Тема 15. Розумний та безпечний будинок. Розумне місто

Зростаюча різноманітність інтелектуальних датчиків, програмних рішень, підключених пристроїв, хмарних сервісів те що встановлено, щоб ми могли працювати в різних формах та форматах у наших живих та робочих середовищах.

Це квартири, офісні будівлі, виробничі поверхи та інші орієнтовані на дії, жваві та чудові місця, мають бути надзвичайно потужними та розширені технологіями. Звичайні і повсякденні об'єкти цифруються, з'єднуються один з одним локальної. Це - все, що в наших місцях, систематично наділяється відповідними та правильними інтелектуальними можливостями шляхом додавання функціональних модулів всередині, а також шляхом інтеграції з віддаленим програмним забезпеченням.

Навіть комунікаційні мережі наповнюються відповідними компетенціями та можливостями, щоб покращити роботу, випадкову та дешеву річ зробити розумною, будь- яку електроніку більш розумною, і в кінцевому підсумку люди - найрозумніші.

Всі види недоліків та залежностей усуваються за допомогою безлічі таких заходів, як стандартизація, адаптери, мости, проміжне програмне забезпечення, загальні інтерфейси API тощо. Можливості підключення і відтворення гарантуються. Пристрої виробляються належним чином та модернізуються, щоб об'єднувати та співпрацювати один з одним для реалізації завдань, орієнтованих на людей. Збирання інформації, агрегація, поширення, важелі впливу для полегшення розуміння інформації та концепцій візуалізації, що постійно посилюються до бачення більш інтелектуальних середовищ.

Пристрої виробляються з використанням дуже сильної фабричної моделі/індустріалізації. Всі високотехнологічні IT-сервери, сховища та мережеві рішення підлягають товарообігу. Це досягається шляхом виявлення та абстрагування всіх видів загальних функціональних можливостей, особливостей та засобів. Всі реалізовані через програмне забезпечення.

Важливі аспекти, такі як модифікованість, заміна, підставість, доступність, витратні можливості тощо легко інтегруються в програмне забезпечення.

Політика та бази знань у поєднанні з менеджером знань з'являються як механізм нового покоління для створення автономічної інфраструктури.

Програмний маршрут рекомендується для встановлення політики та виконання.

«Розумний будинок» призначений для максимально комфортного життя людей за допомогою використання сучасних високотехнологічних засобів.

Принцип роботи системи «розумний будинок» полягає в автоматизації всього, з чого складається житлова споруда: освітлення, кондиціонування, система безпеки, електроенергія, опалення, водопостачання та водовідведення і так далі.

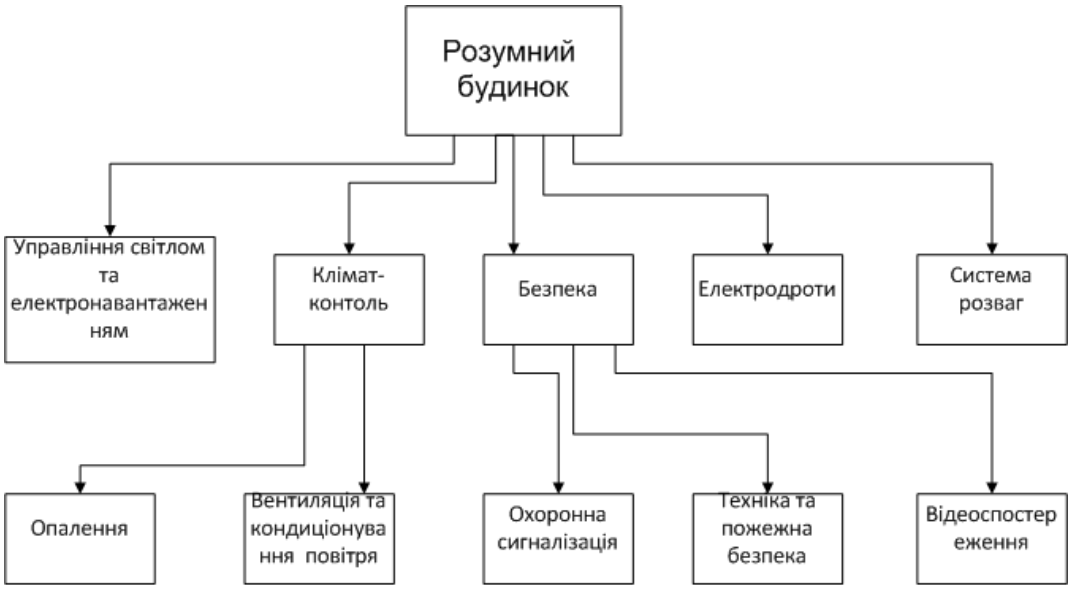

Рисунок 15.1 – Складові «розумного будинку»

До основних підсистем «розумного будинку» відносяться: клімат-контроль, освітлення, мультимедіа (аудіо і відео), охоронні системи, зв'язок і інш.

В останньому випадку це датчики руху, світла, температури, тиску, вологості, вібрації і т.п.

Таким чином, «розумний будинок» складається з програмного і апаратного забезпечення, датчиків і проводової / безпроводової мережі.

У загальному випадку, «розумний будинок» надає його власнику такі переваги:

1) зниження споживання ресурсів (газ, вода, електроенергія);
2) високий рівень комфорту;
3) забезпечення необхідної взаємодії всіх систем об'єкта нерухомості, що автоматизуються, задання різних режимів роботи;
4) зниження ймовірності виникнення аварійних ситуацій;
5) підвищення оперативності, простоти і зручності управління.

Рисунок 15.2 – Компоненти «розумного будинку»

Більшість побутових пристроїв з категорії «розумних» речей можна поділити на дві групи за типом використання Інтернету.

До першої групи належить техніка, яка через WWW оновлює своє програмне забезпечення, отримує нові функції, приймає сигнали, коли знаходиться далеко господаря, і, відповідно, відправляє йому інформацію, яка підтверджує виконані дії та свій стан. Цей тип використання Інтернету

побутовою технікою є найбільш розумним і здатний довести потенційному споживачеві свою корисність.

