УДК 004.056:004.738

Розробка та обґрунтування методів та засобів захисту інформації системи «розумний дім»

Михайло Камінський[0009-0000-4298-8369]
Павло Складанний[0000-0002-7775-6039]

Київський столичний університет імені Бориса Грінченка, Україна

Анотація. Ці тези представляють та пояснють суть захисту інформації системи «розумний дім», показує методи захисту інформації та контролю доступів до систем, показує їх опис та особливості методів.
Ключові слова: smart-house, information security, IoT, data protection, cybersecurity.

Вступ

Сучасні системи «розумного дому» інтегрують безліч пристроїв — сенсорів, контролерів, камер, замків, систем опалення та відеоспостереження — об’єднаних у єдину мережу з віддаленим керуванням. Така інтеграція значно підвищує комфорт і енергоефективність житла, проте водночас створює нові загрози інформаційній безпеці.

Основними ризиками є несанкціонований доступ до мережі, перехоплення або підміна даних, використання IoT-пристроїв для атак (наприклад, DDoS) і компрометація конфіденційної інформації користувачів. Через обмежені обчислювальні ресурси більшості «розумних» пристроїв класичні засоби захисту (антивіруси, IDS/IPS тощо) не завжди можуть бути ефективно застосовані. Тому актуальним завданням є розробка комплексних, адаптивних і ресурсо-ефективних методів та засобів захисту інформації для системи «розумний дім».

Методи та моделі

Дослідження методів захисту інформації у системі «розумний дім», має на увазі аналіз існуючих, актуальних підходів до безпеки середовищ, що забезпечують цілісність, конфіденційність та доступність даних, враховуючи обмеження IoT-пристроїв.

Також, під час дослідження, я визначу їхні слабкі місця та запропоную можливу архітектуру багаторівневої системи безпеки, орієнтованої на реальні сценарії експлуатації системи «розумного дому».

Перед описом обраної системи, потрібно провести порівняння існуючих методів захисту. Для кращої візуалізації та спрощення усі дані запишемо в таблицю 1 із визначенням переваг та недоліків кожного варіанту.

Таблиця 1. Основні методи захисту інформації системи

Метод захисту	Короткий опис	Переваги	Недоліки
Криптографічні методи	Використовуються для забезпечення конфіденційності, цілісності та автентичності даних, які передаються між	Високий рівень захисту даних навіть у випадку перехоплення трафіку; можливість	Потребують додаткових обчислювальних ресурсів (що критично для малопотужних

	пристроями. Найчастіше застосовуються симетричні (AES, ChaCha20) та асиметричні (RSA, ECC) алгоритми.	автентифікації пристроїв і користувачів.	пристроїв); необхідність безпечного зберігання ключів.
Мережеві засоби захисту	Передбачають розмежування мереж, фільтрацію трафіку, контроль доступу і шифрування на рівні протоколів (VPN, TLS, DTLS). Також використовується сегментація — розподіл IoT-пристроїв у окрему підмережу, ізоляція від критично важливих систем (наприклад, комп'ютера чи камери спостереження).	Зменшення ризику несанкціонованого доступу ззовні; можливість централізованого моніторингу мережевої активності; виявлення підозрілих з'єднань і вторгнень.	Потребує налаштування спеціального обладнання (роутери, фаєрволи, шлюзи безпеки); може знизити швидкість обміну даними через додаткову перевірку.
Автентифікація та контроль доступу	Забезпечує, щоб лише авторизовані користувачі та пристрої мали доступ до керування системою чи даних. Використовуються паролі, токени, біометричні методи (Face ID, відбиток пальця), багатофакторна автентифікація (MFA).	Захист від несанкціонованого доступу; можливість персоналізації прав користувачів; підвищення рівня довіри до системи.	Людський фактор (слабкі або повторювані паролі); необхідність постійного оновлення та зберігання облікових даних; біометричні методи можуть створювати ризики для приватності.
Фізичний та апаратний захист	Передбачає фізичну охорону обладнання, використання модулів безпечного зберігання ключів (TPM, HSM), функцій Secure Boot і апаратного шифрування.	Захищає від злому чи модифікації пристроїв; підвищує довіру до системи з боку користувачів.	Не всі побутові IoT-пристрої підтримують такі функції.

Потрібно розуміти що система не може фізично бути захищена лише одним методом, до того ж використовувати виключно один метод захисту є доволі недоцільно та небезпечно.

Результати

Проведений аналіз таблиці основних методів захисту інформації показав, що жоден із методів не є універсальним і повинен застосовуватись у комбінації з іншими.

Криптографічні алгоритми забезпечують високий рівень конфіденційності та цілісності даних, однак потребують значних обчислювальних ресурсів, що обмежує їх використання у малопотужних IoT-пристроях.

Рис. 1. Схема сегментації системи «Розумний Дім»

Мережеві засоби захисту, такі як VPN, TLS чи сегментація мережі, ефективно зменшують ризик несанкціонованого доступу, але вимагають спеціалізованого обладнання та налаштування, що може ускладнювати впровадження в побутових умовах. Автентифікація та контроль доступу залишаються ключовими складовими безпеки, особливо завдяки розвитку біометричних і багатофакторних методів, проте людський фактор усе ще є слабкою ланкою.

