Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Галузь знань 12 – Інформаційні технології

Спеціальність 123 –Комп'ютерна інженерія

на тему «Система профілювання вразливостей при керуванні розумним будинком»

КвРКІ. 016009.17.01.01 ПЗ

Виконав: студент 2 курсу, група КІ2м-20-1 _____ Кривак Д.М.
Підпис Ініціали, прізвище

Керівник кандидат техн. наук, доцент _____ Нічепорук А.О.
Науковий ступінь, вчене звання Підпис Ініціали, прізвище

До захисту допускаю:
Зав. кафедри КІІС, д.т.н., проф.
Т.О. Говорущенко
__ _____ 2022 р.

Хмельницький, 2022

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Освітній рівень магістр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма освітньо-наукова програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

"01" 09 2021 р.

ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ)

Криваку Денису Михайловичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Система профілювання вразливостей при керуванні розумним будинком

Керівник проекту (роботи) Нічепорук А.О., к.т.н., доцент

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 06.01.2022 р. № 1

2. Строк подання студентом проекту (роботи) на кафедру 03.05.2022 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

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

Огляд відомих методів, моделей та систем побудови профілів загроз та вразливостей для систем що використовують IOT

Архітектура та функціональні можливості автоматизованих систем керування розумним будинком

Модель побудови профілів загроз при керуванні розумним будинком

Оцінка ризиків безпеки середовища розумного будинку

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Лисенко С.М., професор кафедри КІІС		
Антиплагіат	Нічепорук А.О., доцент кафедри КІІС		

7. Дата видачі завдання «_06_»_____09_____2021р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики ДРМ з керівником	05.09.2021	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	05.10.2021	виконано
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	05.11.2021	виконано
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	05.12.2021	виконано
5	Робота над науковою статтею	05.01.2022	виконано
6	Робота над розділом 3 – розробка методів для вирішення поставленої задачі	15.02.2022	виконано
7	Робота над розділом 4 – проектування та розробка ПЗ для вирішення поставленої задачі, експериментальна частина	05.04.2022	виконано
8	Оформлення пояснювальної записки згідно вимог	15.04.2022	виконано
9	Попередній захист ДРМ	18.04.2022	виконано
10	Захист ДРМ на засіданні ЕК	До 10.05.2022	

Студент _____ Д.М. Кривак
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ А.О. Нічепорук
Підпис Ініціали, прізвище

РЕФЕРАТ

Тема дипломної роботи: Система профілювання вразливостей при керуванні розумним будинком.

Автор роботи: Кривак Денис Михайлович.

Керівник роботи: Нічепорук Андрій Олександрович.

Пояснювальна записка: 90 с., 4 рис., 12 табл., 1 дод., 24 джерел.

Інтернет речей, розумний будинок, автоматизація, профіль активів, оцінка ризиків, безпека системи.

Об'єктом дослідження є процес виявлення та дослідження кіберзагроз та вразливостей.

Предметом дослідження є система профілювання вразливостей при керуванні розумним будинком.

Метою дипломної роботи є підвищення ступеню реагування на кіберзагрози, шляхом профілювання вразливостей при керуванні розумним будинком.

Для розв'язання поставлених задач використовувалися методи аналітичні та математичні методи дослідження, засоби комп'ютерних мереж, теорія графів та множин, методи оцінки ефективності, сучасні програмні засоби проектування та дослідження, персональний комп'ютер.

Наукова новизна отриманих результатів:

– Удосконалено модель побудови профілів загроз при керуванні розумним будинком, яка на відмінну від відомих залучає враховує особливості архітектури розумного будинку та залучає методологію оцінки ризиків OCTAVE, із обрахунком відносної оцінки ризику, що дозволило розробити профілі загроз та вразливостей для підвищення стійкості проектованих систем розумних будинків;

– Набула подальшого розвитку формалізація моделі інформаційної системи, яка на відмінну від відомих розглядає набір сценаріїв ризику, що дозволило провести розрахунок ризиків інформаційної системи.

На основі проведених досліджень запропонована система профілювання вразливостей при керуванні розумним будинком.

Практична значимість отриманих результатів полягає у тому, що запропонована система дозволить розробити профілі загроз та вразливостей для підвищення стійкості проектованих систем розумних будинків.

Дата
30.04.2022

Підпис

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

IoT – Internet of Things

DFD – Data flow diagram

SDL – Security Development Lifecycle

DoS – Denial of Service

PnG – Person non Grata

CRUD – Create, Read, Update, Delete

MITM – Man In The Middle

WAN – Wide Area Network

LAN – Local Area Network

MCU – Microcontroller Unit

CPU – Central Processing Unit

GPU – Graphics Processing Unit

SoC – System on a chip

WSN – Wireless Sensor Network

ВСТУП

Зростаюча популярність Інтернету речей (IoT) надає широкі можливості для покращення, планування та автоматизації нашого життя. IoT дозволяє поєднувати в мережу та керувати множиною пристроїв, які забезпечують збір, аналіз та передачу даних. Сфера застосування IoT з кожним роком продовжує розширюватися, охоплюючи нові сфери життя, починаючи від розумних будинків, міст та закінчуючи сферою охорони здоров'я.

Проте разом із очевидними перевагами та зручностями, що несе із собою використання IoT, концепція "інтернет речей" залишає для зловмисників ряд потенційних "вузьких" місць у безпеці таких систем. Персональні дані користувачів, зібрані розумними пристроями, завжди мають цінність для хакерів і викрадачів конфеденційної інформації. Крім того, кібератака на IoT-рішення потенційно здатна завдати шкоди фізичним сервісам та фізичній інфраструктурі. При проектуванні та експлуатації систем Інтернету речей важливим завданням є оцінка цих потенційних "вузьких" місць та розроблення повних та вичерпних стратегій по пом'якшенню та усуненню негативних впливів кібератак. Тому метою даного дослідження є визначення можливих кіберзагроз та оцінка їх впливів на критичні інформаційні об'єкти в системі розумного будинку.

Метою роботи є підвищення ступеню реагування на кіберзагрози, шляхом профілювання вразливостей при керуванні розумним будинком.

Об'єктом дослідження є процес виявлення та дослідження кіберзагроз та вразливостей.

Предметом дослідження є система профілювання вразливостей при керуванні розумним будинком.

Методи дослідження. У роботі було застосовано наступні теорії та засоби:

1. Аналітичні та математичні методи дослідження.
2. Засоби комп'ютерних мереж.
3. Теорія графів та множин.
4. Методи оцінки ефективності.

5. Сучасні програмні засоби проектування та дослідження.

6. Персональний комп’ютер.

Наукова новизна роботи:

1. Удосконалено модель побудови профілів загроз при керуванні розумним будинком, яка на відмінну від відомих залучає враховує особливості архітектури розумного будинку та залучає методологію оцінки ризиків OCTAVE, із обрахунком відносної оцінки ризику, що дозволило розробити профілі загроз та вразливостей для підвищення стійкості проектованих систем розумних будинків.

2. Набула подальшого розвитку формалізація моделі інформаційної системи, яка на відмінну від відомих розглядає набір сценаріїв ризику, що дозволило провести розрахунок ризиків інформаційної системи.

Практична цінність роботи полягає в тому, що запропонована система дозволить розробити профілі загроз та вразливостей для підвищення стійкості проектованих систем розумних будинків.

Важливість роботи і висновки. Робота має важливе значення для розвитку та впровадження технологій домашньої автоматизації.

За результатами роботи зроблені наступні висновки: перерахуйте, що в кожному розділі зроблено

1. Проаналізовано існуючі відомі методи, моделі та системи профілювання загроз та вразливостей для систем що використовують IOT.

2. Досліджено та проаналізовано архітектуру та функціональні можливості автоматизованих систем керування розумним будинком.

3. Розроблено модель побудови профілів загроз при керуванні розумним будинком.

4. На основі моделі проведено оцінку ризиків безпеки середовища розумного будинку.

Публікації. За результатми дослідження опубліковано статтю у фахову виданні Computer Systems and Information Technologies:

Morozova O., Tetskyi A., Nicheporuk A., Kruvak D., Tkachov V. Smart Home System Security Risk Assessment // International Scientific Journal «Computer Systems and Information Technologies». 2021. № 3. Pp. 81-88.

Структура та об’єм дипломної роботи. Дипломна складається з вступу, чотирьох розділів, висновку та додатків, її повний зміст 114 сторінок, основний зміст викладено на 90 сторінках, 1-го додатка на 2 сторінках, містить 4 рисунків, 12 таблиць, включає 53 найменувань вітчизняної та зарубіжної літератури.

1 ОГЛЯД ВІДОМИХ МЕТОДІВ, МОДЕЛЕЙ ТА СИСТЕМ ПОБУДОВИ ПРОФІЛІВ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ ДЛЯ СИСТЕМ ЩО ВИКОРИСТОВУЮТЬ IoT

Майже всі програмні системи сьогодні стикаються з різноманітними загрозами, і кількість загроз зростає зі зміною технологій. Щоб запобігти загрозам використовувати недоліки системи, можна використовувати методи моделювання загроз для інформування про заходи захисту.

Моделювання загроз є про активною стратегією оцінки ризиків. Воно включає виявлення потенційних загроз і розробку тестів або процедур для виявлення та реагування на ці загрози. Це передбачає розуміння того, як загрози можуть впливати на системи, класифікацію загроз та застосування відповідних контрзаходів.

Моделювання загроз може допомогти командам безпеки визначити пріоритети загроз, забезпечуючи ефективний розподіл ресурсів та уваги. Це визначення пріоритетів може застосовуватися під час планування, проектування та впровадження безпеки, щоб гарантувати, що рішення є максимально ефективними.

У звичайному режимі моделювання загроз також може допомогти командам безпеки гарантувати, що захист відповідає загрозам, що розвиваються. Якщо ні, нові загрози можуть залишатися незахищеними, залишаючи системи та дані вразливими.

Моделювання загроз також важливе під час прийняття нового програмного забезпечення або створення програмного забезпечення. Це допомагає командам зрозуміти, наскільки інструменти та програми можуть бути вразливими в порівнянні з тим, які засоби захисту пропонуються.

При прийнятті інструментів моделювання загроз допомагає командам зрозуміти, де не вистачає безпеки. Це дозволяє вам прийняти обґрунтоване рішення про те, чи варто використовувати компонент.

Моделювання загроз також може допомогти командам розробників визначити пріоритетність виправлень існуючого програмного забезпечення відповідно до серйозності та впливу очікуваних загроз.

Виконуючи моделювання загроз, можна використовувати кілька методологій. Правильна модель для ваших потреб залежить від того, які типи загроз ви намагаєтеся моделювати і з якою метою.

Для створення використовуються методи моделювання загроз:

1. Абстракція системи.
2. Профілі потенційних зловмисників, включаючи їхні цілі та методи.
3. Каталог потенційних загроз, які можуть виникнути.

Було розроблено багато методів моделювання загроз. Їх можна комбінувати, щоб створити більш надійне та всеосяжне уявлення про потенційні загрози. Не всі з них є вичерпними; одні абстрактні, а інші орієнтовані на людей. Деякі методи зосереджені саме на ризиках або проблемах конфіденційності.

Моделювання загроз має виконуватися на початку циклу розробки, коли потенційні проблеми можна виявити на ранніх стадіях та усунути, запобігаючи набагато більш дорогим виправленням у майбутньому. Використання моделювання загроз для обдумування вимог безпеки може привести до про активних архітектурних рішень, які допоможуть зменшити загрози з самого початку. Моделювання загроз може бути особливо корисним у сфері кібер-фізичних систем [2-12].

У цій роботі я підсумував 12 доступних методів моделювання загроз.

1.1 STRIDE та пов'язані похідні

Винайдений у 1999 році і прийнятий Microsoft у 2002 році, STRIDE на даний момент є найзрілішим методом моделювання загроз. STRIDE розвивався з часом, щоб включати нові таблиці для конкретних загроз і варіанти STRIDE-per-Element і STRIDE-per-Interaction.

STRIDE оцінює детальний дизайн системи. Він моделює систему на місці. Створюючи діаграми потоків даних (DFD), STRIDE використовується для ідентифікації системних сутностей, подій і меж системи. STRIDE застосовує загальний набір відомих загроз на основі своєї назви, яка є мнемонікою. Категорії загроз STRIDE зображені в таблиці 1.1.

Таблиця 1.1 – Категорії загроз STRIDE

	Загроза	Власність порушено	Визначення загрози
S	Spoofing identify (ідентифікувати підробку)	Аутентифікація	Прикидатися чимось або кимось іншим, ніж ви самі
T	Tampering with data (підробка даних)	Цілісність	Змінення чогось на диску, мережі, пам’яті чи в іншому місці
R	Repudiation (відмова)	Не відмова	Стверджувати, що ви щось не зробили або не несли відповідальності; може бути чесним або фальшивим
I	Information disclosure (розкриття інформації)	Конфіденційність	Надання інформації особам, які не мають до неї доступу
D	Denial of service (відмова в обслуговуванні)	Доступність	Вичерпні ресурси, необхідні для надання послуг
E	Elevation of privilege (підвищення привілею)	Авторизація	Дозволити комусь робити те, на що він не уповноважений

STRIDE успішно застосовується в кібер-фізичних систем. Хоча Microsoft більше не підтримує STRIDE, він реалізується як частина життєвого циклу Microsoft SDL за допомогою засобу моделювання загроз, який все ще доступний. Microsoft також розробила подібний метод під назвою DREAD, який також є мнемонікою (потенціал пошкодження, відтворюваність, придатність до експлуатації, постраждалі користувачі, відкритість) з іншим підходом до оцінки загроз.

1.2 PASTA

Process of Attack Simulation and Threat Analysis (PASTA) — це методологія моделювання загроз, орієнтована на ризики, спільно заснована у 2015 році генеральним директором VerSprite Тоні УседаВелесом та лідером із безпеки Марко М. Морана. Організації в усьому світі, як-от GitLab, використовують PASTA як стандарт моделювання внутрішньої загрози через свій підхід, орієнтований на ризики, тенденції до співпраці, дані про загрози, засновані на доказах, і зосередженість на ймовірності кожної атаки.

PASTA дозволяє співпрацювати між розробником і зацікавленими сторонами бізнесу, щоб по-справжньому зрозуміти ризики, властиві вашому додатку, його ймовірність атаки та вплив на бізнес у разі компромісу. Інші традиційні рамки моделювання загроз можуть бути гіперфокусовані на одному компоненті, наприклад, кодуванні або фактичній атаці.

Наприклад, STRIDE (Spoofing, Tampering, Disclosure, Information Disclosure, Denial of Service і Elevation of Privilege) — це мнемоніка, яка використовувалася і рекомендована багатьма. Його легко реалізувати, оскільки це статичний каркас. Однак, з огляду на постійно розвивається ландшафт загроз, не має сенсу мати статичні загрози в кількох галузях. PASTA має ряд переваг перед іншими традиційними методами моделювання загроз. Етапи моделі загрози PASTA зображенні в таблиці 1.2.

Таблиця 1.2 – Етапи моделі загрози PASTA

Визначте цілі.	1. Визначте бізнес-цілі. 2. Визначте вимоги безпеки та відповідності. 3. Аналіз впливу на бізнес.
Визначте технічну область застосування.	1. Зафіксуйте межі технічного середовища. 2. Інфраструктура захоплення | Застосування | Програмні залежності.
Розкладання програми.	1. Визначте випадки використання | Визначте додаток. Точки входу та рівні довіри. 2. Визначити дійових осіб | Активи | Послуги | Ролі | Джерела даних. 3. Діаграмування потоків даних (DFD) | Межі довіри.
Аналіз загроз.	1. Аналіз ймовірнісних сценаріїв атак. 2. Регресійний аналіз подій безпеки. 3. Кореляція та аналітика розвідки загроз.
Аналіз вразливостей і слабких сторін.	1. Запити про наявні звіти про вразливості та відстеження проблем. 2. Картування загроз існуючій уразливості за допомогою дерев загроз. 3. Аналіз недоліків проектування з використанням випадків використання та зловживання. 4. Оцінки (CVSS/CWSS) | Перерахування (CWE/CVE).

Кінець таблиці 1.2 – Етапи моделі загрози PASTA

Моделювання атаки.	1. Аналіз поверхні атаки. 2. Розробка дерева атак | Керівник бібліотеки атаки. 3. Атака на вразливості та аналіз експлойтів за допомогою дерев атак
Аналіз ризику та впливу	1. Кваліфікація та кількісна оцінка впливу на бізнес 2. Ідентифікація контрзаходів та аналіз залишкового ризику 3. Стратегії зменшення ризику ID

Цей метод піднімає процес моделювання загроз на стратегічний рівень, залучаючи ключових осіб, які приймають рішення, і вимагаючи внеску безпеки від операцій, управління, архітектури та розробки. Широко розцінений як структура, орієнтована на ризик, PASTA використовує перспективу, орієнтовану на зловмисників, щоб отримати результати, орієнтовані на активи, у формі перерахування загроз та оцінки.

1.3 LINDDUN

LINDDUN (можливість зв’язування, ідентифікація, невідповідність, виявлення, розкриття інформації, не інформованість, невідповідність) зосереджується на проблемах конфіденційності та може використовуватися для безпеки даних. LINDDUN, що складається з шести кроків (таблиця 1.3), забезпечує систематичний підхід до оцінки конфіденційності.

LINDDUN починається з DFD системи, яка визначає системні потоки даних, сховища даних, процеси та зовнішні об’єкти. Систематично перебираючи всі елементи моделі та аналізуючи їх з точки зору категорій загроз, користувачі LINDDUN визначають застосовність загроз до системи та будують дерева загроз.

Таблиця 1.3 – Кроки LINDDUN

Простір проблем	1. Дайте визначення DFD.
	2. Карта загроз конфіденційності елементів DFD.
	3. Визначте сценарії загроз.
Простір рішення	4. Розставте пріоритети загроз.
	5. Визначте стратегії пом’якшення.
	6. Виберіть відповідних домашніх тварин.

1.4 CVSS

Загальна система оцінки вразливостей (CVSS) фіксує основні характеристики вразливості та створює числову оцінку серйозності. CVSS був розроблений NIST і підтримується Форумом груп реагування на інциденти та безпеки (FIRST) за підтримки та внеску CVSS Special Interest Group.

Ця система призначена для того, щоб допомогти групам безпеки отримати доступ до загроз, виявити вплив та визначити існуючі контрзаходи. Це також допомагає фахівцям з безпеки оцінювати та застосовувати розвідку загроз, розроблену іншими, надійним способом.

CVSS надає користувачам загальну стандартизовану систему оцінки на різних кібер-фізичних платформах. Оцінку CVSS можна обчислити за допомогою калькулятора, доступного в Інтернеті. Оцінка CVSS визначається на основі значень, призначених аналітиком для кожного показника. Показники докладно описані в документації. Метод CVSS часто використовується в поєднанні з іншими методами моделювання загроз.

CVSS враховує притаманні властивості загрози та вплив фактора ризику через час з моменту першого виявлення вразливості. Він також включає заходи, які дозволяють командам безпеки спеціально змінювати оцінки ризику на основі окремих конфігурацій системи.

1.5 Attack Trees

Використання дерев атак для моделювання загроз є одним із найстаріших і найбільш широко застосовуваних методів у кібер-системах, кібер-фізичних системах і суто фізичних системах. Дерева атак спочатку застосовувалися як окремий метод і з тих пір поєднувалися з іншими методами та структурами.

Дерева атак – це діаграми, які зображують атаки на систему у вигляді дерева. Корінь дерева — це мета атаки, а листя — шляхи досягнення цієї мети. Кожна ціль представлена у вигляді окремого дерева. Таким чином, аналіз системних загроз створює набір дерев атак.

У разі складної системи дерева атак можна побудувати для кожного компонента, а не для всієї системи. Адміністратори можуть будувати дерева атак і використовувати їх для прийняття рішень щодо безпеки, для визначення, чи є системи вразливими до атаки, і для оцінки конкретного типу атаки.

