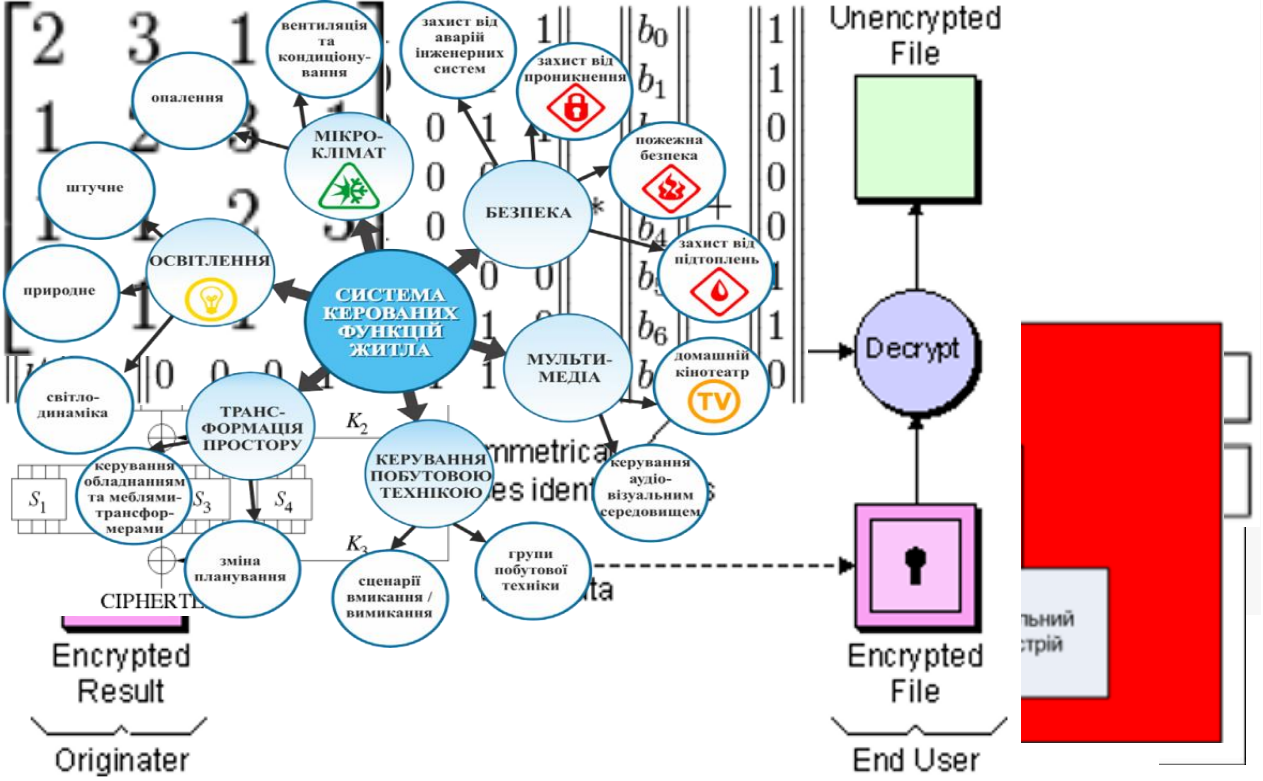

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на освітній ступінь магістр

на тему:

«Забезпечення безпеки в системі розумний дім »»

Виконав: студент 6 курсу, групи БСДМ-61
Спеціальності 125 Кібербезпека_____

Освітньо-професійної програми_____
«Інформаційна та кібернетична безпека»_____
(шифр і назва спеціальності)
_____Авєрін І.Ю.
(прізвище та ініціали)
Керівник __Козачок В. А._____
(прізвище та ініціали)
Рецензент____
(прізвище та ініціали)
Нормоконтролер ___Чумак Н.С._____

КИЇВ – 2019

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Г.І. Гайдур
“___” _____ 2019 року

ЗАВДАНЯ
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

__Авєріну Івану Юрійовичу__
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: Методи за засоби захисту інформації системи «розумний дім»»
керівник бакалаврської роботи:
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від «24» жовтня 2019 року № 487.
2. Строк подання студентом магістерської роботи: 15.12.19р.

3. Вихідні дані до магістерської роботи:

1. Система «Розумний будинок»

2. Антивірусні програми та програмне забезпечення
3. Система інтелектуального керування системою «розумний будинок»
4. Існуючі системи зв'язку в системі «Розумний будинок»
5. Класифікація загроз безпеки інформації
6. Пропозиції щодо захисту інформації в системі «Розумний будинок»

4. Зміст розрахунково–пояснювальної записки (перелік питань, які потрібно розробити):

1. Система «Розумний будинок», загальні відомості
2. Актуальність проблеми забезпечення інформаційної безпеки системи «Розумний будинок»
3. Методи і засоби забезпечення інформаційної безпеки системи «розумний будинок»

5. Перелік графічного матеріалу:

1. Тема
2. Вступ
3. Система «Розумний будинок»
4. Дослідження вразливостей безпеки в системі «Розумний будинок»
5. Забезпечення захисту в системі «Розумний будинок»
6. Висновки

6. Дата видачі завдання: 24 жовтня 2019р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів магістерської роботи	Примітка
1.	Отримання та уточнення постановки завдання	27.10.2019р.	вик.
2.	Підбір науково–технічної літератури та її аналіз	05.11.2019р.	вик.
3.	Збір даних	12.11.2019р.	вик.
4.	Архітектура системи «Розумний будинок»	19.11.2019р.	вик.
5.	Функції, технології і архітектура систем «Розумний будинок»	22.11.2019р.	вик.
6.	Дослідження вразливостей та методів захисту систем «Розумний будинок»	28.11.2019р.	вик.
7.	Висновки, вступ, анотація	03.12.2019р.	вик.
8.	Оформлення та друк пояснювальної записки	06.12.2019р.	вик.
9.	Оформлення презентацій	12.12.2019р.	вик.
10.	Отримання рецензій	14.12.2019р.	вик.
11.	Захист в ДЕК	01.2020р.	

Студент _____ Авєрін І.Ю
(підпис) (прізвище та ініціали)

Керівник магістерської роботи _____ **Козачок В. А. .**
(підпис) (прізвище та ініціали)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент __Авєрін І.Ю____ до захисту магістерської роботи
(прізвище та ініціали)
Спеціальності: 125 Кібербезпека
Освітньо–професійної програми: «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
На тему: «Методи за засоби захисту інформації системи «розумний дім»»
Магістерська робота і рецензія додаються.
Директор інституту _____ САВЧЕНКО В.А.
(підпис)

Довідка про успішність

_____Авєрін І.Ю_____ за період навчання в інституті, на факультеті, у відділенні
(прізвище та ініціали студента)
ННІЗІ з 2018____року до 2020___ року повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.
Секретар інституту, факультету (відділення) _____ __ _Гребенніков А.Б._____
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент __Авєрін І.Ю__ обрав тему роботи, метою якої було дослідити методи та засоби захисту інформації системи «Розумний будинок». Перелік використаних джерел свідчить про вміння дипломником розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи _Авєрін І.Ю._ показав добру теоретичну та практичну підготовку, вміння вирішувати самостійно питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану магістерську роботу студента Авєріна Івана Юрійовича на оцінку **«добре»** та присвоїти йому кваліфікацію 2149.2 професіонал з організації інформаційної безпеки, викладач вищих навчальних закладів.

Керівник магістерської роботи _____ __Козачок В.А__
(підпис)
“___”_____2020 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент __Авєрін І.Ю_____
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії.
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)
_____ ___Гайдур Г.І.___
(підпис) (прізвище та ініціали)
“____”_____2020 рік

ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студента **Авєріна Івана Юрійовича**

на тему: **«Методи за засоби захисту інформації системи «розумний дім»»**

Актуальність:

Розумний будинок - автоматична система управління будівлею. Під «розумним будинком» слід розуміти систему, яка допомагає людині забезпечити повний контроль і моніторинг всіх інженерних систем будівлі. Результати аналізу показують, що системи «розумний дім» мають низький ступінь захищеності. Одним з важливіших аспектів цього питання є проблеми, що виникають при вивченні каналів передачі даних. В зв'язку з цим є вразливість до несанкціонованого доступу, та загрози цілісності інформації. Тому тема магістерської роботи є актуальною.

Позитивні сторони:

1. Зміст роботи відповідає завданню. Студент показав гарний рівень знань і ступінь підготовленості його до майбутньої роботи за фахом.

2. Обґрунтовано проведено дослідження різних вразливостей та забезпечення захисту в системі «розумний дім».

3. Текст викладено грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. В роботі доцільно було б використати метод експетної оцінки для визначення кращого протоколу шифрування.

2.. Виявлено несуттєві недоліки магістерської роботи: недостатньо ілюстративних матеріалів, графіків, стиль викладу не скрізь витриманий.

Висновок:

Вказані зауваження не суттєво впливають на якість виконаної роботи, яка заслуговує оцінки "добре", а студент – Авєрін Іван Юрійович гідний присвоєння кваліфікації 2149.2 професіонал з організації інформаційної безпеки, викладач вищих навчальних закладів.

Якість магістерської роботи	
виконано на замовлення підприємства	
виконано за тематикою НДР	
виконано з макетом	
має практичну цінність	*

Підпис рецензента

_____ _____

(П.І.Б.)

_____

(посада, науковий ступінь, вчене звання)

РЕФЕРАТ

до магістерської роботи

Магістерська робота складається зі вступу, трьох розділів, загальних висновків, а також списку використаних джерел. Загальний обсяг роботи 71 сторінка, 19 рисунків, 4 таблиці, 21 джерело.

Об'єктом дослідження процес застосування технології інтернету речей та захисту його системи

Предметом дослідження є дослідження вразливостей та забезпечення захисту в системі «розумний дім».

Мета роботи: магістерська робота присвячена дослідженням методів та засобів захисту інформації в системі «Розумний дім», для безпечної передачі даних на основі PKI. У роботі було проаналізовано основні криптографічні схеми захисту, та рівень їх надійності.

Велика увага приділяється алгоритмам шифрування, таким як:

- Base64, AES, RSA;
- схемам захисту з відкритим ключем, симетричним та PKI.

Було проведено порівняльну характеристику алгоритмів шифрування, визначено їх недоліки та де вони застосовуються.

Галузь використання – інформаційна система «Розумний дім».

Ключові слова: ПАРОЛЬ, АНАЛІЗ, БЕЗПЕКА, PKI, AES, DES, TRIPLE DES, RSA, ЕЛІПТИЧНІ КРИВІ, ПОРУШНИК, ВРАЗЛИВОСТІ, РОЗУМНИЙ БУДИНОК, КЛІЄНТ – СЕРВЕРНИЙ ДОДАТОК.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AES (Advanced Encryption Standard) – симетричний шифр (стандарт).

DES (Data Encryption Standard) – симетричний шифр (стандарт).

RSA (Rivest, Shamir, Adleman) – асиметричний шифр.

PKI (Public Key Infrastructure) – інфраструктура відкритих ключів.

OSI (open systems interconnection basic reference model) – абстрактна мережева модель для комунікацій і розробки мережевих протоколів.

ЦК — Центральний комп’ютер.

GSM (Group Special Mobile) – глобальна система мобільного зв’язку.

HTTP (Hyper Text Transfer Protocol) — «протокол передачі гіпертексту».

IP — Internet Protocol.

TCP — Transmission Control Protocol.

ПЗ — Програмне Забезпечення.

ІТКС – Інформаційно–телекомунікаційні системи.

СКМ – Структурована кабельна мережа.

ДМ – Дочірні мікроконтролери

ВСТУП

Якщо розглядати розумний будинок по частинах, то майже кожна людина в своєму будинку використовує ті чи інші елементи "Розумного Дому». Це прилади, об'єднані в системи, які призначені зробити наше життя простішим. Як колись, з винаходом пульта до телевізора, чи автоматичної пральної машинки ми почали економити свій час та отримувати більше комфорту, так і сьогодні, встановлюючи інтелектуальний будинок ми отримуємо безліч можливостей для покращення свого проживання в домі. Ми економимо не лише свій час, а й витрати, адже з «Розумним Домом» ми досягаємо максимальної економії енергозатрат (літом до 30%, у зимовий період до 50%). Ми не переймаємось чи вимкнули праску, чи не залишили ввімкненою воду, чи закрили двері, - «Розумний Дім» зробить все за Вас. Ви тримаєте все під контролем.

Розумний будинок складається з набору підсистем, що відповідають за виконання функцій енерго–, тепло– збереження, клімат контролю, безпеки і т.д.. З часом відбулось вдосконалення цих підсистем і збільшення кількості виконуваних ними функцій, тому керувати системою «Розумний будинок» стало легше.

Сучасні «розумні будинки» – це місто в мініатюрі. В них діють служби, що до недавно були невід’ємними частинами звичайного міста. У таких будинках зазвичай присутній адміністратор системи, який і обслуговує цю систему цілодобово. Хоча існує безліч засобів автоматики, яка сама справляється з покладеними на неї завданнями, такими, як наприклад підтримка мікроклімату, опалення, вентиляція будинку, освітлення, пожежна та охоронна сигналізація, контроль входу / виходу і т.д., але управління і обслуговування цих систем вимагає наявності людини.

Обов’язком адміністратора є контроль роботи цих підсистем та вжиття заходів у разі збоїв у їх роботі. Але можуть виникати позаштатні ситуації, коли навіть дії адміністратора можуть виявитися неефективними. Це випадки виникнення загрози людям що знаходяться в будинку та безпосередньо самому

будинку, що мають глобальний характер – пожежа, землетрус, терористична атака і т.д..

Системи забезпечення різних аспектів життя проектуються як автономні. Такі системи, створюються окремо для кожної функції і за допомогою програмних засобів об’єднано в одну. У будинках встановлювалися системи тільки з тими можливостями і з тим ступенем складності, які були необхідні на момент побудови будинку. Подальше розширення і модернізація систем є складними і дорогими завданнями через безліч різних факторів. Витрати на експлуатацію такої системи складаються з витрат на експлуатацію кожної автономної системи окремо.

Вартість експлуатації цих систем висока – в силу їх автономності кожна з них підтримується окремо. Вартість навчання персоналу настільки ж висока, оскільки адміністратори повинні бути ознайомлені з експлуатаційними можливостями кожної автономної системи окремо.

Крім того не останнє місце займає питання безпеки інформації, адже маючи доступ до такого будинку можна завдати дуже великої шкоди його власнику. Оскільки в наш час досить поширеним є віддалене управління та доступ до інформації, слід використовувати захищені схеми, схеми шифрування та захисту, щоб знизити відсоток вразливості та не дати можливості зловмисникам завдати шкоди.

Основним призначенням системи «Розумний будинок» є економія енергоносіїв, що є все більш актуальним у зв’язку з їх подорожчанням в Україні. Тому інтелектуалізація приміщень стає все популярнішою, наздоганяючи світові тенденції до автоматизації побуту. Адже використання «розумної» системи опалення чи системи керування освітленням дозволить значно зменшити енергетичні витрати за рахунок зниження споживання в моменти, коли це не є необхідним.

Розділ 1
ТЕХНОЛОГІЯ «РОЗУМНИЙ БУДИНОК»

«Розумний будинок» – це модернізований будинок, який містить сучасну технологічно–організовану систему, що покликана спростити життя людині. Система забезпечує безпеку, комфорт, та ресурсозбереження для власників, оскільки вміє реагувати на конкретно поставленні завдання і вміє розпізнавати конкретні ситуації, які відбуваються в будинку.

1.1. Історія розвитку

Перші «розумні будинки» з'явилися в США, ще в 50–ті роки XX століття. На той момент це були дійсно унікальні будинки, обладнані спеціальною електронікою, яка керувала та слідкувала за багатьма речами в будинку, наприклад за телевізором, пральною машиною і т.д.. Всі ці побутові прилади були об'єднані в одне ціле, і управлялися з одного пульта, при цьому була можливість контролювати відключення, включення і деякі інші особливості роботи. З часом стали з'являтися інтелектуальні будівлі, які вже були повністю обладнані різною автоматикою, об'єднаною в єдину мережу. Дослідники та розробники стали приділяти особливу увагу не тільки комфортабельності, але і безпеці, а крім того й економії ресурсів завдяки системі «Розумний будинок».

Кошти, які вкладалися в розробку нових технологій для «розумних будинків» були величезними, компанії та інвестори вірили, що в майбутньому це принесе непоганий прибуток. Починаючи з 1978 року, розробники змогли добитися керування електричними побутовими приладами через звичайні дроти, де проводила напруга в 110V. Це був справжній прорив, який дозволив надалі здійснювати розвиток за даною схемою.

Глобальний розвиток почався в 90–і роки XX століття, коли з'явилася чимала кількість різних датчиків і сенсорів, без яких, в наш час, неможливо уявити процес автоматизації.

Сама система «Розумний будинок» втілила у собі безліч інноваційних розробок, які зробили її унікальною з огляду комфорту і безпеки для людини.

Наявність всіх розробок дозволяє сьогодні втілювати мрії багатьох з нас в життя, тепер власнику такого житла необов'язково турбуватися про свій будинок, адже він завжди під контролем обладнання, яке практично не дає збоїв і працює цілодобово увесь рік, навіть коли нікого немає в будинку.

