УДК 004.004
DOI: 10.31673/2412-9070.2021.015558

Я. О. ГАЛАЙ, студент;
А. П. БОНДАРЧУК, доктор техн. наук, професор;
О. М. ТКАЛЕНКО, канд. техн. наук, доцент;
О. В. ПОЛОНЕВИЧ, канд. техн. наук, доцент;
О. В. ЗІНЧЕНКО, канд. техн. наук, доцент,
Державний університет телекомунікацій, Київ

РОЗРОБЛЕННЯ СИСТЕМИ ОЦІНЮВАННЯ БЕЗПЕКИ РОЗУМНИХ БУДИНКІВ НА ОСНОВІ IoT

Запропоновано розроблення системи оцінювання безпеки розумних будинків, які використовують технології Internet of Things.

Інтернет речей (IoT) — це парадигма, що зароджується, зосереджена на взаємозв'язку речей або пристроїв між собою та користувачами. З часом в Інтернеті речей більшість наявних зв'язків «людина взаємодіє з речами» набувають розуміння зв'язку «речі взаємодіють із речами». Очікується, що ця технологія стане важливою віхою в розвитку розумних будинків, аби забезпечити зручністю та ефективністю наше життя та наші будинки. Проте введення технології IoT у наші будинки матиме важливе значення для безпеки цих технологій. Підімкнення всіх розумних об'єктів усередині будинку до мережі Інтернет та між собою може призвести до нових проблем безпеки та конфіденційності, наприклад приватності, автентичності та цілісності даних, що сприймаються та обмінюються об'єктами.

Ці технології дуже вразливі до різних атак небезпеки, які розумний дім на базі IoT ставлять під загрозу для проживання, тому для оцінювання ситуації розумних будинків потрібно визначити ризики безпеки. Щоб будь-яка технологія мала успіх і досягла широкого використання, вона повинна здобути довіру користувачів, забезпечивши достатню безпеку та конфіденційність.

Оскільки будинки дедалі більше комп'ютеризуються та наповнюються пристроями, потенційні атаки комп'ютерної безпеки та їх вплив на мешканців потребують дослідження.

У статті запропоновано методологію, сфокусовану переважно на інформаційних активах, і яка розглядає контейнери (технічні, фізичні та людські) та проводить оцінювання ризику безпеки з метою висвітлення різних недоліків безпеки в розумному домі на базі Інтернету речей, їх наслідків та пропонує заходи щодо виявлених проблем, які задовольняють більшість вимог безпеки. Надано рекомендації для користувачів.

Ключові слова: Internet of Things; автоматизація будинків; розумний будинок; оцінювання ризику безпеки; рекомендації щодо безпеки; загрози безпеці; контрзаходи безпеки.

ВСТУП

Актуальність теми зумовлено потребою розроблення системи оцінювання, яку можна використовувати як до початку імплементації проекту власного розумного будинку, тим самим підвищуючи ознайомленість із можливими небезпеками та як їм протидіяти на етапі розроблення архітектури, так і для вже готових проектів, що дасть можливість власникам розумних будинків оцінити ризики безпеки своїх домівок та вжити відповідних заходів для їх усунення.

Ризик безпеки в розумному будинку — це можливість заподіяння шкоди або втрат, зокрема небажані дії людей чи природи з негативними наслідками. Ці ризики потрібно вирішувати впровадженням засобів контролю, щоб протистояти основній загрозі та мінімізувати вплив.

Безпека належить до виявлення зловмисної поведінки, як, наприклад, грабіжники, несанкціонований доступ до розумного домашнього середовища. Важливим є захист від зловмисників, які намагаються керувати системою. Для різних типів інтелектуальних приладів існують серйозні виклики безпеці, які потрібно вирішити, аби реалізувати різні види їх справжніх переваг.

Новизна дослідження — розроблення практичних правил оцінювання безпеки розумних будинків, що використовують прилади на основі Internet of Things.

