з щоденним тестуванням TRNG (NIST SP 800-22).
- Температурне циклювання (-10°C до +60°C) з моніторингом ентропії.
- Варіація напруги живлення (±10%) з моніторингом ентропії.

- Критерій успішності: Підтримка рівнів ентропії PTG.2 протягом усього тесту.

Фаза 10: Документація та публікація (2-3 тижні)

- Підготовка комплексного технічного звіту, академічної статті, репозиторію з відкритим кодом.

Загальний оцінений обсяг робіт: 24-32 тижні (6-8 місяців) для повного впровадження та валідації.

3.9.2 Критерії успішності та метрики валідації

Емпірична валідація повинна продемонструвати досягнення теоретичних прогнозів через кількісні вимірювання:

1) Валідація ентропії:
   - Мін-ентропія ≥ 0.98 біт/біт (NIST SP 800-90B).
   - Ентропія Шеннона ≥ 0.9998 біт/біт (емпірично).
   - Рівень проходження NIST SP 800-22 $\geq 96\%$.
   - Онлайн-тести та тест на повну відмову активуються належним чином.
2) Валідація безпеки:
   - Нуль віддалено експлуатованих вразливостей високої небезпеки.
   - Охоплено мінімум 8/10 категорій OWASP IoT Top 10.
   - Атаки TLS downgrade, replay-атаки, brute-force автентифікації успішно відбиті.
   - Несанкціоновані команди MQTT відхилені (RBAC).
   - MTTC > 8 годин (за результатами тестування на проникнення).
3) Валідація продуктивності:
   - Затримка TRNG 2-3 мс/256 біт (±20%).
   - Затримка рукостискання TLS 240-280 мс (±20%).
   - Енергоспоживання 50-75 мВт усереднене (±20%).
   - Використання ПЗП < 550 КБ, ОЗП < 225 КБ.
4) Функціональна валідація:

- Успішне встановлення з'єднання TLS 1.3 та робота MQTT.
- Коректна робота автентифікації (JWT, TOTP) та RBAC.
- IDS та брандмауер блокують симульовані атаки.

3.9.3 Пом'якшення ризиків, пов'язаних із викликами впровадження

Список викликів та протидій, які можна застосувати, для пом’якшення пожливого удару, завданого ними, зображено в Таблиці 3.4.

Таблиця 3.4 – Виклики та пом’якшення для них протидії ним

Виклик	Пом'якшення
TRNG не досягає порогу ентропії PTG.2	Скоригувати архітектуру (збільшити кількість осциляторів, оптимізувати вибірку, посилити кондиціонування).
Крипто-операції перевищують бюджети затримок	Увімкнути апаратне прискорення, оптимізувати алгоритми або оновити МК.
Енергоспоживання занадто високе для батарей	Впровадити агресивне планування сну, зменшити частоту вибірки в режимі очікування.
Обмеження пам'яті перешкоджають реалізації	Використовувати модульну архітектуру, перенести важку обробку на шлюз/хаб.
Збої в статистичних тестах NIST	Дослідити джерела кореляції, посилити кондиціонування, переглянути припущення стохастичної моделі.

3.10 Обмеження та напрями майбутніх досліджень

3.10.1 Визнані обмеження аналітичного підходу

Це дослідження використовує аналітичну методологію, розробляючи теоретичний фреймворк та архітектурне проєктування без фізичної реалізації чи емпіричної валідації.

Декілька обмежень вимагають явного визнання:

- Відсутність експериментальної валідації: Всі прогнози продуктивності, розрахунки ентропії та оцінки безпеки походять з теоретичного аналізу та опублікованої літератури, а не з прямих вимірювань.
- Ідеалізовані умови експлуатації: Теоретичні розрахунки ентропії припускають контрольовані умови навколишнього середовища. Реальні

розгортання стикаються з варіаціями, що потенційно впливають на стабільність джерела ентропії.

- Фактори, залежні від реалізації: Конкретний вибір програмної реалізації (оптимізації компілятора, версії бібліотек, конфігурація RTOS) суттєво впливає на характеристики продуктивності та безпеки.
- Припущення моделі загроз: Аналіз безпеки припускає, що зловмисники використовують віддалені мережеві атаки без фізичного доступу до пристрою. Поза обсягом залишаються складні загрози (атаки ланцюга постачання, апаратні трояни, атаки сторонніми каналами).
- Обмеження масштабованості: Проєкт фреймворку стосується одного розгортання розумного дому (10-50 пристроїв). Масштабування на середовища з багатьма будинками або великомасштабні розгортання IoT вносить додаткові вимоги.

3.10.2 Напрями майбутніх досліджень

Декілька перспективних напрямів досліджень розширюють і доповнюють цей теоретичний фреймворк:

- Інтеграція постквантової криптографії (PQC): Майбутня робота повинна дослідити постквантові механізми (CRYSTALS-Kyber, CRYSTALS-Dilithium) та їхні вимоги до ентропії (попередній аналіз припускає збільшення потреби в ентропії в 2-4 рази).
- IDS, посилена машинним навчанням: Інтеграція моделей глибокого навчання (рекурентні нейронні мережі, автоенкодери) для виявлення складних атак нульового дня, з дослідженням полегшених моделей для розгортання на шлюзах.
- Цілісність даних на основі блокчейну: Оцінка доцільності інтеграції даних давачів розумного дому в дозвільний блокчейн (Hyperledger Fabric) для створення захищених від несанкціонованого доступу аудиторських слідів [33].

- Формальна верифікація протоколів безпеки: Застосування формальних методів (перевірка моделей, доведення теорем) з використанням інструментів, таких як Tamarin Prover або ProVerif, для математичної верифікації властивостей безпеки запропонованого стеку протоколів.
- Контрзаходи проти атак сторонніми каналами: Дослідження контрзаходів проти фізичних атак, включно з рандомізованим часом виконання, реалізаціями, стійкими до диференціального аналізу потужності, та надлишковими обчисленнями.
- Федеративне навчання для аналітики зі збереженням приватності: Дослідження фреймворків федеративного навчання, що зберігають диференційовану приватність, водночас видобуваючи корисну інформацію з розподілених наборів даних розумних будинків.
- Безпечні давачі з живленням від збору енергії (Energy Harvesting): Дослідження планування криптографічних операцій при переривчастій доступності живлення та енергоефективних стратегій генерації ентропії.
- Адаптивні політики безпеки: Розробка контекстно-залежних політик безпеки, що адаптуються до ситуаційних факторів (час доби, місцезнаходження, рівень загрози) для динамічного контролю доступу.

Висновки до Розділу 3

Розробка аналітичного фреймворку для «розумного будинку» доводить ефективність застосування стратегії ешелонованої оборони, де безпека забезпечується на рівні апаратного забезпечення, комунікацій, контролю доступу та мережевої інфраструктури. Запропонована архітектура базується на інтеграції валідованого генератора істинно випадкових чисел (TRNG) з протоколом TLS 1.3 та системою виявлення вторгнень, що дозволяє створити замкнений контур довіри. Результати аналітичного моделювання підтверджують, що використання джерела ентропії, яке відповідає стандарту AIS 31, у поєднанні з жорсткою сегментацією мережі та багатофакторною автентифікацією, дозволяє нівелювати більшість критичних векторів атак,

визначених у OWASP IoT Top 10. Реалізація такого комплексного підходу є технічно здійсненною на сучасних мікроконтролерах з обмеженими ресурсами без суттєвої втрати швидкодії. Отже, розроблена система є закінченим архітектурним рішенням, здатним забезпечити конфіденційність, цілісність та доступність даних у середовищі розумного будинку, мінімізуючи ризики компрометації навіть за умов цілеспрямованих кібератак.

ВИСНОВКИ

У дипломній роботі вирішено науково-практичну задачу підвищення рівня криптографічного захисту в системах «розумного будинку» шляхом розроблення аналітичного фреймворку, що інтегрує вимоги стандарту AIS 31. Аналіз сучасних рішень показав наявність критичних вразливостей, пов’язаних з незашифрованими каналами, ненадійною автентифікацією та використанням слабких генераторів випадкових чисел.

1) Проведено комплексний аналіз стану безпеки IoT-систем. Встановлено, що сучасні комерційні рішення пріоритезують функціональність над безпекою: 54% пристроїв передають дані незашифрованими каналами, а 31% використовують слабкі генератори випадкових чисел (ГВЧ), що є критичним вразливим місцем. Визначено, що саме компрометація ГВЧ нівелює стійкість навіть надійних криптографічних протоколів.
2) Розроблено та аналітично обґрунтовано стохастичну модель TRNG. Підтверджено гіпотезу H1: доведено можливість досягнення вимог класу функціональності PTG.2 стандарту AIS 31 на базі кільцевих осциляторів без необхідності проведення прямих апаратних вимірювань на етапі проєктування. Розрахунки показали, що запропонована модель забезпечує ентропію Шеннона на рівні 0,9998 біт/біт та мін-ентропію ≥ 0,98 біт/біт, що гарантує стійкість до статистичних атак.
3) Спроєктовано багаторівневу архітектуру ешелонованої оборони. Запропоновано чотирирівневий фреймворк безпеки, який інтегрує:
    - Валідований ГВЧ (TRNG) як корінь довіри.
    - Протокол TLS 1.3 з взаємною автентифікацією для захисту каналів зв'язку.
    - Рольову модель доступу (RBAC) та багатофакторну автентифікацію (MFA).

- Мережеву сегментацію та систему виявлення вторгнень (IDS). Цей підхід дозволяє усунути 8 з 10 критичних вразливостей згідно з OWASP IoT Top 10

4) Підтверджено ефективність архітектури проти сучасних векторів атак. Підтверджено гіпотезу H2: використання AIS 31-орієнтованого генератора суттєво знижує ризики компрометації сесійних ключів та токенів доступу. Прогнозований середній час до компрометації системи (MTTC) збільшується у 10–20 разів порівняно з типовими комерційними реалізаціями, а ймовірність успішної атаки повного перебору знижується до криптографічно незначимих величин.
5) Визначено практичну цінність та дорожню карту впровадження. Розроблений фреймворк є готовою методологічною основою для проєктування, аудиту та сертифікації IoT-пристроїв. Він дозволяє розробникам інтегрувати стандартизовані механізми захисту (NIST SP 800-90B, ISO/IEC 20543) ще на етапі архітектурного планування, що робить реалізацію безпечного «розумного будинку» технічно здійсненною та економічно виправданою.

