УДК 681.3

АНАЛІЗ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМ «РОЗУМНИЙ ДІМ»

Б. С. Дрегало[1, a], В. М. Степаненко[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

В даній роботі проаналізовані основні загрози інформаційної безпеки «Розумний дім». Також проведена оцінка виділених загроз. Вироблені рекомендації , що до їх вирішення. .

Ключові слова: інформаційна безпека , «Розумний дім»

Вступ

В наш час все більше набуває популярності технологія «Розумний дім». Дана технологія визначається в вікіпедії , як система домашніх пристроїв, здатних виконувати дії і вирішувати певні повсякденні завдання без участі людини. Функціонально пов'язуються між собою усі електроприлади будівлі, якими можна керувати централізовано – з пульта-дисплею. Прилади можуть бути під'єднані до комп'ютерної мережі, що дозволяє керувати ними за допомогою ПК та надає віддалений доступ до них через Інтернет. Завдяки інтеграції інформаційних технологій у домашні умови, усі системи та прилади узгоджують виконання функцій між собою, порівнюючи задані програми та зовнішні показники [1].

В наш час система «Розумний будинок» вважається однією з найперспективніших технологій з постійним розвитком. У США дана технологія вже давно широко застосовується в різних сферах автоматизації житлових будівель. У Європі, в тому числі і в Україні, популяризація та розвиток технології «Розумний будинок» тільки набирає обертів. Найбільш популярними об'єктами для впровадження даної технології є комерційна нерухомість (торговельні центри, офісні будівлі, банки, готелі), державні будівлі (вокзали, аеропорти, спортивні та культурні установи), а також об'єкти домашньої автоматизації [2].

Однак поряд з очевидними перевагами може виникнути цілий ряд проблем, пов'язаних із забезпеченням інформаційної безпеки організацій та осіб, що використовують дану технологію.

Мета

Метою статті є виділення основних загроз і оцінка ризиків інформаційної безпеки, що пов'язана з експлуатацією систем побудованих з використанням даної технології.

[a] mtjcm125@gmail.com

Основні ризики інформаційної безпеки систем «Розумний будинок»

Розглянемо ризики інформаційної безпеки систем, побудованих за технологією «Розумний будинок». Вважаємо, що базовими загрозами інформаційній безпеці є порушення конфіденційності, цілісності та доступності інформації (КЦД). Слід зауважити , що поняття інформаційна безпека в даній роботі буде розглядатися на різних рівнях захисту , тобто будуть розглянуті системи технічного захисту , кіберзахисту та організаційно-правовий рівень.

Під поняттям конфіденційності потрібно розуміти не можливість витоку конфіденційної інформації організації або осіб через системи , що використовують технологію «Розумний дім».

Під цілісністю інформації ми розуміємо такий стан системи, при якому авторизовані користувачі (і сама система) отримують достовірну інформацію про стан підсистем «Розумного будинку».

Під доступністю інформації ми розуміємо такий стан системи, при якому авторизовані користувачі (і сама система), використовуючи елементи «Розумного будинку», можуть реалізовувати дозволені в системі дії. Порушення доступності інформації може призвести до неможливості системи реагувати на різні ситуації, в тому числі і аварійні.

Проведемо оцінку ризиків інформаційної безпеки системи, побудованої за технологією «Розумний будинок». Як приклад візьмемо приміщення офісу, в якому циркулює конфіденційна інформація, існують вимоги щодо забезпечення доступності і цілісності інформації, а також вимоги щодо нормальної життєдіяльності співробітників. Все офісне обладнання підключено через єдину мережу живлення.

Слід зазначити , що точна оцінка ризиків інформаційної безпеки повинна здійснюватися індивідуально для кожної системи з урахуванням конкретних умов до яких можуть відноситися ступінь важливості інформації, що циркулює в системі , розташування самої системи і тд. В даній роботі буде розгляну-

Табл. 1. Загрози інформаційної безпеки «Розумного будинку»

№	Загроза	причини виникнення	можливі наслідки
1	Хакерська атака	Підключення мережі «Розумного будинку» до Інтернет. Відсутність (неефективність) механізмів захисту мережі	Порушення роботи системи, або вихід з ладу її компонентів, а отже і всієї системи. Порушення конфіденційності, цілісності та доступності інформації(КЦДІ)
2	Вплив вірусних і троянських програмна роботу системи	Відсутність (неефективність) антивірусних програм , недостатній контроль трафіку	Порушення роботи системи. Порушення КЦДІ
3	Помилка користувача	Відсутність (неефективність) захисту від неправильних дій користувача	Можливі збої в роботі системи , порушення КЦДІ
4	Наявність порушників в складі обслуговуючогоперсоналу	Відсутність (неефективність) організаційних правил , що до підбору та контролю персоналу	Порушення КЦДІ. Можливі збої в роботі системи , складність збоїв залежить від ступеня доступу до системи
5	Перебої в мережіелектроживлення	Відсутність системи автономного електроживлення	Повних вихід системи з ладу
6	Витік інформації через побічні електромагнітні випромінювання і наведення (ПЕМВН)	Вихід провідників, в яких можуть бути наведення випромінювань , за межі контрольованої зони	Порушення КЦДІ
7	Перехоплення інформації	Доступ зловмисника до провідних каналів або до зони стійкого перехоплення радіосигналів мережі. Недостатній контроль трафіку	Порушення КЦДІ.
8	Несанкціонований доступ до мережі	неефективність механізмів аутентифікації і ідентифікації	Порушення КЦДІ.