1.2. Система інтелектуального керування інженерними системами

Будь–якій людині де б вона не знаходилась важливо відчувати себе в безпеці та почуватися комфортно. Саме ці два завдання – і є основними цілями «розумного будинку».

Інтелектуальна автоматика керує всіма інженерними системами в будинку, дозволяє людині централізовано встановлювати комфортні для себе – температуру, вологість, освітленість в кімнатах, зонах, і забезпечує безпеку.

Система «Розумний будинок» включає в себе наступні об'єкти автоматизації (Рис. 1.)

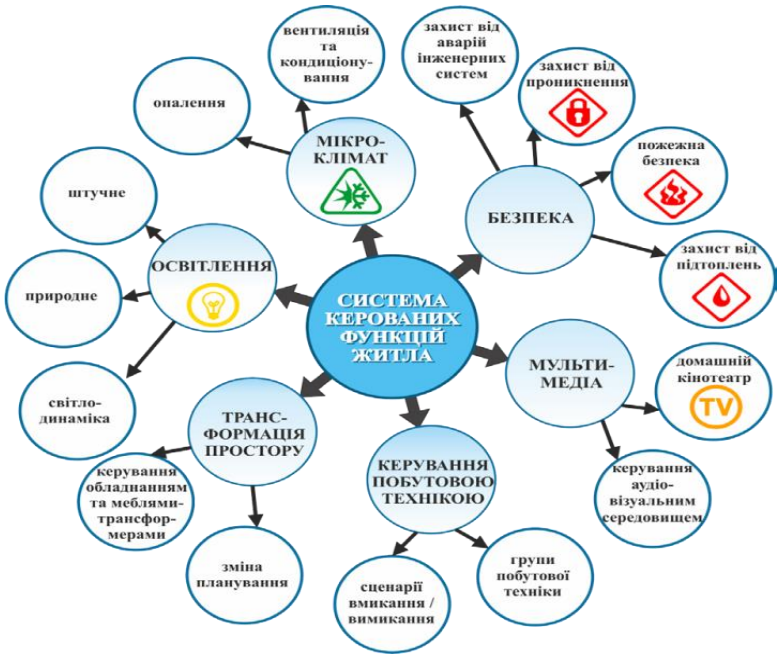

Рис. 1.1.Схема основних складових частин систем інтелектуального керування інженерними системами

Концепція системи «Розумний будинок» передбачає новий підхід в організації життєдіяльності в будинку, при якому на основі комплексу

високотехнологічного обладнання створюється єдина автоматизована система управління, що дозволяє значно збільшити ефективність функціонування всіх систем життєзабезпечення. Головною особливістю цієї системи є об'єднання окремих підсистем різних виробників в єдиний автоматизований комплекс. Підвищення комфорту досягається не тільки шляхом простого і зрозумілого управління окремими підсистемами «розумного будинку», але злагодженої взаємодії всіх підсистем між собою і гармонійного їх розташування в інтер'єрі будинку.

Розглянемо переваги модернізації та оптимізації системи «Розумний будинок». В основі такого будинку лежить інтегрований підхід, плюси якого не тільки в зручності централізованого керування, що виключає збої систем, але й у істотні економії засобів енергопостачання.

Статистичні дані провідних країн світу, де «Розумний будинок» – вже давно сприймається як буденність, свідчать про рентабельність і інвестиційну привабливість цієї технології при використанні якої, споживач одержує наступні переваги:

- зниження експлуатаційних витрат – 30%;
- зниження платежів за електроенергію – 30%;
- зниження платежів за воду – 41%;
- зниження платежів за тепло – 50%;
- зменшення викидів – 32–30%.

Основними характеристиками, за якими оцінюються переваги оснащення середовища житла інтелектуальними системами керування є: економія, безпека, контроль та інформування, гнучкість та можливість розширення, заміна функцій, автоматизація, дизайн.

2.1 Абонентське обладнання IoT

Інтернет речей перетворює кожен куточок життя: будинок, офіс, вулиці міста і його околиці. IoT продукти дають нам більший контроль над дверними замками, освітленням і побутовою технікою; дати уявлення про звички споживання ресурсів; оптимізувати бізнес-процеси; і краще поєднати нас з людьми, системами і навколишнім середовищем, які формують наше повсякденне життя.

Багато продуктів «початкового рівня» IoT плавно входять в повсякденне життя за рахунок спрощення повсякденних завдань. Пошук ключів, розблокувати двері, вмикати світло і вимикати - ці та інші звички можуть бути автоматизовані за допомогою датчиків і інтелектуального програмного забезпечення.

За даними Gartner, Inc. (науково-дослідницька та консультативна корпорація), близько 20,8 млрд пристроїв в мережі Інтернет речей будуть до 2020 року ABI Research вважає, що більше 30 мільярдів пристроїв будуть мати бездротове підключення до Інтернету речей до 2020 року. Ясно, що IoT буде складатися з дуже великого числа пристроїв, які підключені до Інтернету.

Абонентським обладнанням IoT є будь-який нестандартний обчислювальний пристрій, який має бездротове підключення до мережі і має можливість передавати дані в Інтернеті речей.

IoT пристрої включають в себе термостати, лампочки, дверні замки, холодильники, автомобілі, імплантати для RFID і кардіостимуляторів і т.д. (рис

2.1).

Рисунок 2.1 – Обладнання в Інтернеті Речей [12]

В тому ж «розумному» будинку: Користувач приходить додому і його машина спілкується з гаражем, щоб відкрити двері. Термостат вже доведений до його кращої температури, через його близькість зондування. Він проходить через двері, які він відмикає смартфоном або RFID імплантатом. Домашнє освітлення налаштовується на нижчу інтенсивність і вибирає колір для відпочинку, так як його дані з кардіостимулятора вказують на те, що це був напружений день.

IoT пристрої є частиною сценарію, в якому кожні переговори пристрою в будь-якому іншому пов'язане з пристроєм в середовищі для автоматизації будинку і промисловості і спілкуватися більше і більше корисними даними для користувачів, бізнесу та інших зацікавлених сторін. Однак, як це часто буває, технологія перемістилася швидше, ніж механізми щодо збереження конфіденційності користувачів і безпеки.

Розробники очікують побачити дизайнерські проекти вбудованих систем які будуть всюди від лінії складання машин і автоматизація будівельних систем до кардіостимуляторів і навіть зубних щіток.

Робота з цими пристроями, безумовно, новий і інший домен для більшості розробників додатків. І зміною буде інтеграція пристроїв в IoT, що дозволить

зробити їх розвиток більш доступним (рис 2.2). По-перше, ці пристрої часто «обмежені ресурсами.» Вони можуть мати менший обсяг пам'яті, і вони не мають людини на іншому кінці, який може натиснути на опцію або натиснути кнопку, щоб оновити. Багато з цих пристроїв будуть розгортатися в деяких випадках протягом 10 або 15 років, і ніхто не буде торкатись їх. Вони, однак, виробляють величезні обсяги даних датчиків, приймають самостійні рішення і інтеграцію з корпоративними системами (наприклад, аналітика баз даних).

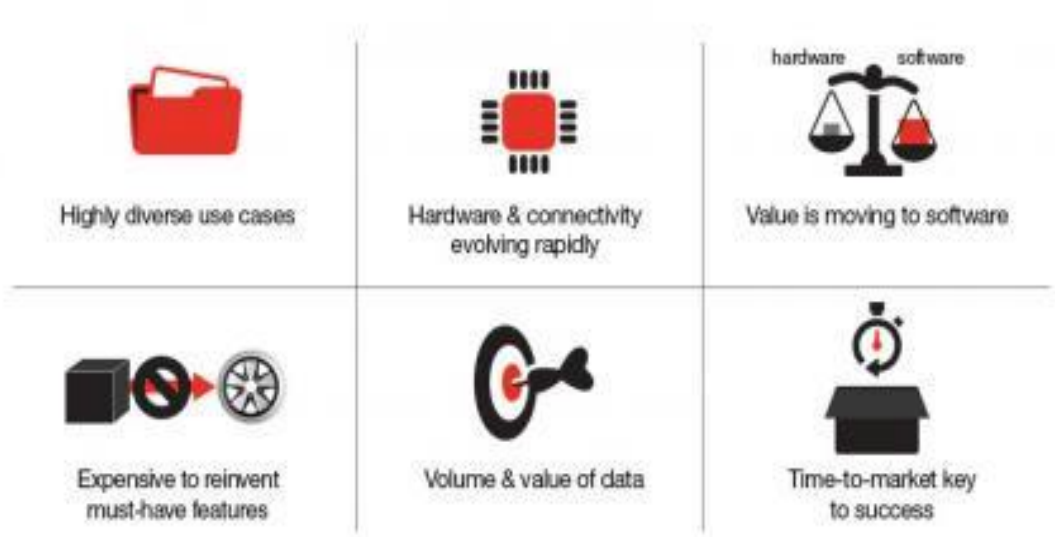

Рисунок 2.2 - IoT змінює пристрій [13]

Що стосується роздрібних споживачів, очевидні зміни в способі життя, що вимагають інтеграції смарт-розваг, техніки, моніторингу здоров’я, управління комунальним господарством та захисту і пристроїв безпеки.

Однак найбільша проблема в буму пристроїв IOT прийде у вигляді нових мереж, які будуть введені, щоб впоратися з додатковим трафіком, який всі ці пристрої будуть генерувати. Це може привести не тільки до заплутаних схем по системній інтеграції, а й створює проблеми безпеки.

1.3. Основні функції системи «Розумний будинок»

Потрібно зауважити, що підібрати кількість і складність елементів подібних систем керування житловим середовищем, можливо для різного рівня

платоспроможності кожного окремого клієнта. У разі, коли замовник не потребує повної комплектації житла усіма можливими системами, що входять до складу систем «розумного будинку», а бажає лише оснастити житло найнеобхіднішими системами, що забезпечують безпеку та комфорт життєдіяльності, виникає ситуація, що радикально відрізняється від умов, коли замовник має бажання створити простір житла, що реагуватиме на найменші зміни, що зможе адаптуватися до потреб господаря та трансформуватися відповідно до його вимог.

На сьогоднішній день вже склалися певні підходи до інтелектуального керування середовищем житла, які можна звести до чотирьох основних концепцій (Табл. 1).

Таблиця 1.1

Концептуальні підходи до інтелектуального керування системою «Розумний будинок»

Найменування концептуального простору	Характеристики
ПРИХОВАНО КОНТРОЛЬОВАНИЙ	Житло оснащується лише базовими системами керування середовищем, що не впливають на зовнішній вигляд помешкання та мають приховане розміщення
КОМПЛЕКСНО КЕРОВАНИЙ	Повний комплекс управління інженерними системами «Розумний будинок» та побутовими приладами за допомогою єдиного центру керування
ІЛЮЗОРНИЙ МУЛЬТИМЕДІА	Застосування повного комплексу систем «розумного будинку», проте основний акцент ставиться на технології ілюзорної зміни середовища
ДИНАМІЧНИЙ	Середовище житла піддається тотальним змінам та трансформаціям за бажанням власника.

Усі зазначені підходи мають стратегічні відмінності один від одного.

Приховано контрольований простір оснащується лише базовими системами керування середовищем, які мають задачу зробити житло безпечним (захист від проникнення, пожежна безпека, захист від підтоплень та витоків газу), забезпечити житло найсприятливішими умовами мікроклімату (опалення, вентиляція та інсоляція), а також керування освітленням. Інсталяція цих систем, що мають приховане розміщення, не впливає на зовнішній вигляд помешкання.

У комплексно керованому просторі додається повна комплектація системами керування та зведення їх у єдину систему з центральним пультом управління.

В ілюзорному мультимедіа просторі основний акцент ставиться на технології ілюзорної зміни середовища – проекції, голографічні зображення, а також створення ілюзій і стилізацій віртуального середовища.

В динамічному просторі додатково середовище житла, за допомогою засобів трансформації стає подібним до живого організму, що змінюється відповідно до потреб та бажань мешканців.

1.3.1. Енергозбереження

Розглянемо їх на прикладі найбільш затребуваної системи енергоефективності – електрозабезпечення (Табл. 2.)

Таблиця 1.2

Порівняльні характеристики звичайної системи електрозабезпечення житла та її аналогу у комплексі систем «Розумний будинок»

Характеристика	Звичайна електрика	Система «Розумний будинок»
1	2	3
Енергозбереження	Немає можливості автоматично регулювати процес споживання електроенергії приладами. Наприклад, блокування обраних приладів при високому тарифі на електроенергію неможливе.	Дозволяє заощадити на освітленні до 40% і на опаленні до 30%. Система сама контролює і регулює роботу кожного пристрою на підставі поточних параметрів відповідно до заданої програми.

Продовження таблиці 2

1	2	3
Безпека	Не вміє розпізнавати позаштатні ситуації (розбите скло, зламані двері) і реагувати відповідним чином (перекривати газ, вимикати електроенергію, блокувати	Контролює доступ в приміщення, стежить за безпекою території, що охороняється. Своєчасно запобігає надзвичайні ситуації та неполадкам в будинку (витік води, газу,

	будинок при проникненні злодіїв).	пожежа, зловмисне проникнення і т. д.).
Контроль та інформування	Не передбачає засоби повідомлення та зв'язку, не вміє розпізнавати надзвичайні ситуації та події, що відбуваються в будинку.	Система інформує про ситуацію в будинку або певну подію через Інтернет, мобільний телефон або безпосередньо з радіо–пульта. Оповіщення здійснюється на вимогу або згідно з заданим графіком, при позаштатних ситуаціях інформує відповідні служби.
Гнучкість та можливість розширення	Розширення або заміна електричної мережі ускладнюються монтажними і додатковими будівельними роботами (свердління стін, прокладання кабелю, шпатлювання, фарбування стін, заміна шпалер).	Елементи системи можна в будь–який час поступово доповнювати, виключаючи необхідність свердлити стіни і прокладати кабель. Будь–які елементи можна спочатку встановити, а потім активувати.
Заміна функцій	Не включає можливість заміни раніше визначених функцій регулятора на вимикач. При необхідності в додатковій розетці / вимикачі необхідно заново свердлити стіни, прокладати кабелі, проводити оздоблювальні роботи.	Система дозволяє змінювати функції елементів, це можливо за допомогою ПК і віддалено (немає необхідності виїзду техніка). Наприклад, з вимикача можна зробити регулятор або навпаки.
Автоматизація	Передбачене тільки ручне керування. Вимагає додаткових тимчасових витрат для налаштування і регулювання роботи побутових приладів. Систему не можна запрограмувати.	Процес керування та контролю роботи домашніх приладів автоматизований. Система може працювати автономно за встановленою програмою або ручним управлінням.

Отже, переваги сучасного підходу до автоматизації та модернізації житлового середовища не викликають жодного сумніву у необхідності популяризації такого підходу до проектування помешкань українців.

Аналіз досвіду реалізації проектів інтелектуального керування середовищем житла в Україні та світі виявив основні відмінності у підході до їх реалізації (Табл. 3).

В Європі системи керування використовуються в першу чергу для економії ресурсів, самі системи випускаються уніфіковані для взаємо інтеграції приладів різних виробників в єдину схему. На відміну від західних країн, на пострадянському просторі підхід до інтелектуалізації житла протилежно інший – призначення систем це імідж власника житла, для створення комфорту у

помешканні і лише як похідна від цього – економія ресурсів. Підхід до випуску та встановлення систем строго індивідуальний. Усіма процесами з проектування, монтажу та програмування інтелектуальних систем займаються вузькі спеціалісти. Велике значення для замовників у нашій країні має автоматизація як така.

Таблиця 3

Відмінності реалізацій проектів інтелектуального керування середовищем житла в Україні та світі

Зрівняльна характеристика	Європа	Україна
Основне призначення	Насамперед енергозбереження, екологічність та раціоналізація використання ресурсів і тільки потім комфорт	Імідж і комфорт (для високо бюджетних проектів); найпростіша охоронно–пожежна сигналізація, іноді з функцією GSM–оповіщення (для мінімальних бюджетів)
Підхід до проектування	Максимальна уніфікація	Виключно індивідуальний
Реалізація проекту	Проекти автоматизації приватних будинків і квартир виконує сам розробник і виробник систем, установкою займаються звичайні, але кваліфіковані монтажники, що працюють строго за схемою	Установкою займаються фахівці; як правило вони працюють із багатьма виробниками систем автоматизації, це дозволяє підбирати систему максимально оптимально для рішення поставлених завдань. Ці ж фахівці займаються проектуванням, монтажем, продажом і запуском побудованого «Розумного будинку»

1.3.2. Контроль аварійних ситуацій

Особливе місце в структурі «розумного будинку» займає система безпеки при аварійних ситуаціях. Вона забезпечує безпечну роботу інженерних систем будинку. В результаті, система безпеки проконтролює правильність роботи систем газопостачання та подачі води і інформує користувача про всі аварійні ситуації, як в будинку, так і на території, що охороняється.

Розглянемо приклад з виходом з ладу систем водопостачання.

Вихід з ладу елементів системи водопостачання не настільки руйнівний, як, наприклад, пожежа, але і це може привести до побутової катастрофи.