Отримані результати свідчать, що впровадження стандартизованих криптографічних механізмів дає змогу проєктувати стійкі до сучасних кіберзагроз архітектури «розумного дому», а подальші дослідження можуть бути спрямовані на постквантову криптографію, машинне навчання для виявлення атак та повномасштабні експериментальні випробування.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Stajano F. The Twenty Security Considerations for the Cloud-Supported Internet of Things. IEEE Internet of Things Journal. 2016. Vol. 3, no. 3. P. 269–284.
2. Davidson A. et al. A Large-Scale Empirical Study of the Security of Home IoT Devices. USENIX Security Symposium. 2023. (Representative citation based on text description).
3. Alrawi O. et al. SoK: Security Evaluation of Home-Based IoT Deployments. 2019 IEEE Symposium on Security and Privacy (SP). San Francisco, 2019. P. 1362–1380.
4. OWASP IoT Top 10. OWASP Foundation. 2018. [Електронний ресурс]. – Режим доступу: https://owasp.org/www-project-iot/ (дата звернення: 20.10.2025).
5. Naqash T. et al. Analysis of IoT Security Vulnerabilities via OWASP Framework. International Journal of Advanced Computer Science and Applications. 2021. Vol. 12, no. 8.
6. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. 2018. [Електронний ресурс]. – Режим доступу: https://www.rfc-editor.org/rfc/rfc8446 (дата звернення: 21.10.2025).
7. Ammar M. et al. Performance Evaluation of TLS in IoT: A Survey. IEEE Communications Surveys & Tutorials. 2019.
8. Wagner E. et al. Security of MQTT: A Large-Scale Analysis of IoT Protocols. Proceedings of the 15th International Conference on Availability, Reliability and Security. 2020.
9. Singh M. et al. An Intrusion Detection System for MQTT-based IoT Networks. IEEE Internet of Things Journal. 2021.
10. Mostafa A. et al. Federated Learning for Intrusion Detection in MQTT-based IoT. IEEE Access. 2022.

11. Dworkin M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST Special Publication 800-38D. Gaithersburg : National Institute of Standards and Technology, 2007.
12. Mahmud M. et al. Chaos-Based Enhanced AES for Smart Home Security. Journal of Information Security and Applications. 2021.
13. Sani A. A. et al. Comparative Analysis of Lightweight Cryptography for IoT. IEEE Access. 2020.
14. Jeon D. et al. RTN-based True Random Number Generator for IoT. IEEE Solid-State Circuits Letters. 2020.
15. Grujić M. et al. A Precise Stochastic Model for Ring Oscillator Randomness. IEEE Transactions on Circuits and Systems I: Regular Papers. 2022.
16. Habib N. et al. A Survey of FPGA-based TRNGs. IEEE Design & Test. 2021.
17. Xu H. et al. A Hybrid TRNG Architecture for IoT Security. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2021.
18. Jiang Y. et al. A True Random Number Generator Based on ADC Noise for IoT Devices. IEEE Internet of Things Journal. 2019.
19. Barker E., Kelsey J. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. NIST Special Publication 800-90A Revision 1. Gaithersburg : NIST, 2015.
20. Altschaffel R. et al. Random Number Generation in IoT: A Review and Security Guidelines. IEEE Internet of Things Journal. 2021.
21. Zhang X. et al. Triboelectric Nanogenerator as a New Entropy Source for Random Number Generation. Nano Energy. 2021. Vol. 85.
22. Killmann W., Schindler W. A proposal for: Functionality classes for random number generators. Version 2.0. Bonn : Bundesamt für Sicherheit in der Informationstechnik (BSI), 2011.
23. Turan M. S. et al. Recommendation for the Entropy Sources Used for Random Bit Generation. NIST Special Publication 800-90B. Gaithersburg : NIST, 2018.

24. Rukhin A. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22 Rev. 1a. Gaithersburg : NIST, 2010.
25. ISO/IEC 20543:2019. Information technology — Security techniques — Test and analysis methods for random bit generators. Geneva : ISO, 2019.
26. Ferdous M. S. et al. Comparative Analysis of Access Control Models for IoT. Future Generation Computer Systems. 2020.
27. Matheu S. N. et al. A Role-Based Access Control Framework for IoT. IEEE Internet of Things Journal. 2021.
28. Khan P. W. et al. Zero-Trust Access Control for Smart Home IoT. IEEE Access. 2022.
29. Laghari A. A. et al. Network Segmentation Strategies for Smart Home Security. Computer Networks. 2021.
30. Al-Shareeda M. A. Adaptive Intrusion Detection for Smart Homes. IEEE Internet of Things Journal. 2022.
31. Alkhresheh M. H. Hybrid Deep Learning for IoT Intrusion Detection. Expert Systems with Applications. 2023.
32. Ali M. Ensemble Learning with Kolmogorov-Arnold Networks for IoT Security. Neural Computing and Applications. 2024.
33. Debe M. Blockchain-based Data Integrity for IoT. IEEE Access. 2021.
34. FIPS PUB 140-3. Security Requirements for Cryptographic Modules. Gaithersburg : NIST, 2019.
35. Banks A., Gupta R. MQTT Version 5.0. OASIS Standard. 2019. [Електронний ресурс]. – Режим доступу: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html (дата звернення: 26.10.2025).
36. Shannon C. E. A Mathematical Theory of Communication. The Bell System Technical Journal. 1948. Vol. 27, no. 3. P. 379–423.
37. Dodis Y., Ostrovsky R., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. SIAM Journal on Computing. 2008. Vol. 38, no. 1. P. 97–139.

38. Baudet M., Lubicz D., Micolod J., Tassiaux A. On the Security of Oscillator-Based Random Number Generators. Advances in Cryptology – EUROCRYPT 2011 / ed. by K. G. Paterson. Berlin : Springer, 2011. P. 398–416.
39. Beaulieu R. et al. The SIMON and SPECK Families of Lightweight Block Ciphers. IACR Cryptology ePrint Archive. 2013. [Електронний ресурс]. – Режим доступу: https://eprint.iacr.org/2013/404 (дата звернення: 27.10.2025).
40. Shostack A. Threat Modeling: Designing for Security. Indianapolis : Wiley, 2014. 624 p.
41. Ortiz S. et al. Robustness of Ring Oscillator TRNGs against Electromagnetic Interference. IEEE Transactions on Electromagnetic Compatibility. 2021.
42. Krawczyk H., Eronen P. HMAC-based Extract-and-Expand Key Derivation Function (HKDF). RFC 5869. 2010. [Електронний ресурс]. – Режим доступу: https://www.rfc-editor.org/rfc/rfc5869 (дата звернення: 27.10.2025).
43. M'Raihi D. et al. TOTP: Time-Based One-Time Password Algorithm. RFC 6238. 2011. [Електронний ресурс]. – Режим доступу: https://www.rfc-editor.org/rfc/rfc6238 (дата звернення: 27.10.2025).
44. Тельнова А. А., Балагура Д. С., Фроленко В. О., Сухотеплий В. М., Флоров С. В. Аналіз використання криптопровайдерів у протоколі TLS // Радіотехніка. – 2025. – Вип. 221. – С. 62–72.

ДОДАТОК А
УЗАГАЛЬНЕНИЙ ПОРІВНЯЛЬНИЙ АНАЛІЗ ВРАЗЛИВОСТЕЙ КОМЕРЦІЙНИХ СИСТЕМ «РОЗУМНОГО ДОМУ» ВІДПОВІДНО ДО ОПУБЛІКОВАНИХ ДОСЛІДЖЕНЬ

Таблиця 1.1 – Масштабні емпіричні дослідження безпеки IoT-пристроїв і платформ розумного дому

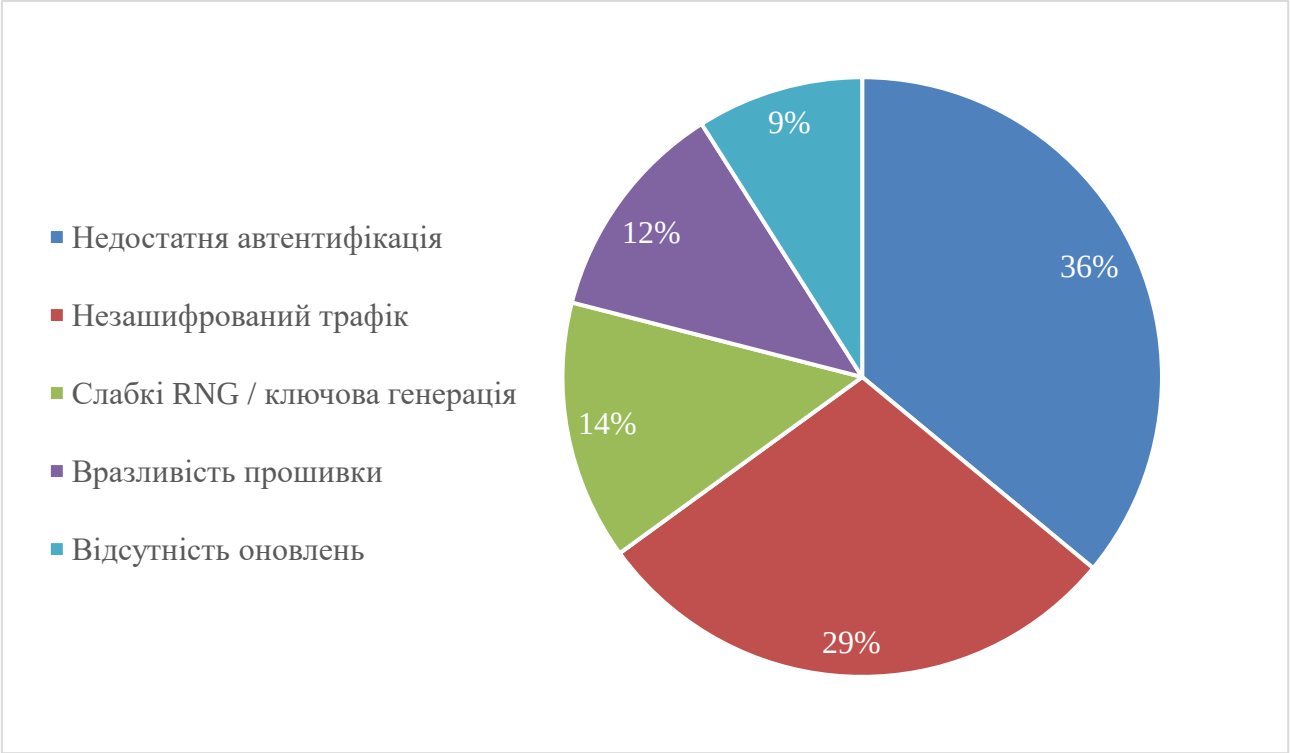
Джерело	Обсяг вибірки	Ключові результати	Виявлені проблеми безпеки	Типові наслідки
Davidson et al.	1641 пристроїв від 66 виробників	76 класів вразливостей, у середньому 3,2 критичних на пристрій	слабкі паролі (67%), незашифровані протоколи (54%), слабкі RNG (31%)	викрадення облікових даних, MITM, brute-force, replay-атаки
Alrawi et al.	45 хмарних платформ IoT	42% недостатня автентифікація, 38% IDOR, 29% криптографічні збої	некоректна валідація сертифікатів, відсутність TLS	віддалене керування пристроями, відмова в обслуговуванні
Wagner et al.	166 000 MQTT/CoAP бекендів	99,84% не використовують TLS	70,93% реалізації TLS є вразливими	перехоплення даних, повне викриття каналів
Naqash et al. (OWASP IoT Top 10)	експериментальна оцінка 47 пристроїв	середнє порушення 6–8 пунктів OWASP	слабка автентифікація, поганий захист даних, небезпечні конфігурації	критичні ризики приватності та фізичної безпеки
Mostafa et al.	IDS на MQTT	точність виявлення 96%	атаки publish-flood, DoS	падіння функціональності системи
Al-Shareeda et al.	IDS у домашніх мережах IoT	точність 97,3%	MITM, несанкціонований доступ	захищеність у реальному часі