Практична значимість дослідження полягає в здобутих результатах, а отриманий перелік та рекомендації стануть корисним внеском, який може бути використаний як основа для специфікації вимог безпеки розумних будинків.

ОСНОВНА ЧАСТИНА

Після огляду літератури, посилаючись на роботу інших, було визначено низку питань, на які потрібно знайти відповіді під час розроблення системи безпеки:

1. Які загрози безпеці виникають у розумних будинках на базі Інтернету речей?
2. Які наслідки та вплив цих загроз?
3. Чи взагалі існують відповідні заходи щодо протидії цим загрозам?
4. Що рекомендувати користувачам?

Для того щоб мати можливість відповісти на зазначені питання дослідження, потрібно вибрати відповідну методологію дослідження. Методологію, прийняту або запропоновану для цього

дослідницького проекту, буде спрямовано на забезпечення надійності результатів, уможливлюючи всебічне оцінювання ризиків, і зосереджено переважно на інформаційних аспектах. Підхід аналізує, як інформація використовується користувачами або системами, а також у ньому приділено особливу увагу місцю, де живе інформація, і як на неї впливають ризики. Інші критично важливі аспекти можна визначити та оцінити, розкривши зв'язок між ними та інформаційним аспектом.

Оцінювання ризику безпеки

Метою оцінювання ризику є розуміння наявної системи та середовища, виявлення ризиків та їх впливу через аналіз зібраної інформації. Метою оцінювання ризику для безпеки є максимізація захисту конфіденційності, цілісності та доступності завдяки наданню рекомендацій, не впливаючи на функціональність та зручність використання.

Оцінювання ризику є найважливішим аспектом будь-якого дослідження безпеки. Він може бути використаний як базовий для унаочнення, скільки змін потрібно для того, щоб відповідати вимогам безпеки. Це допомагає кінцевим користувачам дійти правильного вирішення щодо своїх розумних будинків, а нам дає змогу надавати рекомендації щодо вдосконалення. Адже без оцінювання ризиків упроваджені вирішення безпеки ризикують не відповідати бажаним цілям безпеки системи розумного будинку.

Далі буде виявлено критично важливі інформаційні ресурси для розумного будинку, його вразливі місця і можливі загрози, а також буде запропоновано план зменшення цих ризиків.

Перш ніж розпочати застосування процесів методології оцінювання ризику безпеки покроково, нам потрібно визначити саме оцінювання ризику безпеки, а також усі терміни, якими ми послуговуватимося для легшого сприйняття оцінювання ризику безпеки.

Існує багато визначень, наданих терміну оцінювання ризику безпеки. Відповідно до Посібника з управління ризиками NIST оцінювання ризиків безпеки можна визначити як процес виявлення загроз, імовірності виникнення, наслідків, а потім механізми захисту для пом'якшення наслідків.

Ось деякі визначення цих термінів, які будуть використовуватись у межах процесу оцінювання ризику безпеки.

• *Аспект* — ціннісний ресурс. Це може бути процес, технологія, фізичний об'єкт або людина.

• *Інформаційний актив.* Цінна інформація для організації, яка зберігається у фізичних носіях або передається та обробляється в електронному вигляді.

• *Контейнер інформаційного активу.* Контейнером інформаційного активу є місце, де живе інформація. Контейнери можуть бути технічними (програмне забезпечення, апаратне забезпечення, сервери та мережі), фізичними (на паперах, компакт-дисках, DVD-дисках) або людьми (хто знає про інформацію).

• *Критично важливий інформаційний актив.* Найважливіший актив, який завдає величезної шкоди організації, якщо її вимоги до безпеки порушуються.

• *Загроза.* Потенціал події, яка може завдати шкоди активу або поставити його під загрозу. Він генерується, коли актор загрози використовує вразливість.

• *Вплив.* Відчутний або нематеріальний вплив загрози, що здійснюється на актив.

• *Ризик.* Поєднання загрози та впливу. Ризик — це можливість заподіяння шкоди чи збитків і складається з події, наслідку та невизначеності.

