УДК 681.5

АТОЯН А.С., ГОЛУБЄВ Л.П.
Київський національний університет технологій та дизайну

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ АВТОМАТИЗОВАНИХ СИСТЕМ «РОЗУМНИЙ БУДИНОК»

Мета. *Дослідження можливих вразливостей систем автоматизованого керування підсистемами та параметрами будівлі.*

Методика. *Структурний аналіз автоматизованої системи «Розумний будинок» та аналіз можливих вразливостей , якими можуть скористуватися зловмисники.*

Результати. *Досліджені можливі шляхи порушення роботи системи, як апаратного так і програмного характеру та приведені можливі методи вирішення проблеми.*

Наукова новизна. *У статті розглянуто інноваційні підходи дослідження та вирішення проблеми вразливостей автоматизованої системи «Розумний будинок».*

Практична значимість. *Оскільки подібними системами обладнуються не тільки житлові будинки, а й державні установи, а також стратегічні об'єкти, тому вирішення даної проблеми є дуже актуальною і значимою.*

Ключові слова: *розумний будинок, система, безпека, аналіз, програмне забезпечення, антивірусні засоби.*

Вступ. Системи автоматизованого управління будівлею або системи розумного будинку отримали велику популярність останнім часом. Розумний дім є автоматизована будівля сучасного типу, що організована для зручності людей за допомогою високотехнологічних пристроїв.

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. [1].

Шахраї можуть використати слабкі місця сучасних автоматизованих систем управління життєзабезпеченням. Злочинці можуть остаточно блокувати роботу великих об'єктів, наприклад аеропорту, сіяти хаос, і нарешті систему безпеки всередині, що може призвести до серйозних наслідків.

Постановка завдання. Завдання дослідження полягає у аналізі сучасних систем автоматизованого контролю будинком, виявлення можливих вразливостей, які можуть призвести до порушення роботи будинку в цілому та знаходження методів і пропозицій за для вирішення цієї проблеми.

Результати дослідження. На жаль, більшість систем автоматизації будівель не мають систему захисту проти кібер-атак. Більшість рішень для захисту, пов'язані з установкою стандартних програмам, які виконують функцію брандмауера. Але у випадку

нападу на системи автоматизації будівлі цього недостатньо. У цілому системи автоматизованого управління будівлею мають кілька типів програмного забезпечення. Першим є програмне забезпечення, яке забезпечує функціонування самої мережі «Розумного будинку». Воно розробляється на мовах програмування низького рівня і несе відповідальність за більш низькі рівні мережевої моделі OSI [1].

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

Головною частиною будь-якого комплексу програмного забезпечення 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 високорівневих 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 вразливі, і багато інших, які використовуються для побудови підсистем, часто з неналежною інтеграцією призводять до уразливості. Як уже згадувалося вище, серверне програмне забезпечення 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 програмне забезпечення.

Розглянемо основні канали розповсюдження вірусів [2]:

- 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 отримання вірусу в систему. [3];
- GSM канал. Через канал GSM також можливий несанкціонований контроль системи. Це можливе, 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 машину від локальної мережі;

Повноцінних антивірусних систем, що забезпечують комплексний захист від зловмисних програм, не існує [3]. 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 аунтефікації керуючої програми, яка передає пакети у мережу «Розумного будинку» .

На даний момент, є необхідність створювати спеціальні антивірусні засоби, які можуть забезпечити комплексний захист від зловмисних програм [1]. Зрозуміло, що антивірусні засоби для «Розумних будинків» повинні виконувати наступні важливі 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 проникнення вірусів;
- контролювати мережеве устаткування 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.

Висновки. 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 позволяють повністю захистити систему. Таким чином, створення антивірусних засобів, які здатні забезпечити комплексний захист для системи автоматизованого контролю будинком є важливим завданням у найближчі роки.

Список використаних джерел

1. Гололобов В. Н. «Умный дом» своими руками / В. Н. Гололобов. – М. : НТ Пресс, 2007. - 216с.
2. Технологии мобильной связи: услуги и сервисы / А. Г. Бельтов, И. Ю. Жуков, Д. М. Михайлов, А. В. Стариковский. – М. : ИНФРА-М, 2012. – 206 с.
3. Касперски К. Записки исследователя компьютерных вирусов / К. Касперски. – СПб. : Питер, 2006. – 216 с.

References

1. Hololobov V.N.(2007) *≪Umnuy dom≫ svoymy rukamy [«Smart home» own hands]*. Moscow: NT Press [in Russia].
2. Bel'tov A.H., Zhukov Y.Yu., Mykhaylov D.M.. Starykovskyy A.V. (2012). *Tekhnolohyy mobyl'noy svyazy: usluhy y servysг [Mobile communication technology services and services]*. Moscow: INFA-M [in Russia].
3. Kaspersky K.(2006) *Zapysky yssledovatelya komp'yuternыkh vyrusov Notes of the researcher computer virus]*. Saint Petersburg: Piter [in Russia].

ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ АВТОМАТИЗИРОВАННЫХ СИСТЕМ «УМНЫЙ ДОМ»

АТОЯН А. С., ГОЛУБЕВ Л.П.

Киевский национальный университет технологий и дизайна

Цель. Исследование возможных уязвимостей систем автоматизированного управления подсистемами и параметрами здания.

Методика. Структурный анализ автоматизированной системы «Умный дом» и анализ возможных уязвимостей, которыми могут воспользоваться злоумышленники.

Результаты. Изучены возможные способы взлома системы, как аппаратного так и программного характера и приведены возможные методы решения проблемы.

Научная новизна. В статье рассмотрены инновационные подходы исследования и решения проблемы уязвимости автоматизированной системы «Умный дом».

Практическая значимость. Поскольку подобными системами оснащены не только дома, но и правительственные учреждения, а также стратегические объекты, то решение этой проблемы очень актуальное и значимое.

Ключевые слова: *умный дом, система, безопасность, анализ, программное обеспечение, антивирусные средства.*

RESEARCH VULNERABILITY OF AUTOMATED SYSTEMS "SMART HOME"

ATOYAN A. S.,GOLUBEV L.P.

Kiev National University of Technology and Design

Purpose. Investigation of possible vulnerabilities of automated control subsystems and parameters of the building.

Methodology. Structural analysis of the automated system of "smart house" and the analysis of possible vulnerabilities that could be exploited.

Findings. We studied possible ways to break the system, both hardware and software, and given the nature of the possible methods of solving the problem.

Originality. The article describes the research and innovative approaches to solve the problem of vulnerability of the automated system "smart house".

Practical value. Since such systems are equipped not only at home, but also government agencies, as well as strategic targets, the solution to this problem is very relevant and meaningful

Keywords: *smart home system, safety, analysis, software, anti-virus tools.*