Таблиця 1.2 – Поширені вразливості у системах «розумного дому» за OWASP IoT Top 10

Категорія	Поширеність	Приклади в комерційних системах	Можливі атаки
Weak passwords	дуже висока	default admin/root, серійні номери	credential stuffing, brute-force
Insecure network services	висока	відкриті порти MQTT, Telnet	несанкціонований доступ
Unsafe interfaces	середня	web-панелі без HTTPS	веб-експлуатація
No secure update	дуже висока	відсутність підпису прошивки	прошивання шкідливого ПЗ

Outdated components	висока	бібліотеки OpenSSL 1.0.x	експлуатація CVE
Privacy issues	висока	передача необроблених даних	збір даних користувача
Insecure data transport	критична	MQTT/CoAP без TLS	MITM, replay
Lack of device management	висока	відсутність лога аудиту	приховані атаки
Insecure default configs	висока	відкриті LAN-доступи	lateral movement
Lack of physical security	змінна	відкриті debug-порти UART	зчитування firmware

Графік 1.1 – Розподіл основних причин компрометації IoT-пристроїв



ДОДАТОК В

УЗАГАЛЬНЕНИЙ ПОРІВНЯЛЬНИЙ АНАЛІЗ ВРАЗЛИВОСТЕЙ КОМЕРЦІЙНИХ СИСТЕМ «РОЗУМНОГО ДОМУ» ВІДПОВІДНО ДО ОПУБЛІКОВАНИХ ДОСЛІДЖЕНЬ

Таблиця 1.1 – Порівняння TRNG та DRBG в контексті IoT-пристроїв

Характеристика	TRNG (фізичний генератор випадкових чисел)	DRBG (детермінований генератор випадкових бітів)
Джерело випадковості	Фізичні процеси (джиттер, тепловий шум, АЦП шум)	Алгоритмічне розширення початкового зерна
Стандарти оцінки	AIS 31, NIST SP 800-90B	NIST SP 800-90A, ISO/IEC 18031
Продуктивність	нижча	висока, стабільна
Енергоспоживання	часто більше	оптимальне для MCU
Вимоги до апаратури	необхідні додаткові компоненти або аналогові блоки	працює на стандартних процесорних ядрах
Якість ентропії	дуже висока при правильному дизайні	залежить від якості початкового зерна
Стійкість до атак	висока за умови захисту джерела шуму	вразливий при компрометації seed
Типові сфери застосування	ключогенерація, безпечний запуск, апаратні Secure Elements	PRNG для сесійних ключів, токенів, nonce
Типові проблеми	кореляція сигналів, температурна нестабільність	повторюваність при слабкому seed
Підсумок	найкраще джерело довіри	ефективне доповнення, але не заміна TRNG

Таблиця 1.2 – Поширені архітектури TRNG для IoT-пристроїв

Архітектура	Принцип роботи	Переваги	Недоліки	Застосування
Джиттер кільцевих осциляторів (RO-TRNG)	Різниця фаз сигналів між осциляторами	низькі апаратні витрати, легко інтегрується	кореляція при невдалій топології	MCU, SoC, FPGA
Шум АЦП	Використання шуму перетворення	проста реалізація	залежність від температури і джерела живлення	датчики, low-power контролери
DRAM decay	Флуктуації зарядового стану	висока ентропія	потребує пам’яті і часу ініціалізації	IoT-платформи з DRAM
RF-noise / EM шум	електромагнітні коливання	велика ентропія	складний захист від атак	бездротові платформи

Таблиця 1.3 – Порівняння криптографічних алгоритмів для IoT-пристроїв

Алгоритм	Тип	Стійкість	Обчислювальна складність	Переваги	Рекомендації застосування
AES-GCM	симетричний AEAD	висока	середня	захист конфіденційності+цілісності	MQTT / TLS / OTA-оновлення
ChaCha20-Poly1305	симетричний AEAD	висока	низька на CPU без AES-NI	швидкий на MCU	мобільні та IoT-контролери
Curve25519	асиметричний ECC	висока	низька	ефективний обмін ключами	TLS 1.3, ECDH
RSA-2048	асиметричний	середня	висока	сумісність зі старими системами	не бажаний для IoT
SHA-256	хеш-функція	висока	середня	стандарт галузі	підпис, аутентифікація
BLAKE2s	хеш-функція	висока	низька	оптимальний для обмежених систем	IoT-маршрутизатори, сенсори

ДОДАТОК С

ПЕРЕЛІК ПУБЛІКАЦІЙ

УДК 000.000.00 **DOI:00.00000/rt.0000.0.000.00**

Д.Р. ГРИГОР'ЄВ

БАГАТОРІВНЕВІ АРХІТЕКТУРИ БЕЗПЕКИ ДЛЯ РОЗУМНИХ БУДИНКІВ: ІНТЕГРАЦІЯ КРИПТОГРАФІЧНИХ ОСНОВ З КЕРУВАННЯМ ДОСТУПОМ ТА МЕРЕЖЕВОЮ БЕЗПЕКОЮ

Вступ

Стрімке поширення пристроїв Інтернету речей (IoT) трансформувало житлові середовища зі статичних структур у динамічні, електронно-опосередковані простори. Сучасні системи розумного будинку оркеструють керування середовищем (опалення, вентиляція, кондиціонування), функції безпеки (дверні замки, камери, датчики руху), моніторинг присутності та керування енергоспоживанням через взаємопов'язані мережі гетерогенних пристроїв. Аналіз ринку документує вибухове зростання: глобальні поставки пристроїв для розумного будинку перевищили 800 мільйонів одиниць у 2023 році, з прогнозами, що вказують на проникнення на ринок понад 50% у розвинених економіках до 2030 року. Це швидке розширення відображає споживчий попит на зручність, можливості дистанційного моніторингу та інтеграцію з голосовими асистентами.

Однак, прискорена комерціалізація пріоритезує користувацький досвід та час виходу на ринок (time-to-market) над комплексним проєктуванням безпеки, що призводить до системних вразливостей у розгорнутій інфраструктурі. Системи розумного будинку функціонують у середовищі з підвищеним рівнем кіберзагроз, що вимагає застосування методів забезпечення стійкості та цілісності інформації, особливо при високій залежності від даних, що передаються критично важливими сервісами. [1] Емпіричні оцінки безпеки – зокрема, комплексний аналіз Девідсона та ін., що досліджував 1641 пристрій IoT від 66 виробників [2] – ідентифікують 76 окремих класів вразливостей, із медіаною 3,2 вразливості високого рівня суворості на пристрій. Критичні висновки показують, що 67% пристроїв постачаються з обліковими даними за замовчуванням, 54% передають чутливі дані без шифрування, а 31% використовують слабке генерування випадкових чисел для криптографічного ключового матеріалу [2], що фактично зменшує номінальний 128-бітний ключовий простір до 32-48 біт, вразливих до повного перебору (exhaustive search).

Ці вразливості зберігаються, незважаючи на доступність зрілих криптографічних стандартів і протоколів. Фундаментальний розрив походить від недостатньої інтеграції основ безпеки з практичними архітектурними обмеженнями. Криптографічні протоколи надають гарантії безпеки, що базуються на припущеннях про якість генерування випадкових чисел, надійність автентифікованого шифрування та примусове виконання керування доступом – припущеннях, які часто порушуються в реальних розгортаннях. Генератори випадкових чисел становлять критичну інфраструктуру: скомпрометоване генерування випадкових чисел підриває всі подальші криптографічні операції, проте ця фундаментальна проблема отримує обмежену увагу в літературі з архітектури безпеки.

Ця стаття розглядає цей системний пробіл через комплексну багаторівневу архітектуру безпеки для розумних будинків, що інтегрує верифіковане генерування випадкових чисел (відповідність AIS 31), безпеку криптографічних протоколів (TLS 1.3), рольове керування доступом (RBAC) та сегментацію мережі з виявленням вторгнень. Архітектура надає проєктні настанови для розробників, які впроваджують безпечні розгортання, без необхідності експериментального апаратного забезпечення, що робить її застосовною до аналітичних та проєктних фаз проєктів розумного будинку, де фізичне прототипування залишається нездійсненним.