До другої групи входить техніка, в якій Інтернет є як би стороннім тілом. Сутність рішення в тому, що в абсолютно звичний побутовий прилад, типу мікрохвильовки або холодильника, вбудовується спрощений комп'ютер і дисплей, після чого з їх допомогою можна отримувати мультимедійні розваги там, де їх раніше не було, наприклад, на тій же кухні.

Одним з найперших прикладів побутової техніки, що має підключення до Інтернету, є звичайний тостер, оснащений інтерфейсом для віддаленого включення і повідомлення про готовність підсмаженого тосту. Так техножарт Джона Ромки, одного з перших фахівців в області TCP/IP-протоколу, породив в далекому 1988 році технотренд Інтернету речей, який в наші дні втілюється в життя.

Зростаючий список відомих домашніх мереж та рішень для автоматизації включає в себе наступне:

- Елементи безпеки та спостереження: датчики безпеки для вікон, дверей, руху, розбиття скла та диму можуть надавати найважливішу інформацію про безпеку наших будинків, коли ви знаходитесь вдома або в офісі. IP-захищені камери безпеки та спостереження дуже важливі для забезпечення тісної, нерозбитної та непроникної безпеки. Системи виявлення та попередження вторгнення є іншими відомими модулями безпеки.
- Системи опалення, кондиціонування повітря, системи вентиляції, освітлення та системи відтінків: Комфорт стає вирішальним чинником у будинках нового покоління. Нові машини оснащуються інструментами, щоб забезпечити різні умови навколишнього середовища. Забезпечується зв'язок між різними домашніми пристроями, включаючи світлові вимикачі, настінні сенсорні панелі тощо. Роботи оснащуються різними варіаціями для здійснення

фізичних робіт для людей. Роботи, обладнані Cloud, будуть критично важливим для людей у той час, коли вони стануть розвинутими.

– Обчислювальні та комунікаційні пристрої. В даний час в домашніх умовах використовується широкий спектр обчислювальних машин, починаючи від персональних комп'ютерів (ПК), ноутбуків / ноутбуків / планшетів, маршрутизаторів Wi-Fi та шлюзів, носіїв та смартфонів.
– Розваги, освіта та системи масової інформації. Однією з найважливіших нововведень у медіа-технологіях та продуктах за останні роки.

Сьогодні ми можемо похвалитися фіксованими, портативними, мобільними пристроями для повсякденного навчання. Телевізори, що підтримують IP, виробляються в масових обсягах, різко збільшуючи наш вибір, зручність та комфорт. Веб, інформаційні та побутові прилади є достатніми та новаторськими. Технології для соціальних сайтів (веб 2.0) знаходяться на підйомі, що сприяє підвищенню продуктивності праці для людей та формуванню цифрових спільнот для обміну знаннями в режимі реального часу. Для домашнього кінотеатру, музичних систем hi-fi, DVD-пристроїв, ігрових консолей тощо.

– Домашня мережа: всі пасивні, онімілі предмети перетворюються на цифрові об'єкти. Вони підключаються до бездротової та розумної мережі з усіма видами побутової електроніки, щоб обмінюватися та спілкуватися (безпосередньо [однорангові] або опосередковано, через посередницькі пристрої). Кожного для підключається все більше і більше користувачів, до національної мережі. Домашня мережа також може з'єднуватися із зовнішнім світом через всеохоплюючий Інтернет. Що дозволяє дистанційно спостерігати, управляти та обслуговувати домашні пристрої. Автомобільні мультимедіа, навігаційні та інформаційно-розважальні системи, системи керування паркуванням тощо, також підключаються до домашніх систем безпосередньо або

через проміжне програмне забезпечення на базі коробки для взаємодії та взаємодії в реальному часі.

- Домашній контроль доступу: Е-замки з'являються як найважливіша заходи безпеки для домашнього контролю доступу.
- Розслабляючі та об'єкти настрою: крім об'єктів у певних місцях, таких як тренажерні зали, санаторії, санвузли, гаражі автомобілів, предмети домашнього ужитку, такі як електричні лампи, ліжечка, стільці, шафи, віконні панелі, дивани, бігові доріжки, столи, дивани, автостоянки тощо з'єднуються між собою, щоб значно покращити настрій, стан користувачів.
- Системи охорони здоров'я: медичні кабінети, пігулки та таблетки, гумоїдних роботів і так далі займають перші слоти, що гарантують здорове життя для мешканців житла.
- Кухонна техніка, вироби та посуд. Модульна кухня, що включає в себе всі види електроніки, виявляється ключовим фактором для розумніших будинків. Кавоварки, хлібні тостерів, електронні печі, холодильники, мийки для посуду, кухонні комбайни тощо покращуються, щоб бути розумнішими в домашніх умовах.
- Інтернет-холодильник (Internet refrigerator або Smart refrigerator) – новий клас побутових холодильників, що з'явився на початку XXI століття. Як правило, він має вбудований комп'ютер з постійним підключенням до мережі інтернет і сенсорним екраном на фронтальній панелі

Такий холодильник не тільки зберігає продукти, а й дає можливість користуватися інтернетом, через який можна отримати доступ до різних сайтів (наприклад, з кулінарними рецептами для приготування страв) і навіть замовляти продукти в інтернет-магазинах з доставкою додому. Крім того, за допомогою інтернет-холодильника можна спілкуватися, використовуючи електронну і відеопошту.

Рисунок 15.3 – Інтернет-холодильник

Інтернет-холодильник може надавати цілий ряд сервісів: доступ в Інтернет, відеотелефон, e-mail, TV, MP3- музику, базу даних по улінарних рецептах і правилах харчування, електронне перо, щоб залишити повідомлення, голосові послання. Ряд моделей інтернет-холодильників обладнані телевізійним і радіоприймачем. Крім того, при використанні інтернет-холодильника з'являється можливість вивести на екран картинку з веб-камери зовнішнього відеоспостереження.