Для запобігання сумних наслідків протікання води, в розумному будинку застосовують спеціальні датчики.

Датчики протікання встановлюються в місцях, де ймовірність протікання найбільш висока: найчастіше під ванною або пральною машиною. У разі появи вологи на підлозі, датчики відправлять сигнал на клапани, які перекривають подачу води в систему, запобігши тим самим до затоплення приміщення. У той же момент, «розумний будинок» відправить на мобільний телефон власника сигнал, попередивши про аварію.

Подібні дії будуть зроблені системою безпеки і в разі витоку газу. При появі в повітрі пропану, метану, бутану, зреагують спеціальні датчики, відбудеться аварійне перекриття подачі газу, автоматично включиться витяжна вентиляція, а господарі будинку будуть в терміновому порядку сповіщені про подію за допомогою повідомлення або дзвінка на мобільний телефон.

Таким чином, система безпеки «розумного будинку» не тільки контролює роботу всіх систем, але і реагує на аварійні ситуації, одночасно оповіщаючи при цьому господарів.

1.3.3. Забезпечення безпеки

Часто виникає ситуація, коли необхідно залишити будинок без нагляду на тривалий час. Наприклад, в разі від'їзду у відрядження або на відпочинок. «Розумний будинок» дозволяє імітувати присутність в оселі. Варіантів імітації існує величезна безліч. Всі вони відрізняються за інтенсивністю, частотою і задіяним механізмам. Згідно з розробленим сценарієм, в приміщеннях, в довільному порядку, може включатися і відключатися освітлення, тиха музика або голос. У деяких сценаріях можуть бути передбачені, навіть, звуки води, що ллється з крана, свист чайника і інші свідоцтва присутності в будинку людини.

У разі якщо стороння людина все ж забралася в оселю, спрацює система захисту будинку від проникнення сторонніх осіб. На цей випадок, будинок

обладнаний групою датчиків. Спрацюють датчики відкриття вікон і дверей, а так само датчики руху всередині будинку.

Сигнал про проникнення всередину приміщення або на територію, що охороняється, невідомої людини буде миттєво переданий в службу охорони і на мобільні засоби зв'язку господарів будинку.

Безпеку забезпечують датчики руху і датчики охорони периметра, спільно з системою відеоспостереження. Внутрішні камери в будинку можуть працювати весь день і фіксувати кожну хвилини «життя» будинку. При бажанні, система може бути переведена в режим очікування, в цьому випадку, камери будуть спрацьовувати тільки по руху. В такому випадку, система буде записувати окремий відео фрагмент. За таким же принципом система може вести спостереження не тільки за внутрішнім «життям» будинку, але і за територією навколо нього. Всі сигнали, які передають датчики, в тому числі і запис з камер відеоспостереження, в обов'язковому порядку, вносяться в пам'ять системи, щоб господар завжди міг переглянути, коли і з якого датчика був переданий сигнал. Вести такий контроль можна через мобільний телефон або комп'ютер, в будь–який зручний для господаря момент і в будь– якому зручному місці.

Одним з важливих елементів системи безпеки розумного будинку є магнітно–контактні датчики закриття / відкриття вікон і дверей. У разі, якщо господар збирається поїхати з дому або лягаєте спати система проінформує його про незакриті двері або нещільно закриті вікна.

У разі, якщо користувач вирішив не закривати вікно, то датчик відкриття цього вікна відключиться, а датчики руху в цій кімнаті, будуть переведені в режим зниженої чутливості, щоб виключити помилкові спрацьовування, через коливання штор. Кожному датчику можна задати свій рівень чутливості, щоб він не реагував, наприклад, на найменші коливання або на домашніх тварин. У систему безпеки, так само, може бути включена система управління ролетами і жалюзі, в тому числі, і в складі сценарію.

Наприклад, з настанням темного часу доби, жалюзі будуть автоматично закриватися, щоб з вулиці неможливо було зазирнути у вікна. Крім перерахованих

вище пристроїв, до складу охоронної системи можуть входити датчики розбиття скла і руйнування стін.

1.4. Існуючі технології зв'язку в системі «Розумний будинок»

1.4.1. Технологія X–10

Найпоширенішою технологією на сьогоднішній день для реалізації «Розумного будинку» є X–10. Вона з'явилася на початку 80–х років і стала першою системою, яка зробила можливість реалізувати автоматизований будинок. Програмний алгоритм створений настільки ефективно, що при натисканні однієї кнопки, виконується декілька команд. Також для функціонування системи використовують датчики руху, освітленості, вологості. Більш того система є дуже гнучкою, оскільки вона інтегрується за ліченні години. Працює система від звичайної електропроводки (220 В, 50 Гц), по якій передається сигнал.

Тому X–10 настільки поширена, адже не потрібно прокладати нові кабелі чи руйнувати квартиру, оскільки і так все необхідне вже є.

Технологія X–10 є досить зручною і інтелектуальною, оскільки її можна запрограмувати під будь–які потреби. X–10 не містить центрального контролера: кожний прилад отримує індивідуальний адрес, по якому його знайде відправлена із пульта команда, дана технологія може бути розширена. Якщо користувач прагне удосконалити свою систему, дана технологія дозволяє це, оскільки вона легко інтегрується. До системи легко підключити додаткові модулі, це означає, що ваш дім поступово «розумнішає». Серед всіх позитивних якостей системи є і низька вартість. На сьогоднішній день дана система є найбільш дешевою. Принцип реалізації зображений на рис. 2.

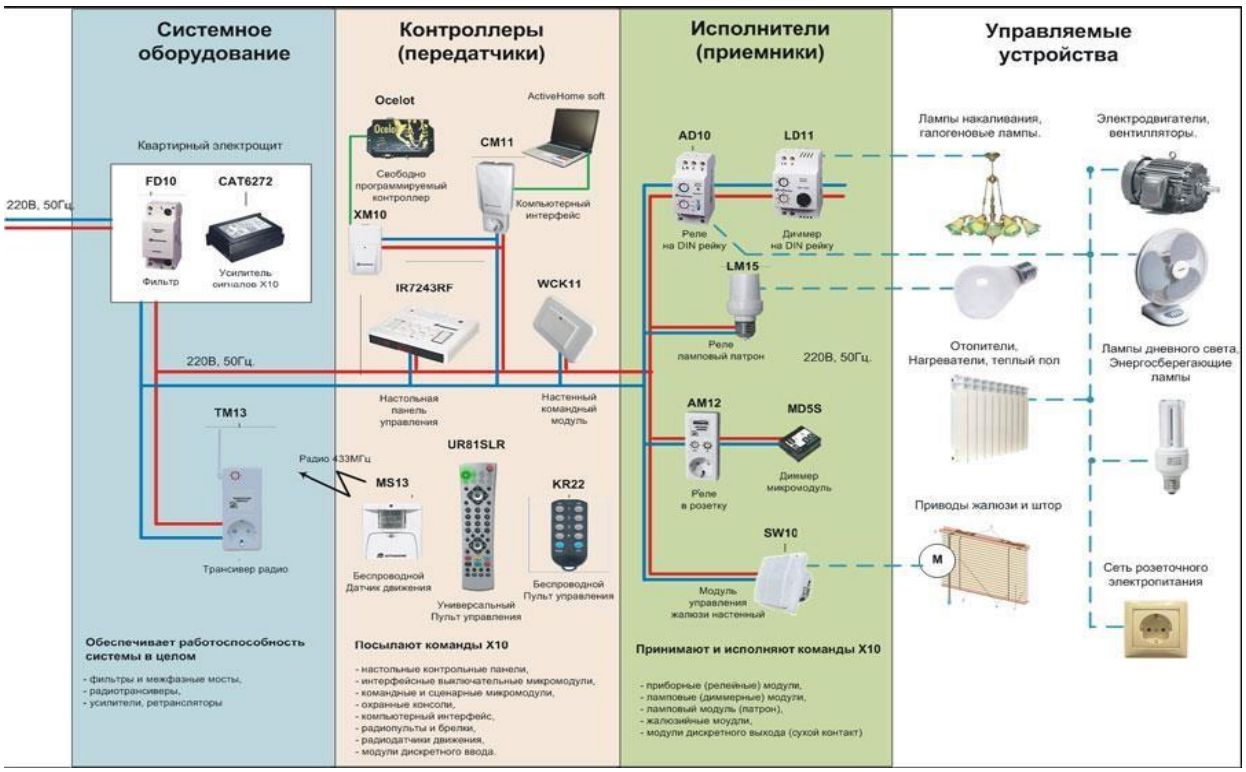

Рис. 1.2. Принцип реалізації технології X–10

Недоліків у технології також достатньо: швидкість передачі даних по електропроводці є досить низькою, крім того є обмеження кількості керуючих груп.

1.4.2. Технологія C–Base

Одна із найпоширеніших технологій для керування «розумним будинком». Кожний мікроконтролер даної системи може налаштовуватися, а ціла мережа таких контролерів може керувати всім будинком. Кожна ланка має свою пам’ять, яка не пошкоджується при збою подачі електроенергії. Це робить систему доволі надійною, тому саме на даній технології будують складні і безпечні системи. Принцип роботи зображений на рис. 2.1.

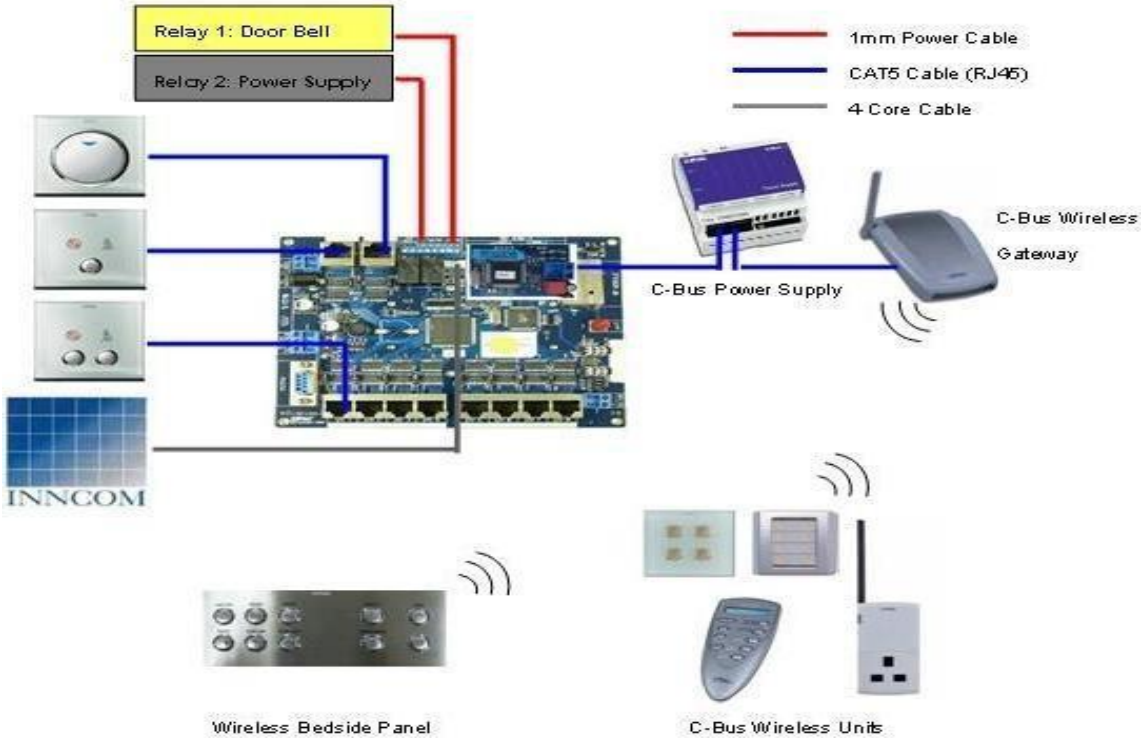

Рис. 1.3. Приклад реалізації технології C–Base

C–Base – це система, яка дозволяє керувати будинком на відстані без наявності сервера, оскільки контролер із постійною IP–адресою підключається до мережі Інтернет і до «розумного будинку», передавання даних відбувається по TCP/IP протоколу. Тобто керувати системою можна з віддаленого телефону чи комп'ютера. Дана технологія дозволяє об'єднати до 100 приладів в одній мережі і 255 мереж в одній системі.

1.4.3. Технологія European Installation Base

Технологія EIB (European Installation Base), як і C–Base, є децентралізованою системою. Вона дуже часто використовується в Європі. Для цієї системи разом із силовим провідником прокладається вита пара, які і є керуючою шиною. Відповідно до неї підключаються всі прилади для зв'язку між собою. Всі прилади зв'язуються один з одним без будь–якої структури чи ієрархії, а також без керуючих блоків. Необхідна інформація зразу подається передатчиком через канал зв'язку (шину) на всі приймачі. І хоча відправлений сигнал потрапляє на всі прилади, на нього реагує тільки той прилад, якому ця інформація адресована.

Якщо приймач не відреагував на отриману команду, то система повторює спробу ще три рази. Після цих спроб передача інформації закінчується, а запам’ятовуючий прилад фіксує помилку. Інформація передається асинхронно і послідовно, при цьому маючи пріоритети повідомлень. При цьому дана технологія є досить добре захищеною і надійною. Принцип роботи зображений на рис. 2.2.

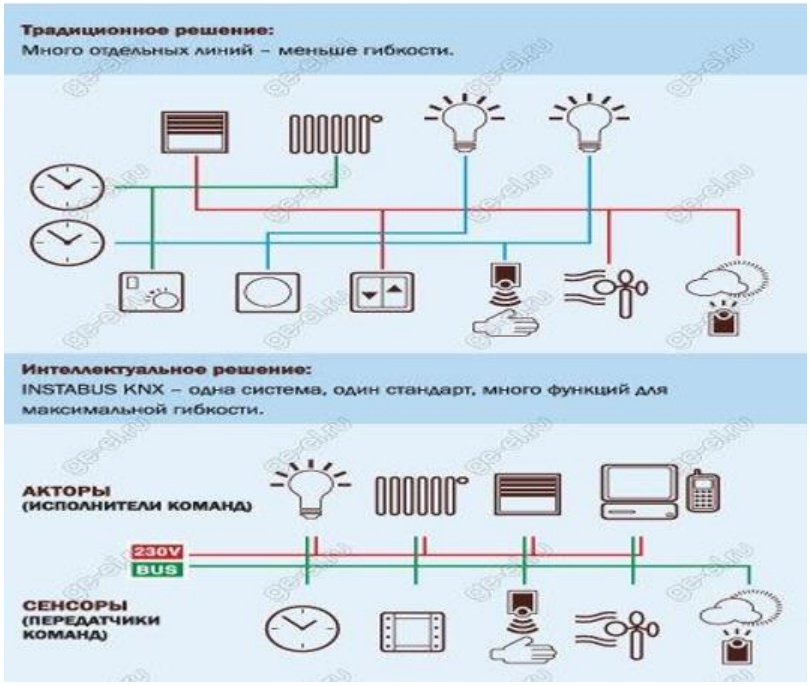

Рис. 1.4. Принцип реалізації технології EIB

Не дивлячись на те, що система є децентралізованою, не важко додати до неї центральний комп’ютер та додаткові модулі управління, тому що вона досить добре інтегрується під будь–які потреби.

1.4.4. Технологія LonWorks

Системи, які побудовані по технології LonWorks, за своєю архітектурою схожі на EIB. Проте завдяки можливості програмувати вбудовані контролери, можна реалізувати складніші проекти. Звичайно, інформація подається тільки, тоді, коли є зовнішні зміни в приміщеннях, тому мережа позбавлена перенавантажень. Принцип роботи зображений на рис. 2.3.

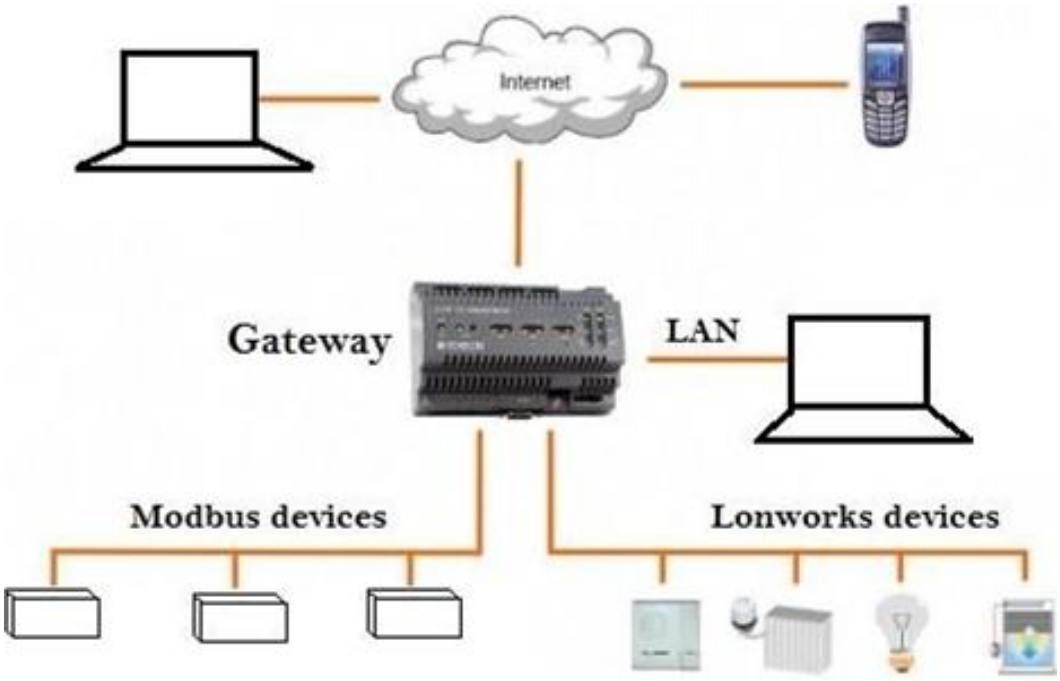

Рис. 1.5. Принцип реалізації технології LonWorks

Система керування реалізується на базі керуючої мережі LON (Local Operation Network), яка має мінімальну кількість рівнів ієрархії. Центрального комп'ютера дана система не має. Технологія LonWorks була створена для автоматизованої промисловості і транспортної системи. Зараз вона використовується для будування розподілених систем з великою кількістю вузлів, віддалених один від одного. Дана технологія є найбільш поширеною в США.

