

АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМИ «РОЗУМНИЙ ДІМ»

Система «розумний дім» – це практично повна автоматизація управління девайсами, пристроями в усіх кімнатах та приміщеннях дому, а також офісах, квартирах і т.д. Система може керувати окремими блоками, так і будинком в цілому. Можлива передача команд на масці або дистанційно за допомогою смартфонів. Під «розумним» домом слід розуміти систему, яка забезпечує безпеку та ресурсозбереження для всіх користувачів. У загальному випадку вона повинна вміти розпізнавати конкретні ситуації, які відбуваються в домі, і належним чином на них реагувати.

Основним елементом, який забезпечує функціонування системи життєзабезпечення «розумного дому» є телекомунікаційна мережа. Через мережу проводиться знімання інформації з різного роду датчиків і передача їх на головний контролер для обробки. Контролер після обробки інформації здійснює передачу сигналів управління на виконавчі елементи (датчики перекриття води, ввімкнення засобів пожежогасіння, блокування дверей і т.д.). Через центральний контролер відбувається налаштування та управління «розумними домом» легальним користувачем, а також через нього при необхідності здійснюється передача заданої інформації користувачу системи через зовнішню мережу при його відсутності у приміщенні (наприклад, при несанкціонованому проникненні, пожежі).

Така телекомунікаційна мережа може бути побудована з використанням як провідних так і бездротових каналів зв'язку, наприклад Wi-Fi, Bluetooth або 4G.

Загрози інформаційної безпеки системи «розумний дім» залежать від методів побудови системи, технологій які використовуються в системі та інформаційних потоків які обробляються системою. Виходячи з цього, реалізація системи «розумний дім» в різних конфігураціях має різні загрози інформаційної безпеки.

Основні загрози для системи «розумний дім»:

- атака хакерів;
- перехват інформації;
- віруси в системі;
- витік інформації технічними каналами.

Також існують інші загрози, які можуть вплинути на роботу системи – це стихійні лиха, перебої в мережі, помилки програмного забезпечення (ПЗ), помилки користувача.

Основні вразливості системи «розумний дім»:

1. Підключення мережі «розумного дому» до інтернету. Таким чином при неефективному захисті можна заразитися вірусними програмами, а також підвищується ймовірність атаки хакерів.

2. При неефективному захисту трафіку, підвищується ймовірність перехвату інформації по каналах трафіку.

3. При поганій системі автентифікації та ідентифікації можливий доступ несанкціонованого користувача за рахунок крадіжки даних.

4. Вихід провідників, в яких можуть бути наводки випромінювань, за межі контрольованої зони.

Система може мати ще такі вразливості, як людський фактор (продаж даних), неефективна система захисту від помилок користувача, помилки про використання неліцензованого ПЗ.

Можливі наслідки загроз:

а) порушення роботи, або вихід з ладу центрального сервера, а отже і всієї системи.

б) порушення конфіденційності інформації, яка передається по каналах зв'язку. Можливий захват управління системою.

в) збої в ПЗ системи, а отже – порушення роботи або вихід з ладу апаратури системи.

Тому, для вирішення проблем інформаційної безпеки системи «розумний дім» необхідно провести ретельний аналіз всіх можливих загроз, та вимог до надійності таких систем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. От умных приборов к интеллектуальному пространству. [Електронний ресурс]. – Режим доступу до ресурсу: http://umnydom.kiev.ua/index.php?nma=catalog&fla=stat&cat_id=3&page=3&nums=24/

2. Система Умный Дом — технология экономии, удобства и комфорта высокого уровня. [Електронний ресурс]. – Режим доступу до ресурсу: http://smarton.com.ua/smart_home/systema_umnyi_dom_intro/