Це дозволяє бачити те, що відбувається у дворі приватного будинку, навіть не покидаючи кухні доглядати за своїм малюком, що знаходяться в дитячій кімнаті і т.д. Деякі пристрої даного типу також можуть стежити за вмістом холодильника, вибираючи оптимальні умови зберігання та заморозки продуктів. Крім цього, інтернет-холодильник відстежує продукти з терміном придатності. Інформація про все це надходить на смартфон користувача і останній, перебуваючи в магазині, може оцінити свої реальні потреби в продуктах.

Робот-пилосос може діяти автономно, програмуватися і управлятися через Інтернет, для чого є ряд сенсорів і інфрачервона вбудована камера. Система управління роботою пилососа робить кілька знімків в секунду створюючи, таким чином, карту всього будинку або окремих його кімнат. Пристрій також має можливість запам'ятовувати оптимальний шлях збирання і визначати своє місцезнаходження в будинку.

Рисунок 15.4 – Робот-пилосос

Акумулятора вистачає на певний час збирання (зазвичай до 1,5 годин), після закінчення якого робот сам відправляється на підзарядку. До пилососа є бездротовий доступ Wi-Fi за допомогою комп'ютера або смартфона. Через ці пристрої можна запустити його і в режимі реального часу спостерігати за тим, що відбувається в кімнаті. Більш того, можна поговорити з людьми, які знаходяться в будинку через систему голосового зв'язку. Вбудований джерело світла дозволяє бачити в повній темряві і перевірити приміщення навіть вночі.

Інтернет мікрохвильова піч має вбудований модем для виходу в інтернет, пам'ять для зберігання завантажувати інформацію і пульт управління. Вона виконує такі завдання:

- скачування рецептів з Інтернету і самопрограмування;
- зв'язок з компаніями - виробниками продуктів;
- дає доступ до системи замовлення продуктів по інтернету.

Інтернет-кондиціонер підключається до інтернету через проводову або безпроводову мережу WiFi і дає користувачеві доступ до управління кондиціонером з будь-якої точки земної кулі. Власник може дистанційно вмикати і вимикати систему, програмувати настройки, вибір між режимами, температуру, швидкість вентилятора, задавати параметри, словом здійснювати будь-які маніпуляції, доступні зі звичайного пульта. Керувати таким кондиціонером можна з будь-якого пристрою (комп'ютер, ноутбук, планшет, смартфон), в якому встановлена спеціальна програма і який має вихід в інтернет.

Рисунок 15.5 – Компоненти «розумного будинку»

Система по догляду за домашніми тваринами покликана забезпечити їм всі необхідні комфортні умови існування. Така система використовується в разі тривалої відсутності господарів будинку - це дозволяє не турбуватися про добробут своїх домашніх улюбленців. Основними завданнями системи по догляду за домашніми тваринами є автоматична подача їжі і пиття, а в разі виникнення непередбачених обставин - інформування господарів про них (по телефону, за допомогою SMS або по електронній пошті). За бажанням можна скласти повний звіт про поведінку домашніх улюбленців під час відсутності господарів - скільки разів і коли їли, коли ходили в туалет, пили воду і т.д.

Можна навіть супроводити цей звіт фотографіями (якщо встановлена камера спостереження) і передавати їх (по електронній пошті, за допомогою MMS) - словом, все, щоб господарі відчували себе комфортно і були впевнені в тому, що їх улюбленцям нічого не загрожує.

Отримані статистичні підрахунки та прогнози про те, що в вже з'являться сотні мікроконтролерів у будь-яких вдосконалених домашніх/офісних середовищах. Надзвичайно популярні технології, такі як картки, чіпи, наклейки, теги, інтелектуальні пил і т. д. дає початок потужному середовищу.

Наші повсякденні місця будуть наповнені і насичені зростаючою кількістю об'єктів, що виробляють та споживають події, екологічний моніторинг та вимірювальні рішення, системи контролю, активації та оповіщення, інтеграційні тканини, автобуси та дисплеї візуалізації та інформаційні панелі, елементи

мережевих та автоматичних пристроїв, десятки кишенькових комп'ютерів, портативних комп'ютерів, переносних приладів та ін., щоб зробити наше життя і місця приємним і придатним для життя.

Тобто розумний будинок – це система, яка забезпечує безпеку, ресурсозбереження та комфорт для всіх його користувачів. Як правило в розумному будинку є центральний процесор – так звані мізки будинку. Цей процесор розпізнає конкретні ситуації, що відбуваються в будинку і реагує на них: керує поведінкою інших систем за допомогою заданих алгоритмів (наприклад, включення світла в коридорі, коли відкривається вхідні двері). За рахунок цього в розумному будинку немає необхідності використовувати десятки різних пультів для кожного телевізора або кондиціонера, або постійно намацувати вимикачі світла в темряві.

Всю систему можна розділити на деякі компоненти: автоматизація, ручне управління, мультимедіа, безпеку.

Автоматизація – в нашому випадку це налаштування роботи системи в залежності від часу доби, рівня освітленості, руху, температури, макросів і сценаріїв.

Ручне управління всім зрозуміло, але не сказати про нього не можна. Це віддалене управління по телефону, комп’ютера, web додатком, бездротове управління електронікою, установка одного пульта для всіх пристроїв (завжди мріяв позбутися від нескінченної кількості пультів).

Мультимедіа – бездротове аудіо / відео, спостереження та інше.

Безпека – напевно, один з найбільш важливих аспектів при виборі розумного будинку. Клієнт може встановити охоронну сигналізацію, світлову / звукову сигналізацію, створити імітацію присутності господарів, додати функцію «паніка» та інше.

«Розумний будинок» являє собою автоматизовану систему управління різними компонентами домашньої інфраструктури.

За допомогою спеціального обладнання, система може розпізнавати типові ситуації і реагувати на них, підключаючи ті чи інші компоненти. При цьому,

«розумний дім» повністю контролює роботу кожного приладу і не допускає нераціонального їх використання.