1.4.5. Технологія AMX, Crestron

Централізована система керування «розумним будинком» AMX, Crestron, яка будується на основі широкого спектру керуючих ЦК і багатьох виконавчо–командних блоків. Принцип роботи зображений на рис. 2.4.

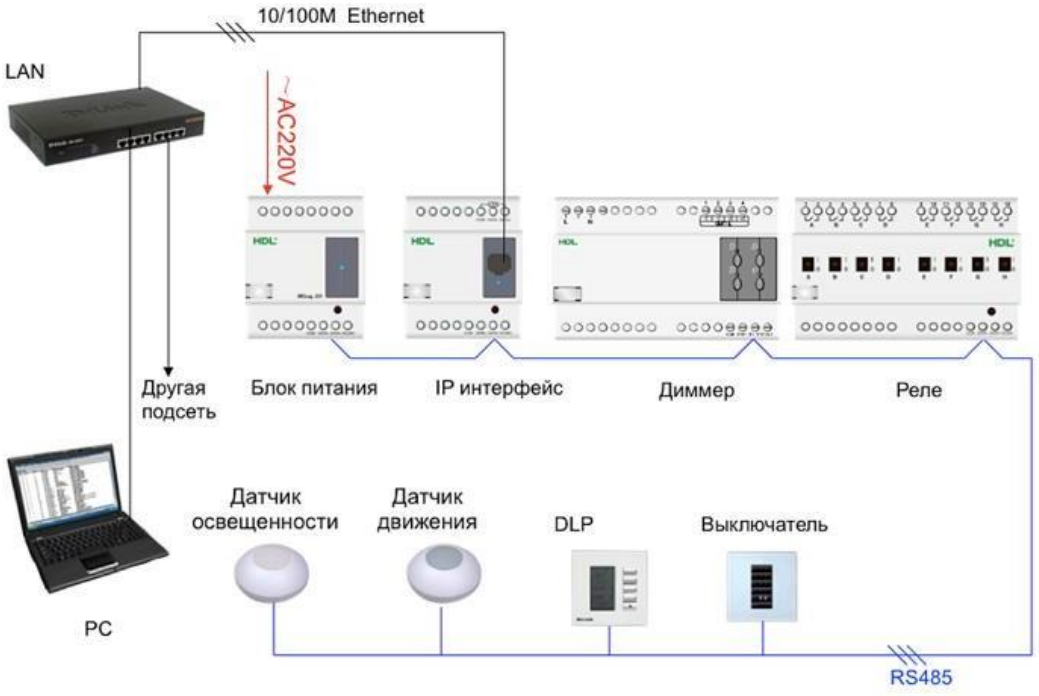

Рис. 1.6. Приклад реалізації технології AMX, Crestron

Функція аналізу інформації знаходиться в потужному ЦК, який приймає сигнали від датчиків і перемикачів, відправляючи їх в керуючий блок. Контролери даної системи є досить гнучкими, оскільки за допомогою них можна побудувати досить складну систему автоматизації, але для цього потрібно висококваліфіковане програмування. Оскільки дана технологія є централізованою, то при відмові ЦК вся система не буде працювати, тому надійністю технологія не володіє.

З наведеного вище видно, що в даний час існує велика кількість різних технологій реалізації системи «Розумний будинок», тому доцільно провести класифікацію цих систем.

1.5. Класифікація систем «Розумний будинок»

Провівши аналіз принципів реалізації існуючих систем можна визначити наступну класифікацію за принципом зв’язку між окремими модулями системи:

- Централізована система;
- Децентралізована система;
- Змішана система.

Перша група – централізована система, яка складається із головного комп’ютера до якого підключенні виконавче–командні модулі. Вони взаємодіють

завдяки центральному комп’ютеру, який подає сигнали керування через канал зв’язку (шина). Всі налаштування зберігаються на сервері, а периферія виконує лише отримані від нього команди.

Архітектуру такої системи зображено на рис. 2.5.

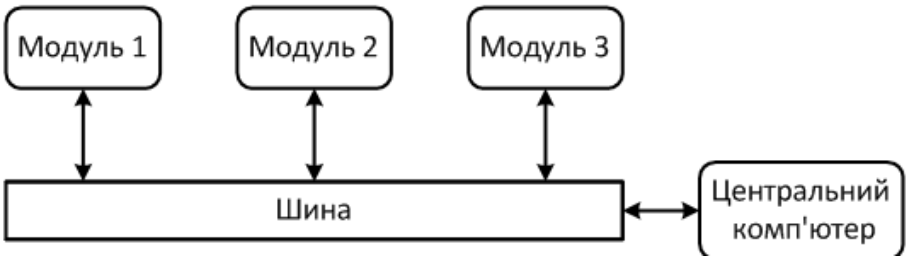

Рис. 1.7. Архітектура централізованої системи

Дана концепція дає можливість зібрати автоматизовану систему з єдиним комплексом виконання та приєднати прилади різних виробників, не зважаючи на різні канали зв’язку, які існують на даний час. Також централізована система володіє високою функціональністю та високоякісним графічним інтерфейсом. Нажаль, існують і негативні сторони даної концепції: висока вартість; значні площі для розміщення технологічного обладнання; відмова центрального контролера призводить до відмови всієї системи; проектування системи вимагає високої кваліфікації і великого досвіду; монтування системи відбувається під час будування приміщення чи його капітального ремонту.

Друга група – децентралізованою системою. Як зрозуміло з назви головний керуючий центр в системі відсутній. Система складається із модулів, які виявляють зміни в характеристиках будинку і реагують на ці зміни завдяки контролеру, який вбудований в модуль. Алгоритми взаємодії прописуються з програми контролера безпосередньо в пам'ять кожного пристрою і для їх зміни пристрій буде необхідно перепрограмувати. У зв'язку з відсутністю центрального компонента, зв'язки між приладами встановлюються безпосередньо і є можливість створення автономних груп, замкнутих одна на одну.

Архітектуру даної системи наведено на рис. 2.6.

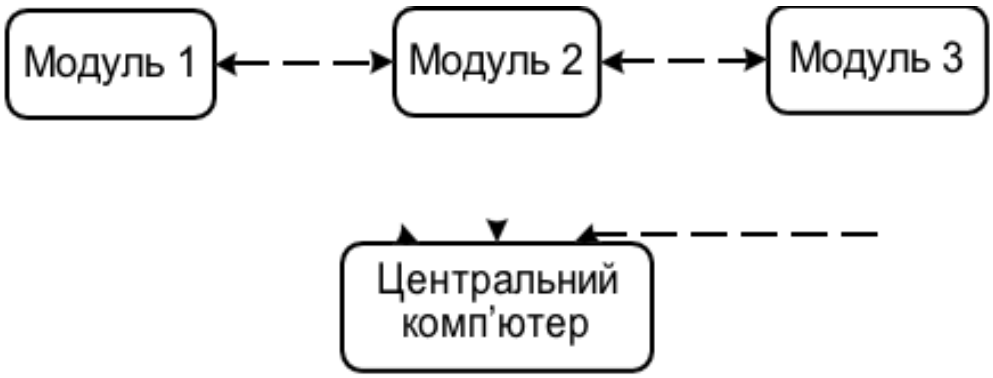

Рис. 1.8. Архітектура децентралізованої системи

Дана концепція не залежить від центрального блоку, тому всі функціональні модулі можуть працювати автономно. Відповідно це підвищує надійність системи в експлуатації. Дана технологія має хороші перспективи для розширення і модернізації апаратури, а також гнучкість при програмуванні задовольняє потреби замовника. До недоліків такої архітектури можна віднести: порівняно високу ціну; проектування системи вимагає високої кваліфікації і великого досвіду.

Третя група є системою, яка включає в себе децентралізовану та централізовану системи, з метою підвищення гнучкості керування та компенсації недоліків, які є в обох систем.

Архітектуру даної системи зображено на рис. 2.7.

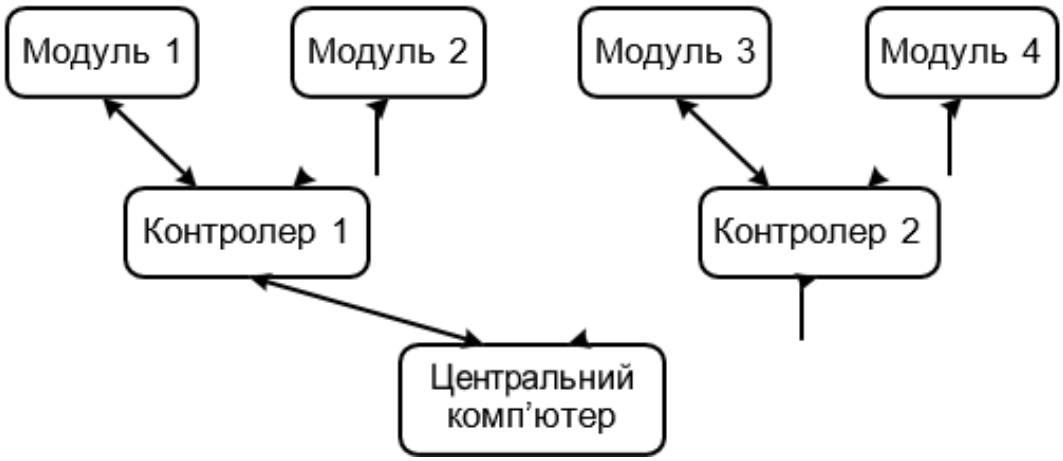

Рис. 1.9. Архітектура змішаної системи

Дана концепція є ефективною з точки зору керування «розумним будинком». Інтелект для вирішення найскладніших задач знаходиться в ЦК, який відповідає за функціонування всієї системи, особливо дочірніх мікроконтролерів (ДМ). ЦК постійно обмінюється інформацією з ДМ через канали зв'язку, а вони відповідно

вже з модулями. Чим цікава ця система, що при відмові ЦК, вона буде працювати, оскільки ДМ мають свою логіку керування, тобто свій алгоритм, який відповідає за виконання різних функцій. ЦК використовується для забезпечення більш складнішого функціонування системи, для більш гнучкішого користування. Без ЦК дочірні контролери не можуть обмінюватися інформацією для більш ефективного керування всієї системи, але надійність під час експлуатації в даній системі є найвища. Звичайно, таку концепцію використовують у важливих воєнних чи наукових центрах для великої надійності захисту даних і забезпечення безпеки будівлі, оскільки дана система є дорогою і потребує багато ресурсів в обслуговувані, проте це не заважає всі бажаючим мати дану систему керування для своїх «розумних будинків».

Розділ 2
ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ БЕЗПЕКИ СИСТЕМИ «РОЗУМНИЙ БУДИНОК»

Системи «розумного будинку» отримала велику популярність останнім часом. «Розумний будинок» є автоматизованою будівлею сучасного типу, що організована для зручності людей за допомогою високотехнологічних пристроїв. «Розумні будинки» - багатофункціональні, і разом з цим складні. У розумному будинку один пристрій може керувати поведінкою інших пристроїв по заздалегідь виробленим алгоритмам. головною особливістю інтелектуальної будівлі є об'єднання окремих пристроїв в єдиний керований комплекс.

Подібними системами обладнуються не тільки житлові будинки, а й державні установи, місця масового скупчення людей, а також стратегічні об'єкти, наприклад, АЕС (Атомні електростанції), аеропорти і т.д. Поєднання різних технологій при побудові однієї автоматизованої системи збільшує кількість можливих недоліків рішення з точки зору безпеки, що, безумовно, привертає увагу зловмисників.

Обслуговування складних об'єктів це комплекс завдань, вирішення яких можливе за допомогою сучасних систем автоматизації життєзабезпечення. Значна частина сучасного обладнання, систем автоматичного керування будівлями різних компаній, можуть бути інтегровані в єдину мережу. Як наслідок, будівлі стають більш функціональними. Однак такі інтеграції мають недоліки. Поєднання різних технологій для створення автоматизованої системи збільшує кількість можливих недоліків безпеки системи. Збільшення кількості пристроїв і технологій, які використовуються в системі, ведуть до зростання вразливості системи. Крім того, процес інтеграції різних рішень не виключає можливість допущення помилки в проектуванні. Це може призвести до появи додаткових слабких місць в системі.

Зловмисники можуть отримати несанкціонований доступ до системи «Розумний дім», використати слабкі місця сучасних автоматизованих систем управління життєзабезпеченням, в наслідок чого можуть остаточно блокувати

роботу великих об'єктів, наприклад аеропорту, сіяти хаос, і нарешті знищити систему безпеки з середини, що може призвести до серйозних наслідків. При заволодінні контролем над системою у зловмисника відкритий широкий спектр можливостей над використанням системи в своїх цілях.

На жаль, більшість систем автоматизації будівель не мають систему захисту проти кібератак. Більшість рішень для захисту, пов'язані з установкою стандартних програмам, які виконують функцію брандмауера. Але у випадку атаки на системи автоматизації будівлі цього недостатньо. У цілому системи автоматизованого управління будівлею мають кілька типів програмного забезпечення.

Першим типом є програмне забезпечення, яке забезпечує функціонування самої мережі «Розумного будинку». Воно розробляється на мовах програмування нижнього рівня і несе відповідальність за нижні рівні мережевої моделі OSI.

Другий тип програмного забезпечення, програми, які відповідають за взаємодію з користувачем через командну мову. Вони зазвичай використовується для зовнішнього або віддаленого управління.

Головною частиною будь–якого комплексу ПЗ є сервер. Туди приходять запити від різних клієнтів. Сервер обробляє всі команди, аналізує параметри системи життєзабезпечення і приймає рішення про здійснення дії. Далі сформована команда передається на драйвери для доступу до мережі. Після чого за допомогою вибраного драйвера здійснюється безпосереднє маніпулювання об'єктами. У зворотному напрямку ланцюг також працює.

Користувальницький інтерфейс може бути реалізований різними способами. Є кілька підходів до реалізації цього компонента програмного забезпечення. Кожен із варіантів залежить від протоколу, який використовується для обміну із сервером системи «Розумний будинок». Це може бути і Web–браузер, який спілкується за допомогою протоколу HTTP, і застосування додатків реалізованих на високо–рівневих мовах програмування під ту чи іншу операційну систему. Це може бути навіть мобільний додаток, який встановлюється на мобільному телефоні користувача і призначений для обміну команд та сервісних

повідомлень через TCP / IP з'єднання або SMS–повідомлення. Варто відзначити, що більшість протоколів, які використовуються для керування об'єктами є за своєю суттю вразливими, і багато інших, які використовуються для побудови підсистем, часто з неналежною інтеграцією призводять до уразливості. Як уже згадувалося вище, серверне ПЗ встановлюється на вибраному комп'ютері. Машина з'єднує багато допоміжних пристроїв для передачі даних. Це можуть бути GSM–модеми, передавачі Bluetooth і Wi–Fi точки доступу. Крім того, часто на цьому сервері встановлено власне ПЗ.

Розглянемо основні канали розповсюдження вірусів:

- *Канал Bluetooth.* Мережа Bluetooth є надзвичайно ненадійною і легко може прийняти файл з вірусом зловмисника без авторизації ;
- *Канал Wi–Fi.* Мережа Wi–Fi може бути легко скомпрометована зловмисником, і він може минаючи систему авторизації, передати вірус на сервер;
- *HTTP канал для віддаленого доступу.* HTTP обмін з мережею Інтернет може бути одним з каналів зараження системи вірусом;
- *GSM канал.* Через канал GSM також можливий несанкціонований контроль системи. Це можливо, наприклад, за допомогою передачі SMS–повідомлень з фальшивим номером відправника;
- *Споріднені канали.* Якщо сервер «Розумного будинку» підключений до локальної мережі будівлі, то вірусна програма може попасти на нього від локальної мережі.

Повноцінних антивірусних систем, що забезпечують комплексний захист від злоякісного ПЗ, не існує. Крім того, код, який властивий вірусам для систем «Розумного будинку», не визнається більшістю сканерів.