Останніми роками цей метод часто використовувався в поєднанні з іншими методами та в рамках таких структур, як STRIDE, CVSS і PASTA.

1.6 Persona non Grata

Підхід Persona non Grata, розроблений в Університеті ДеПола, робить моделювання загроз більш зручним, просить користувачів зосередитися на зловмисниках, їх мотивації та здібностях. Після завершення цього кроку користувачам пропонується обдумати цілі та ймовірні механізми атаки, які зловмисники розгорнуть.

Persona non Grata зосереджується на мотивації та навичках людей-нападників. Він характеризує користувачів як архетипи, які можуть неправильно використовувати систему, і змушує аналітиків розглядати систему з точки зору ненавмисного використання.

Теорія цього підходу полягає в тому, що якщо інженери зможуть зрозуміти, якими можливостями може володіти зловмисник і які типи механізмів вони можуть

використовувати для скомпрометації системи, інженери отримають краще розуміння цілей або слабких місць у своїх власних системах і ступінь які вони можуть бути скомпрометовані.

Деякі критики цього підходу стверджують, що Persona non Grata часто може вивести користувачів на неправильний шлях. Наприклад, для системи, пов’язаної з національною безпекою, користувачі можуть вважати, що система може бути об’єктом складної атаки з боку іншої національної держави. Цей висновок, однак, не враховує той факт, що національна держава може скомпрометувати систему спочатку через набагато простішу точку входу, а потім посилити операції звідти.

З Persona non Grata учасники нашого дослідження повідомили про менше помилкових спрацьовувань, але вони також не змогли отримати вичерпне уявлення про потенційні загрози. Їхнє моделювання загроз, як правило, постійно виробляло лише підмножину типів загроз, які ми визначили як недолік цього підходу.

Хоча команди, які використовували Persona non Grata, не ідентифікували всі загрози, загрози, які вони ідентифікували, відтворювалися послідовно в командах. Це важливо, якщо метою аналізу загроз є виявлення потенційної загрози (в межах цієї підмножини) з [високим?] ступенем довіри. Більше того, якщо розробник моделювання загроз краще обізнаний про типи вразливостей, які є важливими в системі, Persona non Grata є ідеальною, оскільки вона дає користувачеві більший ступінь впевненості в його чи її здатності визначити пріоритетні загрози.

1.7 Security Cards

Картки безпеки – це методологія, заснована на мозковому штурмі та креативному мисленні, а не на підходах до структурованого моделювання загроз. Він розроблений, щоб допомогти командам безпеки враховувати менш поширені або нові атаки.

Цей метод використовує колоду з 42 карт для полегшення діяльності з виявлення загроз: Вплив людини (9 карт), Мотивація супротивника (13 карт), Ресурси противника (11 карт) і Методи противника (9 карт). Різні категорії в

кожному вимірі наведено в таблиці 1.4. Аналітики можуть роздавати карти в настільній грі, моделювати можливі атаки та розглядати, як організація може відреагувати.

Таблиця 1.4 – Розміри картки безпеки

Вплив людини	1. Біосфера. 2. Емоційне благополуччя. 3. Фінансове благополуччя. 4. Персональні дані. 5. Фізичне благополуччя. 6. Відносини. 7. Суспільне благополуччя. 8. Незвичайні впливи.
Мотивація супротивника	1. Доступ або зручність. 2. Цікавість чи нудьга. 3. Бажання або одержимість. 4. Дипломатія чи війна. 5. Злоба чи помста. 6. Гроші. 7. Політика. 8. Захист. 9. Релігії. 10. Самореклама. 11. Світогляд. 12. Незвичайні мотивації.

Кінець таблиці 1.4 – Розміри картки безпеки

Ресурси супротивника	1. Експертиза. 2. Майбутній світ. 3. Безкарності. 4. Внутрішні можливості. 5. Внутрішнє знання. 6. Гроші. 7. Влада і вплив. 8. Час. 9. Інструменти. 10. Незвичайні ресурси.
Методи супротивника	1. Прикриття нападу. 2. Непряма атака. 3. Маніпуляція або примус. 4. Багатофазна атака. 5. Фізична атака. 6. Процесів. 7. Технологічна атака. 8. Незвичайні методи.

Картки безпеки визначають незвичайні та складні атаки. Це не формальний метод, а, скоріше, свого роду техніка мозкового штурму. За допомогою колоди карт аналітики можуть відповісти на запитання про атаку, наприклад:

1. Хто може атакувати?
2. Чому система може бути атакована?
3. Які активи представляють інтерес?
4. Як можна реалізувати ці атаки?

Ця методологія також є хорошим способом для груп безпеки розширити знання про загрози та методи моделювання загроз.

1.8 hTMM

Метод гібридного моделювання загроз (hTMM) був розроблений SEI у 2018 році. Він складається з комбінації SQUARE (метод інженерних вимог до якості безпеки), карток безпеки та дій PnG. Цільові характеристики методу включають відсутність помилкових спрацьовувань, відсутність упущених загроз, постійний результат незалежно від того, хто моделює загрозу, а також економічну ефективність.

Основними етапами методу є:

1. Визначте систему для моделювання загроз.
2. Застосовуйте картки безпеки на основі пропозицій розробника.
3. Видаліть малоймовірні PnG (тобто немає реалістичних векторів атаки).
4. Підсумуйте результати за допомогою підтримки інструментів.
5. Продовжуйте використовувати офіційний метод оцінки ризику.

Тому оптимальним підходом є використання гібридної моделі, що ґрунтується на кращому з кожного з цих методів. Щоб виконати продуктивне та всеосяжне моделювання загроз, включіть такі три аспекти:

1. Структурований підхід.
2. Оптимальна деталізація.
3. Читабельність.

Структурований підхід. Успішний процес має бути схематизованим і прийнятий процедурою. Це дає змогу встановити мету, отримати відповідні деталі та виконати узгоджену процедуру для досягнення поставленої мети. Наприклад, команда розробників програмного забезпечення приймає відповідну модель життєвого циклу розробки програмного забезпечення, таку як Agile або каскад, щоб цілі були чітко зрозумілі та вчасно втілені в бажані програмні продукти. Аналогічно, моделювання загроз має охоплювати структурований підхід, щоб можна було досягти бажаних результатів від вправи.

Оптимальна деталізація. Надання інформації, яку можна легко інтерпретувати та діяти, є критичним фактором для успішного результату процесу.

Споживачами цієї вправи здебільшого є розробники / архітектори / тестувальники програмного забезпечення, які можуть не обов'язково бути експертами з безпеки. Таким чином, надання або надмірної інформації, або мінімальних деталей не тільки вплине на результат вправи, але й на безпеку програмного додатка. Тому публікація оптимальної кількості деталей значною мірою сприятиме успішному результату вправи.

Читабельність. Недостатньо, якщо вправа має структурований підхід і містить лише оптимальні деталі. Найкраще представлення даних гарантує повноту вправи. У розробці програмного забезпечення найкращий спосіб представити складну інформацію або робочий потік у програмі за допомогою DFD. Блок-схема може не підходити для цього сценарію. Подібним чином при моделюванні загроз дані мають бути представлені в доступному для читання форматі, що сприяє загальному спрощенню вправи.

1.9 Quantitative Threat Modeling Method

Цей гібридний метод складається з дерев атаки, методів STRIDE та CVSS, які використовуються в синергії. Він спрямований на вирішення кількох нагальних проблем із моделюванням загроз для кібер-фізичних систем, які мають складну взаємозалежність між своїми компонентами.

Першим кроком методу кількісного моделювання загроз (Quantitative TMM) є створення дерев компонентних атак для п’яти категорій загроз STRIDE. Ця активність показує залежності між категоріями атак і атрибутами низькорівневих компонентів. Після цього застосовується метод CVSS і обчислюються бали для компонентів дерева.

1.10 Trike

Trike був створений як система аудиту безпеки, яка використовує моделювання загроз як техніку. Він розглядає моделювання загроз з точки зору управління ризиками та захисту.

Як і багато інших методів, Trike починається з визначення системи. Аналітик будує модель вимог, перераховуючи й розуміючи акторів системи, активи, намічені дії та правила. На цьому етапі створюється матриця актор-актив-дія, у якій стовпці представляють активи, а рядки — акторів.

Кожна клітинка матриці розділена на чотири частини, по одній для кожної дії CRUD. У цих клітинках аналітик призначає одне з трьох значень: дозволена дія, заборонена дія або дія з правилами. До кожної клітинки прикріплено дерево правил.

Після визначення вимог будується DFD. Кожен елемент зіставляється з вибором акторів і активів. Перебираючи DFD, аналітик визначає загрози, які поділяються на одну з двох категорій: підвищення привілеїв або відмова в обслуговуванні. Кожна виявлена загроза стає кореневим вузлом дерева атаки.

Щоб оцінити ризик атак, які можуть вплинути на активи через CRUD, Trike використовує п’ятибальну шкалу для кожної дії на основі її ймовірності. Актори оцінюються за п’ятибальною шкалою ризиків, які вони, як передбачається, представляти (менше число = вищий ризик) для активу. Крім того, актори оцінюються за тривимірною шкалою (завжди, іноді, ніколи) для кожної дії, яку вони можуть виконати з кожним активом.

1.11 VAST Modeling

Методологія візуального, швидкого та простого моделювання загроз (VAST) була розроблена після огляду недоліків та проблем із впровадженням, притаманних іншим методологіям моделювання загроз. Основний принцип полягає в тому, що для ефективного моделювання загроз має масштабуватися в інфраструктурі та

всьому портфоліо DevOps, безперешкодно інтегруватися в середовище Agile і забезпечувати ефективні, точні та послідовні результати для розробників, команд безпеки та керівників вищого рівня.

Його масштабованість і зручність використання дозволяють використовувати його у великих організаціях по всій інфраструктурі, щоб отримувати ефективні та надійні результати для різних зацікавлених сторін.

Визнаючи відмінності в операціях і занепокоєння між командами розробників та інфраструктури, VAST вимагає створення двох типів моделей: моделей загроз додатків і моделей операційних загроз.

Моделі загроз додатків використовують діаграми потоків процесів, що представляють архітектурну точку зору. Операційні моделі загроз створюються з точки зору зловмисника на основі DFD. Такий підхід дозволяє інтегрувати VAST у розвиток організації та життєвий цикл DevOps.

Ми можемо класифікувати автоматизацію, співпрацю та інтеграцію як три стовпи масштабованого моделювання загроз, пов’язаних із VAST. VAST зосереджується на розробці двох основних моделей загроз; моделі операційної загрози та моделі прикладних загроз.

В результаті консультативної точки зору створюються моделі операційних загроз, щоб більше зосередитися на DFD. Тим часом моделі загроз додатків використовують діаграму потоку процесів, що представляє архітектурну точку зору. Методологія VAST ідеально підходить для підприємств, які шукають ефективні моделі загроз, унікальні для потреб різних зацікавлених сторін.

1.12 OCTAVE

OCTAVE — це гнучка методологія, яка дозволяє невеликій команді, що складається з операційного персоналу та IT, працювати разом для задоволення потреб організації в безпеці.

По суті, це допомагає команді організовано і систематично отримувати знання від співробітників, щоб визначити поточний стан безпеки, ризики для критичних активів і встановити стратегію безпеки.

Метод оцінки оперативно-критичних загроз, активів та вразливості (OCTAVE) — це метод стратегічної оцінки та планування кібербезпеки на основі оцінки ризиків. Він був створений відділом CERT SEI у 2003 році та доопрацьований у 2005 році. OCTAVE зосереджується на оцінці організаційних ризиків і не розглядає технологічні ризики.

Його основними аспектами є операційний ризик, методи безпеки та технології. Існує кілька варіацій OCTAVE, які корисно знати, якщо стандартний OCTAVE не відповідає вашій ситуації.

Існує OCTAVE-S, яка націлена на ситуацію, коли аналіз виконується командою, яка володіє широкими знаннями про організацію, отже передбачає, що немає потреби в семінарах з отримання знань. І є OCTAVE Allegro, який має бути більш впорядкованим і навіть підходить для керування окремими особами без значного участі в організації. []

Зауважте, що незважаючи на те, що хронологічно Allegro прийшов після S, який прийшов після оригінальної OCTAVE, жодне з них не замінює інші. У кожного є свої переваги та ситуації застосування. Насправді, існують ситуації, коли гібридний підхід є найбільш доцільним. OCTAVE має три фази:

1. Створюйте профілі загроз на основі активів. (Це організаційна оцінка.).
2. Визначте вразливість інфраструктури. (Це оцінка інформаційної інфраструктури.).
3. Розробити стратегію та плани безпеки. (Це визначення ризиків для критичних активів організації та прийняття рішень.).

1.13 Порівняння методологій

Таблиця 1.5 – Методології побудови профілів загроз та вразливостей для систем що використовують IOT

Метод моделювання загроз	Характеристики
STRIDE	1. Допоможе визначити відповідні методи пом’якшення. 2. Є найбільш зрілим. 3. Простий у використанні, але займає багато часу.
PASTA	1. Допоможе визначити відповідні методи пом’якшення. 2. Безпосередньо сприяє управлінню ризиками. 3. Заохочує співпрацю між зацікавленими сторонами. 4. Містить вбудовану пріоритетність пом'якшення загроз. 5. Є трудомістким, але має багату документацію.
LINDDUN	1. Допоможе визначити відповідні методи пом’якшення. 2. Містить вбудовану пріоритетність пом'якшення загроз. 3. Може бути трудомістким та забирає багато часу.

Продовження таблиці 1.5 – Методології побудови профілів загроз та вразливостей для систем що використовують IOT

CVSS	1. Містить вбудовану пріоритетність пом'якшення загроз. 2. Має стабільні результати при повторенні. 3. Має автоматизовані компоненти. 4. Має непрозорі розрахунки балів.
Attack Trees	1. Допомагає визначити відповідні методи пом’якшення. 2. Має стабільні результати при повторенні. 3. Простий у використанні, якщо ви вже маєте глибоке розуміння системи.
Persona non Grata	1. Допомагає визначити відповідні методи пом’якшення. 2. Безпосередньо сприяє управлінню ризиками. 3. Має стабільні результати при повторенні. 4. Схильний виявляти лише деякі підмножини загроз.
hTMM	1. Містить вбудовану пріоритетність пом'якшення загроз. 2. Заохочує співпрацю між зацікавленими сторонами. 3. Має стабільні результати при повторенні.
Quantitative TMM	1. Містить вбудовану пріоритетність пом'якшення загроз. 2. Має автоматизовані компоненти. 3. Має стабільні результати при повторенні.

Продовження таблиці 1.5 – Методології побудови профілів загроз та вразливостей для систем що використовують IOT

Trike	1. Допомагає визначити відповідні методи пом’якшення. 2. Безпосередньо сприяє управлінню ризиками. 3. Містить вбудовану пріоритетність пом'якшення загроз. 4. Заохочує співпрацю між зацікавленими сторонами. 5. Має автоматизовані компоненти. Має нечітку, недостатню документацію.
Security Cards	1. Заохочує співпрацю між зацікавленими сторонами. 2. Націлює на неординарні загрози. 3. Призводить до багатьох помилкових спрацьовувань.
VAST Modeling	1. Допомагає визначити відповідні методи пом’якшення. 2. Безпосередньо сприяє управлінню ризиками. 3. Містить вбудовану пріоритетність пом'якшення загроз. 4. Заохочує співпрацю між зацікавленими сторонами. 5. Має стабільні результати при повторенні. 6. Має автоматизовані компоненти. 7. Явно розроблений для масштабування. 8. Має мало загальнодоступної документації.

Кінець таблиці 1.5 – Методології побудови профілів загроз та вразливостей для систем що використовують IOT

Метод моделювання загроз	Характеристики
OCTAVE	1. Допомагає визначити відповідні методи пом’якшення. 2. Безпосередньо сприяє управлінню ризиками. 3. Містить вбудовану пріоритетність пом'якшення загроз. 4. Заохочує співпрацю між зацікавленими сторонами. 5. Має стабільні результати при повторенні. 6. Явно розроблений для масштабування. 7. Займає багато часу і має нечітку документацію.

1.14 Висновки та постановка задачі дослідження

Моделювання загроз може допомогти зробити ваш продукт більш безпечним і надійним. У цьому розділі представлено 12 методів моделювання загроз. Деякі зазвичай використовуються окремо, деякі зазвичай використовуються в поєднанні з іншими, а деякі є прикладами того, як різні методи можна комбінувати.

Щоб вибрати, який метод найкраще підходить для вас, вам потрібно подумати про будь-які конкретні сфери, на які ви хочете орієнтуватися (ризик, безпека, конфіденційність), скільки часу вам доведеться виконувати моделювання загроз, який у вас досвід моделювання загроз, наскільки задіяно зацікавлені сторони, якими хочуть бути, тощо.

Тому постає задача розробки системи профілювання загроз та оцінки ризиків в розумному будинку що дозволить проводити швидкий та доволі точний аналіз

можливих загроз та вразливостей для подальшого реагування та удосконалення безпеки розумного будинку.

Для вирішення поставленої задачі необхідне наступне:

1. Проаналізувати існуючі відомі методи, моделі та системи профілювання загроз та вразливостей для систем що використовують IOT.
2. Дослідити та проаналізувати архітектуру та функціональні можливості автоматизованих систем керування розумним будинком.
3. Розробити модель побудови профілів загроз при керуванні розумним будинком.
4. На основі моделі провести оцінку ризиків безпеки середовища розумного будинку.

2 АРХІТЕКТУРА ТА ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ АВТОМАТИЗОВАНИХ СИСТЕМ КЕРУВАННЯ РОЗУМНИМ БУДИНКОМ

2.1 Архітектура автоматизованих систем керування розумним будинком

Архітектуру системи Інтернету речей, і зокрема розумного будинку, можна представити через три логічні рівні: рівень сприйняття, мережевий рівень та рівень додатків зображені на рисунку 2.1. Розглянемо детальніше кожний рівень системи розумного будинку та проаналізуємо відомі кіберзагрози, що порушують цілісність, доступність та конфіденційність інформації на відповідному рівні [14-22].