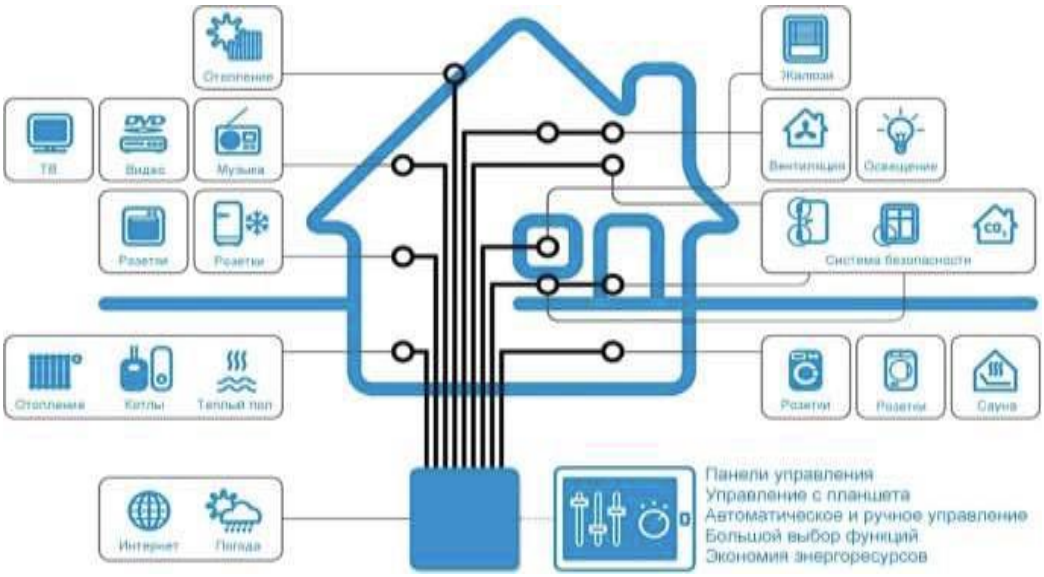

Рисунок 15.6 – Компоненти «розумного будинку»

Таким чином, за рахунок «синергетичного ефекту», розумний будинок дозволяє забезпечити оптимальний режим використання всієї сукупності приладів в будинку. А це дозволяє створити максимально комфортні умови проживання людей при максимально економному споживанні ресурсів.

Вся система «розумний будинок» складається з трьох основних підсистем:

Точка управління. Сучасні технології дозволяю забезпечити управління компонентами системи за допомогою самих різних пристроїв. Це може бути як простий вимикач, так і Touch-панель або iPad. Крім того, управління компонентами системи можна здійснювати за допомогою голосу або бавовни долонями. Дистанційне керування забезпечується за допомогою мобільного телефону, SMS та інших подібних рішень.

Центральний контролер. Це, власне, головний мозок всієї системи. Саме сюди надходить вся інформація про роботу того чи іншого пристрою. Крім того, центральний контролер отримує і обробляє команди, одержувані від точок управління. Завдяки функціям центрального контролера став можливий

ефективний контроль гармонійної роботи всіх приладів в будинку, починаючи від лампочки, до систем вентиляції або опалення.

Виконуючий пристрій. Під цим терміном розуміється вся сукупність приладів і систем в будинку. Це можуть бути, як прості прилади, на зразок мікрохвильової печі або музичного центру, так і вельми складні інтелектуальні системи, на зразок системи опалення або системи відеоспостереження.

Як правило, дана система забезпечує взаємодію кількох систем, інтегрованих в єдину систему управління всіма приладами і комунікаціями будинку. При цьому, найбільш частими компонентами системи «розумний будинок» є такі системи:

Електроживлення будинку. Розумний будинок контролює наявність електроживлення всіх інших систем в будинку. У разі необхідності, він самостійно задіє джерела безперебійного живлення і, в разі необхідності, додаткові генеруючі потужності.

Освітлення. Оптимальне використання освітлювальних приладів, з урахуванням рівня природного освітлення дозволяє забезпечити максимальну економію електричної енергії. Крім того, система забезпечує оптимальні умови для комфортного проживання людей.

Температура, вологість і своєчасне надходження свіжого повітря. Датчики, що вимірюють вищевказані параметри дають команду систем опалення, вентиляції та кондиціонування в автоматичному режимі. А це означає, що «розумний будинок» завжди підтримує оптимальні параметри повітря в приміщенні.

Управління побутовою технікою. Всі прилади, що працюють в будинку, можуть бути об’єднані в єдину мережу. Завдяки цьому, центральний контролер має можливість оптимально організувати роботу відеотехніки і кухонних приладів, систем підігріву ступенів і приводів автоматичних воріт.

Безпека. Сюди входять такі системи, як обмеження доступу в будинок небажаних осіб, контроль витоку газу, сигналізація і відеоспостереження та інші системи, що дозволяють контролювати рівень безпеки в будинку. Крім того,

розумний будинок може забезпечити віддалене інформування про будь-якому інциденті в приміщенні, під час відсутності людей і навіть зімітувати їх присутність.

Слід зауважити, що в кожному конкретному випадку не обов’язкова наявність всіх вищевказаних систем. Технологія «розумний дім» відрізняється гнучкістю, і може бути оптимізована під конкретні вимоги певного клієнта.

Рисунок 14.7 – Система розумний будинок

"Розумний будинок" включає роботу з такими системами оснащення будівель:

1. Електротехнічні роботи

1.1. Освітлення

– Механічне керування

– Дистанційне керування

– Керування рівнем освітлення

– Розумні сценарії (реагування на природне освітлення, рух, тощо)

1.2. Силова проводка (Електрика, розетки звичайні та силові)

– Силові розетки (духовка, бойлер, мікрохвильовка тощо)

– Дистанційне керування

– Контроль розеток в дитячих кімнатах.