Фізичний та апаратний захист створює додатковий рівень безпеки, запобігаючи фізичному втручанню в пристрої, однак не всі IoT-рішення підтримують такі функції через технічні або економічні обмеження.

Отже, оптимальний підхід до захисту середовища «розумного дому» полягає у багаторівневій комбінації методів: криптографічного шифрування, мережевих протоколів безпеки, автентифікації користувачів та фізичного захисту пристроїв. Така стратегія дозволяє забезпечити найвищий рівень цілісності, доступності та конфіденційності даних навіть в умовах обмежених ресурсів IoT-систем.

Обговорення

Зараз актуальність цієї системи, насправді, дуже висока. З розвитком технологій кількість пристроїв, підключених до домашніх мереж, постійно зростає. Це підвищує рівень комфорту користувачів, однак водночас створює нові вектори атак і збільшує ризик несанкціонованого доступу до особистих даних, керування побутовими пристроями чи навіть фізичними системами безпеки. Тому проблема забезпечення захищеного функціонування системи «розумного дому» залишається актуальною та стратегічно важливою у найближчому майбутньому.

Серед головних тенденцій розвитку у цій сфері варто відзначити інтеграцію штучного інтелекту (AI) для автоматичного виявлення аномалій та поведінкових відхилень у мережевій активності та використання блокчейн-технологій для розподіленої автентифікації та збереження журналів доступу без ризику підробки.У майбутньому особливої уваги потребуватимуть питання захисту персональних даних, оновлення

вбудованого програмного забезпечення (firmware) пристроїв, а також міжсумісності систем безпеки різних виробників.

Для підвищення стійкості систем «розумного дому» доцільним є розроблення багаторівневої моделі безпеки, що поєднує технічні (шифрування, автентифікацію, сегментацію мережі), організаційні (регулярне оновлення та моніторинг) та поведінкові (освіченість користувачів) заходи. Лише така інтегрована стратегія дозволить гарантувати стабільність, довіру та безпечне функціонування інтелектуальних житлових систем у майбутньому.

Висновки

Запропонований підхід дозволяє підвищити рівень безпеки систем «розумного дому» шляхом комплексного використання методів шифрування, автентифікації та аналізу поведінки пристроїв.

Використання багаторівневої архітектури забезпечує виявлення як зовнішніх, так і внутрішніх загроз, мінімізуючи вплив атак на загальну працездатність системи.

Подальші дослідження доцільно спрямувати на інтеграцію системи штучного інтелекту для прогнозування загроз і автоматичної адаптації рівня захисту під змінні умови експлуатації.

Джерела

1. Луцький національний технічний університет, Тема 15. Розумний та безпечний будинок. Розумне місто. https://e-tk.lntu.edu.ua/pluginfile.php/20332/mod_resource/content/0/BE.pdf

2. Довженко, Н., Іваніченко, Є., Аушева, Н., Шевчук, Ю., & Луковський, Т. (2025). Дослідження архітектури дата-центрів з інтеграцією IoT-компонентів для забезпечення енергоефективності та кіберстійкості. Кібербезпека: освіта, наука, техніка, 4(28), 547–564. https://doi.org/10.28925/2663-4023.2025.28.835

3. Що таке глушіння бездротової системи безпеки та як йому протистояти | Блог Ajax Systems. Ajax Systems (ua) . Архів оригіналу за 21 вересня 2020. https://web.archive.org/web/20200921031605/https://ajax.systems/ua/blog/what-is-jamming/

4. Войтович О. П., Вишньовський В. В., Савченко К. В. Дослідження безпеки системи розумного будинку https://epsi.vntu.edu.ua/uploads/2017/67-3wbzu2z9ouo8vv4oeo00yr4n7ve8fqpq.pdf

5. Олійник, Я., Платоненко, А., Черевик , В., Ворохоб, М., & Шевчук, Ю. (2025). Методи захисту інформації в технологіях IoT. Кібербезпека: освіта, наука, техніка, 3(27), 100–108. https://doi.org/10.28925/2663-4023.2025.27.705

6. Anastasia Belova, Viktoria Onischenko. Методи забезпечення безпеки розумного будинку. https://csecurity.kubg.edu.ua/index.php/journal/article/view/119

7. М. Маслова, укладання, 2021. https://zounb.zp.ua/wp-content/uploads/2021/07/Rozumnij-budinok-pokazhchik-6.04.21-s-oblozhkoj.pdf

8. Юсупов В. Т. Розробка системи автоматизації – розумний будинок "Modular House", 151 – Автоматизація та комп`ютерно-інтегровані технології. – Харків, 2024 https://openarchive.nure.ua/entities/publication/bc5d0706-12df-4ef7-91bb-ddad78c21a45

9. Довженко, Н., Іваніченко, Є., & Костюк, Ю. (2025). Методика виявлення та локалізації кіберзагроз у хмарних середовищах з інтегрованими IoT-компонентами на основі графових моделей. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 762–776. https://doi.org/10.28925/2663-4023.2025.29.938