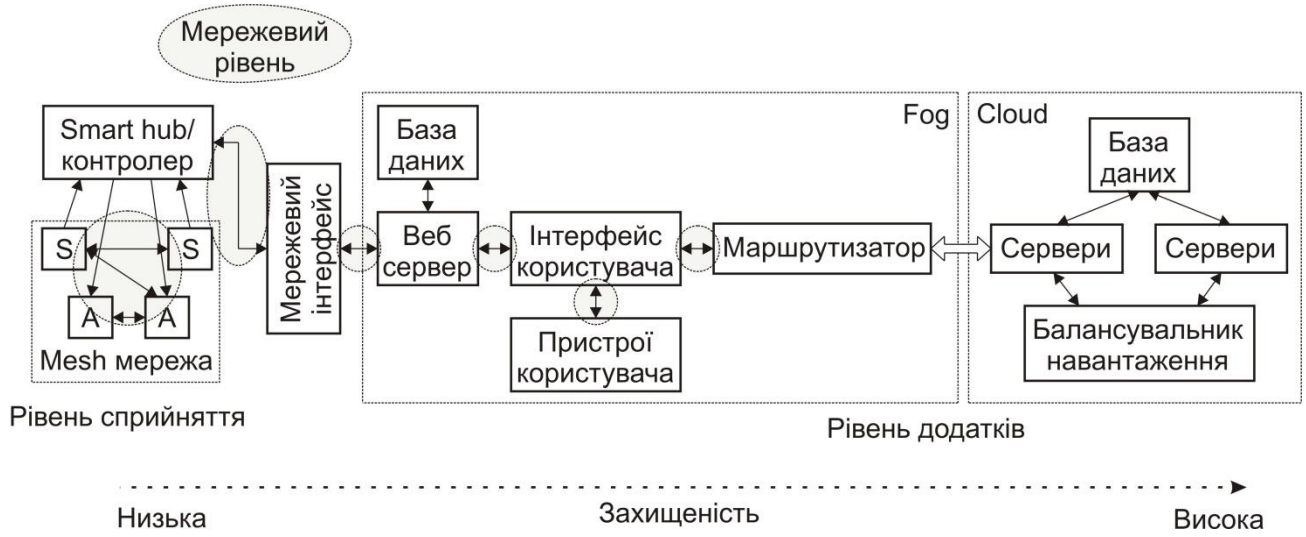


Рисунок 2.1 – Трьохрівнева архітектура систем домашньої автоматизації

2.1.1 Рівень сприйняття

Найбільш наближеним до фізичного середовища рівнем в архітектурі розумного будинку є рівень сприйняття. Головними функціями даного рівня є збір інформації про стан фізичного середовища та реалізація механізмів впливу на нього. Покладені функції реалізуються за допомогою множини датчиків та виконавчих механізмів відповідно. Інформація, яку збирають датчики залежить від природи фізичного середовища та може стосуватись розташування, змін у повітрі

та навколишньому середовищі, руху, вібрації тощо. Виконавчі механізми реалізують принцип перетворення електричної енергії, що передається по провідниках, у інші види енергії. Прикладами виконавчих механізмів можуть бути різного виду двигуни, релейні модулі та автоматизовані крани. Захищеність даного рівня в системі розумного будинку є найнижчою, що «приваблює» зловмисників до проведення атак на пристрої розумного будинку. Найбільш поширеними загрозами безпеки даного рівня сприйняття є:

Підслуховування: підслуховування – це несанкціонована атака порушення конфіденційності інформації в режимі реального часу, при якій зловмисник перехоплює приватні повідомлення, такі як телефонні дзвінки, текстові повідомлення, передачі факсу або відеоконференції. Він намагається вкрасти інформацію, яка передається через мережу. Для доступа до інформації, що надсилається та приймається, використовується незахищений канал передачі даних.

Захоплення вузла: при даній атаці зловмисник отримує повний контроль над ключовим вузлом, таким як вузол шлюзу. Він може передавати всю інформацію, включаючи зв'язок між відправником і одержувачем, ключ, який використовується для забезпечення безпечного зв'язку та інформації, що зберігається в пам'яті.

Фальшивий вузол: це атака, при якій зловмисник додає новий вузол до системи та заповнює мережу підробленими даним. Головною метою цієї атаки є припинення передачі інформації від реальних вузлів мережі. Вузол, доданий зловмисником, споживає енергію реальних вузлів і потенційно контролює його, щоб зруйнувати мережу.

Повторна атака: Вона також відома як атака відтворення. Це напад, під час якого зловмисник підслуховує збереження між відправником і одержувачем і бере автентичну інформацію від відправника. Зловмисник надсилає жертві ту саму автентифіковану інформацію, яка вже була отримана під час його спілкування, демонструючи доказ його особи та справжності. Повідомлення у зашифрованому вигляді, тому одержувач може розглядати його як правильний запит і вживати дії, які бажає зловмисник.

Атаки по часу: це вид пасивної атаки, спрямованої на пристрої з обмеженими обчислювальними ресурсами. В процесі проведення атаки зловмисник виявляє вразливі місця та отримує секрети, що зберігаються в безпеці системи, відстежуючи, скільки часу потрібно системі для відповіді на різні запит або криптографічні алгоритми.

2.1.2 Мережевий рівень

Мережевий рівень виконує транспортну функцію для передачі інформації всередині розумного будинку та є містком між рівнем сприйняття та рівнем додатків. Він передає інформацію, зібрану з фізичних об’єктів, за допомогою датчиків. Носій для передачі може бути бездротовим або дротовим. Він також бере на себе відповідальність за з'єднання розумних речей, мережевих пристроїв та мереж один з одним. Наявність комунікаційної складової робить даний рівень чутливим до атак з боку зловмисників. Він має помітні проблеми безпеки щодо цілісності та автентифікації інформації, яка передається по мережі. Поширеними загрозами безпеки та проблемами для мережевого рівнів є:

Атака відмови в обслуговуванні (DoS): це атака, основною метою якої, є перешкоджання доступу легітимних користувачів до пристроїв або інших мережевих ресурсів. Зазвичай це досягається шляхом заповнення цільових пристроїв або мережевих ресурсів надлишковими запитами з метою унеможливлення або ускладнення використання ними деяких або всіх легітимних користувачів.

Атака "Людина посередині" (MITM) – це атака, при якій зловмисник таємно перехоплює та змінює зв'язок між відправником та одержувачем, які вважають, що вони безпосередньо спілкуються між собою. Оскільки зловмисник контролює процес спілкування, він може читати та змінювати повідомлення відповідно до своїх потреб. Це створює серйозну загрозу безпеці в Інтернеті, оскільки надає зловмиснику можливість захоплювати та обробляти інформацію в режимі реального часу.

Атака на сховище даних: інформація про користувачів зберігається на пристроях зберігання даних або у хмарі. Зловмисник може атакувати як пристрої зберігання даних, так і хмару, і інформація користувача може бути змінена на неправильну інформацію, тим самим порушуючи цілісність та конфіденційність даних.

Експолойт: вид атаки, що реалізується за допомогою фрагменту програмного коду або послідовності команд, що використовують вразливості в програмному забезпеченні. Метою атаки може бути як захоплення контролю над системою, так і порушення її функціонування.

2.1.3 Рівень додатків

Прикладний рівень є найвищим рівнем у логічній ієрархії IoT та визначає всі додатки, які використовують технологію IoT або в яких розгорнуто IoT. Кінцевою областю застосування IoT можуть бути розумні будинки, розумні міста, сфера охорона здоров’я, тощо. Його основне призначення – надання послуг додаткам. Послуги можуть бути різними для кожної програми, оскільки послуги залежать від інформації, яку збирають датчики. На рівні додатків є багато проблем, в яких безпека є ключовим питанням. Зокрема, коли Інтернет речей використовується для створення розумного будинку, він створює багато загроз та вразливостей зсередини та ззовні. При реалізації надійної безпеки в розумному будинку на основі Інтернету речей, однією з основних проблем є те, що пристрої, що використовуються в розумних будинках, мають слабку обчислювальну потужність та малий обсяг пам’яті. Поширеними загрозами безпеки та проблемою прикладного рівня є:

Міжсайтовий скриптинг: це ін'єкційна атака, що дозволяє зловмиснику вставляти сценарій шкідливого коду на стороні клієнта, наприклад у веб сторінки. Виконуючи такі дії, зловмисник може повністю змінити зміст програми відповідно до своїх потреб та використовувати оригінальну інформацію незаконним способом.

Атака шкідливого коду: це код у будь-якій частині програмного забезпечення, основна мета якого, порушення конфіденційності, доступності та

цілісності інформації, а також пошкодження системи. Шкідливе програмне забезпечення може виконувати впровадження власного коду у тіло користувацького додатку, або існувати окремо в пам’яті як самостійний програмний код Засобами, які реалізують даний вид атак виступає цілий ряд зловмисного програмного забезпечення, зокрема віруси, троянські програми, руткіти, програми-вимагачі, тощо.

2.2 Функціональні можливості автоматизованих систем керування розумним будинком

Розумний дім — це будинок, побудований із системами автоматизації, які дозволяють людям дистанційно керувати освітленням, безпекою, розвагами тощо за допомогою телефонів чи комп’ютерів. Кілька розумних систем тепер також включають штучний інтелект. щоб додати інтелектуальні виявлення та розпізнавання образів для подальшої оптимізації споживання. [23-30] Будь-який пристрій Інтернету речей має такі функції (рисунок 2.2):

Рисунок 2.2 – Функціональні можливості розумного будинку

2.2.1 Освітлення

Оскільки освітлення є невід’ємною частиною будівлі. Користувач зможе вибрати час активації, наприклад, вдома 19:00, коли почне темніти, може бути розумним варіантом. Якщо користувач бажає додатково налаштувати налаштування освітлення, має бути доступна опція для реалізації виявлення руху, яка передбачає фактично вхід людини в кімнату, щоб увімкнути освітлення. Це може включати конкретну кімнату в будинку або всі кімнати. У форматі, керованому голосом, користувач міг перевірити, чи ввімкнено світло в будь-якій кімнаті будинку, розмовляючи в гарнітуру Bluetooth. Потім система може запитати користувача, чи перебувають індикатори в необхідному стані.

2.2.2 Безпека

Завдяки досягненням розумних технологій є сенс включити функції безпеки. Користувач зможе керувати постановкою та зняттям сигналізації, а також редагувати конкретні налаштування будильника, наприклад, код ключа. Користувач також може мати можливість налаштувати параметри виявлення вторгнення. Це спрацює спочатку за допомогою зовнішнього освітлення, яке виявить рух, а потім система попередить охоронний персонал або власника будинку про будь-які вікна або двері, які відкриваються примусово, за допомогою електронних датчиків, які підключені до системи.

2.2.3 Температура

Користувач зможе керувати опаленням та охолодженням будинку за допомогою функцій, що стосуються часу та параметрів. Користувач може вибрати, щоб опалення вмикалося, коли зовнішні умови опускаються нижче певної температури, зовні будуть розміщені термочутливі датчики для виявлення різних умов.

2.2.4 Прилади в будинку

За допомогою розумної системи можна керувати живленням усіх побутових приладів. У великому будинку це була б дуже зручна функція, оскільки може бути багато електроприладів, які залишаються в режимі очікування, тому система повинна містити функцію, яка шукає всі джерела живлення в будинку, щоб визначити, де можна заощадити енергію.

2.2.5 Розваги

Для повноцінного розумного будинку розважальні функції були б інноваційною функцією. Найпоширенішим аспектом розважальних функцій, ймовірно, є можливість звучання тонкої музики по всьому домогосподарству, це було б дуже приємно, особливо якщо мешканець мав стресовий день на роботі.

2.2.6 Стан системи

Варто мати можливість перевірити поточний стан системи. Така функція дасть користувачеві можливість сканувати всю систему або окремі її частини на наявність помилок.

2.2.7 Виявлення транспортних засобів

Домашня система повинна мати можливість ініціювати роботу за допомогою мобільного телефону, коли будинок порожній. Система повинна надавати користувачеві можливість вводити назву та номер моделі телефону, щоб його можна було перевірити для використання. Користувач зможе зв’язатися з системою, наближаючись до дому, щоб увімкнути телевізор або духовку та будь-які інші електричні прилади, якими може скористатися власник будинку.

2.2.8 Налаштування телефону

Домашня система повинна мати можливість ініціювати роботу за допомогою мобільного телефону, коли будинок порожній. Система повинна надавати користувачеві можливість вводити назву та номер моделі телефону, щоб його можна було перевірити для використання. Користувач зможе зв’язатися з системою, наближаючись до дому, щоб увімкнути телевізор або духовку та будь-які інші електричні прилади, якими може скористатися власник будинку.

2.2.9 Будильник

Корисною функцією в домашній розумній системі буде функція будильника, наприклад, користувач зможе вибирати з набору звуків пробудження від більш приємних звуків до більш пронизливих типів. У вихідні, ймовірно, будуть обрані більш приємні.

2.3 Модель процесу функціонування автоматизованих систем керування розумного будинку

Функціональний вигляд розумного будинку представлене як об’єднання трьох шарів: індивідуальний рівень, рівень взаємозв’язку та рівня взаємодії. Прямокутники із суцільною заливкою представляють загальні наявні ознаки в розумному будинку, а прямокутники із заливкою візерунком представляють нові особливості, які досліджуються.

Індивідуальний рівень: на цьому рівні розумного будинку орієнтована на пристрій і моделюється як індивідуально розгорнуті домашні пристрої, які функціонують розумним і незалежним чином. Розглядаються такі типи домашніх пристроїв:

1. Термінальні пристрої, такі як розумний динамік та смарт-телевізор.

2. Пристрої домашньої інфраструктури, такі як житловий шлюз і ретранслятор Wi-Fi.

3. Пристрої Інтернету речей, включаючи домашні датчики, приводи та застарілі домашні об’єкти, що живляться від датчиків і приводів.

4. Інші пристрої на основі мікроконтролерів (MCU), такі як пристрої домашньої автоматизації.

Рівень взаємозв’язку: на цьому рівні розумного будинку орієнтований на групу та моделюється як зв’язок та взаємодія окремих пристроїв, а рівень взаємозв’язку описує функції розумного будинку з точки зору домашніх людей.

Рівень взаємодії: на цьому рівні розумного будинку орієнтована на користувача та моделюється як взаємодія між користувачами та домашніми особами, і відповідно рівень взаємодії описує функції розумного будинку з точки зору сервісу користувача [30-40].

2.3.1 Індивідуальний рівень

Індивідуальний рівень описує функції розумного будинку з шести аспектів: апаратне забезпечення, мікро-програмне забезпечення, функції та технічні послуги, програми, безпека та інші функції.

Апаратне забезпечення: з апаратної точки зору людина володіє такими характеристиками:

1. Процесори. Особа повинна мати принаймні один процесор загального призначення (GPP) (наприклад, центральний процесор, мікропроцесор) для роботи в різних прикладних контекстах, повинен мати один або кілька процесорів набору інструкцій (ASIP) (наприклад, графічний процесор (GPU)). , цифровий процесор (DPU)) для прискорення виконання конкретних завдань і може мати один або кілька одно-функціональних процесорів (SPP) (наприклад, таймер, лічильник, аналого-цифровий перетворювач (АЦП)) для реалізації конкретних завдань.

2. Пам'ять. Особа повинна мати енергонезалежну пам’ять (NVM) для загального зберігання додатків і даних, повинна мати один або кілька захищених

ПЗУ для функцій безпеки (наприклад, безпечне завантаження, зберігання криптографічних ключів), може мати один або кілька конкретних NVM (наприклад, NAND Flash, NAND для Not-AND) для підтримки конкретних послуг (наприклад, запис відео або зсув у часі) для кращої продуктивності та ізоляції даних, і повинен мати принаймні одну пам'ять із довільним доступом (RAM) .

3. Введення/виведення (I/O). Відповідно до призначених функцій і послуг користувача, особа повинна мати відповідні інтерфейси вводу/виводу, якими керуватиме процесор(и) та спілкуватися з внутрішніми та зовнішніми компонентами, а також порти вводу/виводу для фізичного з’єднання з іншими пристроями. .

4. Мікроконтролер (MCU) або система на чіпі (SoC). Залежно від складності, особа має використовувати або MCU, або SoC як основу для інтеграції процесорів, контролерів пам’яті та, за бажанням, разом з іншими компонентами (наприклад, пам’яттю та периферійними пристроями вводу-виводу) для збільшення розміру та енергоефективності.

Прошивка: термін мікропрограми використовується тут для позначення набору програм, прив’язаного до конкретних апаратних компонентів пристрою (включаючи завантажувач, ядро/ОС, драйвери та проміжне програмне забезпечення). Особа повинна мати мікро-програмне забезпечення для забезпечення робочого середовища для розроблених функцій, технічних послуг та додатків.

Функції та технічні послуги: особа повинна реалізувати певні функції (наприклад, керування пристроями, виявлення та активація, доставка вмісту) та надавати технічні послуги. На відміну від служби користувача, технічна служба відноситься до представлення однієї або кількох функцій у мережі, що робить функції доступними для виявлення, реєстрації та дистанційного керування іншими пристроями.

Програми: Додаток визначається як розроблена програма для демонстрації функцій та використання технічних послуг користувачами або пристроями. У разі інфраструктурних пристроїв і кінцевих пристроїв особа повинна мати одну або

кілька програм, розгорнутих у пристрої; у випадку пристроїв IoT та інших пристроїв MCU особа може мати одну або кілька програм, розгорнутих на одному пристрої, і одну або кілька програм, розгорнутих в інших термінальних або інфраструктурних пристроях, щоб використовувати технічні послуги, що надаються цим пристроєм.

Безпека: як правило, інфраструктура та термінальні пристрої повинні підтримувати всі наступні функції безпеки, тоді як IoT та інші пристрої MCU також повинні підтримуватися, якщо це дозволяє середовище. З точки зору апаратного забезпечення, особа підтримує безпечне завантаження, що дозволяє встановити ланцюг довіри від апаратного кореня довіри до самого мікро-програмного забезпечення. Особа має захищений елемент (наприклад, криптографічний співпроцесор або довірене середовище виконання) для виконання конфіденційного коду, а також одноразову програмовану пам’ять, що дозволяє приховувати ключ і секрети в апаратному забезпеченні. З точки зору програмного забезпечення, SHE має бути розроблено відповідно до парадигми найменших привілеїв: жодним додаткам не можуть бути надані зайві права чи доступ, і має механізми посилення, такі як захист пам’яті та обов’язковий контроль доступу.

Інші характеристики: особа повинна мати спрощений корпус, щоб включати всі необхідні компоненти з внутрішнім або зовнішнім джерелом живлення. Крім того, особа повинна відповідати існуючим стандартам для забезпечення безпеки будинку, захисту навколишнього середовища, шуму та споживання енергії.

2.3.2 Рівень взаємозв’язку

У цьому шарі розумного будинку є сукупністю всіх пристроїв із наступними функціями.

Мережа: розумного будинку має мати одну або більше точок доступу до мережі, щоб забезпечити підключення до локальної мережі (LAN) для всіх внутрішніх пристроїв і підключення до глобальної мережі (WAN) між розумним будинком та зовнішнім середовищем. Мережа, як правило, керується житловим

шлюзом у централізованому домашньому розгортанні, а в децентралізованому розгортанні один або кілька пристроїв можуть мати незалежні можливості доступу до мережі.

Взаємодія: розумний будинок має підтримувати обмін інформацією між внутрішніми пристроями і, що більш важливо, взаємодію домашніх пристроїв для організації або створення окремих технічних служб разом для покращення функціональності будинку.

Сумісність: під час роботи в мережі та взаємодії домашніх пристроїв стандартні протоколи та моделі (якщо такі є) повинні використовуватися в кожному окремому розумному будинку та охоплювати якомога більше рівнів моделі OSI (тобто від нижнього фізичного рівня до верхнього прикладного рівня) для досягнення сумісності розумного будинку.

Безпека: функція безпеки на рівні з'єднання об'єднує всі функції безпеки від її окремих осіб. Зокрема, мережа та взаємодія повинні бути захищені механізмами контролю доступу та брандмауером, а також увімкнути захищений протокол зв’язку, такий як SSL та HTTPS.

У випадку, коли індивідуальна колекція розгорнута відповідно до децентралізованої архітектури, кожна особа повинна застосовувати свої власні функції безпеки для взаємодії з іншими, тоді як у випадку централізованої архітектури розгортання централізований контрольний пункт (наприклад, житловий шлюз) застосовуватиме захисні елементи до всіх осіб на додаток до самих індивідуальних захисних елементів.

2.3.3 Рівень взаємодії

Рівень взаємодії описує особливості взаємодії між домашніми користувачами та колекцією домашніх людей.

Послуги користувачів: середовище розумного дому в кінцевому підсумку надаватиме одну або кілька користувацьких послуг домогосподарству через окремих осіб, а індивідуальна колекція взаємодіє із зовнішнім середовищем, таким

як хмарні сервери. На відміну від технічної служби, користувацька служба — це операції всього розумного будинку, які приносять користь домашнім користувачам, наприклад, мультимедійні, телекомунікаційні та розважальні послуги. Взявши за приклад користувальницький сервіс ТБ, доставка телевізійного вмісту додому включає запуск серверного набору на хмарному сервері, запуск інтерфейсного набору в домашній приставці, виконання функцій отримання та відображення вмісту в телевізор і за бажанням виконання програми дистанційного керування в мобільному телефоні.

Людино-машинний інтерфейс (HMI): розумного будинку має мати принаймні один HMI, щоб користувачі могли безпосередньо взаємодіяти з окремим рівнем і шаром взаємозв'язку як локально (вдома), так і віддалено (за межами дому). HMI є або у вигляді програмного інтерфейсу з програми, або фізичного пристрою для введення/виведення.