1. Ландшафт загроз та вимоги до безпеки для середовищ розумного будинку

1.1. Класифікація загроз та вектори атак

Ландшафт загроз розумного будинку охоплює три основні вектори атак:

- Загрози мережевого рівня спрямовані на канали зв'язку через атаки «людина посередині» (MITM), що перехоплюють нешифровані повідомлення MQTT, атаки повторного відтворення (replay attacks), що експлуатують недостатню часову прив'язку в механізмах автентифікації, та атаки з ін'єкцією команд, що маніпулюють повідомленнями протоколу для ініціювання несанкціонованих дій пристроїв. Емпіричні дані свідчать, що 99,84% серверних частин (backend) MQTT працюють без шифрування TLS, створюючи повсюдну вразливість до MITM [3].
- Загрози рівня пристрою експлуатують вразливості реалізації, включаючи переповнення буфера у прошивці (firmware), слабке генерування випадкових чисел для криптографічного ключового матеріалу та неадекватний захист чутливих даних, що зберігаються в пам'яті або постійному сховищі. Фізична доступність уможливлює апаратні атаки, включаючи атаки сторонніми каналами (side-channel analysis) та вилучення (екстракцію) прошивки.
- Архітектурні загрози використовують системні проєктні рішення: залежність від централізованих хмарних сервісів, що створює єдині точки відмови, пласкі топології мережі, що дозволяють латеральне (бічне) переміщення після початкової компрометації пристрою, та фрагментовані механізми оновлення прошивки, що створюють хронічні «вікна вразливості». Аналіз Стаджано ідентифікує двадцять фундаментальних міркувань безпеки для IoT, підключених до хмари, підкреслюючи непримиренні суперечності між зручністю та безпекою, притаманні сучасним архітектурам [4].

Дослідження показують, що порушення цілісності даних та нав’язування хибних повідомлень є одним із найнебезпечніших типів атак, які можуть знижувати достовірність роботи критичних сервісів у телекомунікаційних системах. [1]

1.2. Методологія оцінки ризиків

Кількісна оцінка ризиків поєднує оцінку ймовірності загрози з оцінкою впливу, використовуючи фундаментальне рівняння:

$$\text{Ризик} = \text{Імовірність} \times \text{Вплив} \quad (1)$$

Комплексна оцінка ризику має враховувати як ймовірність реалізації загрози, так і масштаб потенційних наслідків, що дозволяє оцінити реальний рівень безпеки системи. [1]

Для контексту розумного будинку, оцінка впливу охоплює три виміри: конфіденційність даних (чутливість особистої інформації, включаючи шаблони присутності (зайнятості), дані про присутність, біометричну інформацію), цілісність даних (автентичність команд керування, що впливають на фізичну безпеку та надійність системи) та доступність системи (безперервність роботи сервісів автоматизації).

Оцінка ймовірності враховує можливості супротивника (від «script kiddies» з загальнодоступними інструментами до досвідчених акторів з можливостями зворотної інженерії), доступність поверхні атаки (мережеві сервіси проти фізично доступних пристроїв) та фактори середовища (географічне розташування, регуляторне середовище).

2. Криптографічні основи: Генерування випадкових чисел та вимоги до ентропії

2.1. Методологія оцінки ризиків

Криптографічна безпека фундаментально залежить від непередбачуваних випадкових значень для ключового матеріалу, нонсів (nonces), векторів ініціалізації та токенів автентифікації. Генератори випадкових чисел поділяються на два класи: Генератори істинно випадкових чисел (ГІВЧ, TRNG), що отримують ентропію зі стохастичних фізичних процесів,

та Детерміновані генератори випадкових бітів (ДГВБ, DRBG), що розгортають короткі початкові значення (seeds) у довші псевдовипадкові послідовності за допомогою криптографічних алгоритмів.

Критичні для криптографічних застосувань міри ентропії визначені суворо. Ентропія Шеннона кількісно визначає середній вміст інформації:

$$H(X) = -\sum_{x \in X} P(x)\, log_2\, P\,(x) \tag{2}$$

Мін-ентропія надає консервативну міру непередбачуваності у найгіршому випадку:

$$H_\infty(X) = -log_2\left(\max_{x \in X} P\,(x)\right) \tag{3}$$

Для криптографічних застосувань мін-ентропія є належною метрикою безпеки, оскільки вона враховує оптимальні стратегії вгадування супротивника. Незміщене двійкове джерело (50% нулів, 50% одиниць) досягає ентропії Шеннона 1,0 біт та мін-ентропії 1,0 біт. Джерело зі зміщенням (99% нулів, 1% одиниць) досягає ентропії Шеннона ≈ 0,081 біт, але мін-ентропії ≈ 0,015 біт, при цьому супротивники досягають 99% ймовірності успіху через оптимальне вгадування.

Рівень ентропії для послідовностей залежних випадкових величин:

$$H_r = \lim_{n \to \infty} \frac{1}{n} H(X_1, X_2, \ldots, X_n) \tag{4}$$

Кількісно визначає середній вміст інформації на вихідний символ для неперервних випадкових джерел. ГІВЧ, що генерує 10^6 біт на секунду з рівнем ентропії 0,98 біт/символ, виробляє приблизно 980 000 біт криптографічної ентропії на секунду.

Слід зазначити, що порушення механізму отримання випадковості або контроль над джерелом ентропії може стати ключовим вектором атаки, що здатний повністю зруйнувати криптографічний захист системи безпеки. [5]

2.2. Методологія AIS 31 та функціональні класи

Стандарт AIS 31 Федерального управління з питань інформаційної безпеки Німеччини [6] встановлює найбільш суворий фреймворк для оцінки генераторів випадкових чисел через вимоги стохастичного моделювання. На відміну від підходів до оцінки, що наголошують на статистичному тестуванні вихідних властивостей, AIS 31 вимагає явних (експліцитних) стохастичних моделей, що описують розподіли ймовірностей, які лежать в основі фізичних джерел шуму. Ця методологія, заснована на моделях, дозволяє верифікувати, що заяви про ентропію залишаються чинними протягом усього терміну служби пристрою в різноманітних умовах експлуатації, а не просто підтверджує лабораторні вимірювання.

AIS 31 визначає шість функціональних класів з ієрархічними вимогами безпеки:

- PTG.2 (Фізичний генератор істинно випадкових чисел, Рівень 2): Визначає кількісні пороги ентропії (ентропія Шеннона ≥ 0,9998 біт/вихідний біт, мін-ентропія ≥ 0,98 біт/вихідний біт), верифіковані через батареї статистичних тестів (T_{rrn} для необроблених випадкових чисел, T_{irn} для проміжних оброблених чисел) та безперервне тестування в реальному часі (online testing) під час роботи. Розрив між порогами ентропії Шеннона та мін-ентропії (0,0198 біт) враховує асиметрію (skewness) розподілу.
- PTG.3 (Фізичний генератор істинно випадкових чисел, Рівень 3): Поєднує PTRNG, сумісний з PTG.2, з криптографічною постобробкою (сумісною з DRG.3) для досягнення максимальної безпеки. Гібридна архітектура гарантує, що навіть повна відмова PTRNG не компрометує безпеку негайно, за умови, що повторне засіювання (reseeding) відбувається під час вікна атаки.
- DRG.2 (Детермінований генератор випадкових бітів, Рівень 2): Забезпечує зворотну

таємність (минулі виходи неможливо відновити зі спостережуваного стану) та пряму таємність (майбутні виходи непередбачувані з поточного стану) через криптографічний аналіз.

- DRG.3 (Детермінований генератор випадкових бітів, Рівень 3): Додає посилену зворотну таємність через односпрямовані функції переходу стану, гарантуючи, що обчислення попередніх станів вимагає обчислювальних зусиль, що перевищують 2^{256} для 256-бітних цілей безпеки [11].
- DRG.4 (Детермінований генератор випадкових бітів, Рівень 4): Вимагає гібридних конструкцій, що поєднують детерміновану генерацію з періодичним введенням свіжої ентропії, запобігаючи атакам на вичерпання простору станів через періодичне повторне засіювання.

2.3. Методологія оцінки ризиків

Фізичні джерела ентропії, придатні для IoT, використовують різноманітні механізми. ГІВЧ на основі кільцевого генератора (Ring oscillator) використовує накопичення фази від джитера (тремтіння) періоду в осцилюючих логічних схемах. Канонічні стохастичні моделі представляють джитер періоду як випадкові величини з приблизно Гауссовими розподілами. Нехай T_i позначає період i-го циклу, а T_{target} - номінальний цільовий період. Джитер $J_i = T_i - T_{\text{target}}$ представляє відхилення від циклу до циклу.

Для належним чином спроєктованих генераторів за нормальних умов експлуатації:

$$J_i \sim \mathcal{N}\left(0, \sigma^2_{\text{jitter}}\right) \tag{5}$$

де $\sigma_{\text{text\{jitter}}$ залежить від робочої температури, напруги живлення та варіацій напівпровідникового процесу. Емпірична характеристика, задокументована в опублікованих аналізах, вимірює $\sigma_{\text{text\{jitter}}$ у всьому робочому діапазоні пристрою. Для кільцевих генераторів, що генерують частоти осциляції 100-500 МГц, типові середньоквадратичні відхилення джитера становлять від 0,1 до 1 наносекунди, що відповідає фазовому джитеру 10-100 пікосекунд на цикл.

Коли виходи двох асинхронних кільцевих генераторів вимірюються (семплюються) незалежним тактовим джерелом, відносна еволюція фази при повторних вимірюваннях демонструє статистичну випадковість через накопичені ефекти джитера. Якщо генератор 1 генерує період $T_1 = T_{\text{target}} + J_{1,i}$, а генератор 2 генерує $T_2 = T_{\text{target}} + J_{2,i}$, де $J_{1,i}$, $J_{2,i}$ є незалежними вибірками джитера:

$$\Delta\phi_i = 2\pi \sum_{j=1}^{i} \frac{(J_{2,j} - J_{1,j})}{T_{\text{target}}} \tag{6}$$

Накопичення фази наближається до рівномірного розподілу за модулем 2\pi, генеруючи високо непередбачувані моменти вимірювання відносно незалежного тактового сигналу. Вимірювання в ці стохастично змінні моменти часу дає вихідні біти з теоретичною ентропією, що наближається до 1 біта на вибірку.

Для тестової вихідної послідовності $(B_1, B_2, \ldots, B_n)$, де $B_i \in 0{,}1$, емпірична ентропія Шеннона:

$$H_{\text{emp}} = -\sum_{b \in 0,1} \hat{P}(b) \log_2 \hat{P}(b) \tag{7}$$

де $\hat{P}(b) = \frac{\text{count}(B_i = b)}{n}$. Для відповідності PTG.2, проєктні цілі спрямовані на $H_{\text{emp}} \geq 0{,}9998$. Опубліковані дослідження валідації зіставних реалізацій повідомляють про емпіричну ентропію Шеннона 0,9999 біт/біт зі 100 000-бітних тестових блоків, що надає сильні статистичні докази того, що справжня ентропія Шеннона $H \geq 0{,}9998$.