Розглянемо вразливості у програмному забезпеченні систем «Розумного будинку» що використовуються зловмисниками :

- відсутність блокування підключення несанкціонованих пристроїв;
- відсутність контролю над трансляцією датаграм в мережі «Розумного

будинку»;

- відсутність аутентифікації керуючої програми, яка передає пакети у мережу «Розумного будинку».

На даний момент, є необхідність створювати спеціальні антивірусні засоби, які можуть забезпечити комплексний захист від злоякісного ПЗ.

Антивірусні програми для «Розумних будинків» повинні виконувати наступні функції:

- контролювати появу на сервері «Розумного будинку» будь–яких сторонніх файлів та програм;
- контролювати несанкціоновані підключення пристроїв до мережі;
- контролювати підключення пристроїв до бездротових каналів передачі даних;
- контролювати взаємодію сервера з мережею Інтернет на предмет появи та проникнення вірусів;
- контролювати мережеве обладнання на предмет DoS–атак;
- забезпечити перевірку файлів, які передаються у мережі;
- виконувати пошук наявності на сервері вірусних програм;
- контролювати цілісність системи «Розумний будинок», за допомогою перевірки поточної конфігурації , керуючих процесів і збережених даних.

На даний момент у світі існують лише програмні засоби захисту систем автоматизованого управління будівлями. Переклад частини реалізованих функцій на апаратну основу не тільки знижує вартість і складність розробок, а й істотно підвищує надійність засобів, що забезпечують безпеку систем «Розумного будинку». Програмні антивірусні продукти не можуть вирішити задачу повного захисту системи через відсутність апаратної складової комплексу. Можна стверджувати, що існуючі програмні антивіруси не дозволяють повністю захистити систему. Таким чином, створення антивірусних засобів, які здатні забезпечити комплексний захист для системи автоматизованого контролю будинком є важливим завданням у найближчі роки.

Зі зростанням технологій зростають можливості для добування, збору, обробки, зберігання, пошуку, відображення та передачі інформації, паралельно і

настільки ж інтенсивно розробляються способи і засоби знищення, спотворення, пошкодження, несанкціонованого доступу до інформації, її блокування, а також порушення функціонування інформаційно–телекомунікаційних систем (ІТКС).

У зв'язку з цим багато разів підвищується роль і значення інформаційної безпеки ІТКМ.

Тому все більш актуальним стає питання про захист систем розумного будинку, в які входять елементи ІТКС, від стороннього втручання і ворожого моніторингу. Під ворожим моніторингом розуміється непомітне для господарів вторгнення в системи розумного будинку з метою ознайомлення з уразливістю системи охорони, збору інформації про мешканців будинку, про розпорядок дня кожного члена сім'ї, особистих і конфіденційних даних і т.д. для подальшого пограбування, шантажу, вимагання і т.п..

Всі елементи системи розумного будинку, які відповідають за зв'язок, охорону, безпеку і системи життєзабезпечення повинні оснащуватися джерелами безперебійного живлення, щоб у випадку відключення електрики зберегти працездатність. Причинами збоїв, стрибків напруги або відключення електрики можуть бути сильний вітер, дерево, що впало на лінії електропередачі, зловмисники, які намагаються таким чином відключити систему охорони і сигналізацію і пробратися в будинок і т.д. і т.п., а система розумного будинку не повинна залежати від цих чинників. Додатково або замість джерел безперебійного живлення можна використовувати встановлений, наприклад, в підвалі, автономний електрогенератор, який включиться при виникненні проблем з електроживленням.

Мережі міжнародного інформаційного обміну, такі як інтернет, істотно розширюють можливості використання інформаційної зброї для перехоплення і знищення важливої інформації. Під інформаційним зброєю будемо розуміти сукупність засобів і методів, які дозволяють викрадати, спотворювати або знищувати інформацію, обмежувати або припиняти доступ до неї законних користувачів, порушувати роботу або виводити з ладу телекомунікаційні мережі і

комп'ютерні системи, що використовуються у забезпеченні життєдіяльності людини.

Існують два найбільш часто використовувані засоби побудови систем розумного будинку: перший спосіб полягає в побудові системи на основі програмованих контролерів, а другий – на основі виділеного комп'ютера, що називається сервером. Але і в тому і в іншому випадку потрібна наявність комп'ютера для зберігання архівів аудіо та відео–записів з камер спостереження, протоколів подій і звітів про стан системи та іншої інформації. У другому випадку для зберігання архівів можна використовувати сервер. Значить, ці комп'ютери повинні бути захищені від стороннього втручання програмними (установка спеціального програмного забезпечення, що обмежує доступ до інформації, а також забезпечує безпеку інформації) і технічними (розміщення апаратури в спеціальній виділеній кімнаті, обмеження доступу до цієї кімнати) засобами.

Для можливості відправки системою протоколів подій господареві, що знаходиться поза домом, необхідне підключення комп'ютера до мережі інтернет. Тоді необхідно використовувати спеціальне програмне забезпечення, яке зможе убезпечити комп'ютер від можливих атак і шкідливих програм з глобальної мережі і не дозволить статися витоку інформації. Крім того, бажано, щоб система вже на етапі запису інформації на комп'ютер шифрувала архіви, використовуючи стійкий до злому метод кодування. І навіть якщо інформація буде вкрадена, то розшифрувати її буде дуже і дуже непросто, а в деяких випадках неможливо.

Захист від програмного впливу здійснюється:

- застосуванням безпечних інформаційних технологій;
- сертифікацією технічних і програмних засобів і проведенням спеціальних перевірок на наявність у них закладок;
- унеможливленням несанкціонованого доступу до інформації, що циркулює в технічних системах;
- застосуванням програмних методів (засобів) захисту інформації.

Щоб зловмисники не змогли вивести з ладу системи розумного будинку, необхідно також прийняти ряд заходів щодо забезпечення безпеки апаратури, що відповідає за працездатність і безпеку цих систем.

Для захисту, від виведення зловмисниками з ладу систем розумного будинку бажано передбачити низку заходів:

- оснастити життєво важливі системи розумного будинку джерелами безперебійного живлення;
- розміщення апаратури, що забезпечує працездатність і безпеку систем розумного будинку (електричний шафа, монтажний шафа, контролери, сервер і т.д.) здійснити у спеціальному приміщенні поза зоною досяжності сторонніх осіб;
- обмежити доступ в зазначений вище приміщення;
- здійснення ремонту, технічної підтримки та заміни елементів систем розумного будинку повинні здійснювати тільки фахівці фірми–інсталятора. Це дозволить уникнути проникнення в систему закладок та інших шкідливих елементів, які згодом можуть вивести з ладу системи розумного будинку.

З появою нових завдань удосконалюються вимоги до захисту інформації які передбачають:

- захист інформації при передачі її по каналах зв'язку, зберіганні та обробці (конфіденційність інформації);
- забезпечення цілісності та достовірності переданої, що зберігається і оброблюваної інформації ;
- автентифікацію сторін, що встановлюють зв'язок (підтвердження автентичності відправника або одержувача інформації);
- контроль доступу до ресурсів мережі, устаткування і даних абонентів;
- крипто живучість при компрометації частини ключової системи;
- шифрування інформації перед передачею і зберіганням;
- надання користувачу доступу до інформації тільки після аутентифікації та перевірки наявності у нього прав доступу до запитуваної інформації;
- забезпечення взаємодії між різними локальними інформаційними системами

при одночасному виключенні можливості «наскрізного» проникнення до найбільш важливих підсистем, в яких циркулює інформація підлягає захисту.

Ще одним способом збору інформації зловмисниками може стати зняття інформації з неекранованої витої пари, яка використовується в більшості випадків для побудови структурованої кабельної мережі (СКМ), на якій згодом будується система розумного будинку. Справа в тому, що при передачі сигналу по неекранованій витій парі вона починає випромінювати електромагнітні хвилі, вловлюючи які спеціальним пристроєм можна перехопити інформацію, що передається.

Але відстань, на якій можна перехопити електромагнітне випромінювання неекранованого кабелю не перевищує півметра. Екранування витих пар зменшує рівень власних випромінювань приблизно на два – три порядки, що вимагає прямого підключення для зняття інформації. Екранування інформаційних кабелів є також найбільш ефективним рішенням для зменшення відстані між силовою і телекомунікаційною проводкою, що дозволяє забезпечити електромагнітну сумісність активного устаткування. Тому при побудові структури СКМ можна комбінувати використання неекранованої і екранованого скручених пар і застосовувати останню тільки в найбільш вразливих частинах мережі.

Бажано також, щоб система розумного будинку мала ряд вбудованих детекторів, здатних виявити порушення цілісності системи та впровадження в її складові частини, а також вміла вчасно попередити господаря (де б той не перебував, в будинку або за його межами) та охоронну організацію про спробу порушення цілісності системи.

Розділ 3
ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ В СИСТЕМІ «РОЗУМНИЙ БУДИНОК»

3.1. Класифікація загроз безпеки

3.1.1. Базові визначення

Під загрозою безпеки інформації розуміють подію або дію, яка може викликати зміну функціонування системи, пов'язану з порушенням захищеності оброблюваної в ній інформації.

Вразливість інформації – це можливість виникнення такого стану, при якому створюються умови для реалізації загроз безпеки інформації.

Атакою на інформаційну систему називають дії, що робляться порушником, які полягає в пошуку і використанні тієї або іншої вразливості. Інакше кажучи, атака на КС є реалізацією загрози безпеки інформації в ній.

Проблеми, що виникають з безпекою передачі інформації при роботі в комп'ютерних мережах, можна розділити на три основні типи:

- перехоплення інформації – цілісність інформації зберігається, але її конфіденційність порушена;
- модифікація інформації – вихідне повідомлення змінюється або повністю підміняється іншим і відсилається адресату;
- підміна авторства інформації.

Специфіка комп’ютерних мереж, з точки зору їх вразливості, пов'язана в основному з наявністю інтенсивної інформаційної взаємодії між територіально рознесеними і різнотипними елементами.

Вразливими є буквально всі основні структурно–функціональні елементи комп’ютерної станції: робочі станції, сервери (Host–машини), міжмережеві мости (шлюзи, центри комутації), канали зв'язку і т.д.

Одна з найпростіших класифікацій наведена на рис. 3.

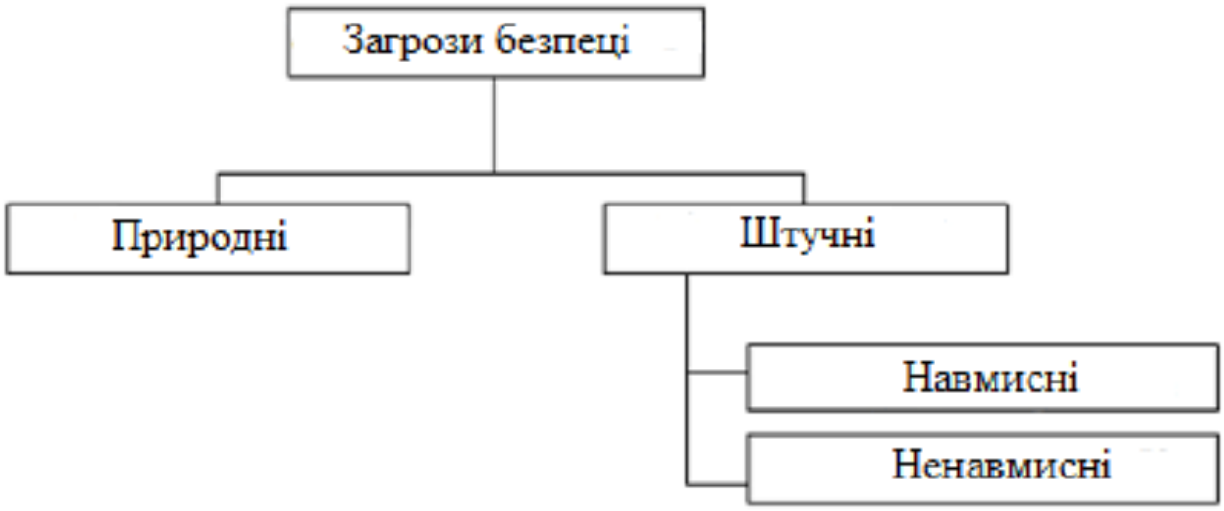

Рис. 3.1. Загальна класифікація загроз безпеки

Природні загрози – це загрози, викликані впливами на інформаційну систему і її елементи об'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини.

Штучні загрози – це загрози інформаційної системи, викликані діяльністю людини.

Серед них виділяють:

- ненавмисні (випадкові) загрози, викликані помилками в проектуванні інформаційної системи і її елементів, помилками в програмному забезпеченні, помилками в діях персоналу і т.п.;
- навмисні загрози, пов'язані з корисливими задумами людей (зловмисників).

Джерела загроз по відношенню до інформаційної системи можуть бути зовнішніми або внутрішніми (компоненти самої інформаційної системи – її апаратура, програми, персонал).

Аналіз негативних наслідків реалізації загроз припускає обов'язкову ідентифікацію можливих джерел загроз, вразливостей, що сприяють їх прояву і методів реалізації.

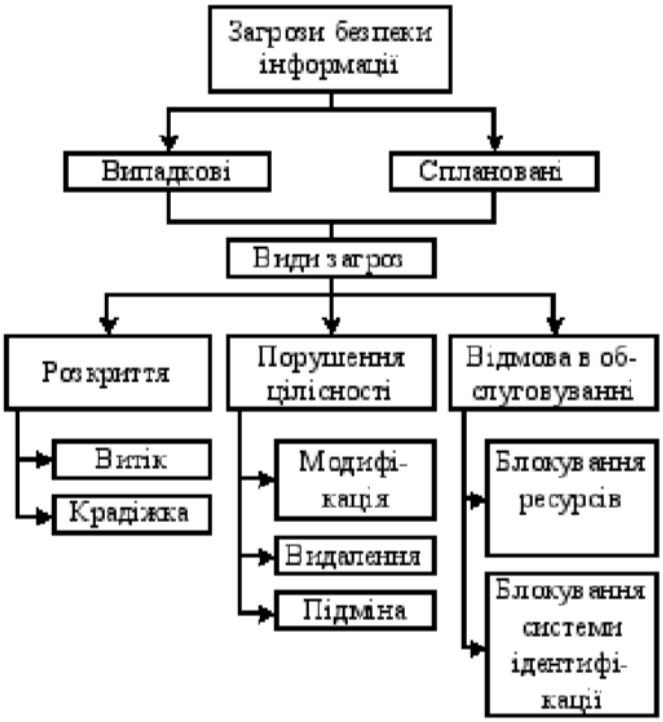

Рис. 3.2. Види загроз безпеки інформації

Загрози класифікуються за можливості нанесення шкоди суб'єкту відносин при порушенні цілей безпеки. Збиток може бути заподіяна будь–яким суб'єктом (злочин, вина або недбалість), а крім того стати наслідком, не залежних від суб'єкта проявів.

При забезпеченні конфіденційності інформації це може бути розкрадання (копіювання) інформації і засобів її обробки, а крім того її втрата (ненавмисна втрата, витік).

При забезпеченні цілісності інформації список загроз такий: модифікація/спотворення інформації; заперечення автентичності інформації; нав'язування неправдивої інформації.

При забезпеченні доступності інформації можливе її блокування, або знищення самої інформації і засобів її обробки.

Класифікація можливостей реалізації загроз, являє собою сукупність можливих варіантів дій джерела загроз певними методами реалізації з використанням вразливостей, які призводять до реалізації цілей атаки.

Мета атаки може не збігатися з метою реалізації загроз і може бути спрямована на отримання проміжного результату, необхідного для досягнення надалі реалізації загрози.

У разі такого не співпадіння атака розглядається як етап підготовки до вчинення дій, спрямованих на реалізацію загрози, тобто як «підготовка до вчинення» протиправної дії. Результатом атаки є наслідки, які є реалізацією загрози і / або сприяють такій реалізації.

3.1.2. Найбільш поширені загрози

Найчастішими і найнебезпечнішими (з точки зору розміру заподіяної шкоди) є ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують комп'ютерну мережу.

Іноді такі помилки і є власне погрозами (неправильно введені дані або помилка в програмі, яка викликала крах системи), іноді вони створюють вразливі місця, якими можуть скористатися зловмисники (такі зазвичай помилки адміністрування). За деякими даними, до 65% втрат – наслідок ненавмисних помилок.

Пожежі та повені не приносять стільки бід, скільки безграмотність і недбалість у роботі.

Очевидно, найрадикальніший спосіб боротьби з ненавмисними помилками – максимальна автоматизація і строгий контроль.

Інші загрози доступності можна класифікувати за компонентами інформаційної системи, на які націлені загрози:

- відмова користувачів;
- внутрішній відмова мережі;
- відмова підтримуючої інфраструктури.

Зазвичай стосовно користувачам розглядаються наступні загрози:

- неможливість працювати з системою через відсутність відповідної підготовки;

- небажання працювати з інформаційною системою (найчастіше проявляється при необхідності освоювати нові можливості і при розбіжності між запитами користувачів і фактичними можливостями і технічними характеристиками);

Крім того до ефективних заходів протидії спробам несанкціонованого доступу відносяться засоби реєстрації. Для цих цілей найбільш перспективними є нові операційні системи спеціального призначення, що широко застосовуються в зарубіжних країнах і отримали назву моніторингу (автоматичного спостереження за можливою комп'ютерною загрозою).