• *Пом'якшення наслідків.* Дія зменшення серйозності ризиків або зменшення ризику організацій за допомогою різних заходів.

Кожен захищений інформаційний аспект має конфіденційність, цілісність та доступність як вимоги безпеки для захисту та продовження. Ці вимоги живуть з інформаційним активом скрізь, поки він живе корисно.

Крім того, вимоги безпеки є основним елементом розроблення та реалізації планів щодо обмеження ризиків. Отже, необхідно враховувати вплив ризиків на ці вимоги безпеки та на план пом'якшення наслідків. Вимоги безпеки або цілі безпеки — це вимоги, що характеризують спосіб захисту інформаційного активу. Тому надзвичайно важливо зберігати конфіденційність, цілісність та доступність інформаційної безпеки.

Ця методологія добре узгоджується з відповіддю на дослідницькі запитання для вирішення проблем дослідження, які можна згрупувати за вісьмома кроками та за чотирма основними фазами, як показано далі.

Крок 1. Встановити критерії вимірювання ризику.

Крок 2. Розробити профіль аспектів інформації.

Крок 3. Визначити контейнери інформаційного майна.

Крок 4. Визначити питання, що викликають занепокоєння.

Крок 5. Визначити сценарії загрози.

Крок 6. Визначити ризики.

Крок 7. Проаналізувати ризики.

Крок 8. Вибрати підхід до пом'якшення наслідків.

Фаза 1. ***Установлення драйверів***. На цьому етапі (крок 1) створюється основа для оцінювання ризику інформаційних активів, розробляючи набір критеріїв оцінювання ризику для розумного будинку.

Ці критерії дають можливість виміряти ступінь впливу зацікавлених сторін розумного будинку в разі виникнення ризику для інформаційного аспекту. Окрім визнання масштабу впливу нам потрібно визначити найбільш значну сферу впливу.

Ці критерії відбивають цілу низку сфер впливу, важливих для зацікавлених сторін розумного будинку. Наприклад, сфери впливу можуть містити в собі охорону здоров'я та безпеку користувачів, фінанси, репутацію, закони та правила тощо. Отже, створюємо ці критерії в кількох сферах впливу, а потім ставимо їх пріоритетами від найважливіших до найменших. Найважливіша категорія дістає найвищий бал (5), а найменш важлива — найнижчий (1).

Фаза 2. ***Профілювання аспектів***. На цьому етапі (кроки 2 і 3) спочатку визначаються критично важливі інформаційні ресурси, а потім складається їх профіль. У процесі профілювання встановлюються чіткі межі для активу, окреслюються його вимоги до безпеки, а потім визначаються всі місця, де актив зберігається, транспортується або обробляється, або де ці аспекти використовуються власниками розумних будинків або автоматизаційною системою розумного будинку, як здійснюється доступ до аспектів та хто відповідає за ці аспекти. Документуються логічні, технічні, фізичні та людські аспекти. Отже, можна визначити точки, в яких вимоги безпеки (конфіденційність, цілісність та доступність) інформаційного аспекту порушуються.

Фаза 3. ***Визначення загроз***. У цій фазі (кроки 4 і 5) увагу зосереджено на виявленні загроз щодо ідентифікованих аспектів у контексті місць, де інформаційний аспект зберігається, транспортується або обробляється. Сфери, що викликають занепокоєння (вразливості), охоплюються та розширюються на сценарії загрози, що додатково деталізують властивості загрози. Визначаються конкретні загрози, які можуть негативно вплинути на безпеку об'єкта.

Фаза 4. ***Визначення та пом'якшення ризиків***. На заключному етапі (кроки 6, 7 і 8) встановлюються ризики для інформаційних активів, акцентуючи увагу на те, як саме сценарії загрози можуть вплинути на розумний дім (наслідки), та їх аналіз. Нарешті, після цього кроку визначається стратегія зменшення наслідків для кожного з виявлених ризиків.