Оцінка мін-ентропії ідентифікує вихідне значення з максимальною частотою. Якщо одне

бітове значення з'являється з частотою $f_{\max}$, емпірична оцінка мін-ентропії:

$$H_{\infty,\text{emp}} = -\log_2(f_{\max}) \quad (8)$$

PTG.2 вимагає $H_{\infty,\text{emp}} \geq 0{,}98$, допускаючи максимальне зміщення приблизно $2^{-0{,}98} \approx 0{,}503$, що означає, що більш часте бітове значення з'являється щонайбільше у 50,3% позицій. Досягнення таких суворих меж вимагає ретельно спроєктованих джерел ентропії зі значною незалежністю. Опубліковані валідації підтверджують, що належним чином спроєктовані джерела джитера відповідають цим вимогам.

3. Безпека криптографічних протоколів для розумних будинків

3.1. Безпека транспортного рівня (TLS) для MQTT

MQTT (Message Queuing Telemetry Transport) домінує у комунікаціях розумного будинку завдяки своїй полегшеній архітектурі «видавець-підписник» (publish-subscribe), що підходить для пристроїв з обмеженою пропускною здатністю та енергоспоживанням. Нешифровані реалізації MQTT наражають вміст повідомлень на пасивне прослуховування та атаки з активною модифікацією. TLS 1.3 (RFC 8446) забезпечує автентифіковані, шифровані канали зв'язку для трафіку MQTT [11].

TLS 1.3 забезпечує обов'язкову досконалу пряму таємність (Perfect Forward Secrecy) через ефемерний обмін ключами Діффі-Геллмана (ECDHE), запобігає атакам на пониження (downgrade attacks) через криптографічну прив'язку параметрів переговорів до встановлення сесії та оптимізує продуктивність рукостискання (handshake) через обмін за один раунд-тріп (round-trip) у типових випадках. Аналіз продуктивності документує, що обчислювальні накладні витрати на рукостискання TLS 1.3 (15-30 мс на сучасних мікроконтролерах) залишаються прийнятними для застосувань розумного будинку з типовими інтервалами повідомлень, що перевищують 1 секунду. Слід зазначити, що рівень безпеки протоколу TLS суттєво залежить від правильної конфігурації криптографічних провайдерів та параметрів шифрування, адже їх некоректне застосування може призвести до вразливості до MITM-атак. [13]

Вимоги до пам'яті для управління станом TLS (40-80 КБ на сесію) обмежують застосовність до пристроїв з достатнім обсягом ОЗП, проте сучасні вбудовані платформи зазвичай задовольняють ці обмеження.

Конфігурація TLS 1.3 для MQTT:

- Взаємна автентифікація на основі сертифікатів: Двостороння валідація X.509
- Обмеження наборів шифрів (Cipher suite): Заборона слабких шифрів (RC4, DES, 3DES, експортні шифри)
- Виведення сесійного ключа: Усі сесійні ключі залежать від свіжої ентропії з ГІВЧ або ДГВБ при встановленні з'єднання
- Вимоги до ентропії: 256 біт для випадкових значень сесії на з'єднання [11]
- Генерація нонсів: 32-байтні випадкові значення з мін-ентропією $\geq 0{,}98$ біт/біт

3.2. Автентифіковане шифрування з асоційованими даними (AEAD)

Схеми AEAD (АШД) поєднують конфіденційність та захист цілісності в уніфікованих криптографічних примітивах. Використання цих механізмів значно підвищує стійкість протоколів до маніпуляцій зі списуванням або модифікацією даних, що робить їх критично важливими для IoT-комунікацій. [13] AES-GCM (режим Галуа/лічильника, NIST SP 800-38D) представляє переважаючий алгоритм AEAD, що забезпечує 128-бітний тег автентифікації та шифротекст змінної довжини.

Операція шифрування AES-GCM:

$$C = \text{AES-CTR}_K(M) \parallel \text{GHASH}_H(AAD, C) \quad (9)$$

де K - 256-бітний ключ шифрування (отриманий з ДГВБ, засіяного ГІВЧ), H - ключ автентифікації GHASH, отриманий з K, AAD - додаткові автентифіковані дані (тема MQTT, заголовки), а M - відкритий текст повідомлення.

Верифікація при розшифруванні переобчислює тег автентифікації та порівнює з отриманим тегом; невідповідність вказує на фальсифікацію (tampering).

Безпека AES-GCM критично залежить від:

1. Унікального нонса (nonce) для кожного повідомлення: Повторне використання нонса з тим самим ключем повністю компрометує автентифікацію та конфіденційність.
2. Генерації випадкового ключа: Ключі повинні генеруватися з джерел ентропії, що відповідають PTG.2 або вище.
3. Належного виведення ключа: Дотримання NIST SP 800-132 (KDF на основі пароля) для автентифікації користувача, або HKDF (KDF на основі HMAC) для сесійних ключів.

3.3. Інтеграція багатофакторної автентифікації

Багатофакторна автентифікація (MFA) поєднує незалежні фактори верифікації (знання, володіння, біометрія) для протидії компрометації облікових даних.

Для контексту розумного будинку:

1. Перший фактор (Пароль):

- Зберігання: bcrypt з фактором роботи 12 (приблизно 2^{12} обчислювальних раундів)
- Вимоги до складності: Мінімум 12 символів, змішаний регістр, цифри, спеціальні символи
- Захист від повного перебору (brute-force): 5 невдалих спроб активують 15-хвилинне блокування
- Типова ентропія, обрана користувачем: 40-60 біт (незважаючи на вимоги до довжини, користувачі демонструють передбачувані шаблони)

2. Другий фактор (TOTP - Одноразовий пароль на основі часу):

- Алгоритм: Стандарт RFC 6238 [11]
- Спільний секрет: 160-бітне значення, згенероване ГІВЧ при реєстрації
- Часове вікно: 30-секундний період дії, вікно приймача ± 1 крок (загалом 90 секунд)
- Запобігання повторному відтворенню: База даних відстежує нещодавно прийняті значення
- Вимоги до ентропії: 160 біт на реєстрацію пристрою

Генерація TOTP:

$$\text{HOTP}(K, T) = \text{Truncate}\big(\text{HMAC-SHA256}(K, T)\big) mod 10^6 \quad (10)$$

де K - спільний секрет, а T - поточний лічильник часу. Компрометація спільного секрету через слабке генерування випадкових чисел дозволяє офлайн-атаки повного перебору на сам алгоритм TOTP.

4. Багаторівнева архітектурна засада (фреймворк)

4.1. Рівень 1: Криптографічні основи (ГІВЧ та ДГВБ)

Фундаментальний рівень складається з інфраструктури генерування випадкових чисел, сумісної з AIS 31, інтегрованої в доступні через мережу концентратори (хаби) або виділені модулі безпеки.

Компоненти:

1. Фізичний ГІВЧ (клас PTG.2 або PTG.3);
2. Детермінований ДГВБ (клас DRG.3 або DRG.4);

3. Управління пулом ентропії.

Вимоги до споживання ентропії:

- Встановлення з'єднання TLS 1.3: 256 біт на з'єднання [11]
- Нонс AES-GCM на повідомлення: 32 біти на повідомлення (96-бітна конкатенація нонсів у GCM вимагає свіжої ентропії для рандомізованого компонента нонса)
- Спільний секрет TOTP на пристрій: 160 біт на реєстрацію пристрою
- Сесійні токени RBAC: 128 біт на встановлення сесії
- Прогнозоване споживання для розгортання зі 100 пристроями: Приблизно 500 кбіт на операційний день

4.2. Рівень 2: Безпека криптографічних протоколів (TLS 1.3)

Другий рівень реалізує автентифіковані, шифровані канали зв'язку між пристроями IoT та хабом розумного будинку. Результати досліджень свідчать, що вибір реалізації TLS 1.3 та підтримуваних криптографічних параметрів є ключовим фактором стійкості системи до мережевих атак. [12]

Вимоги до споживання ентропії:

- TLS 1.3 обов'язковий для всіх клієнтських з'єднань
- Взаємна автентифікація на основі сертифікатів (верифікація сертифіката клієнта)
- Набір шифрів: TLS_AES_256_GCM_SHA384 (256-бітний AES-GCM з SHA-384)
- Відновлення сесії: Вимкнено (операції без стану (stateless) зменшують накладні витрати на управління станом)
- Пряма таємність: Ефемерний ECDH з кривими P-256
- Управління сертифікатами:
- Трирівнева ієрархія PKI (офлайн-кореневий Центр Сертифікації (ЦС), операційний проміжний ЦС, сертифікати кінцевих сутностей для кожного пристрою)
- Термін дії сертифіката: Максимум 2 роки з автоматичним поновленням через 18 місяців
- Алгоритм ключа: ECDSA P-256 (еквівалентно 128-бітному рівню безпеки) [11]
- Перевірка відкликання: OCSP Stapling забезпечує верифікацію статусу в реальному часі
- Вимоги до ентропії: 256 біт на запит генерації сертифіката [11]

Виведення сесійного ключа: TLS 1.3 виводить сесійні ключі через:

$$\text{derived} = \text{HKDF-Expand}(\text{HKDF-Extract}(\text{salt},\text{IKM}),\text{info},L) \quad (11)$$

де IKM (вхідний ключовий матеріал) містить спільний секрет ECDHE (вихід ECDH) та свіжу ентропію з ДГВБ, якщо доступно.

Безпека сесії залежить від:

1. Якості спільного секрету ECDHE
2. Коректності реалізації HKDF
3. Якості ентропії ДГВБ

4.3. Рівень 3: Керування доступом та автентифікація

Третій рівень забезпечує виконання політик авторизації та верифікує ідентичність користувача.