Безпека: рівень взаємодії перегрупує всі функції безпеки окремого рівня та рівня взаємозв'язку. Крім того, розумний будинок має мати механізми автентифікації та авторизації користувачів, щоб забезпечити коректне використання пристроїв, додатків та сервісів користувача домашніми користувачами. Однак необхідно знайти компроміс між рівнем безпеки розумного будинку та зручністю використання для загального домашнього господарства, оскільки ефективні заходи безпеки пов'язані з великим споживанням ресурсів і вартістю зручності використання.

Конфіденційність: розумного будинку забезпечує безпечне та захищене середовище для конфіденційності користувачів і має відповідати стандартам (наприклад, Загальному регламенту про захист даних (GDPR)). Домашні дані, послуги та виявлений контекст будуть доступні лише для легальних пристроїв і користувачів через систему керування конфіденційністю. Крім перерахованих вище загальних ознак рівня взаємодії, ряд особливостей розумного будинку вивчаються як науковцями, так і промисловістю з багатообіцяючими результатами прототипів, а деякі репрезентативні особливості визначені нижче.

Усвідомлення контексту: розумний будинок має бути в змозі автоматично ідентифікувати домашню контекстну інформацію щодо середовища та користувачів (наприклад, діяльність, ситуацію та переваги) і, відповідно, надавати адаптовані послуги користувачам відповідно до визначеного контексту та розширювати функціональні можливості існуючих послуги.

Підтримка прийняття рішень: середовище розумного дому має бути спроможним допомогти користувачам у прийнятті рішень у конкретних ситуаціях, що включає не тільки управлінські та координаційні рішення, а й розумну взаємодію.

Прогноз: розумний будинок має бути здатним передбачати вимоги користувачів за допомогою історії поведінки та надавати пропозиції та рекомендовані послуги відповідно до без чітких вимог.

Підкріплення: розумний будинок має постійно збагачувати свої знання та покращувати якість обслуговування користувачів за допомогою ітеративного навчання з підкріпленням для комфорту та автономності вдома та налаштовувати послуги відповідно до отриманого контексту розумного будинку

2.4 Висновки

В результаті проведення дослідження було розглянуто архітектуру розумного будинку як системи, яка складається з трьох логічних рівнів: сприйняття, мережевого та рівня додатків. Для кожного рівня проведено огляд відомих кіберзагроз. Зокрема визначено критичні інформаційні об’єкти в системі розумного будинку, критерії оцінки ризиків та сценарії кіберзагроз.

Розширення та проектування оптимальних систем IoT все ще є активною сферою досліджень, тому на практиці не всі продукти IoT мають весь набір функцій стандарту. В основному це залежить від випадків використання та галузі, в яку необхідно впровадити екосистему. Інтернет речей (IoT) — це технологія підключених розумних пристроїв, яка має додаткові варіанти використання в різних галузях. Зі збільшенням використання в різних галузях стає необхідністю

визначити загальний стандарт екосистем IoT. Як стандарт дизайну, будь-який пристрій IoT має деякий загальний набір функцій, як-от підключення, аналітика, керування кінцевими точками тощо

Завдяки широкому охопленню функцій розумного будинку як фундаментальних, так і передових аспектів, ця робота також ілюструє семантичний потенціал технології для подальшого зв’язування та розвитку розумного будинку.

3 МОДЕЛЬ ПОБУДОВИ ПРОФІЛІВ ЗАГРОЗ ПРИ КЕРУВАННІ РОЗУМНИМ БУДИНКОМ

3.1 Оцінка ризиків інформаційної безпеки системи розумного будинку на основі методології OCTAVE Allegro

При проектуванні та експлуатації систем розумного будинку важливим завданням є визначення кіберзагроз, оцінка їх впливу на потенційно “вузькі” місця системи та розроблення повних та вичерпних стратегій по пом’якшенню та усуненню негативних впливів кібератак. Причому, чим швидше буде проведено оцінку та прийнято відповідні заходи, тим більша імовірність забезпечення цілісності, доступності та конфіденційності інформації. Розглянемо процес оцінки ризиків інформаційної безпеки системи розумного будинку. Для оцінки ризиків використаємо методологію OCTAVE Allegro.

OCTAVE Allegro є методологію, що дозволяє упорядкувати та оптимізувати процес оцінки ризиків інформаційної безпеки, що дозволяє організації отримати достатні результати за невеликі витрати часу, людських та інших обмежених ресурсів. Основний фокус методології OCTAVE Allegro полягає у розгляді людей, технології та засобів у контексті їх ставлення до інформації та бізнес-процесів та послуг, які вони підтримують.

Методологія OCTAVE Allegro визначає вісім послідовних етапів, організованих у 4 фази (рисунок 3.1): визначення критеріїв, профілювання об’єктів, визначення загроз, визначення та пом’якшення ризиків.

За допомогою таблиць OCTAVE Allegro, є можливість фіксувати результати кожного кроку оцінки ризику та використовувати їх як вхідні дані для наступних кроків. Окремі кроки застосовуються до кожного окремого інформаційного об’єкту. Для проведення оцінки ризиків безпеки використаємо шаблон OCTAVE Allegro [40-50].

Розглянемо детальніше застосування методології OCTAVE Allegro для оцінки ризиків безпеки системи розумного будинку.

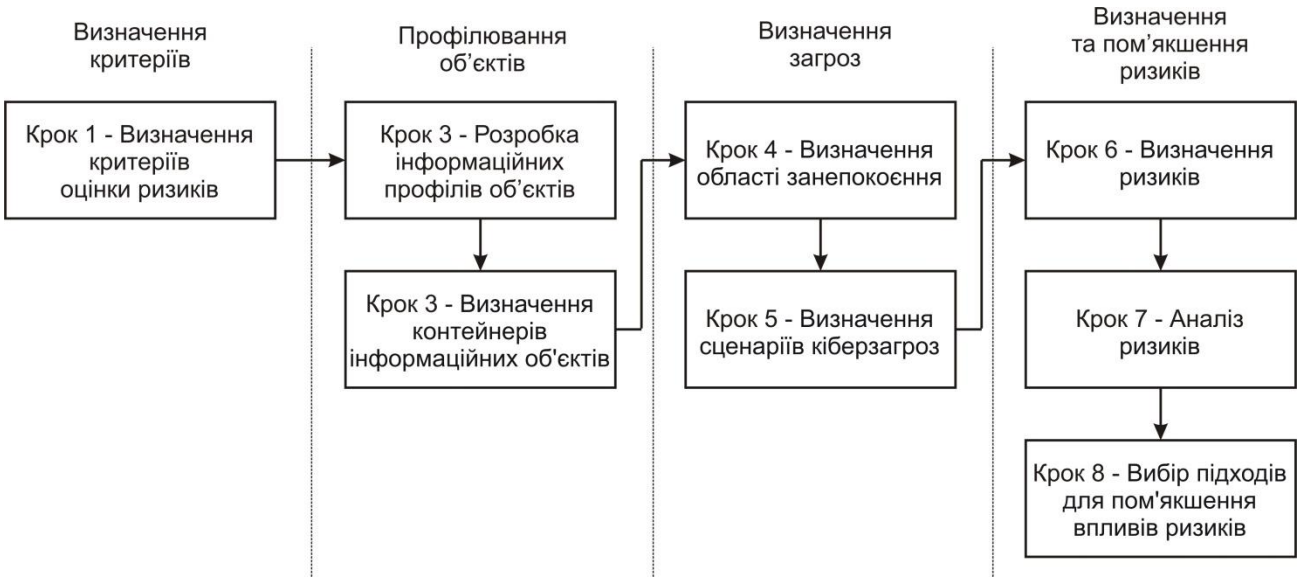


Рисунок 3.1 – Кроки методології OCTAVE Allegro

3.2 Визначення критеріїв оцінки ризиків

Метою цього кроку є встановлення того, що може бути наслідком ризику для бізнес-стратегії та завдань чи критичних факторів успіху (комерційні зацікавлені сторони) та для мешканців розумного будинку (некомерційні зацікавлені сторони). Цей крок складається з двох активностей.

Перша активність передбачає визначання набору якісних та кількісних заходів для оцінки впливу ризиків на виявлені критично важливих інформаційних активів у системі розумний будинок. В процесі другої активності виконується пріоритезація зони впливу відповідно до їх важливості для власника розумного будинку або зацікавлених сторін.

Критеріїв оцінювання методології OCTAVE Allegro включають наступні категорії: репутація та довіра клієнтів; життя, здоров'я, безпека; штрафи та юридичні санкції; фінансові збитки; продуктивність.

Перш ніж заповнювати таблиці OCTAVE Allegro, слід визначити, хто є зацікавленими сторонами, для яких проводиться оцінка ризиків у системі розумного будинку. Для системи розумного будинку можна виділити наступні зацікавлені сторони: не комерційні стейкхолдери, що представлені кінцевими споживачами системи розумного будинку та комерційні стейкхолдери – виробники

програмного та апаратного забезпечення, приватні і державні компанії, що займаються встановленням та розгортанням систем домашньої автоматизації, тощо.

Таким чином, для критерію оцінки ризиків життя, здоров'я та безпека встановлено пріоритетність на рівні 5 (найвищий), для репутації – 4, для фінансових збитків – 3, для продуктивності – 2. Найнижчий пріоритет має категорія штрафи та юридичні санкції з відповідним рівнем пріоритету 1.

3.3 Розробка профілю інформаційних об’єктів

На цьому кроці слід провести ідентифікацію критичних інформаційних об’єктів та провести їх профілювання. У процесі профілювання визначимо чіткі межі для об’єкту в системі розумного будинку, вимоги до його безпеки та ідентифікуємо всі місця , де даний об’єкт зберігається, транспортується та зберігається. Такі кроки дозволять ідентифікувати вразливі місця критичних інформаційних об’єктів.

Першим кроком у процесі розробки профілів інформаційних об’єктів є власне ідентифікація цих об’єктів. Слід відзначити, що рівень додатків розглядатись не буде в зв’язку з його більшою захищеністю інформаційних активів. Для рівня сприйняття та мережевого рівня розумного будинку можна виділити наступні критичні інформаційні об’єкти: інформація, зібрана пристроями (датчики); дані камери відеоспостереження; облікові дані користувача (ім’я користувача та пароль); інформаційні ресурси (документи, зображення, користувацькі файли); інформація про налаштування розумного будинку; структура розумного будинку (інформація про пристрої); інформація про журнал подій (інформація про стан розумного будинку); мобільні пристрої / пристрої користувача; інформація про місцезнаходження.

3.4 Визначення контейнерів інформаційних об’єктів

Після опису профілів критичних інформаційних об’єктів, згідно із методологією OCTAVE Allegro, здійснюється ідентифікація контейнерів інформаційних об’єктів. Контейнер інформаційного об’єкту – це місце, де знаходиться інформація. Контейнери можуть бути технічними (програмне забезпечення, програмне забезпечення, сервери та комунікаційні мережі), фізичними (паперові носії, флеш носії, компакт-диски) або люди (хто знає про інформацію). Вони також можуть бути як внутрішніми, так і зовнішніми для організації. Проаналізуємо (технічні, фізичні та людські) контейнери для критичного інформаційного об’єкту «інформація, зібрана пристроями (датчиками)».

3.5 Визначення області занепокоєння

Метою цього кроку є визначення проблемних областей в раніше ідентифікованих інформаційних об’єктах. Для кожного ідентифікованого інформаційного об’єкту визначаються конкретні проблеми, які можуть негативно вплинути на безпеку цього об’єкту. На цьому кроці здійснюється опис потенційних впливів, якщо загроза відбулася, та умов, що спричиняють цю подію. За описом, який ґрунтується на місцях зберігання інформаційних об’єктів, визначених на кроці 3, отримується детальне розуміння того, з якого місця інформаційного об’єкту може розпочатись порушення безпеки.

3.6 Визначення сценаріїв кіберзагроз

Наступним кроком є побудова сценаріїв загроз для кожного ідентифікованого інформаційного активу. Сценарій загрози включає один або кілька об’єктів, дійову особу (актора), засоби, мотиви та список небажаних результатів. Актор може бути як природним (шторм, повінь, пожежа чи інше лихо),

автоматизованим (шкідливе програмне забезпечення), так і розумним (злочинець, активіст чи інша людина, яка має намір заподіяти школу розумному будинку). Засобом виступає вразливість та експлойт, які використовується суб’єктом проти інформаційного активу. Мотив – це бажання актора застосувати засоби до інформаційного об’єкту. Небажаним результатом є пошкодження інформаційного активу. Результатом завжди є розкриття, зміна, переривання або знищення. Даний крок дозволяє визначити сценарії загроз, які в більшій мірі можуть бути реалізовані. Загрози визначаються за допомогою контейнерів, у яких зберігаються або передаються активи.

3.7 Визначення ризиків

Ризик – це можливість заподіяння шкоди або втрати (даних, програмних, технічних пристроїв) і складається з події, наслідку та невизначеності. Загроза може мати численні потенційні негативні наслідки для організації. Наприклад, порушення системи електронної комерції організації може вплинути на репутацію організації з клієнтами, а також на її фінансове становище. З метою визначення ризиків для кожного інформаційного об’єкту застосовується сценарій загроз до його складових за умови реалізації сценарію загрози та оцінки впливу на зацікавлених сторін розумного будинку.

3.8 Аналіз ризиків

На даному етапі визначені ризики на кроці 6 оцінюються за допомогою критеріїв оцінювання, встановлених на першому кроці. Ці бали використовуються для визначення пріоритетності ризиків, і як результат, для пом'якшення впливу ризиків на систему розумного будинку.

Таким чином, для кожного ризику інформаційного об’єкта потрібно виконати наступні дії: призначити значення “високий”, “середній” та “низький” у області Значення стовпця з урахуванням критеріїв оцінки ризиків (таблиця 1);

обчислити оцінку для кожної зони впливу шляхом множення пріоритетності зони впливу на значення впливу (високий = 3, середній = 2, низький = 1). Після запису результату у стовпчик оцінок, формується підсумкова оцінка, що є відносним показником ризику.

3.9 Вибір підходів для пом’якшення впливів ризиків

На останньому, проаналізовані на попередньому кроці ризики, використовуються для вироблення стратегії щодо пом'якшення потенційного впливу ризиків на інформаційні об’єкти системи розумного будинку. Таким чином на цьому кроці здійснюється вибір підходу для боротьби з кожною загрозою згідно із їх пріоритетністю. Існує кілька підходів до вибору: прийняти, зменшити загрозу чи вплив, передати загрозу або відкласти.

Після виявлення ризиків (відповідно до загрози та вразливості) та оцінки ризиків можна визначити план пом'якшення, щоб уникнути або обмежити виявлені ризики та негативні наслідки, що випливають з них. Виконаємо оцінку ризику для інформаційного об’єкту «інформація, зібрана пристроями (датчиками)».

Зазначені кроки методології OCTAVE Allegro проводяться для кожного критичного інформаційного об’єкту. Проведений процес оцінки ризиків дозволяє проаналізувати інформаційні об’єкти в системі розумного будинку, які є критичними з точки зору безпеки, провести аналіз ризиків та їх впливів на об’єкти, та запропонувати можливі контрзаходи з метою захисту інформаційних об’єктів та створення системи розумного дому більш безпечним.

3.10 Формалізація моделі побудови профілів загроз при керуванні розумним будинком

У різних наукових галузях, особливо в комп’ютерних науках, формальне моделювання є важливим інструментом, який використовується для дослідження складних структур, систем або алгоритмів. Формальні моделі часто необхідні для

виконання автоматичного та напівавтоматичного моделювання або перевірки особливостей складних систем. Поточний аналіз ризиків і пов'язані з ним терміни не мають відповідної формалізації, яка б гарантувала універсальність або можливість виконання дослідження в автоматичний або напівавтоматичний спосіб.

Тут представлена формальна модель інформаційної системи. Зазначені структури призначені для точного визначення графіка для розрахунку значень ризику та алгоритму його побудови. Модель може бути використана для аналізу організації та її IT-активів і ресурсів.

Нехай A — набір деяких активів:

$$A = \{a_i : i = 1, \dots, n_A\}. \tag{3.1}$$

Крім того, розглянемо такі кінцеві множини:

$V = \{v_j : j = 1, \dots, n_V\}$ - набір класів вразливості;

$T = \{t_k : k = 1, \dots, n_T\}$ - набір класів загроз;

$S = \{s_l : l = 1, \dots, n_S\}$ - набір сценаріїв ризику;

$DP = \{dp_s : s = 1, \dots, n_{DP}\}$ - комплекс заходів, що знижують потенціал;

$DI = \{di_t : t = 1, \dots, n_{DI}\}$ - комплекс заходів, що зменшують вплив;

Наведені вище набори визначають класи вразливостей системних активів, що стосуються загроз, загроз для активів, сценаріїв ризику та заходів, що зменшують потенційні можливості та вплив загроз, що виникають внаслідок втрат активів.

Припустимо, що впорядкована множина R задана з n значеннями аргументів системи, що відповідають множинам A, V, DP, DI і M, W, C (див. нижче). У цьому наборі $R = [r_{min}, r_{max}] \in N$; виділяють мінімальне r_{min} і максимальне r_{max} значення. Тепер визначте допоміжну функцію $value_A$, яка присвоює даному активу $a \in A$ значення трьох основних параметрів безпеки (конфіденційність, цілісність, та наявність):

$$value_A : A \rightarrow R^* \times R^* \times R^*, \tag{3.2}$$

де $R^* = R + \{null\}$ а $null \in R^*$ — нейтральне значення. Для цього значення аргументу даний об'єкт не має визначеної ознаки, і тому йому не можна призначити значення.

Усі аргументи функції $value_A$ та відповідні їй значення утворюють масив $M^A_{n_A \times 3}$, що містить n_A рядків (n_A — кількість активів/аргументів) і три стовпці. Будь-якому активу (рядку) цього масиву присвоєно значення класифікації щодо виділених рівнів конфіденційності, цілісності та доступності, записаних у трьох послідовних стовпцях. Якщо деяке значення не визначено для даного активу (нульове значення), йому не можна призначити функції конфіденційності, цілісності або доступності. Активи системи можуть бути піддані деяким загрозам. Насправді дана загроза може бути реалізована тоді і тільки тоді, коли цей актив має відповідну вразливість. Природна вразливість (так зване «природне опромінення», незалежно від застосовуваних заходів безпеки) може виникнути внаслідок «форс-мажорних» подій і як ненавмисних, так і навмисних дій.

Визначимо ще одну допоміжну функцію, яка призначає три значення залежно від параметрів AEV (аварії, помилки та добровільності) даному природному опроміненню:

$$value_V : V \rightarrow R^* \times R^* \times R^*. \tag{3.3}$$

Як і в попередньому випадку, усі аргументи функції $value_V$ та відповідні їй значення утворюють масив $M^V_{n_V \times 3}$ з трьома стовпцями та n_V рядками, n_V — кількість розглянутих вразливостей (аргументів). Будь-якій вразливості (рядку) цього масиву присвоюються значення вразливості щодо спеціальної дії (Нещасний випадок, Помилка, Добровільна).

У будь-якій IT-системі впроваджуються деякі контрзаходи, щоб зменшити потенційні загрози та впливи, що впливають на активи системи. Залежно від цих загроз відповідні заходи можуть зменшити певний потенціал та/або вплив.

Визначено дві додаткові функції для визначення значень заходів, що зменшують потенціал і вплив:

$$value_{DP} : DP \times S \times N \rightarrow R, \quad (3.4)$$

$$value_{DI} : DI \times S \times N \rightarrow R, \quad (3.5)$$

де N — множина натуральних чисел.

Тепер визначимо функцію, яка призначає набори вразливостей активам.