Загроза + Вплив = Ризик. Аналізуємо ризики та присвоюємо якісне значення для опису ступеня впливу на зацікавлені сторони розумного будинку, коли реалізується сценарій загрози та наслідки впливу (оцінювання ризиків). Значення впливу визначається критеріями оцінювання ризику. Оціночна інформація використовуватиметься для визначення пріоритетних заходів щодо пом'якшення наслідків.

Далі починаємо сортувати виявлені ризики за їх оцінками. Класифікуємо ризики та призначаємо підхід до пом'якшення для кожного з них. Нарешті, розробляємо стратегію зменшення наслідків для всіх профілів ризику, які було вирішено зменшити.

Мотивація вибору методології

Оцінюючи ризик безпеки, важливо знати, що саме захищати і чому.

Очевидно, що захист інформаційних активів є необхідною складовою захисту безпеки розумного будинку, оскільки він визначає майбутнє та успіх системи розумного будинку. Ось чому в цій статті головну увагу приділено безпеці інформаційних активів та тому, де ця інформація живе, здійснюючи оцінювання ризику безпеки в розумному будинку. Якщо ми зосередимося на інформаційних активах в оцінюванні, то всі інші важливі активи можуть бути легко оцінені й оброблені як місця розташування інформаційних аспектів, де вони проживають. Це є точною методологією для цієї мети, оскільки вона забезпечує найкращу дорожню карту для досягнення цілей, а саме відповіді на дослідницькі питання.

Розроблена система оцінювання найкраще узгоджується з відповідями на проблеми дослідження порівняно з іншими методологіями оцінювання ризику безпеки, які було розглянуто. Вона складається з восьми етапів, організованих у чотири фази, і ці кроки легко можна скласти для вирішення дослідницьких проблем. За допомогою робочих аркушів, передбачених методологією, ми можемо охопити результати кожного кроку в оцінюванні ризику та використати їх для введення в наступний крок, який слідує. Таким чином, це дає змогу нам постійно зосереджуватись на аспекті поетапно під час процесу оцінювання ризику та легше досліджувати проблемні ситуації.

ВИСНОВКИ

Було виконано комплексне оцінювання ризиків безпеки за допомогою розробленої системи оцінювання безпеки та визначено 10 важливих інформаційних критеріїв для проведення оцінювання. Процес оцінювання ризиків призвів до виявлення майже 15 ризиків для безпеки як усередині, так і за межами розумного будинку.

Результатами роботи є відповідні контрзаходи для зменшення ризиків до прийнятного рівня, оскільки 100% безпеки ніколи не можна досягти. У важко зв'язаному та складному середовищі, такому як розумний дім на базі IoT, зловмисник, який компрометує систему домашньої автоматизації, може завдати широкий спектр шкоди. Оцінювання ризику встановлено для виявлення найсерйозніших потенційних небезпек. Одне з основних

джерел ризику пов'язане з пристроями та давачами. Ризики для обладнання стосуються крадіжок та дефектів, маніпуляцій та саботажу різних пристроїв, що використовуються в автоматизованих системах розумного дому, і також потребують пильної уваги.

У рамках мережного спілкування основними ризиками є невідповідна автентифікація та відсутність захищеного каналу зв'язку та шифрування. Найбільш серйозним ризиком є людський фактор, оскільки люди становлять найбільший ризик у системах розумної автоматизації дому, оскільки власниками розумних будинків можуть бути люди різного віку, деякі з них, особливо ті, хто має обмежені технічні знання, є більш уразливими до атак соціальної інженерії, неправильного використання та неправильної конфігурації системи. Таким чином, мети дослідження було досягнуто і надано відповіді на питання дослідження.

Список використаної літератури

*1. **Steinberg J.** These Devices May Be Spying On You (Even In Your Own Home). 2014 [Електронний ресурс]. URL:*

http://www.forbes.com/sites/josephsteinberg/2014/01/27/these-devices-may-bespying-on-you-even-in-your-own-home/.