Моніторинг здійснюється самою операційною системою, причому в її обов'язки входить контроль за процесами введення–виведення, обробки та знищення машинної інформації. ОС фіксує час несанкціонованого доступу та програмних засобів, до яких був здійснений доступ. Крім цього, вона робить негайне оповіщення служби комп'ютерної безпеки про посягання на безпеку комп'ютерної системи з одночасною подачею на друк необхідних даних (лістингу). Останнім часом в США і низці європейських країн для захисту комп'ютерних систем діють теж спеціальні підпрограми, що викликають самознищення основної програми при спробі несанкціонованого перегляду вмісту файлу з секретною інформацією за аналогією дії «логічної бомби».

Завдання забезпечення безпеки:

- Захист інформації в каналах зв'язку і базах даних криптографічними методами;
- Підтвердження автентичності об'єктів даних і користувачів (автентифікація сторін, що встановлюють зв'язок);
- Виявлення порушень цілісності об'єктів даних;
- Забезпечення захисту технічних засобів і приміщень, в яких ведеться обробка конфіденційної інформації, від витоку по побічних каналах і від можливо впроваджених у них електронних пристроїв знімання інформації;
- Забезпечення захисту програмних продуктів і засобів обчислювальної техніки від впровадження в них програмних вірусів і закладок;

- Захист від несанкціонованих дій по каналу зв'язку від осіб, не допущених до засобам шифрування, але мають мети компрометації секретної інформації та дезорганізації роботи абонентських пунктів.
- Організаційно–технічні заходи, спрямовані на забезпечення захисту конфіденційних даних.

3.1.3. Програмні атаки

Як засіб виведення мережі зі штатного режиму експлуатації може використовуватися агресивне споживання ресурсів (зазвичай – смуги пропускання мереж, обчислювальних можливостей процесорів або оперативної пам'яті). По розташуванню джерела загрози таке споживання підрозділяється на локальне та віддалене. При прорахунках в конфігурації системи локальна програма здатна практично монополізувати процесор і / або фізичну пам'ять, тим самим зменшивши швидкість виконання інших програм до нуля.

Найпростіший приклад віддаленого споживання ресурсів – атака, що отримала найменування «SYN–повінь». Вона являє собою спробу переповнити таблицю «напіввідкритих» TCP–з'єднань сервера (встановлення з'єднань починається, але не закінчується). Така атака щонайменше ускладнює встановлення нових сполучень з боку легальних користувачів, тобто сервер виглядає як недоступний.

По відношенню до атаки «Papa Smurf» уразливі мережі, що сприймають ping–пакети з широкомовними адресами. Відповіді на такі пакети «з'їдають» смугу пропускання.

Віддалене споживання ресурсів останнім часом проявляється в особливо небезпечній формі – як скоординовані розподілені атаки, коли на сервер з безлічі різних адрес з максимальною швидкістю спрямовуються цілком легальні запити на з'єднання та / або обслуговування. Часом початку «моди» на подібні атаки можна вважати лютий 2000 року, коли жертвами виявилися кілька найбільших систем електронної комерції (точніше – власники та користувачі систем). Якщо має місце архітектурний прорахунок у вигляді розбалансованості між пропускною

здатністю мережі і продуктивністю сервера, то захиститися від розподілених атак на доступність вкрай важко.

Для виведення систем зі штатного режиму експлуатації можуть використовуватися вразливі місця у вигляді програмних і апаратних помилок. Наприклад, відома помилка в процесорі Pentium I давала можливість локальному користувачеві шляхом виконання певної команди «підвісити» комп'ютер, так що допомагає тільки апаратний RESET.

Програма «Teardrop» віддалено «підвішує» комп'ютери, експлуатуючи помилку в збірці фрагментованих IP–пакетів.

3.1.4. Класифікація заходів забезпечення безпеки

За способами здійснення всіх заходів забезпечення безпеки комп'ютерних мереж поділяються на: правові (законодавчі), морально–етичні, організаційні (адміністративні), фізичні, технічні (апаратно–програмні).

До правових заходів захисту відносяться діючі в країні закони, укази та нормативні акти, що регламентують правила поводження з інформацією, що закріплюють права та обов'язки учасників інформаційних відносин у процесі її обробки та використання, а також встановлюють відповідальність за порушення цих правил, перешкоджаючи тим самим неправомірному використанню інформації і є стримуючим фактором для потенційних порушників.

До морально–етичних заходів протидії належать норми поведінки, які традиційно склалися або складаються в міру поширення комп'ютерних мереж у країні або суспільстві. Ці норми здебільшого не є обов'язковими, як законодавчо затверджені нормативні акти, проте, їх недотримання веде звичайно до падіння авторитету, престижу людини, групи осіб або організації. Морально–етичні норми бувають як неписані (наприклад, загальновизнані норми чесності, патріотизму і т.п.), так і писані, тобто оформлені в деякий звід (статут) правил чи приписів.

Організаційні (адміністративні) заходи захисту – це заходи організаційного характеру, що регламентують процеси функціонування системи обробки даних, використання її ресурсів, діяльність персоналу, а крім того порядок взаємодії

користувачів із системою таким чином, щоб найбільшою мірою утруднити чи виключити можливість реалізації загроз безпеці.

Вони включають:

- заходи, здійснювані при проектуванні, будівництві та обладнанні мереж та інших об'єктів систем обробки даних;
- заходи щодо розробки правил доступу користувачів до ресурсів мереж (розробка політики безпеки);
- розподіл реквізитів розмежування доступу (паролів, ключів шифрування тощо);
- заходи, здійснювані при підборі й підготовці персоналу;
- організацію охорони і надійного пропускного режиму;
- організацію явного і прихованого контролю за роботою користувачів;
- заходи, здійснювані при проектуванні, розробці, ремонті і модифікаціях обладнання та програмного забезпечення і т.п.;
- організацію обліку, зберігання, використання та знищення документів і носіїв з інформацією;

Фізичні заходи захисту засновані на застосуванні різного роду механічних, електро– або електронно–механічних пристроїв і споруд, спеціально призначених для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів мереж і захищається, а ще і технічних засобів візуального спостереження, зв'язку та охоронної сигналізації.

Технічні (апаратні) заходи захисту засновані на використанні різних електронних пристроїв, що входять до складу КС і виконують (самостійно або в комплексі з іншими засобами) функції захисту.

Програмні методи захисту призначаються для безпосереднього захисту інформації за трьома напрямками:

a) апаратури;
b) програмного забезпечення;
c) даних і керуючих команд.

Для захисту інформації при її передачі зазвичай використовують різні методи шифрування даних перед їх введенням в канал зв'язку або на фізичний носій з наступною розшифровкою. Як показує практика, методи шифрування дозволяють досить надійно приховати зміст повідомлення.

Всі програми захисту, що здійснюють управління доступом до інформації, функціонують за принципом відповіді на питання: хто може виконувати, які операції і над якими даними.

Доступ може бути визначений як:

- загальний (безумовно що надається кожному користувачеві);
- відмова (безумовну відмову, наприклад дозвіл на видалення інформації);
- залежний від події (керований подією);
- залежний від змісту даних;
- залежний від стану (динамічного стану комп'ютерної системи);
- частотно–залежний (наприклад, доступ дозволений користувачеві тільки один чи певну кількість разів);
- по імені або іншим ознакам користувача;
- залежний від повноважень;
- за дозволом (наприклад, по паролю);
- за процедурою.

Завдання забезпечення безпеки:

- Виявлення порушень цілісності об'єктів даних;
- Захист інформації в каналах зв'язку і базах даних криптографічними методами;
- Забезпечення захисту технічних засобів і приміщень, в яких ведеться обробка конфіденційної інформації, від витоку по побічних каналах і від можливо впроваджених у них електронних пристроїв знімання інформації;
- Підтвердження автентичності об'єктів даних і користувачів (аутентифікації сторін, що встановлюють зв'язок);

- Забезпечення захисту програмних продуктів і засобів обчислювальної техніки від проникнення в них програмних вірусів і закладок;
- Організаційно–технічні заходи, спрямовані на забезпечення цілісності конфіденційних даних;
- Захист від несанкціонованих дій по каналу зв'язку від осіб, не допущених до засобів шифрування, але мають мету компрометації секретної інформації та дезорганізації роботи абонентських пунктів.

3.2. Схема передачі даних розумного будинку та виявлення потенційної небезпеки

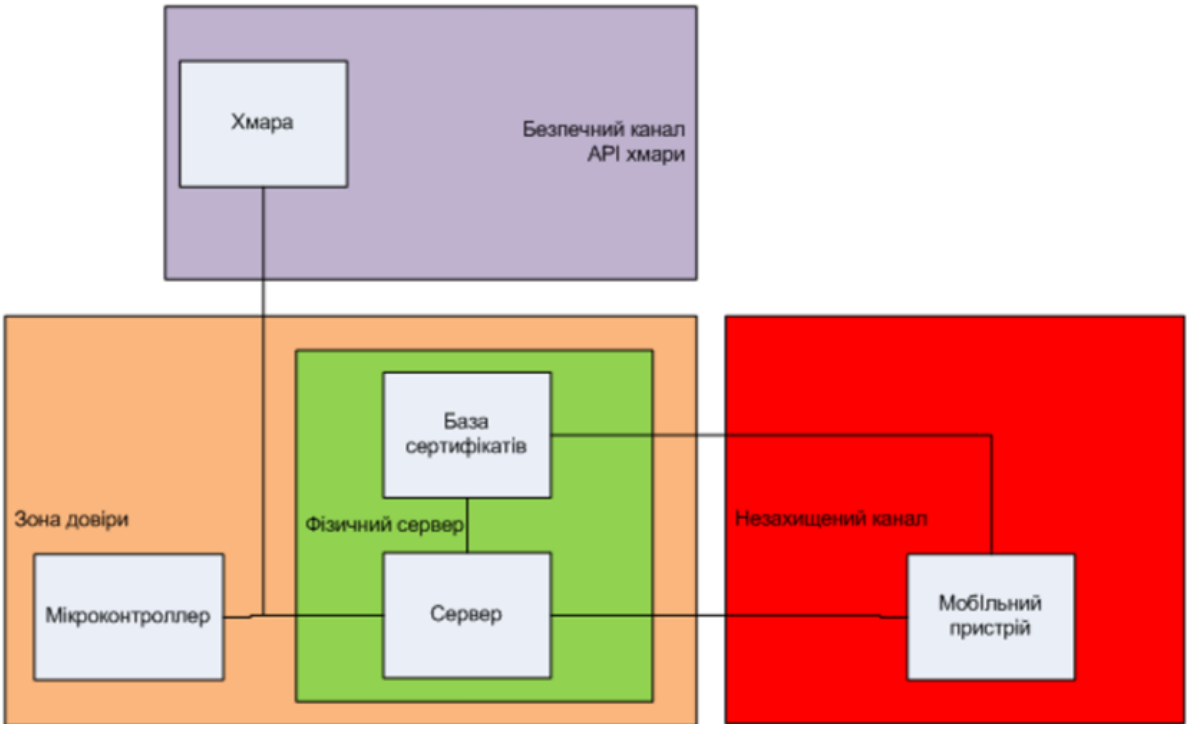

Рис. 3.3. Схема передачі даних

База сертифікатів – частина фізичного сервера, що зберігає всі цифрові підписи, до яких має повний доступ логічний сервер та частковий доступ користувач зі свого мобільного пристрою.

Мікроконтролер – пристрій, що безпосередньо відповідає за керування «розумним будинком».

В рамках локальної мережі (мережі сервера) дані вважаються умовно захищеними.

Небезпеку становить незахищений канал користувача. Один з класичних сценаріїв – man–in–the–middle, тобто можливість інших осіб підключитись в канал між сервером та користувачем та видавати себе за когось з цих ключових осіб, беручи на себе роль невидимого посередника. Для того, щоб не допустити витік інформації, слід використовувати схеми з шифрування даних.

3.3. Схеми шифрування

3.3.1. Системи з відкритим ключем

Відомо, що як би не були складні і надійні криптографічні системи – їх слабке місце при практичній реалізації – проблема розподілу ключів. Для того щоб був можливий обмін конфіденційною інформацією між двома суб'єктами системи, ключ повинен бути згенерований одним з них, а потім якимось чином, знову ж у конфіденційному порядку, переданий іншому. Тобто в загальному випадку для передачі ключа знову ж потрібне використання якоїсь криптосистеми. Для вирішення цієї проблеми на основі результатів, отриманих класичною та сучасною алгеброю, були запропоновані системи з відкритим ключем.

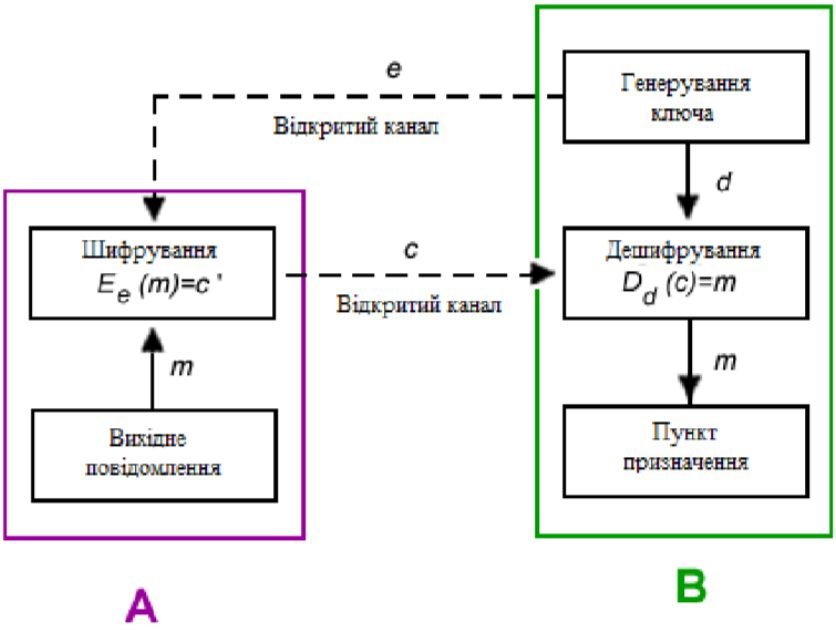

Рис. 3.4. Система з відкритим ключем

Суть їх полягає в тому, що кожним адресатом системи генеруються два ключі, зв'язані між собою за певним правилом. Один ключ оголошується відкритим, а інший закритим. Відкритий ключ публікується і доступний кожному, хто бажає послати повідомлення адресату. Секретний ключ зберігається в

таємниці. Вихідний текст шифрується відкритим ключем адресата і передається йому. Зашифрований текст в принципі не може бути розшифрований тим же відкритим ключем. Розшифрувати повідомлення можливо тільки з використанням закритого ключа, який відомий тільки самому адресату.

У криптографії з відкритими ключами є ряд переваг перед класичною (тобто симетричною) криптографією. Найбільш корисне з них стосується управління ключами. Давайте розглянемо стандартну симетричну криптосистему. Ключ шифрування є теж ключем розшифрування, таким чином, перший не може бути розкритий. Це призводить до того, що дві легальні сторони (відправник і одержувач) домовляються заздалегідь про алгоритм шифрування і ключах.

При використанні ж криптосистем з відкритим ключем сторони не зобов'язані зустрічатися, знати один одного і мати секретні канали зв'язку. Ця перевага стає ще більш актуальною у випадку великої кількості користувачів системи. Тоді, наприклад, один користувач може «закрито» зв'язатися з іншим, взявши деяку інформацію (відкритий ключ) із загальнодоступної бази даних (банку ключів).

Іншою важливою перевагою є довжина ключа. У систем з відкритим ключем довжина ключа шифрування не має значення, оскільки він відкритий і загальнодоступний. Тому і довжина ключа розшифрування не так важлива (одержувач тільки зберігає його в секретному місці). Зазначені вище дві переваги, що стосуються управління ключами, – головні для криптосистем з відкритим ключем. Різниця ключів (відкритого і особистого) в криптографії з відкритими ключами дозволила створити такі технології: електронні цифрові підписи, розподілена перевірка справжності, узгодження загального секретного ключа сесії, шифрування великих обсягів даних без попереднього обміну загальним секретним ключем.

Відомі алгоритми:

- RSA (Rivest–Shamir–Adleman)
- ECC (Elliptic Curve Cryptography)

- Алгоритм електронного цифрового підпису DSA (Digital Signature Algorithm,);
- Алгоритм DH (Diffie–Hellman), застосовуваний для вироблення спільного секретного ключа сесії.