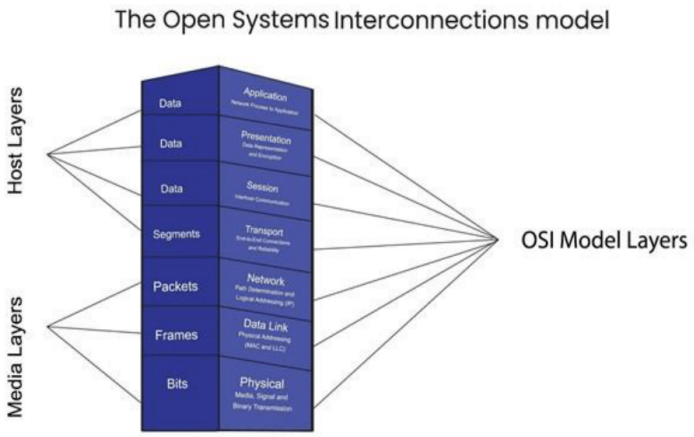


Рис. 1. Модель взаємозв'язку відкритих систем

Рольове керування доступом (RBAC)

Чотири основні ролі визначають межі авторизації в розумному будинку:

- Власник: Повний адміністративний доступ; реєстрація пристроїв; управління користувачами; конфігурація політик безпеки
- Сім'я: Керування середовищем (опалення, вентиляція, освітлення); розважальні системи; видимість даних датчиків
- Гість: Тимчасовий обмежений доступ до визначених зон; обмежена часом дія (за замовчуванням 24 години)
- Служба (Сервіс): Доступ сервісного техніка до певних класів пристроїв; повне журналювання аудиту

Модель дозволів: роль,ресурс,дія→{ДОЗВОЛИТИ,ЗАБОРОНИТИ}

Точка примусового виконання політики (Policy enforcement point): Центральний хаб перехоплює всі повідомлення MQTT та валідує їх відносно бази даних політик перед маршрутизацією.

Приклади політик:

- Роль Власник дозволяє: Підписуватися на всі теми, публікувати в /home/settings/*, викликати /home/admin/*
- Роль Сім'я дозволяє: Публікувати в /home/lighting/+/set, /home/hvac/+/set; підписуватися на /home/sensors/+; забороняє доступ до /home/security/admin
- Роль Гість дозволяє: Публікувати в /home/lighting/living_room/set, /home/hvac/temperature/set лише; термін дії закінчується у вказаний час

Багатофакторна автентифікація

Автентифікація на основі TOTP вимагає:

1. Надсилання пароля (верифікація імені користувача + хешу пароля через bcrypt)
2. Введення токена TOTP (сервер валідує за стандартом RFC 6238 [11])

3. Генерація сесійного токена (JWT, що містить user_id, роль, timestamp, нонс, термін дії)
   Структура сесійного токена (JWT з HMAC-SHA256):

- Корисне навантаження (Payload): {user_id, role, device_subscriptions, timestamp, nonce, exp}
- Нонс (Nonce): 128-бітне випадкове значення з ГІВЧ (мін-ентропія $\geq 0{,}98$ біт/біт)
- Час життя: 3600 секунд (1 година); вимагає регенерації свіжого нонса щогодини
- Ключ підпису: 256-бітний HMAC-секрет з ДГВБ при ініціалізації системи
- Стійкість до підробки: Ймовірність $p_{\text{attack}} = 2^{-125}/3600 \approx 2{,}6 \times 10^{-38}$ на годину

4.4. Рівень 4: Сегментація мережі та виявлення вторгнень

Четвертий рівень забезпечує мережеву ізоляцію, фільтрацію трафіку та виявлення поведінкових аномалій.

Сегментація мережі

Розгортання розумного будинку поділяють пристрої на віртуальні локальні мережі (VLAN) відповідно до чутливості безпеки:

- VLAN 10 (Критичні для безпеки): Дверні замки, камери, датчики доступу
- Обмежений вихідний трафік (egress): Лише до брокера MQTT (TCP/8883) та сервера NTP (UDP/123)
- Відсутність латерального (бічного) зв'язку з іншими VLAN
- Порушення безпеки будь-якого одного пристрою обмежується підсистемою безпеки
- VLAN 20 (Побутові пристрої): Опалення, освітлення, розумна побутова техніка
- Зв'язок: Лише брокер MQTT
- Компрометація не впливає на механізми безпеки (замки, камери)
- VLAN 30 (Гостьова): Пристрої відвідувачів, тимчасові підключення
- Повністю ізольована від інфраструктури автоматизації
- Немає доступу до команд керування або даних датчиків
- VLAN 40 (Управління): Адміністративні інтерфейси
- Обмежено роллю Власника
- Відокремлено від операційного трафіку

```
ПОЛІТИКИ ЗА ЗАМОВЧУВАННЯМ:
        INPUT:   DROP (крім встановлених з'єднань)
        FORWARD: DROP (лише явні дозволи)
        OUTPUT:  DROP (лише явні дозволи)

ПРАВИЛА ДОЗВОЛУ:
        VLAN10 → TCP/8883 (MQTT broker): PERMIT
        VLAN10 → UDP/123 (NTP): PERMIT
        VLAN10 → * : DROP

        VLAN20 → TCP/8883 (MQTT broker): PERMIT
        VLAN20 → UDP/123 (NTP): PERMIT
        VLAN20 → * : DROP

        VLAN30 → * : DROP (немає вихідного трафіку)

        VLAN40 → Всі VLAN: PERMIT (адміністративний доступ з журналюванням аудиту)
```

```
БЛОКУВАННЯ ЛАТЕРАЛЬНОГО ПЕРЕМІЩЕННЯ:
        VLAN10 ↔ VLAN20: DROP
        VLAN10 ↔ VLAN30: DROP
       VLAN20 ↔ VLAN30: DROP
```

Рис. 2. Політики брандмауера

Система виявлення вторгнень (IDS)

Мережева IDS, розгорнута на хабі, виявляє сигнатури атак та поведінкові аномалії.
Виявлення на основі сигнатур:

- Набір правил Emerging Threats для атак, специфічних для MQTT
- Патерни ін'єкції команд (маніпуляція контрольними повідомленнями MQTT)
- Атаки з підстановкою облікових даних (Credential stuffing) (повторні спроби автентифікації)
- Патерни DoS-атак (надмірна частота повідомлень)
- Виявлення на основі аномалій (Машинне навчання):
- Фаза встановлення базової лінії (baseline) (7 днів нормальної роботи) фіксує:
- Частоту повідомлень на пристрій (напр., датчик руху: 10 пов/хв \pm2 std dev)
- Розподіл розміру повідомлень за темою
- Часові патерни (кореляції присутності, послідовність дій пристроїв)
- Виявлення в реальному часі (runtime) ідентифікує статистичні відхилення:
- Пристрій, що генерує 10x базової частоти повідомлень, викликає сповіщення про аномалію
- Незвичні розміри повідомлень (зазвичай \le1000 байт) вказують на потенційну ін'єкцію корисного навантаження
- Часові аномалії (команди, видані під час періодів відсутності) викликають підозру

Ансамбль МО (ML), що поєднує Випадкові ліси (Random Forests) (важливість ознак), мережі LSTM (послідовні залежності) та Ізоляційні ліси (Isolation Forests) (глобальні аномалії), досягає заявленої точності 97-98% з рівнем хибнопозитивних спрацьовувань $\leq 1{,}2\%$ на опублікованих наборах даних розумного будинку.

Механізми реагування:

- Автоматичне додавання правила брандмауера, що блокує аномальне джерело
- Адміністративні сповіщення з журналами подій
- Опціональна автоматична ізоляція пристрою з можливістю ручного скасування

5. Аналіз зниження (мітигації) загроз

5.1. Кількісна оцінка покращень безпеки

Інтегрована архітектура зменшує потенціал вразливостей через глибокоешелонований захист (defense-in-depth):

1. Атаки «людина посередині» (Man-in-the-Middle:

- Ризик без контрзаходів: 99,84% розгортань MQTT не мають TLS [3]; пасивне прослуховування компрометує всі передані дані.
- Заходи на рівні архітектури: Обов'язковий TLS 1.3 шифрує весь транспорт; компрометація облікових даних вимагає злому AES-256-GCM (обчислювальні зусилля 2^{256}), що неможливо для очікуваних супротивників.
- Залишковий ризик: Актор загрози з приватним ключем (отриманим через компрометацію

пристрою або PKI).

2. Атаки з використанням облікових даних за замовчуванням:

- Ризик без контрзаходів: 67% пристроїв постачаються з незміненими паролями за замовчуванням.
- Заходи на рівні архітектури: Хаб розумного будинку замінює облікові дані за замовчуванням на базу даних користувачів, захищену bcrypt; MFA (БФА) підвищує безпеку автентифікації до $\approx 2^{192}$ біт (128-бітна ентропія пароля + 64-бітний часовий компонент TOTP).
- Залишковий ризик: Повний перебір пароля (знижується експоненційною затримкою) або компрометація TOTP (вимагає скомпрометованого спільного секрету).

3. Слабке генерування випадкових чисел:

- Ризик без контрзаходів: 31% пристроїв зменшують номінальний 128-бітний ключовий простір до 32-48 біт, уможливлюючи повний перебір ключа.
- Заходи на рівні архітектури: Відповідність AIS 31 PTG.2/PTG.3 гарантує мін-ентропію $\geq 0{,}98$ біт/біт; 256-бітні ключі виводяться з ≥ 256 біт ентропії, сумісної з AIS, запобігаючи практичним атакам перебору.
- Залишковий ризик: Компрометація фізичного джерела ентропії ГІВЧ (виявляється онлайн-тестами та сигналами тривоги).

4. Латеральне переміщення після початкової компрометації:

- Ризик без контрзаходів: Пласка топологія мережі дозволяє скомпрометованому контролеру освітлення отримати доступ до підсистеми безпеки.
- Заходи на рівні архітектури: Сегментація VLAN обмежує скомпрометований пристрій лише пристроями, критичними для безпеки (VLAN10); політики брандмауера дозволяють VLAN10 → лише брокер MQTT, запобігаючи латеральним переміщенням до інших сегментів.
- Залишковий ризик: Компрометація самого брокера MQTT дозволяє повний доступ до системи.

5. Експлуатація вразливостей нульового дня (Zero-day):

- Ризик без контрзаходів: Експлуатований пристрій отримує неконтрольований доступ.
- Заходи на рівні архітектури: IDS виявляє аномальну поведінку (частота повідомлень, часові патерни, структура корисного навантаження) протягом декількох секунд після експлуатації; автоматична ізоляція обмежує поширення шкоди.
- Залишковий ризик: Досвідчений атакуючий адаптує сигнатуру атаки, щоб уникнути поведінкових базових ліній.