*2. **Evans D.** The internet of things. How the Next Evolution of the Internet is Changing Everything, Whitepaper, Cisco Internet Business Solutions Group (IBSG). 2011 [Електронний ресурс]. URL:*

http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

*3. **Montano C., Lundmark M., Mähr W.** Control vs convenience: critical factors of smart homes // In 2nd Scandinavian Student Interaction Design Research Conference. 2006.*

*4. **Madakam S., Ramaswamy R., Tripathi S.** Internet of Things (IoT): A Literature Review // Journal of Computer and Communications. 2015. Vol. 3(05). 164 p.*

*5. **Security** in networked building automation systems. na. / W. Granzer, W. Kastner, G. Neugschwandtner, F. Praus. 2006.*

*6. **Al-Qutayri M. A., Jeedella J. S.** Integrated Wireless Technologies for Smart Homes Applications. INTECH Open Access Publisher, 2010.*

*7. **De Silva L. C., Morikawa C., Petra I. M.** State of the art of smart homes // Engineering Applications of Artificial Intelligence. 2012. Vol. 25(7). P. 1313–1321.*

Я. О. Галай, А. П. Бондарчук, О. Н. Ткаленко, О. В. Полоневич, О. В. Зинченко

РАЗРАБОТКА СИСТЕМЫ ОЦЕНКИ БЕЗОПАСНОСТИ УМНОГО ДОМА НА ОСНОВЕ IoT

Предложена разработка системы оценки безопасности умных домов, которые используют технологии Internet of Things.

Интернет вещей (IoT) — это зарождающаяся парадигма, которая сосредоточена на взаимосвязи вещей и устройств между собой и пользователями. Со временем в Интернете вещей большинство имеющихся связей «человек взаимодействует с вещами» приобретают понимание связи «вещи взаимодействуют с вещами». Ожидается, что эта технология станет важной вехой в развитии умных домов, чтобы обеспечить удобство и эффективность нашей жизни и нашего дома. Однако введение технологии IoT в наши дома будет иметь важное значение для безопасности этих технологий. Подключение всех разумных объектов внутри дома к сети Интернет и между собой может привести к новым проблемам безопасности и конфиденциальности, например приватности, подлинности и целостности данных, которые воспринимаются и обмениваются объектами.

Эти технологии очень уязвимы к различным атакам опасности, которые умный дом на базе IoT ставят под угрозу для проживания, поэтому для оценки ситуации умных домов нужно определить риски безопасности. Чтобы любая технология имела успех и достигла широкого использования, она должна получить доверие пользователей, обеспечив достаточную безопасность и конфиденциальность. Поскольку дома все больше компьютеризируются и наполняются устройствами, потенциальные атаки компьютерной безопасности и их влияние на жителей требуют исследования.

В статье предложена методология, сфокусированная преимущественно на информационных активах, и которая рассматривает контейнеры (технические, физические и человеческие) и проводит оценку риска безопасности с целью освещения различных недостатков безопасности в разумном доме на базе Интернета вещей, их последствий и предлагает меры по выявленным проблемам, удовлетворяющим большинство требований безопасности. Даны рекомендации для пользователей.

Ключевые слова: Internet of Things; автоматизация зданий; умный дом; оценки риска безопасности; техника безопасности; угрозы безопасности; контрмеры безопасности.

Y. O. Halai, A. P. Bondarchuk, O. M. Tkalenko, O. V. Polonevych, O. V. Zinchenko

DEVELOPMENT OF A SYSTEM FOR THE SECURITY ASSESSMENT FOR SMART HOMES BASED ON THE IoT

This article is about developing a security assessment system for smart homes that use Internet of Things technology.

The Internet of Things (IoT) is a nascent paradigm focused on the relationship of things or devices to each other and users. Over time, most connections on the Internet of Things go from «people interact with things» to «things interact with things». This technology is expected to be an important milestone in the development of smart homes to bring convenience and efficiency to our lives and our homes. But the introduction of this IoT technology in our homes will be important for the safety of these technologies. Connecting all

smart objects inside the house to the Internet and to each other leads to new security and privacy issues, such as the confidentiality, authenticity, and integrity of the data that is perceived and exchanged.