1.3. Електрощитова

– Блоки безперебійного живлення

– Стабілізація напруги

– Захист від пожежі

– Захист від ураження

– Захист від обриву нуля

– Контроль над споживанням

1.4. Слабовольтні мережі, датчики контролю

– Температури

– Вологості

– Руху

– Освітлення

– Гази/повітря

2. Контроль Опалення/Вентиляція

– Газ

– Котельна

– Твердопаливний котел

3. Безпека

4. Відеоспостереження

– Закритий/відкритий контур

5. Мультимедія/розваги

6. Керування шторами

7. Захист від протікання води

8. Керування голосом

9. Самонавчання

10. Інтеграції із сервісами (календар, будильник, знаходження по GPS)

11. Інтеграція із сучасною побутовою технікою

12. Підтримка сучасних стандартів і протоколів розумного будинку (KNX, ZigBee, і ін.)

13. Контроль на замками
14. Енергозбереження
15. Датчик шуму
16. Центральний порохотяг

Загрози «розумного будинку»

Експерти наполегливо заявляють про те, що постачальники послуг і пристроїв ринку IoT порушують принцип наскрізної інформаційної безпеки (ІБ), який рекомендований для всіх ІКТ-продуктів і послуг. Згідно з цим принципом, ІБ повинна закладатися на початковій стадії проектування продукту або послуги і підтримуватися аж до завершення їх життєвого циклу.

Але що ж ми маємо на практиці? Ось, наприклад, деякі дані досліджень корпорації HP (літо 2014 роки), метою яких було не виявити якісь конкретні небезпечні інтернет-пристрої і викрити їх виробників, але позначити проблему ІБ-ризиків в світі IoT в цілому.

Дослідники HPE звертають увагу на проблеми як на стороні власників пристроїв, так і на проблеми, над якими повинні подумати розробники. Так, на самому початку експлуатації користувачеві обов'язково потрібно замінити фабричний пароль, встановлений за замовчуванням, на свій особистий, оскільки фабричні паролі однакові на всіх пристроях і не відрізняються стійкістю. На жаль, роблять це далеко не всі. Оскільки не всі прилади мають вбудовані засоби ІБ-захисту, власникам також слід подбати про встановлення зовнішнього захисту, призначеної для домашнього використання, з тим щоб інтернет-пристрою не стали відкритими шлюзами в домашню мережу або прямими інструментами заподіяння шкоди.

В ході проведеного HP дослідження виявлено, що приблизно в 70% проаналізованих пристроїв не шифрується бездротової трафік. Веб-інтрефейс 60% пристроїв експерти HP порахували небезпечним через небезпечну організацію доступу і високих ризиків міжсайтового скриптинга. У більшості

пристроїв передбачені паролі недостатньою стійкості. Приблизно 90% пристроїв збирають ту чи іншу персональну інформацію про власника без його відома.

Всього ж фахівці HP нарахували близько 25 різних вразливостей в кожному з досліджених пристроїв (телевізорів, дверних замків, побутових ваг, домашніх охоронних систем, електророзеток ...) і їх мобільних і хмарних компонентах.

Висновок експертів HP невтішний: безпечної екосистеми IoT на сьогоднішній день не існує. Особливу небезпеку речі Інтернету таять в собі в контексті поширення цільових атак (APT). Варто тільки зловмисникам проявити інтерес до будь-кого з нас, і наші вірні помічники зі світу IoT перетворюються в зрадників, нарозхрист відкривають доступ в світ своїх власників.

Слабкі місця IoT:

- перехід на IPv6;
- живлення датчиків;
- стандартизація архітектури і протоколів, сертифікація пристроїв.
- інформаційна безпека;
- стандартні облікові записи від виробника, слабка аутентифікація;
- відсутність підтримки з боку виробника для усунення вразливостей
- важко або неможливо оновити ПЗ і ОС;
- використання текстових протоколів і непотрібних відкритих портів;
- використовуючи слабкість одного гаджета, хакеру легко потрапити у всю мережу;
- використання незахищених мобільних технологій;
- використання незахищеною хмарної інфраструктури;
- використання небезпечного ПЗ.

Оскільки Інтернет речей продовжує інтегрувати, здавалося б, безглузді і незв'язані об'єкти, то повноцінна домашня операційна система виглядає цілком вірогідною. Хоча це перетворить Ваш будинок в оптимізований життєвий простір, повністю призначений для забезпечення Вашого комфорту, тим не

менш, вона може також нести Вам серйозні ризики стати жертвою кібер-атаки в Вашому власному будинку.

Рисунок 15.8 – Загрози «розумного будинку»

Центральна ланка будь-якої системи безпеки розумного будинку майбутнього - це його замок. До речі, недавнє дослідження показало, що розумні замки лякаюче легко можна зламати, в результаті чого вони не можуть гарантувати виконання своєї основної функції, для якої, власне кажучи, вони й існують.

Існуючі системи досить прості для кібер-хакерів і не є перешкодою для того, щоб проникнути в Ваш будинок. А що якщо далі хакери в майбутньому зможуть використовувати це технологічне досягнення проти Вас? Якщо розумний замок можна зламати, щоб його відкрити, можливо, хакери знайдуть спосіб, як повністю його закрити, щоб Ви не могли його відкрити. В цьому випадку в майбутньому можна буде досить тихо проникати в чужий будинок: хакер зможе контролювати всі події віддалено. Більш того, він зможе вимагати у

своїх жертв який-небудь розумний викуп за те, щоб вони могли потрапити в свої власні будинки. До речі, це може бути ідеєю для сценарію якого-небудь страшного фільму (Зовсім один вдома), але це жахлива думка. Якщо всі Ваші пристрої безпеки взаємопов'язані, то кібер-злочинці потенційно могли б отримати доступ також до Вашої домашньої сигналізації і навіть ключів від Вашого автомобіля.

Задимлений екран - тривога про пожежу. Одна функція безпеки, яка вже вбудована в деякі доступні на ринку детектори диму, - це можливість, що дозволяє розумному будинку отримувати інформацію (і використовувати її в подальшій роботі) від інших смарт- пристроїв, що дозволяє системі реагувати відповідним чином в разі небезпеки. Ця функція впроваджена для безпеки користувача, дозволяючи домашній системі, яка виявила пожежу, наприклад, розблокувати всі двері в будинку, щоб допомогти вибратися з нього якомога швидше. Це відмінний приклад того, як виробники IoT-рішень працюють над прозорою інтеграцією і взаємодією смарт-пристроїв всередині розумного будинку.