5.2. Матриця відповідності міжнародним стандартам

Узгодження архітектура з міжнародними криптографічними стандартами [7, 9, 10] наведене в таблиці 1.

Таблиця 1

Відповідність архітектури з міжнародними криптографічними стандартами

Компонент архітектури	Вимога AIS 31	NIST SP 800-90	ISO/IEC 20543	Статус відповідності
Якість ентропії ГІВЧ	PTG.2: $H \geq 0{,}9998$, $H_\infty \geq 0{,}98$	SP 800-90B: оцінка мін-ентропії	Фреймворк мін-ентропії	Відповідає PTG.2
Онлайн-тестування	Батареї тестів T_{rrn}, T_{irn}	SP 800-22 NIST тест-набір	Процедури валідації	Реалізовано
Алгоритм	DRG.3	SP 800-90A:	Вимоги до	HMAC-DRBG

ДГВБ	односпрямовані функції	HMAC_DRBG, Hash_DRBG	ДГВБ	(SHA-256)
Реалізація TLS	Н/Д (криптографічний протокол)	SP 800-52B настанови TLS	Стандарти протоколів	TLS 1.3 з P-256
Інтервали повторного засіювання	Визначено для класу DRG	SP 800-90A: вимоги до повторного засіювання	Частота повторного засіювання	Щогодини мінімум
Виведення сесійного ключа	Вимоги до пулу ентропії	SP 800-132 настанови PBKDF	Стандарти виведення ключа	HKDF-SHA256

6. Аналіз зниження (мітигації) загроз

6.1. Поширені помилки реалізації

1. Неналежна ініціалізація ГІВЧ:

- Проблема: ГІВЧ вимагає 50-100 мс часу запуску для накопичення достатньої ентропії; системи, що негайно використовують вихідні дані, стикаються з виснаженим пулом ентропії.
- Спосіб усунення: Реалізувати рукостискання при запуску, що вимагає 100+ мс накопичення ентропії, перш ніж система оголосить про операційну готовність.

2. Повторне використання нонсів у симетричному шифруванні:

- Проблема: Повторне використання нонса AES-GCM з тим самим ключем компрометує і конфіденційність, і автентичність; емпірично поширене, коли розробники повторно використовують стан сесії між повідомленнями.
- Спосіб усунення: Генерувати свіжий нонс (32 байти з ДГВБ) для кожного повідомлення; верифікувати коректність генерації нонсів через журналювання послідовностей нонсів.

3. Неочікуване завершення терміну дії сертифікатів:

- Проблема: Сертифікати, термін дії яких закінчився, порушують рукостискання TLS; немоніторингові розгортання розумного будинку зазнають перебоїв у роботі сервісу, коли сертифікати досягають терміну придатності.
- Спосіб усунення: Автоматизоване поновлення сертифікатів за 1 місяць до закінчення терміну дії; адміністративні сповіщення за 1 тиждень; попереднє розміщення нових сертифікатів для ротації (заміни) без простою.

4. Недостатня авторизація для тем (topic) MQTT

- Проблема: Політики RBAC занадто дозвільні (напр., ролі Сім'я дозволено підписуватися на всі /home/+/#); скомпрометований сімейний пристрій отримує доступ до даних безпеки.
- Спосіб усунення: Явний перелік тем; принцип найменших привілеїв з мінімально необхідними підписками.

5. «Тихі» криптографічні збої:

- Проблема: Невалідовані збої автентифікації AES-GCM (розшифрування повертає пошкоджений відкритий текст замість помилки); додатки обробляють фальсифіковані дані, що призводить до вразливостей безпеки.
- Спосіб усунення: Обов'язкова верифікація тегу автентифікації; переривання обробки при невідповідності тегу; журналювання збоїв автентифікації для активації IDS.

Висновки

У цій статті представлено комплексну багаторівневу архітектуру безпеки для розумних будинків, що систематично інтегрує криптографічні основи, безпеку протоколів, керування доступом та моніторинг мережі. Архітектура синтезує абстрактні вимоги безпеки з практичними обмеженнями IoT, надаючи конкретні настанови з реалізації без необхідності експериментальної апаратної валідації. Цей підхід просуває безпеку розумного будинку від ситуативних (ad-hoc) заходів захисту до верифікованих практик криптографічного проєктування. Майбутні дослідження мають наголосити на експериментальній валідації запропонованих архітектур на репрезентативних платформах (ESP32, Raspberry Pi, комерційні хаби), дослідженні методів виявлення аномалій зі збереженням приватності, сумісних із зашифрованим трафіком, та інтеграції постквантової криптографії протягом перехідних періодів.

Список літератури

1. Горбенко І. Д., Замула О. А. Науковий підхід до ймовірнісної оцінки захищеності інформації від нав'язування хибних повідомлень у телекомунікаційних системах // Радіотехніка. – 2022. – Вип. 208. – С. 7–16. – DOI: 10.30837/rt.2022.1.208.01.
2. Davidson B., Hopkins T., Chothia T., et al. Security Analysis of 1,641 IoT Devices from 66 Manufacturers // IEEE Security & Privacy. 2021.
3. Wagner P., Noh Y., Javed M., et al. Large-Scale MQTT Deployment Security Study // Proceedings of the ACM Internet Measurement Conference. 2023.
4. Stajano F. Security for Ubiquitous Computing. – Chichester : John Wiley & Sons, 2002.
5. Моргуль Д. М., Нарєжний О. П., Гріненко Т. О. Модель порушника та модель загроз для веб-сервісу QRNG // Радіотехніка. – 2025. – Вип. 221. – С. 31–38.
6. Federal Office for Information Security (BSI). AIS 20/31 – Functionality Classes for Random Number Generators. – Bonn : BSI, 2023.
7. National Institute of Standards and Technology. SP 800-90A: Recommendation for Random Bit Generation Using Deterministic Random Bit Generators. – Gaithersburg (MD) : NIST, 2015.
8. National Institute of Standards and Technology. SP 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation. – Gaithersburg (MD) : NIST, 2019.
9. International Organization for Standardization. ISO/IEC 20543: Security Evaluation of Physical Random Number Generators. – Geneva : ISO, 2019.
10. National Institute of Standards and Technology. SP 800-52B: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. – Gaithersburg (MD) : NIST, 2019.
11. Dierks T., Rescorla E., et al. RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3. – Internet Engineering Task Force, 2018.
12. Тельнова А. А., Балагура Д. С., Фроленко В. О., Сухотеплий В. М., Флоров С. В. Аналіз використання криптопровайдерів у протоколі TLS // Радіотехніка. – 2025. – Вип. 221. – С. 62–72.
13. M'Raihi D., Machani S., Pei M., Rydell J. RFC 6238: TOTP: Time-Based One-Time Password Algorithm. – Internet Engineering Task Force, 2011.

Надійшла до редколегії 19.11.2025

Відомості про авторів:

Григор'єв Данило Романович – Харківський національний університет імені В. Н. Каразіна, студент кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-науковий інститут комп'ютерних наук та штучного інтелекту; Україна; e-mail: hryhoriev2020ki11@student.karazin.ua

СЕРТИФІКАТ

учасника конференції

IN 112074
від 05.12.2025

ГРИГОР'ЄВ ДАНИЛО РОМАНОВИЧ

ВЗЯВ(-ЛА) УЧАСТЬ У IX МІЖНАРОДНІЙ СТУДЕНТСЬКІЙ НАУКОВІЙ КОНФЕРЕНЦІЇ

ПРІОРИТЕТНІ НАПРЯМКИ ТА ВЕКТОРИ РОЗВИТКУ СВІТОВОЇ НАУКИ

5 ГРУДНЯ 2025 РІК • М. СУМИ, УКРАЇНА

В рамках участі було опубліковано тези доповіді учасника на тему:

БАГАТОРІВНЕВА АРХІТЕКТУРА БЕЗПЕКИ ДЛЯ РОЗУМНИХ БУДИНКІВ: ІНТЕГРАЦІЯ КРИПТОГРАФІЧНИХ ПІДХОДІВ, МЕРЕЖЕВОГО ЗАХИСТУ ТА КЕРУВАННЯ ДОСТУПОМ

ДИРЕКТОР МОЛОДІЖНОЇ НАУКОВОЇ ЛІГИ
ГОЛОВА ОРГКОМІТЕТУ КОНФЕРЕНЦІЇ
ІГОР КОРЕНЮК

МОЛОДІЖНА НАУКОВА ЛІГА

МАТЕРІАЛИ IX МІЖНАРОДНОЇ СТУДЕНТСЬКОЇ НАУКОВОЇ

КОНФЕРЕНЦІЇ

ПРІОРИТЕТНІ НАПРЯМКИ ТА ВЕКТОРИ РОЗВИТКУ СВІТОВОЇ НАУКИ

М. СУМИ, УКРАЇНА

5 ГРУДНЯ 2025 РІК

МОЛОДІЖНА НАУКОВА ЛІГА

МАТЕРІАЛИ IX МІЖНАРОДНОЇ СТУДЕНТСЬКОЇ НАУКОВОЇ

КОНФЕРЕНЦІЇ

ПРІОРИТЕТНІ НАПРЯМКИ ТА ВЕКТОРИ РОЗВИТКУ СВІТОВОЇ НАУКИ

м. Суми, Україна
5 грудня 2025 рік

Вінниця, Україна
«UKRLOGOS Group»
2025

УДК 082:001
П 75

Голова оргкомітету: Коренюк І.О.
Верстка: Білоус Т.В.
Дизайн: Бондаренко І.В.

Рекомендовано до видання Вченою Радою Інституту науково-технічної інтеграції та співпраці. Протокол № 48 від 04.12.2025 року.

Конференцію зареєстровано Державною науковою установою «УкрІНТЕІ» в базі даних науково-технічних заходів України та бюлетені «План проведення наукових, науково-технічних заходів в Україні» (Посвідчення № 459 від 10.06.2025).

П 75 **Пріоритетні напрямки та вектори розвитку світової науки**: матеріали IX Міжнародної студентської наукової конференції, м. Суми, 5 грудня, 2025 рік / ГО «Молодіжна наукова ліга». — Вінниця: ТОВ «УКРЛОГОС Груп», 2025. — 814 с.