These technologies are very vulnerable to various security attacks that make a smart home based on IoT unsafe to live in, so security risks need to be assessed to assess the situation of smart homes. For any technology to be successful and widely used, it must gain the trust of users, ensuring sufficient security and confidentiality. As in all sectors, maintaining security will be the most important challenge to overcome. As homes become more computerized and filled with devices, potential computer security attacks and their impact on residents need to be investigated.

This paper uses a methodology that focuses mainly on information assets and examines containers (technical, physical and human) and conducts security risk assessments to highlight various security vulnerabilities in the smart home based on the Internet of Things, the consequences and proposing measures against identified problems. that meet most safety requirements. Finally, it offers recommendations for users.

Keywords: Internet of Things; house automation; smart house; security risk assessment; safety recommendations; security threats; security conterarguments.

УДК 621.39:649.8 **DOI:** 10.31673/2412-9070.2021.015961

А. Ю. НІКІТЧЕНКО, студент;
Н. Д. ЯКОВЕНКО, канд. фіз.-мат. наук;
І. М. СРІБНА, канд. техн. наук, доцент;
Н. Ю. КОНДРАТЕНКО, канд. пед. наук,
Державний університет телекомунікацій, Київ

ВПЛИВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ЖИТТЯ ЛЮДЕЙ З ОСОБЛИВИМИ ПОТРЕБАМИ

Новітні технології відкривають широкі можливості для застосування людьми з особливими потребами. Зокрема, цифрові технології набагато більш значущі для людей з обмеженими можливостями, ніж для інших, адже такі технології не лише допомагають комфортніше облаштувати свій побут, а й надають можливість жити максимально повним життям, взаємодіючи з навколишнім світом.

У статті розглянуто питання впливу інформаційних технологій на життя людей з обмеженими можливостями.

Ключові слова: мобільний додаток; люди з обмеженими можливостями; ІТ-технології; допоміжні технології (Assistive Technologies).

Вступ

Останніми роками стає дедалі більш зрозумілим той факт, що життя сучасного суспільства неможливе без інформаційного простору. Люди з обмеженими можливостями як ніхто відчувають потребу в сучасних ІТ-технологіях для спрощення свого життя і вирішення багатьох нагальних проблем. Тому на ринку інформаційних технологій у великій кількості репрезентовано продукти для людей з особливими потребами.

Люди з обмеженими можливостями стикаються з різноманітними складностями в сьогоднішньому інформаційному просторі. Але сучасні технології допомагають їм у розв'язанні багатьох проблем. Такі технології називають допоміжними (Assistive Technologies). Високотехнологічні допоміжні технології відкривають велику кількість можливостей для взаємодії людей з особливими потребами з навколишнім світом незалежно від типу інвалідності. Наприклад, використовуючи комп'ютерні технології для таких завдань, як читання та написання документів, спілкування з іншими людьми та пошук інформації в Інтернеті, студенти та працівники з обмеженими можливостями здатні самостійно працювати з більш широким спектром даних.

Метою статті є дослідження та аналіз впливу інформаційних технологій на життя людей з особливими потребами в сучасному світі.

Основна частина

Нині сучасні інформаційні технології набули надзвичайного поширення в усіх сферах людського життя. Зокрема важливою сферою використання ІТ-технологій є спрощення побуту та діяльності людей з особливими потребами. Розрізняють три основних види продуктів для людей з обмеженими можливостями на ринку ІТ-технологій:

- фізичні продукти;
- програмні продукти;
- комбіновані продукти.

До фізичних продуктів належить різноманітне устаткування та технологічні пристрої. Програмні продукти мають у своєму складі програми, що полегшують людям із особливими потребами роботу з обчислювальною технікою. Комбіновані вирі-