Однак є одне застереження: якщо ця технологія буде використовуватися кіберзлочинцями, то існує ймовірність створення небажаної ланцюгової реакції, яка в кінцевому підсумку може, навпаки, знизити рівень безпеки розумного будинку.

Ще один спосіб, коли хакер міг би потенційно здалеку нашкодити, - це створення хибної тривоги про пожежу, яка відправляється в пожежні служби. Хаотична сцена може виглядати у вигляді задимленого екрану, що також в результаті може зробити Вас легкою здобиччю для інших потенційно шкідливих кібер-атак.

Чи можна використовувати IoT-пристрої для кібер-атаки? Легко. Зловмисники, як правило, працюють на маси: наприклад, розподілені атаки на відмову в обслуговуванні (DDOS), коли тисячі електронних листів або запитів відправляються на якийсь сервер, щоб уповільнити його роботу або взагалі вивести його з ладу. В цьому випадку в майбутньому ми можемо зіткнутися з

ситуаціями, коли хакери спробують «завалити» якомога більше машин в надії на те, що якась їх частина буде працювати неправильно, що призведе до тяжких наслідків. Взагалі-то, лякає така перспектива. Можливо, саме з цієї причини урядові органи говорять про потенційні небезпеки Інтернету речей, пов'язаних з кібер-атаками.

Остерігайтеся холодильника. В мультсеріалі «Сімпсони» був епізод, коли Мардж нападає на домашню операційну систему з штучним інтелектом, яка готує їжу, але таємно планує «позбутися» від інших членів сім'ї. Звичайно, це кумедна пародія, але бентежить те, що нам буде потрібно всього кілька технологічних досягнень, щоб ці події вже перестали бути смішними, а опинилися жахливою дійсністю. Добре, припустимо, що Ваш холодильник поки не веде з Вами інтелектуальних бесід, і вже тим більше, не опрацьовує якісь вбивчі схеми щодо Вашої родини. Однак ще два роки тому ЦРУ відзначили загрозу з боку смарт- холодильників в розумних будинках. До чого б це? ЦРУ заметушилося від того, що холодильник використовувався як частина бот-мережі для виконання DDOS-атаки. І все це відбувалося зовсім непомітно для господаря цього холодильника, який навіть і гадки не мав про те, що його смарт-пристрій може виконувати якісь диявольські дії, крім як охолоджувати і зберігати їжу.

Сертифікація пристроїв IoT для захисту від хакерів. 11 жовтня 2016 року стало відомо про плани Єврокомісії - ввести обов'язкову сертифікацію або іншу аналогічну процедуру всіх приладів, що підключаються до інтернету речей. Передбачається вжити заходів на державному рівні, що повинно перешкодити хакерам використовувати інтернет речей для створення ботнетів. Як варіант, не виключається установка на пристрої мережі спеціальних уніфікованих чіпів, які убезпечать їх від атак хакерів. Ці заходи, на думку чиновників Єврокомісії, повинні підвищити рівень довіри до інтернету речей в суспільстві і перешкодити хакерам створювати ботнети з підключається техніки.

«Заходи щодо захисту інтернету речей від хакерів слід приймати саме на державному рівні, оскільки в контролі потребують не тільки самі прилади, а й

мережі, до яких вони підключені, а також хмарні сховища. Схема сертифікації інтернету речей можна порівняти з європейською системою маркування енергоспоживаючих товарів, прийнятої в 1992 році.

Маркування є обов'язковою для автомобілів, побутової техніки та електричних ламп. Але виробники техніки вважають систему подібної маркування неефективною для захисту від хакерів. Замість цього вони вважали за краще б встановити в прилади стандартний чіп, який буде відповідати за безпеку підключення до інтернету.» - Тібо Клейнер (Thibault Kleiner), заступник європейського комісара з цифрової економіки та суспільству.

До групи приладів, що підключаються до інтернету, входять відеокамери, телевізори, принтери, холодильники та інша техніка. Велика частина цих пристроїв незадовільно захищена від хакерських атак. Самі по собі ці пристрої можуть не подавати інтересу для злочинців. Однак хакери зламують їх, щоб використовувати в якості роботів для створення ботнетів, за допомогою яких можна атакувати більш серйозні системи. Більшість власників зламаних пристроїв навіть не підозрюють, як використовується їхня техніка.

Як приклад наведена масштабна DDoS-атака на інтернет-ресурс Krebs On Security, в вересні 2016 року. «Інтенсивність запитів від ботнеті під час атаки досягла 700 Гб / с. У складі ботнету більш 1 млн камер, відорегістраторов та інших підключених до інтернету речей пристроїв. Це не перший резонансний випадок, коли подібні пристрої стають частиною ботнету, проте вперше мережа складалася майже повністю з таких приладів.» - Брайан Кребс (Brian Krebs), власник ресурсу.

За даними Gartner, до інтернету речей підключено близько 6 млрд приладів, а до 2020 року їх число досягне 20 млрд, що створить хакерам ширші можливості для проведення масштабних атак за допомогою ботнетів.

У споживачів немає впевненості в безпеці пристроїв IoT. Компанія Gemalto оприлюднила в жовтні 2017 року статистику: виявляється, 90% споживачів не довіряють безпеці пристроїв Інтернету речей. Ось чому понад дві третини

споживачів і майже 80% організацій підтримали уряди, що беруть заходи щодо забезпечення безпеки IoT.

Основні побоювання споживачів (згідно двом третинам респондентів) стосуються хакерів, які можуть встановити контроль над їх пристроєм.

Фактично, це викликає більше занепокоєння, ніж витік даних (60%) і доступ хакерів до особистої інформації (54%). Незважаючи на те, що пристроями IoT володіє більше половини (54%) споживачів (в середньому, по два пристрої на людину), тільки 14% вважають себе обізнаними про безпеку цих пристроїв. Така статистика показує, що як споживачам, так і підприємствам, необхідно додаткову освіту в даній сфері.