3.3.2. Вразливості систем з відкритим ключем

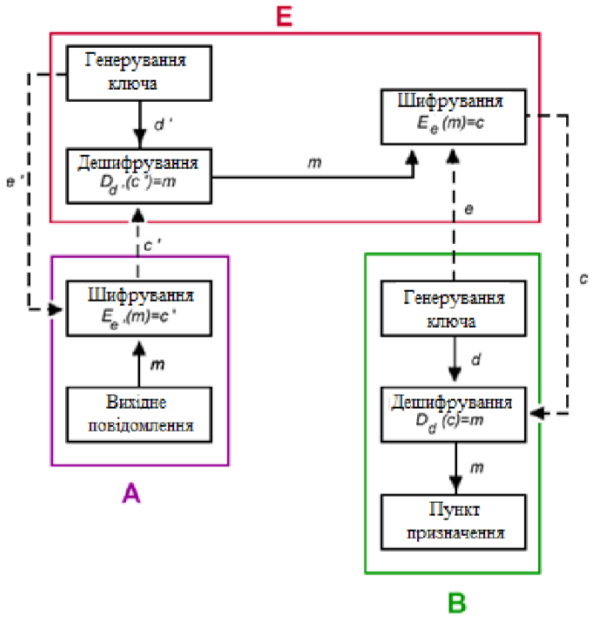

Рис. 3.5. Вразливості систем з відкритим ключем

Здавалося б, що асиметричні алгоритми шифрування – ідеальна система, яка не потребує безпечного каналу для передачі ключа шифрування. Це передбачало б, що два легальних користувача могли б спілкуватися з відкритого каналу, не зустрічаючись, щоб обмінятися ключами. На жаль, це не так. На Рис 3.5 наглядно демонструється, що є можливість захопити систему.

Асиметричні алгоритми шифрування з активним перехватчіком.png

У цій моделі зловмисник перехоплює відкритий ключ e, посланий користувачем системи. Потім створює пару ключів e' і d', «маскується» під того хто передає повідомлення, посилаючи отримувачу відкритий ключ e ', який, як думає отримувач, відкритий ключ, посланий йому відправником. Зловмисник перехоплює зашифровані повідомлення, розшифровує їх за допомогою секретного ключа d', заново зашифровує відкритим ключем e і відправляє повідомлення відправнику. Таким чином, ніхто з учасників не здогадується, що є третя особа, яка може як просто перехопити повідомлення m, так і підмінити його на хибне

повідомлення m'. Це підкреслює необхідність аутентифікації відкритих ключів. Для цього зазвичай використовують сертифікати. Розподілене управління ключами в PGP вирішує проблему за допомогою поручителів.

Ще одна форма атаки – обчислення закритого ключа, знаючи відкритий. Криптоаналітика знає алгоритм шифрування E, аналізуючи його, намагається знайти D. Цей процес спрощується, якщо криптоаналітик перехопив кілька крипто текстів c, посланих особою A особі B.

Більшість криптосистем з відкритим ключем засновані на проблемі факторизації великих чисел. Наприклад, RSA використовує в якості відкритого ключа n два великих числа. Складність злому такого алгоритму полягає в труднощі розкладання числа n на множники. Але це завдання вирішити реально. І з кожним роком процес розкладання стає все швидше.

3.3.3. Інфраструктура відкритих ключів

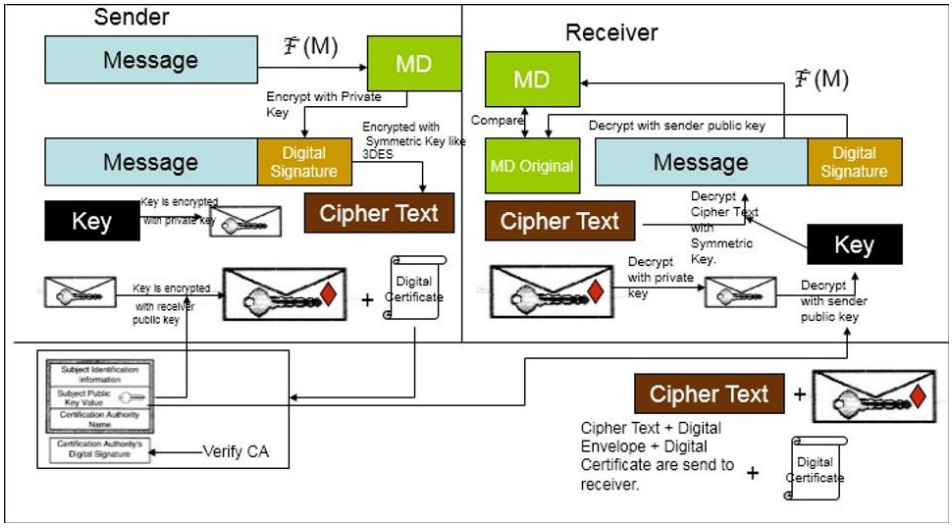

Рис. 3.6. PKI

Шифрування з відкритим ключем (асиметричним ключем) використовує пару ключів для шифрування і дешифрування змісту. Пара ключів складається з одного відкритого та одного закритого ключа, які математично пов'язані між собою. Людина, яка має намір надійно співпрацювати з іншими може поширювати відкритий ключ, але вона повинна тримати закритий ключ в таємниці. Вміст що шифрується за допомогою однієї з клавіш можуть бути розшифровані за допомогою іншої.

Припустимо, наприклад, що відправник хоче послати захищене повідомлення електронної пошти одержувачу.

Це може бути досягнуто наступним чином:

Обидва мають власні ключові пари. Вони зберегли свої ключі надійно і відправили їх відкриті ключі один одному безпосередньо.

Відправник використовує відкритий ключ одержувача щоб зашифрувати повідомлення і відправляє його.

Одержувач в свою чергу використовує свій закритий ключ для того щоб розшифрувати повідомлення.

Цей спрощений приклад підкреслює принаймні одну очевидну річ: відправник повинен мати відкритий ключ, який використовується для шифрування повідомлення. Тобто, він не може знати з упевненістю, що ключ, який використовується для шифрування насправді належав одержувачу. Цілком можливо, що інша сторона моніторила канал зв'язку між ними і замінила ключ.

Інфраструктура відкритих ключів (PKI) складається з програмного забезпечення та апаратних елементів, які довірена третя сторона може використовувати, щоб встановити цілісність і право власності відкритого ключа. Довірена сторона, називається центром сертифікації (CA), як правило, це досягається шляхом видачі підписаних (шифрованих) довічних сертифікатів, які підтверджують особистість суб'єкта сертифіката і пов'язують його з відкритим ключем, що міститься в сертифікаті. CA підписує сертифікат, використовуючи свій закритий ключ. Він видає відповідний відкритий ключ для всіх зацікавлених сторін у власний сертифікат ЦС. При використанні CA, попередній приклад може бути змінений таким чином:

Припустимо, що CA випустила цифровий сертифікат, який містить відкритий ключ. CA самостійно шифрує цей сертифікат за допомогою закритого ключа, який відповідає відкритому ключу в сертифікаті.

Користувачі згодні використовувати CA для перевірки їх ідентичності. Одержувач просить сертифікат відкритого ключа з ЦС.

СА перевіряє її особистість, обчислює хеш змісту, які будуть складати її сертифікат, підписує хеш за допомогою закритого ключа, відповідного відкритого ключа в опублікованому сертифікаті ЦС, створює новий сертифікат, пов'язуючи зміст сертифікату та підписавши хеш, і робить новий сертифікат публічно доступним.

Відправник отримує сертифікат, розшифровує підписані документи за допомогою відкритого ключа центру сертифікації, обчислює новий хеш вмісту сертифікату і порівнює два хеші. Якщо вони збігаються, підпис перевіряється і відправник може сміливо вважати, що відкритий ключ в сертифікаті дійсно належить одержувачу.

В цілому, процес підписання сертифіката дозволяє перевірити відправнику, що відкритий ключ не підроблений або пошкоджений під час транспортування. Перед видачою сертифікату, СА шифрує хеш за допомогою власного секретного ключа, і включає в себе зашифрований хеш виданого сертифіката. Відправник перевіряє вміст сертифікату за допомогою розшифрування хешу з відкритим ключем СА, виконуючи окремий хеш вмісту сертифікатів, і порівнюючи два хеші. Якщо вони збігаються, відправник може бути на 100% впевненим, що сертифікат і відкритий ключ не були змінені.

Таблиця 4

Структура PKI

Елемент	Опис
База сертифікатів	Зберігає всі дозволені сертифікати
Архів сертифікатів	Зберігає відмінені, заблоковані сертифікати.
Орган сертифікації	Корінь довіри PKI
Орган реєстрування	Система засвідчення.

3.3.4. Симетричні криптосистеми

Симетричне шифрування передбачає використання одного і того ж ключа і для шифрування, і для розшифровки. До симетричних алгоритмів застосовуються дві основні вимоги: повна втрата всіх статистичних закономірностей в об'єкті шифрування і відсутність лінійності.

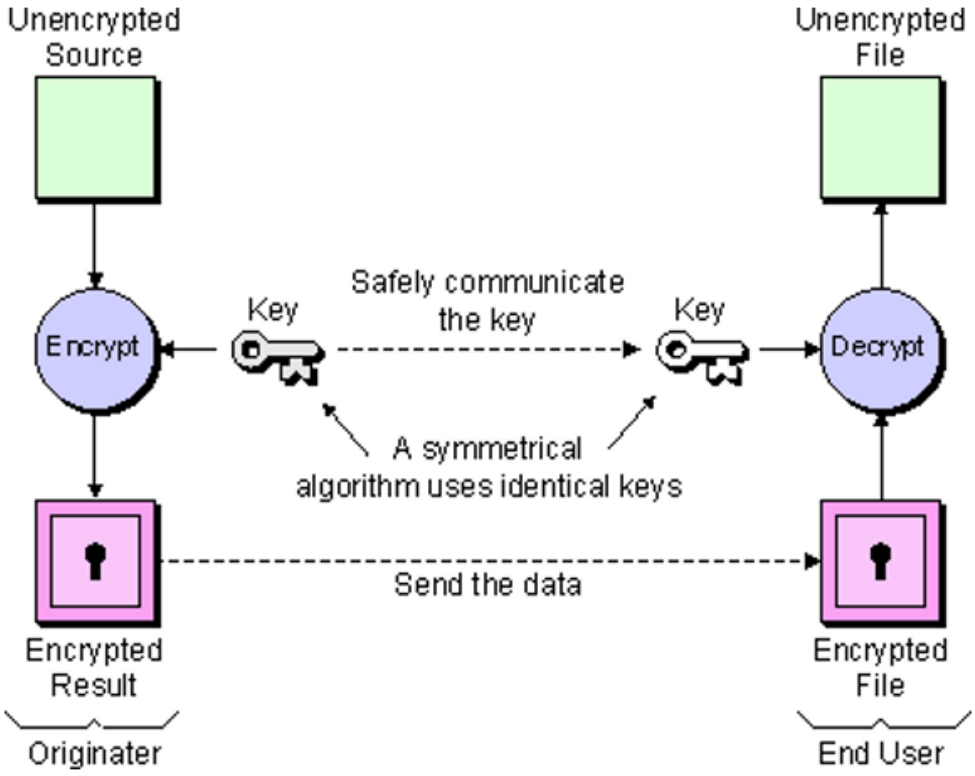

Рис. 3.7. Симетрична криптосистема

Прийнято розділяти симетричні системи на блокові і потокові.

У блокових системах відбувається розбиття вихідних даних на блоки з подальшим перетворенням за допомогою ключа.

У поточних системах виробляється якась послідовність, яка в подальшому накладається на саме повідомлення, і шифрування даних відбувається потоком по мірі генерування. Схема зв'язку з використанням симетричної криптосистеми представлена на Рис 3.6.

Схема зв'язку з використанням симетричною криптосистеми, де М – відкритий текст, К – секретний ключ, який передається по закритому каналу, $E \cdot n$ (М) – операція шифрування, а $D \cdot k\ (M)$ – операція розшифрування.

Зазвичай при симетричному шифруванні використовується складна і багатоступенева комбінація підстановок і перестановок вихідних даних, причому ступенів (проходів) може бути безліч, при цьому кожній з них повинен відповідати «ключ проходу». Операція підстановки виконує першу вимогу, що пред'являється до симетричного шифру, позбавляючись від будь–яких статистичних даних шляхом перемішування бітів повідомлення за певним заданим законом. Перестановка необхідна для виконання другої вимоги – додання алгоритмом не лінійності. Досягається це за рахунок заміни певної частини повідомлення заданого обсягу на стандартне значення шляхом звернення до вихідного масиву.

Симетричні системи мають як свої переваги, так і недоліки перед асиметричними.

До переваг симетричних шифрів відносять високу швидкість шифрування, меншу необхідну довжину ключа при аналогічній стійкості, велику вивченість і простоту реалізації.

Недоліками симетричних алгоритмів вважають в першу чергу складність обміну ключами зважаючи на велику ймовірність порушення секретності ключа при обміні, який необхідний, і складність управління ключами у великій мережі.

3.4. Алгоритми шифрування

3.4.1. AES

Є комбінацією S–box і P–box, оскільки окремо вони не пропонують істотної криптостійкості. S–box використовується для одиничної перестановки біт, після чого повідомлення передається на P–box, де воно «перемішується» (всі біти піддаються перестановці), потім складається по модулю з раундовим ключем і передається на наступний шар мережі.

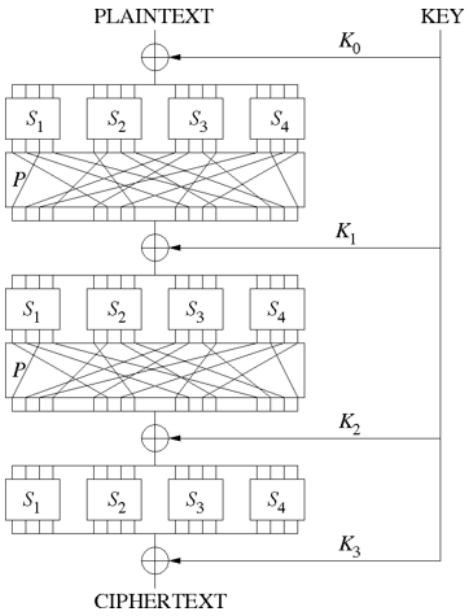

Рис. 3.8. SP box

Алгоритм:

- KeyExpansion – генерація раундових ключів.
- InitialRound
  - AddRoundKey – додавання по модулю 2 проміжного масиву з раундовим ключем
- Rounds (для всіх раундів)
  - SubBytes – нелінійна перестановка байт, використовуючи SP– мережі
  - ShiftRows – циклічний зрушення 3 останніх рядків
  - MixColumns – комбінування (змішування) 4 байт кожного рядка з використанням зворотного лінійного перетворення
  - AddRoundKey
- FinalRound
  - SubBytes
  - ShiftRows
  - AddRoundKey

Використовуючи S–box (будується згідно властивостей поля Галуа), відбувається незалежна заміна байт масиву State. Береться зворотне число b в полі Галуа.

$$\begin{Vmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{Vmatrix} = \begin{Vmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{Vmatrix} * \begin{Vmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{Vmatrix} + \begin{Vmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{Vmatrix}$$

Рис. 3.9. Операції перетворення

Таким чином, надається захист від атак, заснованих на простих алгебраїчних властивостях.

Циклічний зсув кожного рядка вліво на певну величину, а саме на n–1, де n – номер рядку. Це справедливо у випадку використання блоків розміром 128 і 196 біт, для 256 біт ситуація дещо інша: зсув відбувається на n, для n = 0.

Разом з попередньою процедурою вносить в шифротекст розсіювання. Крім змішування 4 байт кожного рядка, відбувається перемножування на фіксовану матрицю:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Рис. 3.10. Матриця перемноження

Трактується це наступним чином:

Множення на 1 – ніяких змін.

Множення на 2 – зрушення вліво

Множення на 3 – зрушення вліво і підсумовування по модулю 2 з початковим значенням.

AES має досить простий математичний опис, але тим не менш є криптостійким і всі спроби знайти в ньому серйозну вразливість не мали успіху.

Єдиний спосіб боротьби зловмисників з AES – це атака не на сам захист, а на систему, використовуючи її вразливості.

AES прийнятий як стандарт і широко використовується у всіх сферах (є одним з найпоширеніших).

3.4.2. RSA

Криптографічний асиметричний алгоритм (або алгоритм з відкритим ключем), побудований з використанням довгої арифметики і односторонніх функцій.

Односторонньою називається функція виду $y=f(x)$, яка володіє такими особливостями:

1) При відомому аргументі розрахувати функцію є тривіальним завданням, яка відносно просто може бути вирішена.
2) При відомому значенні функції знайти аргумент не представляється можливим з практичної точки зору. Іншими словами, за розумний час неможливо його знайти.

На відміну від симетричних шифрів, розрізняють public (відкритий) і private (закритий) ключі. У більшості випадків, відкритий ключ публікується, в той час як закритий тримається в строгому секреті. Це пов'язано з тим, що закритий ключ значно «більше» за розміром, ніж відкритий, таким чином, його важче зламати.

Генерація ключів:

1) Вибір 2 простих цілих чисел (як правило, їх розмір як мінімум 1024 біт кожне) p і q.
2) Розрахунок модуля ключа як добуток: $n = p \cdot q$.
3) Розрахунок функції Ейлера: $F(n) = F(p) \cdot F(q) = (p - 1) \cdot (q - 1)$.
4) Вибір E – взаємно простого з $F\ (n)$. Як правило це просте число з невеликою кількістю одиничних біт. E називається відкритою експонентою і є частиною відкритого ключа. Важливо пам'ятати, що при виборі малих значень відкритої експоненти криптостійкість може різко знизитися.