Визначення 1. Уразливістю інформаційної системи IS є будь-яка функція:

$$vul : A \rightarrow 2^V. \quad (3.6)$$

Відповідно до цього визначення, функція вразливості призначає належні класи вразливості кожному системному активу і таким чином дозволяє створити список активів та їх вразливостей. Цей список є відправною точкою для наступного кроку в процесі управління ризиками – оцінки ризиків. Тепер ми можемо визначити загальну системну загрозу:

Визначення 2. Загальною загрозою для системи є будь-яка функція:

$$thr : \overline{A \times V} \rightarrow 2^T, \quad (3.7)$$

де множина $\overline{A \times V}$— множина всіх пар (a, v), що належать $A \times V$, які відповідають умовам $\exists X \subseteq V\ (v \in X \wedge X \in vul(a))$. Ця функція визначає загрози для активів із набору A щодо їх уразливостей із набору V.

Визначення 3. Інформаційна система IS являє собою такий набір упорядкованих 4-х кортежів:

$$IS = \{(a, value_A(a), vul(a), thr(a, v)) : a \in A \wedge (a, v) \in \overline{A \times V}\}. \quad (3.8)$$

Відповідно до цього визначення, IS інформаційної системи — це набір активів із визначеними значеннями, які можуть мати вразливості, використані загрозами. Наведене вище визначення є стандартом для більшості методів, включаючи MEHARI (CLUSIF, 2010), CRAMM (CCTA, 1987) та OCTAVE (CMU, 2006). Сценарії ризику, що відповідають Визначенню 4, призначаються активам, уразливим до загроз.

Сценарії ризику, що відповідають Визначенню 4, призначаються активам, уразливим до загроз.

Визначення 4. Загальним сценарієм ризику системи є будь-яка функція:

$$scen: \overline{A \times T} \rightarrow 2^S, \tag{3.9}$$

де множина $\overline{A \times T}$ — множина всіх пар (a, t), що належать $A \times T$, що відповідають умовам $\exists_{v \in V} \exists_{X \subseteq T} (t \in X \wedge X \in thr(a, v))$.

Ця функція визначає сценарії ризику для активів від A щодо загроз від T.

Щоб визначити значення ризику для IS, необхідно визначити дії, які вживає організація (впровадження заходів безпеки) для зменшення потенційних можливостей та зменшення впливу даного ризику. Ці дії визначені нижче.

Визначення 5. Загальна потенційна дія (дія, пов'язана із заходами, що впроваджуються в організації для зменшення ймовірності вразливості) IS є функцією:

$$mis_{pot} : \overline{A \times S} \rightarrow 2^{DP}, \tag{3.10}$$

де множина $\overline{A \times S}$ — множина всіх пар (a, s), що належать $A \times S$, що відповідають умовам $\exists_{s \in S} \exists_{X \subseteq S} (s \in X \wedge X \in scen(a, t))$.

Ця функція визначає потенційні дії для активів і відповідні сценарії ризику від S.

Не всі передбачені потенційні дії повинні застосовуватися до певної системи для даного сценарію. Отже, визначається набір реалізованих потенційних дій:

$$\overline{\mathrm{DP}} = \left\{(\mathrm{s}, \mathrm{dp}) \in \mathrm{S} \times \mathrm{DP} : \exists_{a \in A} \left(\mathrm{dp} \in \mathrm{X} \wedge \mathrm{X} \in \mathrm{mis}_{pot}(\mathrm{a}, \mathrm{s})\right)\right\}. \quad (3.11)$$

Цей набір визначає потенційні дії, реалізовані для заданих сценаріїв ризику. Ці дії можуть бути превентивними (Baskerville, 1994) або превентивними та застережливими (CLUSIF, 2010).

Подібним чином визначається загальна впливова дія.

Визначення 6 Загальна дія впливу (дія, пов'язана із заходами, що впроваджуються в організації та зменшують вплив) IS – це функція:

$$mis_{imp} : \overline{A \times S} \rightarrow 2^{DI}. \quad (3.12)$$

Ця функція визначає дії впливу (зменшення впливу) для активів від A та відповідних сценаріїв ризику від S.

Як зазначалося раніше, не всі передбачені дії впливу повинні застосовуватися в даній системі. Отже, визначається набір реалізованих впливів:

$$\overline{\mathrm{DI}} = \left\{(\mathrm{s}, \mathrm{di}) \in \mathrm{S} \times \mathrm{DI} : \exists_{a \in A} \exists_{X \subseteq S} \left(\mathrm{di} \in \mathrm{X} \wedge \mathrm{X} \in \mathrm{mis}_{pot}(\mathrm{a}, \mathrm{s})\right)\right\}. \quad (3.13)$$

Цей набір визначає дії впливу, реалізовані для даного сценарію ризику. Дії можуть бути детективними та коригувальними (Baskerville, 1994) або захисними, паліативними та рекуперативними (CLUSIF, 2010).

Методи визначення значень потенціалу та впливу залежать від методології впровадження контрзаходів. Після ретельного і детального розгляду підходів, запропонованих у MEHARI, CRAMM і OCTAVE, автори цієї статті прийняли рішення, запропоновані в MEHARI. Цей вибір продиктований загальнодоступністю (на основі ліцензії GNU) оновлених баз знань щодо загроз,

вразливостей, контрзаходів та взаємовідносин фізичних та логічних контрзаходів для аналізованих сценаріїв ризику. Крім того, значення, присвоєні детальним питанням в анкетах аудиту, є порівнянними. У методах MEHARI і CRAMM відрізняються лише діапазони значень (ENISA2, 2010). Значення потенційних і впливових дій розраховуються за такою формулою:

$$\mathrm{CM}_{s,j} = \left\lfloor (r_{max} - r_{min}) \frac{\sum R_i \times P_i}{\sum P_i} + r_{min} + 0.5 \right\rfloor, \quad (3.14)$$

де $j \in DP \cup DI$ являє собою реалізований контрзахід; $\lfloor x \rfloor$ вказує на округлення результату x до числа, що належить множині R (до найнижчої точки x у цій множині);R_i є відповіддю на контрольне запитання (значення 1 або 0); $P_i = value_X(j, s, no(R_i))$ – це значення, присвоєне i-му запитанню, де X = DP або DI, яке залежить від визначеного типу j контрзаходи сценарію s і номера питання $no(R_i)$ пов'язана з відповіддю R_i; а $CM_{s,j} \in R$ – зважене значення контрзаходу, що зменшує потенціал і вплив деякої загрози.

Для розрахунку вагового значення показників $CM_{s,j}$ на основі формули (14) доступна база знань (тобто набори анкет із відповідним чином обраними питаннями аудиту). У свою чергу, питання аудиту сформульовані, щоб дозволити оцінити значення можливостей або впливів, що зменшують контрзаходи. У таблиці 3.1 наведено зразковий фрагмент анкети аудиту (CLUSIF, 2010).

Цільова стадія, після розрахунку зваженої величини для потенційних можливостей або впливів зменшення контрзаходів, полягає у визначенні значень ризику $W^{s,a}$ для будь-якого ідентифікованого сценарію ризику на основі масиву ризиків $M^{s,a}$.

Припустимо, що такі масиви попередньо визначені:

1. масив зменшення потенціалу $M^s_{pot\ n\times n\times n}$, який робить оголошене значення потенціалів зменшення контрзаходів $W^s_{pot}[i, j, k] \in R$ залежним від $CM_{s,j}$ (для конкретного $j = dp_1, \ldots, dp_{n_{DP}}$) і значення $value_V(v)$;

2. масив зменшення впливу $M^{s}_{imp\ n\times n\times n}$, який робить оголошене значення впливів, що зменшують контрзаходи $W^{s}_{\text{imp}}[i,j,k] \in R$, залежними від $CM_{s,j}$ (для конкретного $j = di_1, \ldots, di_{n_{DI}}$);

3. масив зменшення реального впливу $M^{s}_{imp\ n\times n}$, який робить оголошене значення реальних впливів, що зменшують контрзаходи $W^{s,a}_{imp}[i,j] \in R$, залежними від значення W_s, невизначеного з масиву $M^{s}_{imp}\ n \times n\ \times n$ і значення вартості активу $value_A(a)$;

4. масив ризику $M^{s,a}_{n\times n}$, який робить оголошене значення ризику $W^{s,a}[i,j] \in R$ залежним від значення W^{s}_{pot}, визначеного з масиву $M^{s}_{pot}\ n \times n \times n$, і значення $W^{s,a}_{imp}$ невизначено з масиву $M^{s,a}_{imp}\ n \times n$.

Таблиця 3.1 Зразковий фрагмент аудиторської анкети.

Питання аудиту: Домен: IT-виробниче середовище		
Питання	Відповідь	Значення
Управління та обробка інцидентів		
Чи було проведено детальний аналіз подій або послідовності подій, які можуть вплинути на безпеку (відмови у підключенні, реконфігурація, зміни в продуктивності, доступ до конфіденційних даних чи інструментів тощо)?	1	2
Чи реєструються ці події та чи корисні параметри для їх подальшого аналізу?	0	4
Чи існує програма, здатна проаналізувати ці записи та вимірювання продуктивності та зробити висновки (приладна панель, діагностика аномалій тощо) для перевірки компетентною командою?	1	4

Значення визначених масивів M^s_{pot}, M^s_{imp}, $M^{s,a}_{imp}$ і $M^{s,a}$ повинні залежати від критичності бізнес-процесів у даній організації і не повинні прийматися «жорстоко», як пропонується в більшості розглянутих методів (наприклад, CRAMM або MEHARI). Критичність процесу залежить від значень уразливості $value_V(v)$, вартості активів $value_A(a)$ та ефективності реалізованих можливостей зменшення контрзаходів $DP\,(dp_s : s = 1,\ldots,n_{DP})$ та впливу $DI\,(di_t : t = 1,\ldots,n_{DI})$.

Для масивів, визначених, як зазначено вище, також визначаються такі набори масивів:

$$M_{pot} = \bigcup_s : \exists_{dp \in DP}(s, dp) \in \overline{DP}\{M^s_{pot}\}, \tag{3.15}$$

$$M_{imp} = \bigcup_s : \exists_{di \in DI}(s, di) \in \overline{DI}\{M^s_{imp}\}, \tag{3.16}$$

$$M^a_{imp} = \bigcup_s : \exists_{di \in DI}(s, di) \in \overline{DI}\{M^{s,a}_{pot}\}, \tag{3.17}$$

$$M = \bigcup_{(a,s) \in \overline{A \times S}}\{M^{s,a}\}. \tag{3.18}$$

Відповідно до запропонованої моделі останнім етапом аналізу та вимірювання ризику є визначення значень ризику для сукупності всіх ідентифікованих і класифікованих активів в IS:

$$W = \bigcup_{a \in A}\{W^a\}, \tag{3.19}$$

де

$$W^a = \bigcup_{(a,s) \in \overline{A \times S}}\{W^{s,a}\}, \tag{3.20}$$

величина ризику для активів IS системи.

Запропонована формальна модель аналізу ризиків не лише дає змогу визначити значення ризику для ідентифікованих та класифікованих активів, але й відповідає рекомендаціям OECP та сімейству міжнародних стандартів ISO/IEC 2700x.

Визначення 7. Система безпеки SEC_{IS} інформаційної системи IS являє собою впорядкований кортеж:

$$\left(IS, V, vul, T, thr, S, scen, DP, mis_{pot}, DI, mis_{imp}, M, W, C\right), \quad (3.21)$$

де параметри системи були визначені раніше, а C — коефіцієнт відповідності для всіх зон безпеки.

Кортеж, що визначає систему безпеки SEC_{IS}, містить усі компоненти, згадані в рекомендаціях та стандартах OECP щодо безпеки мереж та систем *IS* (активи, загрози, вразливості, контрзаходи).

Ці компоненти відповідають сімейству міжнародних стандартів ISO/IEC 2700x, включаючи ISO/IEC 27002 (2007) і ISO/IEC 27005 (2008). ISO/IEC 27005 (2008) визначає, як ідентифікувати та класифікувати активи *A*, вразливості *V* та загрози *T*, а також визначає виведення значень ризику *W* на основі попередньо визначеного масиву ризиків *M*, чиї стовпці та рядки описують потенційні дії та дії (скорочено *DP-DI*).

Детальний опис впровадження, підтримки та покращення *IS* системи безпеки в організації представлено в ISO/IEC 27002 (2007) (вибір і впровадження контрзаходів, що зменшують потенціал *DP* і вплив *DI*).

Рекомендації OECP щодо безпеки IT-систем, зокрема мережевих систем, повністю описані в ISO/IEC 27002 (2007). Цей стандарт містить рекомендації та загальні правила щодо початку діяльності, впровадження, підтримки та вдосконалення процесів управління інформаційною безпекою.

Рекомендації стосуються одинадцяти сфер (кожна визначає рівні/категорії безпеки), тобто політики безпеки, фізичну безпеку та безпеку навколишнього середовища, управління системою та мережею та відповідність законодавчим вимогам і стандартам. У таблиці 3.2 наведено приклади категорій безпеки.

Таблиця 3.2 Деякі категорії безпеки випливають із стандартних рекомендацій.

Категорії безпеки, що випливають із вимог ISO/IEC 27002:2005			
Рівень 1	Рівень 2	Рівень 3	Опис
9			Фізична та екологічна безпека
	9.1		Захищені зони
		9.1.5	Робота в безпечних зонах
	9.2		Безпека обладнання
		9.2.2	Допоміжні утиліти
		…	……
11			Контроль доступу (вимоги OECD)
	11.1		Вимоги бізнесу щодо контролю доступу
		11.1.1	Політика контролю доступу
	11.2		Керування доступом користувачів
		11.2.3	Керування паролями користувачів
	…		……

Припустимо, що зміст таблиці 3.2 можна описати за допомогою таких даних:

1. U - кількість зон безпеки;
2. U^i - кількість категорій безпеки щодо i-ї зони безпеки ($i = 1, \dots, U$);
3. $U^{i.j}$ - кількість доступних класів протидії в i-й зоні та j-ій категорії безпеки ($i = 1, \dots, U, j = 1, \dots, U^i$);

4. $U^{i.j.k}$ - кількість доступних класів контрзаходів в *i*-й зоні, *j*-й категорії безпеки та *k*-му класі контрзаходів ($i = 1, \dots, U, j = 1, \dots, U^i, j = 1, \dots, U^{ij}$);

Таким чином, на основі запропонованої моделі оцінки ризиків можна оцінити відповідність аналізованої системи безпеки SECIS відповідним рекомендаціям і стандартам OECP на рівнях сфер безпеки, категорій безпеки та класів контрзаходів:

1. коефіцієнт відповідності $C \in R$ для всіх зон безпеки

$$C = \left[(r_{max} - r_{min}) \frac{\sum_{i=1}^{U} \sum_{j=1}^{U^i} \sum_{k=1}^{U^{i.j}} \sum_{m=1}^{U^{i.j.k}} R_m^{i.j.k}}{\sum_{i=1}^{U} \sum_{j=1}^{U^i} \sum_{k=1}^{U^{i.j}} U_{i.j.k}} + r_{min} \right], \quad (3.22)$$

2. коефіцієнт відповідності $C_i \in R$ для *i*-ї зони безпеки

$$C_i = \left[(r_{max} - r_{min}) \frac{\sum_{j=1}^{U^i} \sum_{k=1}^{U^{i.j}} \sum_{m=1}^{U^{i.j.k}} R_m^{i.j.k}}{\sum_{j=1}^{U^i} \sum_{k=1}^{U^{i.j}} U_{i.j.k}} + r_{min} \right]; i = 1, \dots, U \quad (3.23)$$

3. коефіцієнт відповідності $C_{i,j} \in \Re$ для *i*-ої зони безпеки та *j*-ї категорії безпеки

$$C_{i.j} = \left[(r_{max} - r_{min}) \frac{\sum_{k=1}^{U^{i.j}} \sum_{m=1}^{U^{i.j.k}} R_m^{i.j.k}}{\sum_{k=1}^{U^{i.j}} U_{i.j.k}} + r_{min} \right]; i = 1, \dots, U, j = 1, \dots, U^i \quad (3.24)$$

4. коефіцієнт відповідності $C_{i,j,k} \in R^-$ для *i*-ої зони безпеки, *j*-ї категорії безпеки та *k*-го класу контрзаходів.

$$C_{i.j.k} = \left[(r_{max} - r_{min}) \frac{\sum_{m=1}^{U^{i.j.k}} R_m^{i.j.k}}{U_{i.j.k}} + r_{min} \right]; \quad (3.25)$$

$$i = 1, \dots, U, j = 1, \dots, U^i, k = 1, \dots, U^{i.j} \quad ,$$

де $R_m^{\text{i.j.k}}$ – відповідь на m-е питання аудиту (1 або 0) щодо i-ої зони безпеки, j-ї категорії безпеки та k-го класу контрзаходів.

Коефіцієнт відповідності C розраховується на основі наявної бази знань (створеної з так званих «наборів анкет», що містять відповідним чином підібрані питання аудиту, віднесені до третього рівня, тобто категорій безпеки). У таблиці 3.3 наведено частину зразкової аудиторської анкети.

Таблиця 3.3 Частина зразкової аудиторської анкети категорії «Мережа політика контролю доступу»

11.1.1	Політика контролю доступу до мережі	Відповідь	
		Да	Ні
1.1.1-1	Чи існує обов'язкова процедура/процедури надання профілю (наприклад, відповідно до ролі) для певної групи та надання прав доступу до мережі для цієї групи?	1	
11.1.1-2	Чи існує суворий контроль процесу визначення профілів і прав доступу до мережі?		0
11.1.1-3	Чи проводиться щорічний аудит наданих профілів і прав доступу до мережі та способу керування ними?	1	

Визначення графа.

Формальне визначення графіка G, що представляє процес розрахунку значень системного ризику W для ресурсів/активів системної IS, представлено нижче.

Визначення 8. Нехай $G = (V, E)$, де множина вершин:

$$V = \{IS \cup A \cup scen(\overline{A,T}) \cup \overline{DP_{v_i}} \cup \overline{DI_{t_i}} \cup M_{pot} \cup M_{imp} \cup M \cup W\}, \quad (3.26)$$

і набір ребер відповідає таким умовам:

(1) $E \subseteq V \times V$,

(2) $(IS, a) \in E, for\ any\ a \in A$,

(3) $(a, s) \in E, for\ any\ a \in A\ and\ s \in S, if\ s \in scen(a)$,

(4) $\big(s, (s, dp)\big) \in E, for\ any\ s \in S\ and\ dp \in DP, if\ (s, dp) \in \overline{DP}$

(5) $\big(s, (s, di)\big) \in E, for\ any\ s \in S\ and\ di \in DI, if\ (s, di) \in \overline{DI}$

(6) $\Big((s, dp),\ \big(M^s_{pot}, W^s_{pot}\big)\Big) \in E, for\ any\ s \in S\ and\ dp \in DP, if\ (s, dp) \in \overline{DP}$

(7) $\Big((s, di),\ \big(M^s_{imp}, W^s_{imp}\big)\Big) \in E, for\ any\ s \in S\ and\ di \in DI, if\ (s, di) \in \overline{DI}$

(8) $\Big(\big(M^s_{pot}, W^s_{pot}\big), (M^s, W^s)\Big) \in E, for\ any\ s \in S$

(9) $\Big(\big(M^s_{imp}, W^s_{imp}\big), \big(M^{s,a}_{imp}, W^{s,a}_{imp}\big)\Big) \in E, for\ any\ (a, s) \in \overline{A \times S}$

(10) $\Big(\big(M^{s,a}_{imp}, W^{s,a}_{imp}\big), (M^{s,a}, W^{s,a})\Big) \in E, for\ any\ (a, s) \in \overline{A \times S}$

(11) $\big((M^{s,a}, W^{s,a}), W^a\big) \in E, for\ any\ (a, s) \in \overline{A \times S}$

Алгоритм

Алгоритм розрахунку величини ризику W для ресурсів/активів системної IS на основі графіка G є двочастковим і включає введення системних даних та обчислення значень для окремих параметрів (функцій):

1. введення системних даних:
   a) введіть набір активів/ресурсів A та їх значення $value_A(a)$;
   b) введіть набір уразливостей V та їх значення $value_V(v)$;
   c) введіть набір сценаріїв *scen*;
   d) ввести набір масивів M^s_{pot}, M^s_{imp}, $M^{s,a}_{imp}$, $M^{s,a}$;
2. побудова системного графіка та розрахунок значення:

a) визначити множину $\overline{A \times S}$;

b) обчислити значення W_{pot}^{s}, W_{imp}^{s}, $W_{imp}^{s,a}$, $W^{s,a}$;

c) обчислити значення W^{a};

d) розрахувати коефіцієнт відповідності C;

3.11 Висновки

Застосування технології IoT у розумних будинках відкриває як можливості, так і ризики для безпеки. Розумні будинки на основі IoT дуже вразливі до різних загроз безпеці як всередині, так і поза домом. Якщо безпека розумного дому або розумного пристрою буде порушена, конфіденційність, особиста інформація та навіть безпека користувача будуть під загрозою. Тому необхідно вжити відповідних заходів, щоб зробити розумні будинки більш безпечними та придатними для проживання.

