Вразливості IoT-пристроїв у системах «розумного будинку»

Сивець Богдана, студентка (ORCID: 0009-0002-9369-7697)

[1] *Київський національний університет будівництва і архітектури, м. Київ,Україна*

АНОТАЦІЯ

У роботі розглядаються особливості побудови систем «розумного будинку» та роль IoT-пристроїв у їх функціонуванні. Аналізуються типові елементи таких систем — від засобів комфорту до пристроїв контролю й безпеки, а також визначаються основні вразливості: слабкі облікові дані, відсутність оновлень, незахищені канали зв'язку, помилки у хмарних сервісах, відсутність сегментації мережі, біометричні та фізичні ризики. Показано можливі наслідки їх експлуатації зловмисниками та наведено рекомендації щодо зменшення ризиків для користувачів і виробників.

Ключові слова: розумний будинок, інтернет речей (IoT), кіберзагрози, інформаційна безпека, біометрична автентифікація, вразливості, хмарні сервіси.

1. ВСТУП

Розумний будинок — це система, у якій взаємодіють пристрої різного рівня: від тих, що відповідають за комфорт (освітлення, клімат-контроль, побутова техніка), до засобів контролю та безпеки — камер, замків, сигналізацій і датчиків руху. Усе це об'єднується в єдину систему, що працює за принципом Інтернету речей (IoT): пристрої підключені до мережі, збирають дані та обмінюються ними для узгодженої роботи. Завдяки такій архітектурі користувач може керувати системою як централізовано, через хаб чи сервер, так і безпосередньо з персональних пристроїв: смартфона, персонального комп'ютера або за допомогою голосового асистента.

Користувач отримує більше зручності й контролю над власним простором, може налаштовувати систему під себе й керувати нею навіть на відстані. Але водночас із цими перевагами з'являються й ризики: зростає ймовірність витоку персональних даних, втручання у роботу пристроїв чи навіть повного несанкціонованого доступу до всієї мережі розумного дому.

2. ІОТ ЯК СЛАБКА ЛАНКА У СИСТЕМАХ «РОЗУМНОГО БУДИНКУ»

IoT-пристрої в більшості випадків створюються з акцентом на зручність і функціональність, тоді як питання безпеки залишаються другорядними. Обмежені технічні ресурси, відсутність перевірених оновлень і залежність від хмарних сервісів у поєднанні з великою кількістю різних протоколів роблять такі системи більш вразливими до зовнішніх атак. Зламаний пристрій перетворюється на «троянського коня»: він здатний відкрити доступ до локальної мережі, даних користувачів або навіть бути використаним для віддаленого доступу й керування з боку зловмисника.

Для власників житла це означає ризик втрати приватності, фінансових збитків і загрозу фізичній безпеці — від використання камер для шпигунства чи шантажу до застосування пристроїв у масштабних кібератаках.

2.1. Приклади типових IoT-пристроїв у розумному домі:

Розумний дім формується з безлічі пристроїв, які виконують різні функції та водночас взаємодіють між собою. Одні з них відповідають за комфорт: це освітлення, яке може автоматично вмикатися за розкладом або реагувати на рух, і термостати, що підтримують температуру з урахуванням звичок мешканців. Інші мають прямий стосунок до безпеки — камери спостереження, замки з біометричною автентифікацією, системи сигналізації та датчики руху. Поступово у «розумний» сегмент переходить і побутова техніка: холодильники відстежують запаси продуктів, кавоварки запускаються заздалегідь, а пральні машини надсилають сповіщення про завершення циклу на мобільний застосунок.

Окрему роль відіграють віртуальні асистенти, які можуть виконувати голосові команди, інтегруючи одразу кілька пристроїв у єдиний сценарій. Сюди ж додаються датчики диму, вологи та напруги — вони не належать до «комфорту» у звичному розумінні, проте саме вони першими сигналізують про аварійні ситуації та можуть запобігти серйозним наслідкам.

Усі ці елементи об'єднує те, що більшість із них підключені до хмарних сервісів і пов'язані з персональними акаунтами користувачів. Це робить систему зручною та гнучкою у налаштуванні, але одночасно створює додаткові ризики: компрометація облікового запису чи витік особистих та важливих даних.

3. ВРАЗЛИВОСТІ ІОТ-ПРИСТРОЇВ

3.1. Дефолтні та слабкі облікові дані

Багато пристроїв постачаються з типовими логінами й простими паролями. Наслідок — автоматизовані сканери й інструменти для підбору паролю легко зламують такі пристрої, це може призвести до несанкціонованого перегляду конфіденційної інформації, віддаленого керування, доступ до камер та датчиків. Захист в цьому випадку забезпечується завдяки застосуванню унікальних довгих паролів або ключів, обмеженням числа спроб входу з блокуванням, використанням менеджерів паролів.

3.2. Ненадійні або відсутні оновлення прошивки

Відсутність регулярної підтримки та неперевірені оновлення залишають відомі вразливості відкритими значний час. Це створює можливість масового використання старих CVE та тривалої компрометації пристроїв. Вирішення — обирати пристрої від виробників, які забезпечують підтримку

протягом життєвого циклу пристрою, впровадженням цифрового підпису прошивок і механізмів цілісності, а також планом безпечного автоматичного оновлення.