та лише приблизна оцінка ризиків для розуміння певних аспектів , що до необхідності використання механізмів забезпечення інформаційної безпеки таких систем.

Виділимо найбільш ймовірні загрози, через які може відбутися порушення інформаційної безпеки «Розумного будинку». В таблицю 1 були внесені данні , що до ймовірної вразливості , причині її виникнення та можливих наслідків її реалізації порушником.

Аналіз ризиків системи

Аналіз ризиків буде проводатися за такими параметрами:

Вплив порушення КЦДІ на систему (тобто , як може вплинути вихід тої чи іншої функції на загальну роботу системи) :

Високий рівень впливу на систему – порушення конфіденційність, цілісність і доступність елементів системи може заподіяти організації (власникам) значний або катастрофічний збиток.

Середній рівень впливу на систему – порушення конфіденційність, цілісність і доступність елементів системи може заподіяти організації (власникам) середній збиток. Порушення нормальної роботи системи.

Низький рівень впливу на систему – порушення конфіденційність, цілісність і доступність елементів системи не може заподіяти організації (власникам) значний збиток.

Ймовірності реалізації загрози на вразливі елементи системи(оцінка через кількісну можливість для реалізації за певний проміжок часу):

Висока. Кількість реалізації загрози один і більше раз впродовж одного року.

Середня. Загроза може виникнути в впродовж двох-трьох років.

Низька. Виникнення загрози в межах трьох років малоймовірно.

Ефективність реалізації загрози(збитки , що принесе за собою реалізація тої чи іншої загрози):

Висока – значний збиток для активу.

Середня – середній або обмежений збиток.

Низька – незначний збиток або відсутність такого.

В таблицю 2 були внесені данні , що були отримані при аналізі , був знайдений загальний рівень ризику в залежності від характеристики наведених вище параметрів аналізу.

Висновки

В результаті оцінки ризиків , найнебезпечнішими виявилися ті загрози в яких зловмисник може брати під контроль всю систему. Тому вкрай необхідним є проведення заходів щодо захисту телекомунікаційної мережі, розмежування прав доступу користувачів, також правильна робота з персоналом. Слід звернути увагу на таку проблему , як втрата електроживлення , що є вагомою загрозою для систем «Розумний дім». Тому проектування подібних систем є неможливим без детальної оцінки ризиків для конкретних умов

Табл. 2. Рівень ризику для виділених загроз «Розумного будинку»

№	Загроза	Вплив порушення КЦДІ	Ймовірності реалізації	Ефективність реалізації	Загальний ризик
1	Хакерська атака	Високий вплив	Висока	Висока	Високий
2	Вплив вірусних і троянських програмна роботу системи	Високий вплив	Висока	Висока	Високий
3	Помилка користувача	Низький вплив	Висока	Низька	Середній
4	Наявність порушників в складі обслуговуючого персоналу	Середній вплив	Середн	Середня	Середній
5	Перебої в мережі-електроживлення	Високий вплив	Низька (якщо є автономне джерело електроживлення) Висока (якщо автономного електроживлення немає)	Висока	Високий/ Середній
6	Витік інформації через побічні електромагнітні випромінювання і наведення (ПЕМВН)	Середній вплив	Середня	Середня	Середній
7	Перехоплення інформації	Середній вплив	Середня	Середня	Середній
8	Несанкціонований доступ до мережі	Середній вплив	Висока	Середня	Середній

використання систем на технології «Розумний дім» з аналізом всіх потенційних загроз і вразливостей.

Перелік використаних джерел

1. «Розумний дім» [онлайн ресурс] – Режим доступа: \www/ URL: `https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D0%B7%D1%83%D0%BC%D0%BD%D0%B8%D0%B9_%D0%B4%D1%96%D0%BC`
2. «Розумний дім» [онлайн ресурс] – Режим доступа: \www/ URL: `http://umnydom.kiev.ua/index.php?nma=catalog&fla=stat&cat_id=3&page=1&nums=24/` – 05.03.2011 г.
3. Кузьміч А. Невтомний працівник. Розумні домашні системи [Текст]/ А. Кузьміч// Журн. S.M.A.R.T. — 2009. – № 2.- С. 10-13.