5) Визначення закритою експоненти D, як мультиплікативно зворотного до E по модулю F (n). Іншими словами, потрібно знайти таке D, щоб виконувалася така умова: $d \cdot e = 1 \ mod \ F(n)$. На практиці вона обчислюється за допомогою розширеного алгоритму Евкліда.
6) Пара $\{E, n\}$ – відритий ключ.
7) Пара $\{D, n\}$ – закритий ключ.

Алгоритм шифрування:

1) Переклад повідомлення M в число m. Не важко здогадатися, що цей пункт визначає сферу використання RSA як підпис, оскільки великі повідомлення не доцільно шифрувати таким способом. На практиці за допомогою RSA найчастіше шифрують симетричний ключ, наприклад AES, (для безпечної його передачі по каналу зв'язку) а останній використовують безпосередньо для шифрування даних.
2) Взяти відкритий ключ $\{E, n\}$.
3) Шифротекст C визначається за формулою: $C = m \cdot E \ (mod \ n)$

Алгоритм розшифрування:

1) Прийняти шифротекст C.
2) Взяти свій закритий ключ $\{D, n\}$.
3) Початкове повідомлення визначається за формулою: $m = C \cdot D \ (mod \ n)$

Примітка: якщо сеансовий ключ більше, ніж n, тоді його розбивають на блоки потрібної довжини і шифрують окремо.

Розширений алгоритм Евкліда, рішення рівняння типу $a \cdot x + b \cdot y =$

1) Покладемо початкову одиничну матрицю
2) Обчислимо залишок від ділення $r = a \ mod \ b$
3) Якщо $r = 0$, другий стовпець матриці E – рішення задачі (вектор)
4) З рівняння $a = b \cdot q + r$ виведемо $q = a \cdot r \ / \ b$
5) Замінимо .

Примітка: якщо як a покласти E, а в якості b – модуль, тоді x – закрита експонента.

В результаті обчислення можна отримати негативну закриту експонента.

Щоб змінити знак, достатньо використовувати наступну формулу:

$$D = (D + n) \, mod \, n$$

Криптостійкість:

Основним «проломом» у криптостійкості RSA може бути погано обрана відкрита експонента та / або пара простих чисел p і q. Завдання визначити секретну експоненту вкрай складне і вимагає занадто великої обчислювальної потужності і чималого часу. Враховуючи той факт, що RSA ключі періодично змінюються (приблизно раз на рік), прямий злом є практично не досяжним завданням.

Застосування:

Як вже було сказано, RSA найчастіше використовують для цифрового підпису або шифрування іншого, більш «простого» ключа (що є практично одним і тім же завданням). Причиною цьому є великі обчислювальні витрати, які визначають розміри вхідних повідомлень.

3.5. Вибір системи шифрування

Проаналізуємо системи та алгоритми описані вище. Із систем найоптимальнішою є система з використанням PKI, адже саме вона забезпечує надійний канал для передачі сесійного ключа між сервером та клієнтом. В якості сертифікату візьмемо деякий ключ, відомий тільки користувачеві та базі сертифікатів, причому база сертифікатів зберігає ключ в парі з публічним ключем користувача. Тоді система передачі даних буде приймати наступний вигляд (для зручності розіб’ємо на 2 етапи: авторизація та безпосередньо зв’язок між 2 вузлами):

1) Авторизація
   - Клієнт підписує кодову фразу «SH0» (яка означає запит авторизації) своїм таємним ключем.
   - Сервер отримує повідомлення та надсилає його до бази сертифікатів.

- Якщо база сертифікатів знаходить вказаний підпис, відбувається авторизація, а саме: сервер отримує з бази публічний ключ клієнта та надсилає йому зашифрований цим ключем AES сесійний ключ, включивши теж фразу «SH1»; інакше генерується виключення «SH4».

1) Сесія «спілкування»

- Отримавши сесійний ключ, тепер клієнт та сервер можуть передавати один одному дані за допомогою кодової фрази «SH2»
- По закінченню, клієнт відсилає «SH3» з закодованою фразою «exit», що призводить до припинення сесії та знищення сесійного ключа відповідно.

Раз на рік система сертифікатів повинна перегенеровувати ключі, щоб звести вірогідність злому до мінімуму.

Слід не забувати, що є безпосередньо мікроконтролери, що відповідають за зчитування та керування пристроями. З самого початку ми визначили локальну мережу сервера як «зона довіри», але існує ймовірність, що злочинець може перебувати біля серверу, але відносно нетривалий час, тобто такий час, за який неможливо підібрати ключ для такого тривіального алгоритму шифрування, як Base64. Цей алгоритм досить добре підходить для таких цілей через те, що він не перевантажує відносно малопотужні мікроконтролери, даючи таким чином деякий захист інформації, і в той же час не створює зайві затримки.

3.6. Тести системи безпеки

Для перевірки коректної роботи описаного вище модуля запропоновані наступні тести:

1) Перевірка на розрізнення команд

- Спробувати почати з відправки повідомлення (SH2), очікуваний результат – виключення SH4.
- Відправити запит на авторизацію (SH0) при використанні коректного сертифікату. Очікуваний результат – SH1.

- Відправити запит на авторизацію (SH0) при використанні неіснуючого сертифікату. Очікуваний результат – SH4.
- Завершити сесію та спробувати відправити повідомлення (SH2), очікується реакція SH4.

1) Перевірка на коректність шифрування невеликих об’ємів даних

- Зашифрувати повідомлення локально «Hello, Word!».
- Зашифрувати попереднє повідомлення та передати через Internet.
- Зашифрувати та відправити по мережі зображення.

1) Перевірка на коректність шифрування великих об’ємів даних

- Зашифрувати файл з однотипних символів. Перевірити згенерований файл на «простоту».
- Зашифрувати та передати повідомлення вагою до 1 МБ.

1) Перевірка роботи системи сертифікатів

- Використати функціонуючий сертифікат, що пов’язаний з даним мобільним пристроєм, очікується позитивна реакція.
- Використати робочий сертифікат іншого пристрою, очікується виключення.
- Використати неіснуючий сертифікат. Очікується виключення.

1) Спроба man–in–the–middle атаки

- Створити міні–програму на серверній стороні, яка буде посередником між логічним сервером та клієнтом.
- Підмінити коди. Очікуваний результат – виключення SH4 для будь–чого.

3.7. Поради щодо забезпечення безпеки

Менш ніж 10 років тому власники «розумних будинків» могли з легкістю визначити, що в їх відсутність в будинку побував по сторонній (злочинець): по зламаному замку або розбитому вікні. Тепер же, завдяки повсюдному поширенню IoT–пристроїв, здійснити незаконне вторгнення стало ще простіше: захист вхідних дверей, як і камеру, можна досить легко віддалено вимкнути. Більш того, завдяки підключенню до смарт–термостату або «розумної» розетки зловмисник

може отримати інформацію про час, коли домовласники зазвичай знаходяться поза домом.

Рекомендацій, виконання яких може істотно знизити ризик злому:

1) Використовувати багатофакторну автентифікацію. Додайте додатковий фактор аутентифікації, крім застарілої технології захисту паролем. Цю пораду дав Джеррі Ірвін (Jerry Irvine), директор з інформаційних технологій у Prescient Solutions. На організованій страховою компанією HSB конференції він зазначив, що сьогодні самого лише пароля недостатньо для забезпечення безпеки.

В якості додаткового фактору захисту може бути обраний одноразовий код, що приходить в SMS–повідомленні, або один з варіантів біометричної аутентифікації: сканування відбитку пальця або сітківки ока. Таке рішення дозволить захистити важливі дані навіть якщо зловмисник зможе дізнатися ім'я користувача і пароль.

2) Інсталюйте оновлення системи безпеки, особливо на нові пристрої. Пора позбавлятися від звички відхиляти «настирливі» нагадування про наявність оновлень безпеки. Справа в тому, що хакери постійно знаходять нові вразливості в системі захисту пристроїв, а розроблювані патчі є способом усунути слабкі місця.

Більшість «розумних» домашніх пристроїв не оновлюються автоматично, тому раз на місяць користувачам потрібно заходити в фірмовий додаток і перевіряти наявність нових версій програмного забезпечення. Навіть якщо ви недавно придбали пристрій в магазині, не полінуйтеся при його установці переконатися, що воно отримало всі оновлення.

3) Встановіть захист від шкідливого ПО. Кожен пристрій повинен мати власну систему захисту від шкідливих програм. Тривалий час вважалося, що захист MacBooks здатен ефективно справлятися з усіма загрозами, але Джеррі Ірвін довів, що такий стан речей встигло змінитися. При цьому важливо завантажувати перевірене надійне, рекомендований фахівцями з безпеки.

4) Не підключайте смарт–пристрій до тієї ж мережі, що і основний комп'ютер. Це можна зробити шляхом створення окремого каналу зв'язку спеціально для «розумної» техніки або поділу локальної мережі з допомогою VLAN.
5) Змінюйте ім'я користувача і пароль, задані за замовчуванням. Якщо пристрій поставляється з ім'ям користувача і паролем, заданими за замовчуванням, ці відомості хакер може легко знайти на форумах. Вибирайте безпечні паролі з використанням різних чисел, знакових символів, рядкових і заголовних літер.

ВИСНОВКИ

Таким чином, в ході даної магістерської роботи мною визначено схему потоків даних, потенційні вразливі місця та засоби захисту системи «Розумний будинок». Запропонована криптографічна схема на основі сукупності Base64 та PKI, що за умови справності сервера, являється практично невразливою. Виходячи з викладеної вище інформації, мною було зроблено ряд наступних висновків.

Сьогодні ніхто з впевненістю не зможе озвучити точну цифру сумарних втрат від злочинів здійснених у сфері IT, пов'язаних з несанкціонованих доступом до даних та інформації. Це в першу чергу пов’язано з небажанням компаній які постраждали від рук хакерів оприлюднювати інформацію про свої втрати, адже не завжди втрати від розкрадання інформації можна точно оцінити в фінансовому еквіваленті.

Причини з яких відбувається активізація комп'ютерних злочинів і пов'язаних з ними грошових втрат досить багато, основними можна виділити:

- Перехід від традиційної «паперової» технології зберігання і передачі інформації на електронну і недостатній при цьому розвиток технології захисту інформації;
- Комп'ютерні мережі, просто не зможуть функціонувати і розвиватися нормально якщо будуть ігнорувати проблеми пов’язані з захистом та безпекою інформації;
- Підвищення складності програмних засобів що призводить до зменшення їх надійності та збільшення кількості вразливостей.

Для прогнозування напрямку розвитку системи «Розумний будинок, необхідно проаналізувати усі доступні на сьогодні факти. Сама концепція «розумного будинку» доволі перспективна та цікава.

На даний час велика кількість компаній, в тому числі в Україні, пропонують свої послуги зі створення «розумних будинків». Сама ж технологія реалізується дешево, з використанням існуючих силових кабелів або безпроводову, а ось

настройка системи «Розумний будинок», особливо якщо вона керується програмно з комп'ютера – річ досить складна, як і будь–які нові технології, до яких люди довго звикають, і обійдеться власникам будинку не так вже й дешево. Ряд деяких рішень необхідно враховувати ще при розробці дизайну приміщень «розумного будинку». Ідеальне місце застосування таких технологій – приватні будинки та заміські котеджі. В принципі, враховуючи, що власники заміських будинків витрачають великі гроші на їх утримання, вартість такого рішення буде відносно невеликою.

У «розумному будинку» вся електроніка і побутова техніка – від кліматичних систем до телевізорів – управляється надзвичайно складними комп'ютерними системами. «Розумний будинок» включає світло і музику, коли гості і близькі входять в будинок і переміщуються по кімнатах. При цьому світловий та музичний супровід у міру пересування відвідувача по апартаментам будинку змінюється відповідно до побажань господаря, які збережені в налаштуваннях. Людині не потрібно задавати температурний режим в приміщеннях або налаштовувати освітлення – встановлена «інтелектуальна» система станом господаря розпізнає, яка температура і освітлення необхідні йому в даний момент для повного комфорту. Для забезпечення зручності в квартирі можуть використовуватися різноманітні технології, починаючи від саморобних пристроїв і закінчуючи АСУ.

ПЕРЕЛІК ПОСИЛАНЬ

1. Е.А. Тесля. «Умный дом» своими руками. Строим интеллектуальную цифровую систему в своей квартире / Е.А. Тесля – Санкт Петербург, 2008. – 224 с.
2. Т. Р. Элсенпитер, Дж. Велт. «Умный Дом строим сами» / Т. Р. Элсенпитер, Дж Велт/ КУДИЦ–ОБРАЗ. 2005. – 384 с.
3. В.Н. Харке «Умный дом. Объединение в сеть бытовой техники и систем коммуникаций в жилищном строительстве» / В.Н. Харке– М.: Техносфера, 2006. – 292 с.
4. В.Н. Гололобов. «Умный дом» своими руками. / В.Н. Гололобов – М.: НТ Пресс, 2007. – 416 с.
5. Т. Р. Элсенпитер, Дж. Велт. «Умный Дом строим сами» / Т. Р. Элсенпитер, Дж Велт / КУДИЦ–ОБРАЗ. 2005. – 384 с.
6. М. Э. Сопер. Практические советы и решения по созданию «Умного дома» М. Э. Сопер. – М.: НТ Пресс, 2007. – 432 с.
7. Ярочкин В.И. Информационная безопасность. – М.: Изд–во «Академический проект», 2004. – 640 с.
8. 4. Ф. Широков. Bluetooth: на пути к миру без проводов./ Открытые системы, 2001. – № 2, http://www. radioscanner.ru/info/article95/
9. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. – М.: Изд–во «Интернет–университет информационных технологий – ИНТУИТ.ру», 2005. – 608 с.
10. Teslyuk V. Automation of the smart house system–level design / Teslyuk V., Beregovskyi V., Pukach A. // Informatyka Automatyka Pomiary w Gospodarce i Ochronie Środowiska. Polish magazin. Zeszyt 4. – 2013. – P. 81–84.
11. Береговський В. В. Методи та моделі автоматизованого проектування системи “інтелектуального будинку” на базі нейроконтролерів / Береговський В. В., Теслюк В. М., Матвійчук К. В., Денисюк П. Ю. // Науковий вісник НЛТУ

України : Збірник науково–технічних праць. – Вип. 26.7. – Львів : РВВ НЛТУ України, 2016. – С. 342–349.

12. Teslyuk T. The model of smart house lighting subsystem analysis on the basis of Petri net theory / Taras Teslyuk, Vasyl Beregovskyi, Yuryy Tertula, Roman Chupa // Proceedings of the 7th International Conference of Computer Science and Information Technologies (CSIT'2012), April 14–19, 2012. – Lviv: Publishing House Vezha&Co., 2012. – P. 172–173.
13. Системы "Умный дом" [Электронный ресурс]. URL: http://www.vashdom.ru/articles/research_2.htm.
14. Варганич Е. Рынок автоматизации в Украине. Итоги 2012 года: реалии vs потенциал // Automation Weekly UA. – 2013.– №2. –С. 6–9.
15. Жиленков Н. «Умный дом» — перспективы развития // Современные технологии автоматизации. – 2009. – № 1. – С. 60–2
16. Smart house Розумний будинок [Електронний ресурс]. – Режим доступу: URL http://buchuk.domen.uz.ua/index.php?id=smatr–house.
17. Что такое Умный Дом. Знакомство с системой [Электронный ресурс]. – Режим доступу: URL http://smarton.com.ua/smart_home.
18. Система Розумний будинок [Електронний ресурс]. – Режим доступу: URL http://ittel.com.ua/proektuvannya–inzhenernix–merezh/sistema–rozumnij–budinok
19. Центральні елементи розумного будинку [Електронний ресурс]. – Режим доступу: URL http://sutem.com.ua/021%20inels.php – Назва з екрану
20. Какие бывают «умные дома». Обзор. [Электронный ресурс]. – Режим доступу: URL http://www.besmart.su/article/kakie–byvayut–umnye–doma.
21. ВІСНИК КНУТД №3 (86), 2015 Серія «Технічні науки».
22. Найбільш поширені функції системи «Розумний будинок» [Електронний ресурс] // Режим доступу: http://megapredmet.ru/1-76622.html
23. Безопасность в умном доме: 5 аспектов [Електронний ресурс] // Режим доступу: http://umnydom.com/bezopasnost-v-umnom-dome-5-aspektov/ 435/
24. РОЗУМНІ МІСТА: ЩО НАС ЧЕКАЄ НАСТУПНІ 50 РОКІВ? [Електронний ресурс] // Режим доступу: http://www.korydor.in.ua/ ua/ideas/smart-cities.html

25. «Умные» технологии от Ericson [Електронний ресурс] // Режим доступу:https://keddr.com/2014/08/umnyie-tehnologii-ot-ericsson-otvecha et-voytseh-bayda/

26. Интернет вещей в умном городе [Електронний ресурс] // Режим доступу: http://www.iksmedia.ru/articles/4990900-Internet-veshhej-v-umnom-gorode.html

27. Как построить «умный город»: опыт Huawei [Електронний ресурс] // Режим доступу: http://www.cnews.ru/articles/2015-0914_kak_postroit _umnyj_gorod _opyt_ huawei

28.