3.3. Незашифрований трафік і вразливі протоколи зв'язку

Передача даних незахищеними каналами (HTTP, незашифрований MQTT/CoAP тощо) дозволяє перехоплювати й модифікувати повідомлення, здійснювати replay-атаки або отримувати критичну інформацію. Наслідки включають витік облікових даних, підміну команд й компрометацію систем контролю. Впровадження TLS/HTTPS, автентифікації на транспортному рівні та відмова від застарілих протоколів значно знижують подібні ризики.

3.4. Уразливі хмарні сервіси та API

Коли робота пристрою прив'язана до хмарних сервісів, будь-яка помилка в налаштуваннях або вразливість у механізмах доступу відкриває шлях до керування ним здалеку, навіть якщо локальна мережа захищена. У таких випадках небезпеку становлять витоки токенів, неправильно задані ролі користувачів чи відсутність додаткових перевірок під час входу. Захист забезпечується простими, але обов'язковими речами: двофакторною автентифікацією, обмеженням прав, регулярною перевіркою токенів і контролем дій через журнали доступу.

3.5. Відсутність сегментації мережі

Коли всі пристрої — від робочих комп'ютерів і серверів до датчиків і камер — підключені в одну мережу, виникає спільна зона ризику. Достатньо скомпрометувати один менш захищений елемент, щоб далі рухатися мережею й отримати доступ до важливих ресурсів. Щоб зменшити такі ризики, доцільно розділяти IoT-пристрої на окремі сегменти, наприклад у виділені VLAN чи гостьові мережі, і обмежувати їхні зв'язки з іншими підсистемами. Це дозволить локалізувати можливу атаку та не дозволить їй поширитися на всю інфраструктуру.

3.6. Біометричні та автентифікаційні слабкості

Біометричні системи автентифікації нерідко залишаються вразливими через відсутність захисту від підробок або слабку реалізацію перевірки «живості». Це відкриває можливість використання фальшивих відбитків, зображень обличчя чи голосових записів. Особливість біометрії полягає в тому, що її шаблони є незмінними: на відміну від паролів, вони не можуть бути «перегенеровані» у випадку компрометації. Тому такі дані потребують максимальної обережності у зберіганні та використанні. Доцільним підходом вважається застосування біометрії у складі багатофакторної автентифікації, поєднання з методами перевірки живості та зберігання шаблонів у зашифрованому вигляді чи в апаратно захищених модулях.

3.7. Фізична безпека та відмовостійкість.

Пристрої, розміщені у доступних місцях, можуть бути піддані фізичним атакам, демонтажу або відключенню живлення. Наявність єдиної точки відмови (central controller) підсилює ризики зупинки роботи системи. Рекомендовано передбачати фізичний захист критичних компонентів, резервні джерела живлення, механізми локальної роботи пристроїв у режимі офлайн та аварійні процедури відновлення доступу.

3.8. Уразливості прошивки та програмного забезпечення

Важливо також враховувати ризики на рівні прошивки: відкриті інтерфейси налагодження або можливість запису кастомного коду дозволяють інтегрувати бекдори або обхідні механізми на апаратному рівні. Профілактика передбачає відключення інтерфейсів налагодження у кінцевих збірках, використання механізмів захисту пам'яті та забезпечення цілісності прошивки.

3.9. Адміністративні помилки та соціальна інженерія

Неправильна конфігурація, надмірні привілеї, повторне використання паролів або фішингові атаки на операторів систем часто стають входом для компрометації. Захист вимагає політик мінімальних привілеїв, періодичного аудиту доступів, процедур відновлення облікових записів та регулярного навчання персоналу і мешканців щодо соціальної інженерії.

4. ВИСНОВКИ

Для зниження ризиків варто дотримуватися низки рекомендацій. По-перше, користувачам варто приділяти увагу базовій гігієні безпеки: змінювати стандартні паролі, оновлювати прошивки, відокремлювати IoT-пристрої в окрему мережу та використовувати багатофакторну автентифікацію там, де це можливо. По-друге, виробники повинні впроваджувати механізми цифрового підпису оновлень, забезпечувати шифрування трафіку, а також пропонувати користувачам прозорі інструменти контролю доступу. По-третє, перспективним напрямом є розробка нормативних вимог і стандартів для IoT у житлових системах, які уніфікуватимуть вимоги до безпеки та підвищать довіру до технологій.

Список літератури

[1] Розумні технології для захисту будинку та квартири. Sowa. URL: https://www.sowa.kiev.ua/blog-uk/rozumni-tekhnolohiyi-dlya-zakhystu-budynky-i-kvartyry/

[2] Kirvan P., Yasar K., Shea S. What is a Smart Home? Everything You Need to Know |Definition from TechTarget. Search IoT. URL: https://www.techtarget.com/iotagenda/definition/smart-home-or-building

[3] OWASP Internet of Things | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-project-internet-of-things/

[4] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, "Smartphones attacking smart homes," in Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, 2016. http://www2.ee.unsw.edu.au/~vijay/pubs/conf/16wisec.pdf