Фактично, майже кожна організація (96%) і кожен споживач (90%) відчувають необхідність в правилах щодо забезпечення безпеки Інтернету речей, прийнятих на рівні уряду.

Контроль над смарт-пристроями. Уразливість в мобільному і хмарному додатках LG SmartThinkQ дозволили дослідникам Check Point віддалено увійти в хмарний додаток SmartThinQ, і, заволодівши обліковим записом LG, отримати контроль над пилососом і вбудованої в нього відеокамерою.

Отримавши контроль над обліковим записом конкретного користувача LG, зловмисник може контролювати будь-який пристрій LG або пристрій, пов'язаний з цим обліковим записом, включаючи пилососи, холодильники, плити, посудомийні і пральні машини, фени та кондиціонери, розповіли в компанії. Уразливість HomeHack дає хакерам можливість стежити за сімейним життям користувачів за допомогою відеокамери робота-пилососа Hom- Bot, яка в режимі реального часу надсилає відео в додаток LG SmartThinQ в рамках функції HomeGuard Security. Залежно від моделей пристроїв LG зловмисники можуть також включати і відключати посудомийні або пральні машини. Наразі таку уразливість усунено.

Атаки на «розумний будинок»

Очевидно, що «розумний дім» знаходиться в небезпеці, оскільки, крім проводових загроз існують атаки по безпроводовим мережах і тому є більш уразливими, в наслідок використання відкритого середовища в якості носія даних і широкомовної природи безпроводових з'єднань.

Пасивні атаки

Аналіз трафіку і прослуховування комунікаційного каналу неавторизованими особами класифікується як пасивна атака. Атаки, націлені виключно на отримання передаються даних є пасивними по своїй натурі. Найбільш частими є наступні види атак спрямовані на порушення конфіденційності даних:

- Моніторинг і прослуховування. Даний вид атаки зустрічається найбільш часто. За допомогою підслуховування зловмисник може з легкістю отримати доступ до передається даними. При передачі контрольної інформації про конфігурацію мережі, дана техніка може становити найбільшу небезпеку для конфіденційності даних.
- Аналіз трафіку. Навіть коли інформація передається в зашифрованому вигляді, залишається ймовірність використання зловмисником техніки аналізу комунікаційних патернів. Активність сенсорів потенційно може розкрити досить інформації для нанесення зловмисником шкоди сенсорної мережі.

Активні атаки

Різні модифікації даних під час комунікації, здійснювані неавторизованими особами, класифікуються як активні атаки. Нижче надаються описи активних атак.

Атаки маршрутизації

Атаки, які здійснюються на мережевому рівні (network layer) моделі OSI називаються атаками маршрутизації. Наступні атаки маршрутизації зустрічаються найбільш часто:

Змінена маршрутна інформація. Найбільш схильні до даної атаки децентралізовані мережі, де кожен вузол є маршрутизатором і відповідно може змінювати маршрутну інформацію. Внаслідок даної атаки можуть відбуватися закільцьовування маршруту, збільшуватися час пакета даних в шляху до точки призначення і т. д.

Вибіркова розсилка. Скомпрометований вузол сенсорної мережі може вибірково видаляти певні пакети. Особливо ефективною дана атака може бути в комбінації з атаками, які збирають велику кількість трафіку на одному вузлі мережі. В результаті даної атаки серйозно страждає цілісність і доступність даних, що може істотно знизити рівень сервісу, що надається сенсорної мережею.

Атака «бездонна воронка» (Sinkhole Attack). Дана атака характерна тим, що скомпрометований вузол мережі починає діяти подібно воронці, використовуючи весь трафік сенсорної мережі. Особливо в мережах з протоколом маршрутизації, заснованому на широкомовній розсилці, зловмисник «слухає» запити на маршрути і відповідає сенсорним вузлам, що «знає» найкоротший маршрут до базової станції.

Як тільки скомпрометованому вузлу вдалося встати між сенсорним вузлом, що транслює і базовою станцією, він може виробляти будь-які дії з пакетами даних, що надходять.

«Шаманська атака» (Sybil attack). Під час даної атаки один скомпрометований вузол може використовувати кілька псевдо ідентифікаторів, видаючи себе відразу за кілька вузлів. Подібні атаки використовуються для порушення механізму розподіленого зберігання, механізмів маршрутизації, механізмів агрегації даних, механізмів голосування в мережі і т. д. По суті будь-

яка мережа з рівноправними вузлами (особливо бездротові і децентралізовані мережі) є схильною до даної атаки.

Атака (Wormhole attack). Дана атака передбачає створення спеціального шляху між двома і більше скомпрометованими вузлами сенсорної мережі для передачі по ним перехоплених пакетів, доступних тільки для атакуючої системи. Подібні атаки представляють серйозну загрозу безпеці сенсорної мережі тому, що не вимагають компрометації вузла сенсорної мережі. Тоді коли вузол В (базова станція або звичайний вузол) використовує широкомовну розсилку для запиту маршруту, зловмисник отримує даний запит і перенаправляє його до найближчого сусіда. Будь-який вузол, який отримав подібний перенаправлений запит розглядає себе як вузол, що знаходиться в зоні досяжності вузла В і запам'ятовує вузол В як свого «батька». Навіть якщо цей вузол знаходиться на великій відстані від вузла В і його відокремлюють від вузла В безліч сенсорних вузлів, він буде розглядати вузол В як наступний від себе.

Флуд атака (HELLO flood attack). Дана атака є широкомовною атакою, покликаною направити в сенсорну мережу масу необов'язкових повідомлень, які повинні позбавити мережу різноманітних ресурсів - канальної ємності, обчислювальної потужності, енергетичних ресурсів і т.д. Під час подібної атаки зловмисник за допомогою високочастотного радіопередавача з достатньою обчислювальною потужністю розсилає Hello пакети до безлічі вузлів сенсорної мережі. Вузли, які отримали Hello пакети, розглядають скомпрометований вузол як свого сусіда. Під час наступної передачі даних, вони будуть використовувати отриманий адресу з Hello пакетів для відправки. Таким чином, зловмисник отримає доступ до даних.