На основі відомих методів, моделей та систем розроблено модель створення профілю загроз та вразливостей, яка дозволяє максимально описати всі відомості про критичний об’єкт та спрогнозувати можливі загрози та вразливості що б провести ретельний аналіз та розробити стратегію для запобігання або мінімізування можливих втрат.

4 ОЦІНКА РИЗИКІВ БЕЗПЕКИ СЕРЕДОВИЩА РОЗУМНОГО БУДИНКУ

4.1 Система профілювання загроз при керуванні розумним будинком

Бездротові розумні датчики стали дуже привабливими пристроями для моніторингу та відстеження рухомих об’єктів у програмах розумного дому; тому вони стали мішенню різних атак. Існують різні атаки на WSN, наприклад атаки, пов’язані з доступністю служб (атаки переливання, заглушення та повторне відтворення), мережевою маршрутизацією (несанкціоноване оновлення маршрутизації та атаки на червоточини) та автентифікацією вузлів (атаки підслуховування та імітації).

Хоча розумні будинки на основі IoT отримують багато переваг, ці розумні будинки сприйнятливі до різних атак. Особа може напряму атакувати пристрій взаємозв’язку (наприклад, шлюз) або польовий пристрій, використовуючи його мережевий або локальний комунікаційний інтерфейс (тобто атакуючи пристрій), і пристрій може бути видано за допомогою його несправного сертифіката.

Побутову техніку можна підключати до дротової або бездротової мережі через домашній шлюз. Атака на домашній шлюз може негайно призвести до атаки на всю домашню мережу, оскільки це точка, на якій можна встановити зовнішнє з’єднання.

Необхідно захищати розумні будинки від атак, як на рівні магістралі, так і на рівні управління, що походять як ззовні, так і зсередини розумного будинку. Атака може відбуватися на рівні трафіку, на рівні контролю або на рівні магістральної мережі. Пряма атака на точку підключення пристрою (наприклад, шлюз) або польовий пристрій може бути здійснена за допомогою його мережевого або локального комунікаційного інтерфейсу.

Наприклад, маніпулювання цінами на електроенергію може призвести до зменшення рахунку супротивника за рахунок користувача (тобто рахунок користувача збільшується). У дослідженні було запропоновано методику, яка може бути використана для ефективного виявлення спроби взлому та викрадення

інформації зібраної датчиками розумного будинку для використання у власних цілях.

З точки зору апаратного забезпечення IoT, пристрої IoT є мобільними і можуть надходити в дане інтелектуальне середовище з невідомого домену. Проблема в тому, що навіть відомий пристрій міг бути змінений під час його відсутності. Типи вразливостей безпеки включають злом домашнього пристрою, вірусну атаку, витік інформації, підробку вмісту та порушення конфіденційності.

Існують різні способи проникнення в розумні будинки. Залежно від намірів супротивника, будуть цікаві різні групи пристроїв розумного дому. Перші широкомасштабні атаки, швидше за все, будуть спрямовані на продукти групи контролюючих систем, оскільки вони найбільш схожі на існуючі цілі і підключені майже до будь-якого іншого розумного будинку.

Дослідження показало, що зловмисник має дві різні можливості отримати доступ до функцій контролю: мережеві атаки та атаки на пристрої. Під час мережевих атак зловмисник може спробувати перехопити, маніпулювати, сфабрикувати або перервати передані дані.

Атаки на пристрої можна класифікувати на атаки на програмне забезпечення, фізичні або інвазивні атаки та атаки на бічні канали. Крім того, існує ймовірність того, що зловмисник може замаскуватися під внутрішнього користувача через інтерактивне цифрове телебачення або отримати доступ до телевізора нелегально за допомогою інших засобів контролю побутової техніки.

У літературі є кілька досліджень оцінки ризику. Однак ці дослідження підкреслюють ризики для загальних систем Інтернету речей і не залежать від доменів застосування IoT. Загалом, оцінки ризиків, розроблені для архітектури IoT, можуть охоплювати три рівні Інтернету речей, але не обов’язково, щоб ці дослідження охоплювали ризики безпеки в розумних будинках через відсутність поведінки користувачів і міркувань фізичної безпеки в контексті IoT- розумні будинки на базі.

4.2 Результати застосування системи профілювання загроз при керуванні розумним будинком

Це дослідження зосереджено головним чином на безпеці інформаційних активів і на тому, де ця інформація існує під час проведення оцінки ризику безпеки середовища розумного дому. Майже всі важливі активи можна легко оцінити та обробити за допомогою інформаційних контейнерів. OCTAVE Allegro добре підходить для оцінки ризиків розумних будинків завдяки можливості мати контейнер для активів, який охоплює як кібер-, так і фізичну безпеку.

Використовуваний метод має вісім кроків, згрупованих у чотири основні фази (рисунок 3.1).

4.2.1 Фаза встановлення драйверів

Метою фази встановлення драйверів є створення основи для оцінки ризику інформаційних активів шляхом розробки набору критеріїв вимірювання ризику для розумного будинку. Ці критерії дають можливість оцінити ступінь впливу на зацікавлені сторони розумного дому в разі порушення інформаційних активів.

Крім розпізнавання масштабів впливу, необхідно визначити найбільш значущу зону впливу. Ці критерії відображають ряд сфер впливу, які важливі для мешканців розумного будинку.

Наприклад, сфери впливу можуть включати здоров’я та безпеку користувачів, фінанси, репутацію, а також закони та правила.

Критерії оцінки ризиків зображенні в таблиці 4.1.

Таблиця 4.1 – Критерії оцінки ризиків

	Низький	Середній	Високий
Критерій	Критерій оцінки ризиків – життя, здоров'я, безпека (пріоритет – 5)		
Життя (не комерційні стейкхолдери)	Жодних втрат або значної загрози для життя кінцевих користувачів.	Життю користувачів загрожує небезпека, але, отримавши медичну допомогу, вони одужають.	Втрата людського життя
Здоров’я (не комерційні стейкхолдери)	Погіршення здоров’я мінімальне, і таке, що негайно піддається лікуванню із відновленням на протязі декількох днів.	Тимчасове погіршення здоров'я користувачів.	Значне порушення здоров'я користувачів. Термін одужання більше одного місяця. Набуття хронічних захворювань.
Безпека (не комерційні стейкхолдери)	Безпека кінцевого споживача поставлена під сумнів	Мінімальний вплив на безпеку кінцевого споживача. Наявність адміністративного правопорушення	Безпека кінцевого споживача порушена. Наявність кримінального правопорушення
…	…	…	…

Кінець таблиці 4.1 – Критерії оцінки ризиків

Критерій	Критерій оцінки ризиків – штрафи та юридичні санкції (пріоритет – 1)		
Штрафи (комерційні стейкхолдери)	Стягнення штрафів у розмірі менше 100 тис. грн.	Стягнення штрафів у розмірі від 100 до 300 тис. грн.	Стягнення штрафів у розмірі більше 300 тис. грн.
Позови (комерційні стейкхолдери)	Реєстрація судових позовів на суму меншу за 100 тис. грн.	Реєстрація судових позовів на суму меншу від 100 до 300 тис. грн.	Реєстрація судових позовів на суму більше 300 тис. грн.
Розслідування (комерційні стейкхолдери)	Відсутність запитів від уряду чи інших слідчих установ	Запит на інформацію від уряду чи іншої слідчої установи	Уряд або інше слідча установа розпочинає поглиблене розслідування проти стейкхолдерів

4.2.2 Фаза створення профілю активів

Під час фази створення профілю активів, яка включає кроки 2 і 3, показані на рисунку 3.1, критичні інформаційні активи спочатку ідентифікуються, а потім профілюються (таблиця 4.2). У процесі профілювання встановлюються чіткі межі для активу та визначаються вимоги безпеки. Після цього визначаються всі місця, де актив зберігається, транспортується або обробляється. Крім того, слід визначити, де ці активи використовуються власниками розумних будинків або системами розумного дому, як доступ до цих активів і хто несе відповідальність за

ці активи. Логічні, технічні, фізичні та людські активи документуються (таблиця 4.3).

Таблиця 4.2 – Профіль критичного інформаційного об’єкту «інформація, зібрана пристроями (датчиками)»

(1) Критичний об’єкт Що є критично важливим інформаційним об’єктом?	(2) Обґрунтування вибору Чому цей інформаційний об’єкт є важливим для організації?	(3) Опис Який узагальнюючий опис цього інформаційного об’єкту?
Інформація, зібрана пристроями (датчиками)	Даний інформаційний об’єкт є важливою складовою у процесі функціонування системи розумного будинку та є основним джерелом вхідних даних про стан навколишнього середовища. Компрометація цього інформаційного об’єкту може призвести до порушення функціонування системи та прояву ризиків, пов’язаних, наприклад, із пожежею або повінню.	Цей інформаційний об’єкт визначає вихідні дані з пристроїв, наприклад він визначає, які дії будуть виконувати виконавчі механізми. Ця інформація визначає безпеку та зручність розумного будинку, які є головними цілями системи розумного будинку.

Продовження таблиці 4.2 – Профіль критичного інформаційного об’єкту «інформація, зібрана пристроями (датчиками)»

(4) Власник(и) Кому належить цей інформаційний актив?		
Власником цього інформаційного об’єкту є система розумного будинку, на якій лежить основна відповідальність за дану інформацію		
(5) Вимоги безпеки Які вимоги безпеки до цього інформаційного активу?		
Конфіденційність	Переглянути цей інформаційний ресурс можуть лише авторизовані працівники:	Доступом до цього інформаційного об’єкту володіють лише мешканці розумного будинку. Також цю інформацію можуть потребувати постачальники послуг для надання належних послуг відповідно до договорів
Цілісність	Тільки авторизовані користувачі можуть модифікувати цей інформаційний актив:	Тільки мешканці мають право маніпулювати цим інформаційним об’єктом.

Кінець таблиці 4.2 – Профіль критичного інформаційного об’єкту «інформація, зібрана пристроями (датчиками)»

Доступність	Даний інформаційний об’єкт має бути у розпорядженні цих користувачів протягом 24 годин, 7 днів на тиждень.	Даний об’єкт має бути готовий до використання, коли це буде потрібно мешканцям або іншим спорідненим системам. Цей інформаційний об’єкт повинен бути доступним цілодобово для забезпечення функціонування системи розумного будинку. Нетривале відключення не повинно порушити функціонування системи, в той час як тривале переривання (більше 8 годин) спричинило б значні проблеми.
(6) Найважливіші вимоги безпеки Яка найважливіша вимога безпеки для цього інформаційного активу?		
Конфіденційність	Цілісність	Доступність

Таким чином, визначаються слабкі місця, на яких вимоги безпеки, з точки зору тріади конфіденційності, цілісності та доступності, інформаційного активу можуть бути скомпрометовані.

Таблиця 4.3 – Контейнери інформаційного об’єкту «інформація, зібрана пристроями (датчиками)»

Технічні інформаційні контейнери		
№	Опис контейнеру	Власник
Внутрішні		
1	Файл даних	Власник розумного будинку/ мешканці
2	База даних: інформаційний ресурс знаходиться на серверах баз даних і веб-серверах.	Власник розумного будинку/ мешканці
3	Внутрішня мережа розумного будинку. Вся інформація поширюється по даній мережі.	Власник розумного будинку/ мешканці
4	Пристрої користувача	Мешканці
Зовнішні		
5	Інтернет: ці інформаційні об’єкти поширюються Інтернетом щоразу, коли кінцевий користувач під’єднується до системи розумного будинку поза межами дому через пристрої користувача (смартфон, планшет тощо).	–
Фізичні інформаційні контейнери		
Внутрішні		
1	Паперові носії	Власник розумного будинку/ мешканці
2	Носії інформації	
Зовнішні		
–	–	–

Кінець таблиці 4.3 – Контейнери інформаційного об’єкту «інформація, зібрана пристроями (датчиками)»

Людські інформаційні контейнери		
Внутрішні		
1	Члени сім’ї	мешканці
Зовнішні		
2	Гості	Гості
3	Сервісний персонал	Сервісний персонал

4.2.3 Фаза визначення загроз

На цьому етапі, який включає кроки 4 і 5 (рисунок 3.1), основна увага приділяється ідентифікації загроз безпеці від ідентифікованих активів у контексті місць, де інформаційний актив зберігається, транспортується або обробляється. Уразливі місця безпеки або проблемні зони визначаються та розширюються на сценарії загроз, які в подальшому формують властивості загрози.

Нарешті, виділено конкретні загрози, які можуть негативно вплинути на безпеку активів.

4.2.4 Фаза пом'якшення ризику

На етапі пом'якшення ризику, який включає кроки 6, крок 7 і крок 8, показані на рисунку 3.1, ризики кібер та фізичної безпеки щодо інформаційних активів визначаються шляхом визначення того, як сценарії загроз можуть вплинути на систему розумного дому. Оцінка здійснюється шляхом аналізу впливу або наслідків цих загроз на середовище розумного дому (таблиця 4.4). Нарешті, для кожного з виявлених ризиків визначається стратегія пом’якшення. Ризики аналізуються і присвоюється якісне значення, щоб описати ступінь впливу на користувачів розумного дому. Значення впливу виводиться з критеріїв оцінки ризику, а інформація про оцінку використовується для ранжирування

ідентифікаторів ризиків і визначення пріоритетності пропонованих дій з пом'якшення.

Таблиця 4.4 – Оцінка ризику для інформаційного об’єкту «інформація, зібрана пристроями (датчиками)»

Оцінка ризику для інформаційного об’єкту	Загроза	Інформаційний об’єкт	Інформація, зібрана пристроями (датчиками)
		Сфера занепокоєння	1) Зміна показників датчика газу може призвести до хибного реагування на наявність газу в приміщенні, що може позначитись на здоров’ї та житті мешканців 2) Отримання даних із датчика руху можна використати для визначення присутності мешканців будинку. 3) Зчитування стану замків дверей та систем сигналізації можна використати, щоб визначити, коли розумний будинок зайнятий. 4) DoS атаки на рівень сприйняття (компрометація каналу зв’язку) систем розумного будинку продукує не можливість сприйняття фізичних параметрів датчиками, що тим самим унеможливлює виявлення таких ризиків, як пожежа, повінь, несподівані рухи тощо.
		(1) Дійова особа Хто здійснюватиме вплив на інформаційний об’єкт створюючи загрозу безпеці?	Зловмисник (хакер, недобросовісний постачальник програмних та апаратних засобів)

Продовження таблиці 4.4 – Оцінка ризику для інформаційного об’єкту «інформація, зібрана пристроями (датчиками)»

<table>
<tr><td rowspan="8">Оцінка ризику для інформаційного об’єкту</td><td rowspan="6">Загроза</td><td>(2) Засоби
Яким чином дійова особа здійснить це? Що вони повинні зробити для цього?</td><td colspan="3">Засоби взлому
Вразливості в апаратному забезпеченні</td></tr>
<tr><td>(3) Мотив
Який виграш отримає дійова особа здійснивши порушення безпеки?</td><td colspan="3">Фінансова вигода, задоволення персональних амбіцій.</td></tr>
<tr><td>(4) Результат
Яким чином це відобразиться на інформаційному об’єкті?</td><td colspan="3">○ Розкриття ○ Знищення
• Зміна • Переривання</td></tr>
<tr><td>(5) Вимоги безпеки
Яким чином будуть порушені вимоги безпеки інформаційного об’єкту?</td><td colspan="3">Лише авторизовані члени розумного будинку повинні мати доступ до цієї інформації та змінювати її.</td></tr>
<tr><td>(6) Імовірність
Яка імовірність відтворення подібного впливу?</td><td>• Висока</td><td>○ Середня</td><td>○ Низька</td></tr>
<tr><td colspan="2">(7) Наслідки
Які будуть наслідки для організації або власника інформаційного об’єкта при порушенні вимог безпеки?</td><td colspan="3">(8) Важкість
Наскільки серйозними є ці наслідки для організації чи власника об’єкту в залежності від зони впливу?</td></tr>
</table>

Продовження таблиці 4.4 – Оцінка ризику для інформаційного об’єкту «інформація, зібрана пристроями (датчиками)»

Оцінка ризику для інформаційного об’єкту	У випадку порушення вимог безпеки для цього інформаційного об’єкту система розумного будинку не в змозі буде відстежувати та контролювати критично важливі показники давачів, що може призвести до негативних наслідків, пов’язаних як із фізичною природою (пожежа, підтоплення), так із людським фактором (проникнення, крадіжка речей). В обох випадках прояви негативних наслідків можуть призвести до великих фінансових втрат.	Зони впливу	Значення	Оцінка
		Репутація та довіра клієнтів (4)	Висока (3)	4*3 = 12
		Фінансова (3)	Висока (3)	9
		Продуктивність (2)	Низька (1)	2
		Життя, здоров'я, безпека (5)	Висока (3)	15
		Штрафи та юридичні санкції (1)	Низька (1)	1
	Відносне значення оцінки ризику			39

(9) Пом’якшення ризиків

Виходячи з загальної оцінки цього ризику, які дії слід вжити?

○ Прийняти	○ Відкласти	• Пом’якшити	○ Передати

Щодо ризиків, які було вирішено пом’якшити, слід виконати наступні дії.

Якого контейнера будуть стосуватись дії?	Який адміністративний, технічний та фізичний контроль слід застосували до цього контейнера? Який залишковий ризик все ще буде прийнято організацією?
Технічний	Обмежити доступність мережевого трафіку лише для авторизованих користувачів; використання протоколів передачі даних із шифруванням (наприклад, SSL/TLS) а також використовувати захищену віртуальну приватну мережу (VPN)

Кінець таблиці 4.4 – Оцінка ризику для інформаційного об’єкту «інформація, зібрана пристроями (датчиками)»

Фізичний	Зберігайте всі фізичні дані в надійному місці. Регулярне оновлення апаратного забезпечення; створення резервних копій всієї важливої інформації.
Люди	Інформування мешканців стосовно безпечного управління розумним будинком а також розробка програми навчання безпеці для мешканців розумного будинку

4.3 Висновки

Проведено оцінку ризиків інформаційної безпеки системи розумного будинку із залученням методології OCTAVE Allegro для інформаційного об’єкту, що представляє інформацію, зібрану датчиками розумного будинку.

Представлена тут формальна модель відповідає рекомендаціям та стандартам OECP. Переваги цієї моделі в тому, що вона універсальна і відкрита. Крім того, представлена модель дозволяє вільно вибирати будь-яку схему для класифікації активів, потенційних можливостей, впливу та ризиків.

У запропонованій моделі сценарії загроз будуються шляхом узгодження ресурсів вразливостей і загроз. Ці сценарії, у свою чергу, пов’язані з контрзаходами, які підлягають аудиту. Такий підхід значно прискорює процес аналізу ризиків і зменшує його навантаження. Як наслідок, основною перевагою запропонованого методу (у порівнянні з іншим, що використовується в даний час) є значно вищий рівень автоматизації роботи аудитора, тобто весь процес аудиту зводиться до виявлення та класифікації ресурсів та інших видів діяльності. (включаючи формування аудиторських анкет) обмежується лише підтвердженням пропозицій, запропонованих аудитором.