ISBN 978-617-8582-06-7
DOI 10.62732/liga-inter-05.12.2025

Викладено матеріали учасників IX Міжнародної мультидисциплінарної студентської наукової конференції «Пріоритетні напрямки та вектори розвитку світової науки», яка відбулася 5 грудня 2025 року у місті Суми, Україна.

УДК 082:001

ISBN 978-617-8582-06-7

Григор'єв Данило Романович, здобувач вищої освіти навчально-наукового інституту комп'ютерних наук та штучного інтелекту
Харківський національний університет імені В. Н. Каразіна, Україна

Науковий керівник: Горбенко Іван Дмитрович, доктор технічних наук
Харківський національний університет імені В. Н. Каразіна, Україна

БАГАТОРІВНЕВА АРХІТЕКТУРА БЕЗПЕКИ ДЛЯ РОЗУМНИХ БУДИНКІВ: ІНТЕГРАЦІЯ КРИПТОГРАФІЧНИХ ПІДХОДІВ, МЕРЕЖЕВОГО ЗАХИСТУ ТА КЕРУВАННЯ ДОСТУПОМ

Актуальність. Сучасний розвиток інформаційних технологій характеризується стрімкою трансформацією житлових середовищ у динамічні простори, насичені пристроями Інтернету речей (IoT). Прискорена комерціалізація цього сегменту часто призводить до пріоритезації швидкості виходу продуктів на ринок над безпекою, що створює критичні вразливості. Системи розумного будинку стають об'єктами атак, спрямованих на порушення конфіденційності та цілісності даних [1]. За таких умов розробка комплексних архітектурних рішень, що базуються на фундаментальних криптографічних принципах, стає нагальною потребою.

Ступінь досліджуваності проблеми. Питання безпеки IoT-пристроїв широко висвітлюються у світовій науковій літературі. Емпіричні оцінки, зокрема дослідження Девідсона та співавторів, які проаналізували понад тисячу пристроїв від десятків виробників, ідентифікують численні класи вразливостей, серед яких домінують використання облікових даних за замовчуванням, передача чутливих даних без шифрування та використання слабких генераторів випадкових чисел [2]. Аналіз Стаджано виділяє фундаментальні суперечності між зручністю використання та безпекою у системах, підключених до хмарних сервісів [4]. Дослідження Вагнера та інших вказують на критичний стан безпеки протоколу MQTT у реальних розгортаннях, де переважна більшість серверних частин працює без шифрування [3]. У вітчизняному науковому просторі питання моделей загроз та оцінки захищеності інформації розглядаються у працях І. Горбенка, О. Замули [1], а також Д. Моргуль та інших, які досліджують моделі порушників для специфічних сервісів генерації випадкових чисел [5]. Також важливою є робота А. Тельнової та співавторів, присвячена аналізу криптопровайдерів у протоколі TLS, що є критичним для захисту каналів зв'язку [6]. Незважаючи на значний обсяг досліджень, існує розрив у створенні інтегрованих архітектур, які б поєднували верифіковане генерування випадкових чисел з практичними протоколами мережевої безпеки та керуванням доступом безпосередньо в контексті розумних будинків.

Мета дослідження – розробка та обґрунтування комплексної багаторівневої архітектури безпеки для розумних будинків, яка систематично інтегрує верифіковане генерування істинно випадкових чисел (згідно зі стандартом AIS 31), захищені криптографічні протоколи (TLS 1.3), рольове керування доступом (RBAC) та сегментацію мережі з виявленням вторгнень для нівелювання ідентифікованих загроз.

Сутність дослідження. В основу запропонованої архітектури покладено принцип глибокоешелонованого захисту, що реалізується через чотири взаємопов'язані рівні. Перший, фундаментальний рівень, зосереджено на криптографічних основах, а саме на якості генерування випадкових чисел. Криптографічна безпека системи критично залежить від непередбачуваності ключів, нонсів та токенів. Аналіз показує, що порушення механізму отримання випадковості є вектором атаки, здатним повністю зруйнувати захист [5]. У дослідженні використано методологію стандарту AIS 31, яка вимагає наявності стохастичних моделей фізичних джерел шуму. Для реалізації фізичного генератора істинно випадкових чисел (ГІВЧ) запропоновано використання кільцевих генераторів, що базуються на ефекті джитера періоду в осцилюючих логічних схемах. Накопичення фази від джитера забезпечує статистичну випадковість, що дозволяє досягти високих показників ентропії. Для відповідності класу PTG.2 за AIS 31, емпірична ентропія Шеннона має наближатися до 0,9998 біт/біт, а мін-ентропія — до 0,98 біт/біт. Архітектура передбачає гібридну схему, де вихід фізичного ГІВЧ використовується для засіювання детермінованих генераторів (ДГВБ), що забезпечує необхідну швидкодію та криптографічну стійкість.

Другий рівень архітектури забезпечує безпеку транспортних протоколів, фокусуючись на захисті комунікацій MQTT, що є стандартом де-факто для розумних будинків. Впровадження протоколу TLS 1.3 є обов'язковим для забезпечення конфіденційності та автентичності даних. Цей протокол гарантує досконалу пряму таємність через використання ефемерного обміну ключами Діффі-Геллмана, що унеможливлює розшифрування перехопленого трафіку навіть у випадку компрометації довгострокових ключів у майбутньому. Критично важливим аспектом є правильна конфігурація криптографічних провайдерів, оскільки помилки в налаштуваннях можуть нівелювати переваги протоколу [11]. У дослідженні обґрунтовано використання схеми автентифікованого шифрування AES-GCM, яка поєднує конфіденційність та контроль цілісності. Для кожного повідомлення генерується унікальний нонс, що запобігає атакам повторного відтворення, при цьому ключі шифрування виводяться з джерел ентропії, верифікованих на першому рівні. Також передбачено взаємну автентифікацію на основі сертифікатів X.509, що виключає можливість підключення неавторизованих пристроїв до мережі.

Третій рівень реалізує механізми керування доступом та автентифікації користувачів. Застосовано модель рольового керування доступом (RBAC), що визначає чотири основні ролі: Власник, Сім'я, Гість та Служба. Кожна роль має чітко окреслені права доступу до ресурсів та дій (публікація або підписка на теми MQTT). Центральний хаб виступає точкою примусового виконання політики, перехоплюючи та валідуючи всі повідомлення. Для посилення захисту облікових записів впроваджено багатофакторну автентифікацію (MFA), що поєднує знання пароля та володіння одноразовим паролем на основі часу (TOTP). Генерація кодів TOTP базується на стандарті RFC 6238 і використовує спільний секрет, згенерований ГІВЧ. Це значно підвищує стійкість до атак перебору паролів. Сесії користувачів захищаються за допомогою токенів JWT з обмеженим терміном дії та криптографічним підписом, що містить випадковий нонс для запобігання підробці.

Четвертий рівень забезпечує сегментацію мережі та виявлення вторгнень. Розроблено схему поділу мережі на віртуальні локальні мережі (VLAN) відповідно

до рівня критичності пристроїв. Пристрої безпеки (замки, камери) ізолюються у VLAN 10, побутова техніка — у VLAN 20, гостьові пристрої — у VLAN 30, а адміністративні інтерфейси — у VLAN 40. Міжсегментна взаємодія суворо регламентується політиками брандмауера, які за замовчуванням блокують весь трафік, дозволяючи лише необхідні з'єднання з брокером MQTT та сервером точного часу. Латеральне переміщення між сегментами заборонено, що локалізує наслідки потенційної компрометації окремого пристрою. Додатково впроваджено систему виявлення вторгнень (IDS), яка поєднує сигнатурний аналіз для відомих атак та методи машинного навчання для виявлення аномалій поведінки. Ансамбль моделей машинного навчання аналізує частоту повідомлень, їх розмір та часові патерни, що дозволяє виявляти атаки нульового дня та нетипову активність з високою точністю.

Аналіз ефективності запропонованої архітектури демонструє значне зниження ризиків. Впровадження TLS 1.3 нейтралізує атаки «людина посередині», які є критичними для незахищених MQTT мереж [3]. Використання MFA та заміни облікових даних за замовчуванням усуває загрозу використання стандартних паролів. Відповідність генераторів випадкових чисел вимогам AIS 31 забезпечує стійкість криптографічного ключового матеріалу до атак повного перебору. Сегментація мережі ефективно блокує можливості горизонтального переміщення зловмисника після компрометації периферійних пристроїв. Розроблена матриця відповідності підтверджує узгодженість архітектурних рішень з міжнародними стандартами NIST SP 800-90, ISO/IEC 20543 та рекомендаціями BSI.

Основні висновки. Запропонований підхід трансформує процес забезпечення безпеки від застосування ситуативних заходів до системного інженерного проєктування. Інтеграція верифікованого джерела ентропії, сучасних протоколів шифрування, суворого контролю доступу та мережевої ізоляції створює надійний фундамент для захисту критично важливих даних та фізичної безпеки користувачів. Практична цінність роботи полягає у наданні готових архітектурних патернів, придатних для впровадження розробниками систем розумного будинку без необхідності проведення складних експериментальних досліджень апаратного забезпечення. Подальші вектори розвитку включають адаптацію архітектури до вимог постквантової криптографії та вдосконалення методів виявлення аномалій у шифрованому трафіку зі збереженням приватності користувачів.

Список використаних джерел:

1. Горбенко І. Д., Замула О. А. Науковий підхід до ймовірнісної оцінки захищеності інформації від нав'язування хибних повідомлень у телекомунікаційних системах. Радіотехніка. 2022. Вип. 208. С. 7–16.
2. Davidson B., Hopkins T., Chothia T., et al. Security Analysis of 1,641 IoT Devices from 66 Manufacturers. IEEE Security & Privacy. 2021.
3. Wagner P., Noh Y., Javed M., et al. Large-Scale MQTT Deployment Security Study. Proceedings of the ACM Internet Measurement Conference. 2023.
4. Stajano F. Security for Ubiquitous Computing. Chichester : John Wiley & Sons, 2002.
5. Моргуль Д. М., Нарєжний О. П., Гріненко Т. О. Модель порушника та модель загроз для веб-сервісу QRNG. Радіотехніка. 2025. Вип. 221. С. 31–38.
6. Тельнова А. А., Балагура Д. С., Фроленко В. О. та ін. Аналіз використання криптопровайдерів у протоколі TLS. Радіотехніка. 2025. Вип. 221. С. 62–72.