Інші атаки

Відмова в обслуговуванні.

Даний вид атаки може бути результатом ненавмисного виходу з ладу вузлів сенсорної мережі або ж результатом дій зловмисників. Найпростіша атака такого роду спрямована на витрату всіх ресурсів, доступних скомпрометованому

вузлу за допомогою відправки непотрібних пакетів даних, таким чином перешкоджаючи легітимним користувачам мережі отримувати призначені їм сервіси і ресурси. Дана атака має на увазі не тільки спроби зловмисника зруйнувати мережу або розірвати з'єднання, але і будь-яка подія, що знижує здатність мережі надавати певні послуги і ресурси. Безліч типів подібних атак може бути здійснено на різних рівнях моделі OSI.

Захоплення вузла (node subversion)

Захоплення вузла зловмисником може спричинити розкриття важливої інформації, наприклад, криптографічних ключів, що в свою чергу може спричинити компрометацію всієї сенсорної мережі.

Несправність вузла (malfunction)

Несправний в результаті атаки вузол генерує невірні дані, що може порушити цілісність сенсорної мережі, особливо, якщо несправний вузол є вузлом, що агрегує дані, наприклад, головним вузлом кластера.

Простій вузла / вихід з ладу

Простій вузла або його вихід з ладу трапляється тоді коли вузол перестає функціонувати. У разі виходу з ладу головного вузла кластера, протокол сенсорної мережі повинен бути здатний надати альтернативний маршрут для пакетів даних.

Фізичні атаки

Вузли мережі часто встановлюються в середовищах із зовнішніми впливами. В таких середовищах маленький впливаючий фактор вузлів сенсорної мережі в поєднанні з відсутністю постійного нагляду за ними робить їх схильними до різних фізичних атак. На відміну від інших видів атак, фізичні атаки руйнують сенсори незворотньо.

Спотворення повідомлення

Будь-яка зміна контенту повідомлення зловмисником неминуче компрометує цілісність передачі даних.

Хибний вузол

Даний вид атак передбачає впровадження в мережу вузла, який посилає вузлів сенсорної мережі некоректні дані. Дана атака є однією з найбільш небезпечних атак, оскільки запроваджений вузол, який поширює зловмисний код, може привести до загибелі всю сенсорну мережу.

Копіювання вузла мережі

Концептуально дана атака полягає в наступному: зловмисник намагається впровадити заздалегідь підготовлені вузли в існуючу сенсорну мережу, використовуючи ідентифікатори вже існуючих вузлів в даній мережі. Для цього зловмисник фізично захоплює один вузол мережі з метою отримання його унікальних даних. За допомогою впровадження реплікованих вузлів зловмисник може з легкістю управляти сегментом мережі.

Алгоритм надання захисту системи “Розумний будинок”

1. Стандартизація: мережа IoT в даний час є переважно бездротовою, це робить безпеку набагато складнішою, ніж традиційні дротові мережі через різноманіття нових протоколів і стандартів щодо радіочастот та радіозв'язку. Пристрої та система в цілому має відповідати стандартам, щоб забезпечити безпеку вашої системи та не зробити її уразливою для злочинців.

2. Сертифікація пристроїв/перевірка справжності: окрім відповідності стандартам, необхідно забезпечувати складові мережі сертифікатами, що видаються центрами сертифікації, для можливості перевірки пристроїв, що бажають проникнути в Вашу мережу та можуть їй зашкодити. Така перевірка допомагає проаналізувати певний пристрій на реєстрацію в своєрідній базі та надасть інформацію стосовно якості і можливості нанести збитки.

3. Аутентифікація: пристрої IoT повинні бути законними користувачами. Методи досягнення такого роду аутентифікації від статичних паролів до двофакторної аутентифікації, біометрії та цифрових сертифікатів. Унікальним для IoT є те, що пристрої(наприклад, вбудовані датчики) повинні розпізнати інші пристрої. Саме це зменшує ймовірність проникнення чужорідного тіла в системі.

4. Шифрування: необхідне для запобігання несанкціонованого доступу до даних. Це важко забезпечити через розмаїття пристроїв IoT та апаратних профілів. Проте шифрування має бути частиною повного процесу управління безпекою. На сьогоднішній день вчені сперечаються з приводу надійності того чи іншого варіанту та використання його в IoT, проте вже розроблений чіп для шифрування на еліптичних кривих, що може застосовуватися в пристроях Інтернету речей.

5. Захист інтерфейсу: більшість виробників обладнання та програмного забезпечення надають доступ до пристроїв через програмний інтерфейс(API). Їх забезпечення вимагає наявності аутентифікації та авторизації пристроїв, які потребують обміну даними. Тільки авторизовані пристрої, розробники та програми здатні здійснювати зв'язок між захищеними пристроями.

6. Механізми доставки: потрібні постійні оновлення та патчі, необхідні для подолання мінливої тактики кібератакерів. Це вимагатиме знань у патчах, що виправлятиме прогалини в критичному програмному забезпеченні на льоту.

7. Аналітика безпеки та прогнозування загроз: необхідно не лише стежити та контролювати дані пов'язані з безпекою, а також використовувати їх для прогнозування майбутніх загроз. Вони повинні доповнювати традиційні підходи, які шукають дії, що виходять за рамки встановленої політики.

8. Контроль доступу: якщо який-небудь компонент скомпрометовано, контроль гарантує, що вторгнення матиме мінімальний доступ до інших частин системи, наскільки це можливо. Механізми контролю доступу на базі пристроїв аналогічні мережевим системам, навіть якщо хтось зможе вкрасти корпоративні облікові дані для входу в систему, скомпрометована інформація буде обмежуватися лише тими областями мережі, де вона авторизована.

9. Фізична безпека: окрім безпеки внутрішньої, мережі необхідний захист ззовні, тобто, наприклад, якщо це датчик, то він має бути розміщений таким чином, щоб зловмисник не мав до нього прямого фізичного доступу і був непомітний для нього.