ВИСНОВКИ

За результатами проведеного дослідження запропоновано систему профілювання загроз при керуванні розумним будинком. Запропонована методологія забезпечує оптимізацію процесу оцінки ризиків інформаційної безпеки, щоб організація могла отримати достатні результати з невеликими вкладами часу, людей та інших обмежених ресурсів..

В першому розділі представлений опис відомих методів, моделей та систем побудови профілів загроз та вразливостей для систем що використовують IoT. Проведено аналіз та порівняння методів, моделей та систем та вибрано методологію Octave Allegro як базову для проведення дослідження.

В другому розділі розглянуто концепцію Інтернету речей, наведено загальну архітектуру IoT системи та розумного будинку в цілому. Проведено огляд функціональних можливостей та модель процесу функціонування розумного будинку.

В третьому розділі запропоновано модель профілювання загроз та вразливостей а також оцінки ризиків в розумному будинку, що базується на використанні моделі з методології Octave Allegro. В результаті виконання моделі буде отримано оцінку можливої загрози та розроблена стратегія запобігання або ж пом’якшення впливу цієї загрози. Перевагою моделі є її надійність, яка забезпечує достатньо точний результат.

У четвертому розділі на основі моделі профілювання загроз та вразливостей в розумному будинку запропоновано удосконалення системи профілювання загроз при керування розумним будинком, яка застосовує критерії які направленні на специфіку розумного будинку, його архітектуру та функціональні можливості, що дозволило підвищити ступінь автоматизації процесів профілювання інформаційних активів та загроз які мають на меті зашкодити або оволодіти цими активами у розумних будинках.

За темою дипломної роботи опубліковано статтю у фахову виданні Computer Systems and Information Technologies:

Morozova O., Tetskyi A., Nicheporuk A., Kruvak D., Tkachov V. Smart Home System Security Risk Assessment // International Scientific Journal «Computer Systems and Information Technologies». 2021. № 3. Pp. 81-88.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. V. Mavroeidis and S. Bromander, Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence, *2017 European Intelligence and Security Informatics Conference (EISIC)*, pp. 91-98, 2017, doi: 10.1109/EISIC.2017.20.

2. O. Jacq, D. Brosset, Y. Kermarrec and J. Simonin, Cyber attacks real time detection: towards a Cyber Situational Awareness for naval systems, *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, pp. 1-2, 2019, doi: 10.1109/CyberSA.2019.8899351.

3. S. Yang, J. Wang, J. Zhang and H. Li, Cyber Threat Detection and Application Analysis, *2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pp. 46-49, 2016, doi: 10.1109/CyberC.2016.17.

4. A. Khalid, A. Zainal, M. A. Maarof and F. A. Ghaleb, Advanced Persistent Threat Detection: A Survey, *2021 3rd International Cyber Resilience Conference (CRC)*, pp. 1-6, 2021, doi: 10.1109/CRC50527.2021.9392626.

5. J. Ali, Intrusion Detection Systems Trends to Counteract Growing Cyber-Attacks on Cyber-Physical Systems, *2021 22nd International Arab Conference on Information Technology (ACIT)*, pp. 1-6, 2021, doi: 10.1109/ACIT53391.2021.9677429.

6. A. Rao, N. Carreón, R. Lysecky and J. Rozenblit, Probabilistic Threat Detection for Risk Management in Cyber-physical Medical Systems, in *IEEE Software*, vol. 35, no. 1, pp. 38-43, January/February 2018, doi: 10.1109/MS.2017.4541031.

7. S. ur Rehman and V. Gruhn, An approach to secure smart homes in cyber-physical systems/Internet-of-Things, *2018 Fifth International Conference on Software Defined Systems (SDS)*, pp. 126-129, 2018, doi: 10.1109/SDS.2018.8370433.

8. K. Karimi and S. Krit, Smart home-Smartphone Systems: Threats, Security Requirements and Open research Challenges, *2019 International Conference of Computer Science and Renewable Energies (ICCSRE)*, pp. 1-5, 2019, doi: 10.1109/ICCSRE.2019.8807756.

9. J. Bugeja, A. Jacobsson and P. Davidsson, An analysis of malicious threat agents for the smart connected home, *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 557-562, 2017, doi: 10.1109/PERCOMW.2017.7917623.

10. M. N. Anwar, M. Nazir and K. Mustafa, Security threats taxonomy: Smart-home perspective, *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*, pp. 1-4, 2017, doi: 10.1109/ICACCAF.2017.8344666.

11. S. G. Abbas, S. Zahid, F. Hussain, G. A. Shah and M. Husnain, A Threat Modelling Approach to Analyze and Mitigate Botnet Attacks in Smart Home Use Case, *2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE)*, pp. 122-129, 2020, doi: 10.1109/BigDataSE50710.2020.00024.

12. A. Gai, S. Azam, B. Shanmugam, M. Jonkman and F. De Boer, Categorisation of security threats for smart home appliances, *2018 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1-5, 2018, doi: 10.1109/ICCCI.2018.8441213.

13. A. M. Gamundani, A. Phillips and H. N. Muyingi, An Overview of Potential Authentication Threats and Attacks on Internet of Things(IoT): A Focus on Smart Home Applications, *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 50-57, 2018, doi: 10.1109/Cybermatics_2018.2018.00043.

14. M. Ibrahim and I. Nabulsi, Security Analysis of Smart Home Systems Applying Attack Graph, *2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)*, pp. 230-234, 2021, doi: 10.1109/WorldS451998.2021.9514050.

15. S. E. Bondarev and A. S. Prokhorov, Analysis of internal threats of the system “smart home” and assessment of ways to prevent them, *2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp. 788-790, 2017, doi: 10.1109/EIConRus.2017.7910676.

16. S. Erfani, M. Ahmadi and L. Chen, The Internet of Things for smart homes: An example, *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, pp. 153-157, 2017, doi: 10.1109/IEMECON.2017.8079580.

17. A. Qashlan, P. Nanda and X. He, Security and Privacy Implementation in Smart Home: Attributes Based Access Control and Smart Contracts, *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 951-958, 2020, doi: 10.1109/TrustCom50675.2020.00127.

18. G. Dorai, E. A. Williams, H. Chi and R. A. Alo, "Is your Smart Home a Secure Home?" - Analysis of Smart Home Breaches and an Approach for Vulnerability Analysis and Device Isolation, *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, pp. 1-6, 2020, doi: 10.1109/WF-IoT48130.2020.9221420.

19. G. Kavallieratos, V. Gkioulos and S. K. Katsikas, Threat Analysis in Dynamic Environments: The Case of the Smart Home, *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 234-240, 2019, doi: 10.1109/DCOSS.2019.00060.

20. J. Ryoo, S. Tjoa and H. Ryoo, An IoT Risk Analysis Approach for Smart Homes (Work-in-Progress), *2018 International Conference on Software Security and Assurance (ICSSA)*, pp. 49-52, 2018, doi: 10.1109/ICSSA45270.2018.00021.

21. A. D. Prajanti and K. Ramli, A Proposed Framework for Ranking Critical Information Assets in Information Security Risk Assessment Using the OCTAVE Allegro Method with Decision Support System Methods, *2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC)*, pp. 1-4, 2019, doi: 10.1109/ITC-CSCC.2019.8793421.

22. K. Abdullah, I. N. Isnainiyah and M. I. Faried, Risk Management Analysis on Organizational Website Using Octave Allegro Method, *2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*, pp. 201-206, 2020, doi: 10.1109/ICIMCIS51567.2020.9354298.

23. A. Yeboah-Ofori, S. Islam and E. Yeboah-Boateng, Cyber Threat Intelligence for Improving Cyber Supply Chain Security, *2019 International Conference*

on Cyber Security and Internet of Things (ICSIoT), pp. 28-33, 2019, doi: 10.1109/ICSIoT47925.2019.00012.

24. M. H. Mohd Pakhari, N. Jamil, M. E. Rusli and A. A. Abdul Rahim, Implementation of Token Parsing Technique for Regex Based Classification of Unstructured Data for Cyber Threat Analysis, *2020 8th International Conference on Information Technology and Multimedia (ICIMU)*, pp. 395-398, 2020, doi: 10.1109/ICIMU49871.2020.9243415.

25. S. Zhao, S. Li, L. Qi and L. D. Xu, Computational Intelligence Enabled Cybersecurity for the Internet of Things, in *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 4, no. 5, pp. 666-674, Oct. 2020, doi: 10.1109/TETCI.2019.2941757.

26. M. Sarrab and S. M. Alnaeli, Critical Aspects Pertaining Security of IoT Application Level Software Systems, *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 960-964, 2018, doi: 10.1109/IEMCON.2018.8614993.

27. Bandyopadhyay, S.; Sengupta, M.; Maiti, S.; Dutta, S. A Survey of Middleware for Internet of Things. *In Recent Trends in Wireless and Mobile Networks, Proceedings of the Third International Conferences, WiMo 2011 and CoNeCo 2011*, pp. 288–296, Ankara, Turkey, 26–28 June 2011; Özcan, A., Zizka, J., Nagamalai, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2011.

28. Papadopoulos, K.; Zahariadis, T.; Leligou, N.; Voliotis, S. Sensor Networks Security Issues in Augmented Home Environment. *In Proceedings of the 2008 IEEE International Symposium on Consumer Electronics*, pp. 1–4, Las Vegas, NV, USA, 9–13 January 2008.

29. J. Shams, N. A. G. Arachchilage and J. M. Such, Vision: Why Johnny Can't Configure Smart Home? A Behavioural Framework for Smart Home Privacy Configuration, *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 184-189, 2020, doi: 10.1109/EuroSPW51379.2020.00033.

30. P. Zdankin and T. Weis, Longevity of Smart Homes, *2020 IEEE International Conference on Pervasive Computing and Communications Workshops*

(PerCom Workshops), pp. 1-2, 2020, doi: 10.1109/PerComWorkshops48775.2020.9156155.

31. H. Chi, Q. Zeng, X. Du and J. Yu, Cross-App Interference Threats in Smart Homes: Categorization, Detection and Handling, *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 411-423, 2020, doi: 10.1109/DSN48063.2020.00056.

32. F. James, I. Ray and D. Medhi, Situational Awareness for Smart Home IoT Security via Finite State Automata Based Attack Modeling, *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, pp. 61-69, 2021, doi: 10.1109/TPSISA52974.2021.00007.

33. A. Sivanathan, D. Sherratt, H. H. Gharakheili, V. Sivaraman and A. Vishwanath, Low-cost flow-based security solutions for smart-home IoT devices, *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1-6, 2016, doi: 10.1109/ANTS.2016.7947781.

34. M. M. Rathore, E. Bentafat and S. Bakiras, Smart Home Security: A Distributed Identity-Based Security Protocol for Authentication and Key Exchange, *2019 28th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1-9, 2019, doi: 10.1109/ICCCN.2019.8847034.

35. A. Saha, S. Rahman, M. Pipattanasomporn and M. Kuzlu, On security of a home energy management system, *IEEE PES Innovative Smart Grid Technologies, Europe*, pp. 1-5, 2014, doi: 10.1109/ISGTEurope.2014.7028872.

36. V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli and O. Mehani, Network-level security and privacy control for smart-home IoT devices, *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 163-167, 2015, doi: 10.1109/WiMOB.2015.7347956.

37. J. Chen and Q. Zhu, Security as a Service for Cloud-Enabled Internet of Controlled Things Under Advanced Persistent Threats: A Contract Design Approach, in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2736-2750, Nov. 2017, doi: 10.1109/TIFS.2017.2718489.

38. A. Kaur and G. Singh, Encryption Algorithms based on Security in IoT (Internet of Things), *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*, pp. 482-486, 2021, doi: 10.1109/ISPCC53510.2021.9609495.

39. G. Spanos et al., A Lightweight Cyber-Security Defense Framework for Smart Homes, *2020 International Conference on INnovations in Intelligent SysTems and Applications (INISTA)*, pp. 1-7, 2020, doi: 10.1109/INISTA49547.2020.9194689.

40. R. Czechowski, Cyber-physical security for Low-Voltage Smart Grids HAN security within Smart Grids, *2015 16th International Scientific Conference on Electric Power Engineering (EPE)*, pp. 77-82, 2015, doi: 10.1109/EPE.2015.7161077.

41. A. J. Alam Majumder, C. B. Veilleux and J. D. Miller, A Cyber-Physical System to Detect IoT Security Threats of a Smart Home Heterogeneous Wireless Sensor Node, in *IEEE Access*, vol. 8, pp. 205989-206002, 2020, doi: 10.1109/ACCESS.2020.3037032.

42. A. Seeam, O. S. Ogbeh, S. Guness and X. Bellekens, Threat Modeling and Security Issues for the Internet of Things, *2019 Conference on Next Generation Computing Applications (NextComp)*, pp. 1-8, 2019, doi: 10.1109/NEXTCOMP.2019.8883642.

43. M. AbuNaser and A. A. A. Alkhatib, Advanced survey of Blockchain for the Internet of Things Smart Home, *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, pp. 58-62, 2019, doi: 10.1109/JEEIT.2019.8717441.

44. H. H. Al Oliwi, Z. A. Husain and R. Rafeh, Integrating Blockchain and Internet of Things for Smart Homes, *2021 Computing, Communications and IoT Applications (ComComAp)*, pp. 77-82, 2021, doi: 10.1109/ComComAp53641.2021.9652936.

45. H. Nguyen-An, T. Silverston, T. Yamazaki and T. Miyoshi, Generating IoT Traffic in Smart Home Environment, *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1-2, 2020, doi: 10.1109/CCNC46108.2020.9045343.

46. T. Nagamani, W. H. Beniga, K. S. Dhanish and A. Sherine Benitta, Anti-Theft Monitoring for a Smart Home, *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 76-82, 2022, doi: 10.1109/ICSSIT53264.2022.9716311.

47. D. Meyer, J. Haase, M. Eckert and B. Klauer, A threat-model for building and home automation, *2016 IEEE 14th International Conference on Industrial Informatics (INDIN)*, pp. 860-866, 2016, doi: 10.1109/INDIN.2016.7819280.

48. Y. Ashibani and Q. H. Mahmoud, "User Authentication for Smart Home Networks Based on Mobile Apps Usage," 2019 28th International Conference on Computer Communication and Networks (ICCCN), 2019, pp. 1-6, doi: 10.1109/ICCCN.2019.8847149.

49. E. Y. Güven and A. Y. ÇAMURCU, Physical Attack Detection for Smart Objects, *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, pp. 1-5, 2018, doi: 10.1109/IDAP.2018.8620791.

50. A. Sivanathan, F. Loi, H. H. Gharakheili and V. Sivaraman, Experimental evaluation of cybersecurity threats to the smart-home, *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1-6, 2017, doi: 10.1109/ANTS.2017.8384143.

51. T. Hussain, C. Nugent, A. Moore and J. Liu, An Analysis of the Impact of Uncertainty on the Internet of Things: A Smart Home Case Study, *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pp. 1916-1921, 2019, doi: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00336.

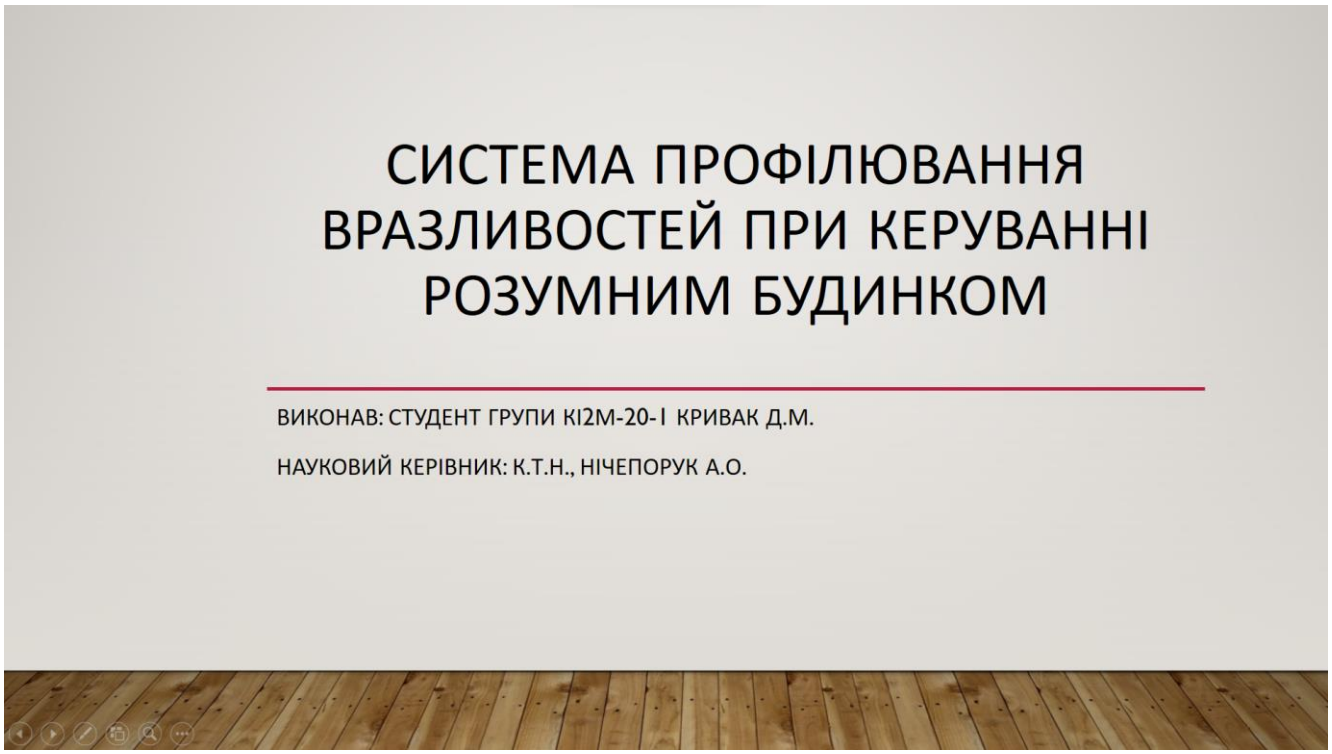
52. D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri and G. Baldini, "Security and privacy issues for an IoT based smart home," 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017, pp. 1292-1297, doi: 10.23919/MIPRO.2017.7973622.

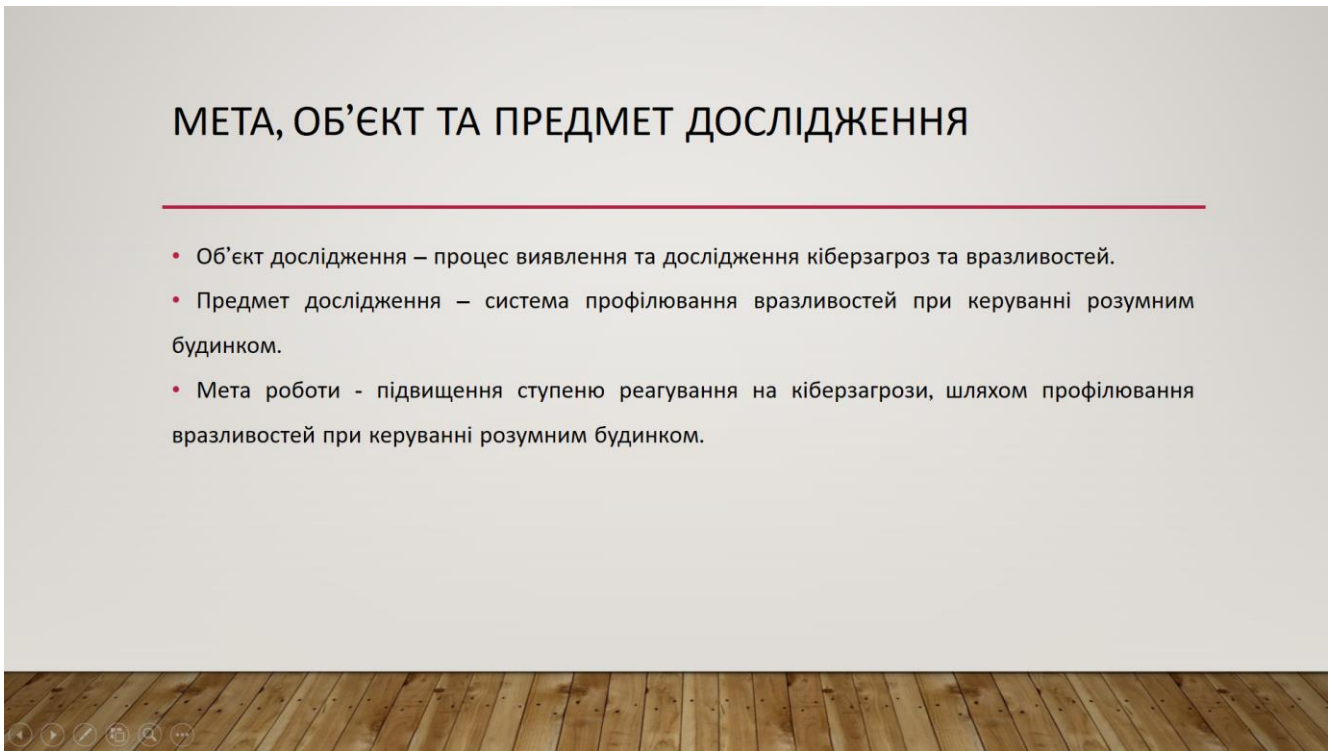
53. A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger and A. S. Uluagac, A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications, in *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1125-1159, Secondquarter 2021, doi: 10.1109/COMST.2021.3064507.

ДОДАТОК А

(обов’язковий)

Презентація доповіді





НАУКОВА НОВИЗНА

- Удосконалено модель побудови профілів загроз при керуванні розумним будинком, яка на відмінну від відомих залучає враховує особливості архітектури розумного будинку та залучає методологію оцінки ризиків OCTAVE, із обрахунком відносної оцінки ризику, що дозволило розробити профілі загроз та вразливостей для підвищення стійкості проектованих систем розумних будинків.
- Набула подальшого розвитку формалізація моделі інформаційної системи, яка на відмінну від відомих розглядає набір сценаріїв ризику, що дозволило провести розрахунок ризиків інформаційної системи.

ПОСТАНОВКА ЗАДАЧІ

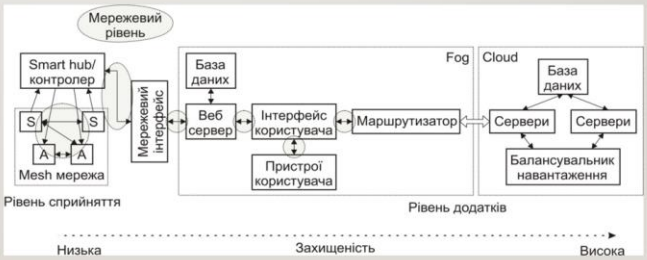
- Бездротові розумні датчики стали дуже привабливими пристроями для моніторингу та відстеження рухомих об'єктів у програмах розумного будинку; тому вони стали мішенню різних атак. Існують різні атаки на WSN, наприклад атаки, пов'язані з доступністю служб, мережевою маршрутизацією та автентифікацією.
- Тому постає задача дослідити архітектуру та функціональні можливості автоматизованих систем керування розумним будинком а також розробити систему профілювання загроз та оцінки ризиків в розумному будинку що дозволить проводити швидкий та доволі точний аналіз можливих загроз та вразливостей для подальшого реагування та удосконалення безпеки розумного будинку.

ПОСТАНОВКА ЗАДАЧІ

- Це дослідження зосереджено головним чином на безпеці інформаційних активів і на тому, де ця інформація існує під час проведення оцінки ризику безпеки середовища розумного дому. Майже всі важливі активи можна легко оцінити та обробити за допомогою інформаційних контейнерів. OCTAVE Allegro добре підходить для оцінки ризиків розумних будинків завдяки можливості мати контейнер для активів, який охоплює як кібер-, так і фізичну безпеку.
- Використовуваний метод має вісім кроків, згрупованих у чотири основні фази.

АРХІТЕКТУРА ТА ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ АВТОМАТИЗОВАНИХ СИСТЕМ КЕРУВАННЯ РОЗУМНИМ БУДИНКОМ

- Архітектуру системи Інтернету речей, і зокрема розумного будинку, можна представити через три логічні рівні: рівень сприйняття, мережевий рівень та рівень додатків.



РІВЕНЬ СПРИЙНЯТТЯ

- Найбільш наближеним до фізичного середовища рівнем в архітектурі розумного будинку є рівень сприйняття. Головними функціями даного рівня є збір інформації про стан фізичного середовища та реалізація механізмів впливу на нього. Покладені функції реалізуються за допомогою множини датчиків та виконавчих механізмів відповідно. Інформація, яку збирають датчики залежить від природи фізичного середовища та може стосуватись розташування, змін у повітрі та навколишньому середовищі, руху, вібрації тощо.

РІВЕНЬ СПРИЙНЯТТЯ

- Захищеність даного рівня в системі розумного будинку є найнижчою, що «приваблює» зловмисників до проведення атак на пристрої розумного будинку.
- Найбільш поширеними загрозами безпеки даного рівня сприйняття є:
  - Підслуховування
  - Захоплення вузла
  - Фальшивий вузол
  - Повторна атака
  - Атаки по часу

МЕРЕЖЕВИЙ РІВЕНЬ

- Мережевий рівень виконує транспортну функцію для передачі інформації всередині розумного будинку та є містком між рівнем сприйняття та рівнем додатків. Він передає інформацію, зібрану з фізичних об'єктів, за допомогою датчиків. Носій для передачі може бути бездротовим або дротовим. Він також бере на себе відповідальність за з'єднання розумних речей, мережевих пристроїв та мереж один з одним.

МЕРЕЖЕВИЙ РІВЕНЬ

- Наявність комунікаційної складової робить даний рівень чутливим до атак з боку зловмисників. Він має помітні проблеми безпеки щодо цілісності та автентифікації інформації, яка передається по мережі. Поширеними загрозами безпеки та проблемами для мережевого рівнів є:
  - Атака відмови в обслуговуванні (DoS)
  - Атака "Людина посередині"
  - Атака на сховище даних
  - Експолойт

РІВЕНЬ ДОДАТКІВ

- Прикладний рівень є найвищим рівнем у логічній ієрархії IoT та визначає всі додатки, які використовують технологію IoT або в яких розгорнуто IoT. Кінцевою областю застосування IoT можуть бути розумні будинки, розумні міста, сфера охорона здоров'я, тощо. Його основне призначення – надання послуг додаткам. Послуги можуть бути різними для кожної програми, оскільки послуги залежать від інформації, яку збирають датчики.

РІВЕНЬ ДОДАТКІВ

- На рівні додатків є багато проблем, в яких безпека є ключовим питанням. Зокрема, коли Інтернет речей використовується для створення розумного будинку, він створює багато загроз та вразливостей зсередини та ззовні. При реалізації надійної безпеки в розумному будинку на основі Інтернету речей, однією з основних проблем є те, що пристрої, що використовуються в розумних будинках, мають слабку обчислювальну потужність та малий обсяг пам'яті. Поширеними загрозами безпеки та проблемою прикладного рівня є:
  - Міжсайтовий скриптинг
  - Атака шкідливого коду

ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ АВТОМАТИЗОВАНИХ СИСТЕМ КЕРУВАННЯ РОЗУМНИМ БУДИНКОМ

- Розумний дім — це будинок, побудований із системами автоматизації, які дозволяють людям дистанційно керувати освітленням, безпекою, розвагами тощо за допомогою телефонів чи комп'ютерів. Кілька розумних систем тепер також включають штучний інтелект. щоб додати інтелектуальні виявлення та розпізнавання образів для подальшої оптимізації споживання.

ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ АВТОМАТИЗОВАНИХ СИСТЕМ КЕРУВАННЯ РОЗУМНИМ БУДИНКОМ

- Будь-який пристрій Інтернету речей має такі функції:
  - Освітлення (налаштування роботи освітлення)
  - Безпека (керування постановкою та зняттям сигналізації)
  - Температура (керування опаленням та охолодженням будинку за допомогою функцій, що стосуються часу та параметрів)
  - Прилади в будинку (керування живленням усіх побутових приладів)
  - Розваги (керування музичної системи або телевізором)
  - Стан системи (можливість перевірити поточний стан системи)
  - Виявлення транспортних засобів
  - Налаштування телефону
  - Будильник (можливість налаштування набору звуків пробудження від більш приємних звуків до більш пронизливих типів)

ПРОФІЛЮВАННЯ ЗАГРОЗ ТА ОЦІНКА РИЗИКІВ. ФАЗА ВСТАНОВЛЕННЯ ДРАЙВЕРІВ

- Метою фази встановлення драйверів є створення основи для оцінки ризику інформаційних активів шляхом розробки набору критеріїв вимірювання ризику для розумного будинку. Ці критерії дають можливість оцінити ступінь впливу на зацікавлені сторони розумного дому в разі порушення інформаційних активів.
- Крім розпізнавання масштабів впливу, необхідно визначити найбільш значущу зону впливу. Ці критерії відображають ряд сфер впливу, які важливі для мешканців розумного будинку.
- Наприклад, сфери впливу можуть включати здоров'я та безпеку користувачів, фінанси, репутацію, а також закони та правила.

ПРОФІЛЮВАННЯ ЗАГРОЗ ТА ОЦІНКА РИЗИКІВ. ФАЗА ВСТАНОВЛЕННЯ ДРАЙВЕРІВ. (КРИТЕРІЇ ОЦІНКИ РИЗИКІВ)

	Низький	Середній	Високий
Критерій	Критерій оцінки ризиків – життя, здоров'я, безпека (пріоритет – 5)		
Життя (не комерційні стейкхолдери)	Жодних втрат або значної загрози для життя кінцевих користувачів.	Життю користувачів загрожує небезпека, але, отримавши медичну допомогу, вони одужають.	Втрата людського життя .
Здоров'я (не комерційні стейкхолдери)	Погіршення здоров'я мінімальне, і таке, що негайно піддається лікуванню із відновленням на протязі декількох днів.	Тимчасове погіршення здоров'я користувачів.	Значне порушення здоров'я користувачів. Термін одужання більше одного місяця. Набуття хронічних захворювань.

ПРОФІЛЮВАННЯ ЗАГРОЗ ТА ОЦІНКА РИЗИКІВ. ФАЗА ВСТАНОВЛЕННЯ ДРАЙВЕРІВ. (КРИТЕРІЇ ОЦІНКИ РИЗИКІВ)

	Низький	Середній	Високий
Безпека (не комерційні стейкхолдери)	Безпека кінцевого споживача поставлена під сумнів.	Мінімальний вплив на безпеку кінцевого споживача. Наявність адміністративного правопорушення.	Безпека кінцевого споживача порушена. Наявність кримінального правопорушення.
…	…	…	…
Критерій	Критерій оцінки ризиків – штрафи та юридичні санкції (пріоритет – 1)		
Штрафи (комерційні стейкхолдери)	Стягнення штрафів у розмірі менше 100 тис. грн.	Стягнення штрафів у розмірі від 100 до 300 тис. грн.	Стягнення штрафів у розмірі більше 300 тис. грн.

ПРОФІЛЮВАННЯ ЗАГРОЗ ТА ОЦІНКА РИЗИКІВ. ФАЗА ВСТАНОВЛЕННЯ ДРАЙВЕРІВ. (КРИТЕРІЇ ОЦІНКИ РИЗИКІВ)

	Низький	Середній	Високий
Позови (комерційні стейкхолдери)	Реєстрація судових позовів на суму меншу за 100 тис. грн.	Реєстрація судових позовів на суму меншу від 100 до 300 тис. грн.	Реєстрація судових позовів на суму більше 300 тис. грн.
Розслідування (комерційні стейкхолдери)	Відсутність запитів від уряду чи інших слідчих установ.	Запит на інформацію від уряду чи іншої слідчої установи.	Уряд або інше слідча установа розпочинає поглиблене розслідування проти стейкхолдерів .

ПРОФІЛЮВАННЯ ЗАГРОЗ ТА ОЦІНКА РИЗИКІВ. ФАЗА СТВОРЕННЯ ПРОФІЛЮ АКТИВІВ

- Під час фази створення профілю активів критичні інформаційні активи спочатку ідентифікуються, а потім профілюються. У процесі профілювання встановлюються чіткі межі для активу та визначаються вимоги безпеки. Після цього визначаються всі місця, де актив зберігається, транспортується або обробляється. Крім того, слід визначити, де ці активи використовуються власниками розумних будинків або системами розумного дому, як доступ до цих активів і хто несе відповідальність за ці активи. Логічні, технічні, фізичні та людські активи документуються.
- Таким чином, визначаються слабкі місця, на яких вимоги безпеки, з точки зору тріади конфіденційності, цілісності та доступності, інформаційного активу можуть бути скомпрометовані.

ПРОФІЛЮВАННЯ ЗАГРОЗ ТА ОЦІНКА РИЗИКІВ. ФАЗА СТВОРЕННЯ ПРОФІЛЮ АКТИВІВ. (КОНТЕЙНЕРИ ІНФОРМАЦІЙНОГО ОБ'ЄКТУ)

№	Опис контейнеру	Власник
	Технічні інформаційні контейнери	
	Внутрішні	
1	Файл даних	Власник розумного будинку/ мешканці
2	База даних: інформаційний ресурс знаходиться на серверах баз даних і веб-серверах.	Власник розумного будинку/ мешканці
3	Внутрішня мережа розумного будинку. Вся інформація поширюється по даній мережі.	Власник розумного будинку/ мешканці
4	Пристрої користувача	Мешканці

ПРОФІЛЮВАННЯ ЗАГРОЗ ТА ОЦІНКА РИЗИКІВ. ФАЗА СТВОРЕННЯ ПРОФІЛЮ АКТИВІВ. (КОНТЕЙНЕРИ ІНФОРМАЦІЙНОГО ОБ'ЄКТУ)

№	Опис контейнеру	Власник
	Зовнішні	
5	Інтернет: ці інформаційні об'єкти поширюються Інтернетом щоразу, коли кінцевий користувач під'єднується до системи розумного будинку поза межами дому через пристрої користувача (смартфон, планшет тощо).	-
	Фізичні інформаційні контейнери	
	Внутрішні	
I	Паперові носії	Власник розумного будинку/ мешканці
2	Носії інформації	Власник розумного будинку/ мешканці
	Зовнішні	
-	-	-

ПРОФІЛЮВАННЯ ЗАГРОЗ ТА ОЦІНКА РИЗИКІВ. ФАЗА СТВОРЕННЯ ПРОФІЛЮ АКТИВІВ. (КОНТЕЙНЕРИ ІНФОРМАЦІЙНОГО ОБ'ЄКТУ)

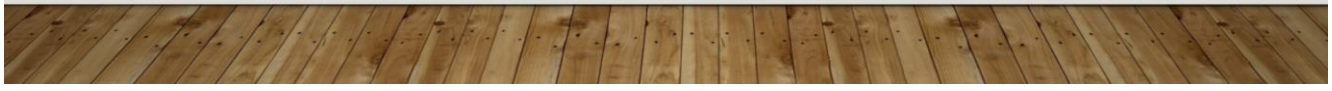
№	Опис контейнеру	Власник
	Людські інформаційні контейнери	
	Внутрішні	
I	Члени сім'ї	Мешканці
	Зовнішні	
2	Гості	Гості
3	Сервісний персонал	Сервісний персонал

ПРОФІЛЮВАННЯ ЗАГРОЗ ТА ОЦІНКА РИЗИКІВ. ФАЗА СТВОРЕННЯ ПРОФІЛЮ АКТИВІВ. (ПРОФІЛЬ КРИТИЧНОГО ІНФОРМАЦІЙНОГО ОБ'ЄКТУ)

Критичний об'єкт **Що є критично важливим інформаційним об'єктом?**	**Обґрунтування вибору** **Чому цей інформаційний об'єкт є важливим для організації?**	**Опис** **Який узагальнюючий опис цього інформаційного об'єкту?**
Інформація, зібрана пристроями (датчиками)	Даний інформаційний об'єкт є важливою складовою у процесі функціонування системи розумного будинку та є основним джерелом вхідних даних про стан навколишнього середовища. Компрометація цього інформаційного об'єкту може призвести до порушення функціонування системи та прояву ризиків, пов'язаних, наприклад, із пожежею або повінню.	Цей інформаційний об'єкт визначає вихідні дані з пристроїв, наприклад він визначає, які дії будуть виконувати виконавчі механізми. Ця інформація визначає безпеку та зручність розумного будинку, які є головними цілями системи розумного будинку.

ПРОФІЛЮВАННЯ ЗАГРОЗ ТА ОЦІНКА РИЗИКІВ. ФАЗА СТВОРЕННЯ ПРОФІЛЮ АКТИВІВ. (ПРОФІЛЬ КРИТИЧНОГО ІНФОРМАЦІЙНОГО ОБ'ЄКТУ)

Власник(и) **Кому належить цей інформаційний актив?**		
Власником цього інформаційного об'єкту є система розумного будинку, на якій лежить основна відповідальність за дану інформацію		
Вимоги безпеки **Які вимоги безпеки до цього інформаційного активу?**		
Конфіденційність	Переглянути цей інформаційний ресурс можуть лише авторизовані працівники.	Доступом до цього інформаційного об'єкту володіють лише мешканці розумного будинку. Також цю інформацію можуть потребувати постачальники послуг для надання належних послуг відповідно до договорів.



ПРОФІЛЮВАННЯ ЗАГРОЗ ТА ОЦІНКА РИЗИКІВ. ФАЗА СТВОРЕННЯ ПРОФІЛЮ АКТИВІВ. (ПРОФІЛЬ КРИТИЧНОГО ІНФОРМАЦІЙНОГО ОБ'ЄКТУ)

Цілісність	Тільки авторизовані користувачі можуть модифікувати цей інформаційний актив.	Тільки мешканці мають право маніпулювати цим інформаційним об'єктом.
Доступність	Даний інформаційний об'єкт має бути у розпорядженні цих користувачів протягом **24** годин, **7** днів на тиждень.	Даний об'єкт має бути готовий до використання, коли це буде потрібно мешканцям або іншим спорідненим системам. Цей інформаційний об'єкт повинен бути доступним цілодобово для забезпечення функціонування системи розумного будинку. Нетривале відключення не повинно порушити функціонування системи, в той час як тривале переривання (більше **8** годин) спричинило б значні проблеми.

ПРОФІЛЮВАННЯ ЗАГРОЗ ТА ОЦІНКА РИЗИКІВ. ФАЗА СТВОРЕННЯ ПРОФІЛЮ АКТИВІВ. (ПРОФІЛЬ КРИТИЧНОГО ІНФОРМАЦІЙНОГО ОБ'ЄКТУ)

Найважливіші вимоги безпеки **Яка найважливіша вимога безпеки для цього інформаційного активу?**		
Конфіденційність	Цілісність	Доступність

ПРОФІЛЮВАННЯ ЗАГРОЗ ТА ОЦІНКА РИЗИКІВ. ФАЗА ВИЗНАЧЕННЯ ЗАГРОЗ

- На цьому етапі основна увага приділяється ідентифікації загроз безпеці від ідентифікованих активів у контексті місць, де інформаційний актив зберігається, транспортується або обробляється. Уразливі місця безпеки або проблемні зони визначаються та розширюються на сценарії загроз, які в подальшому формують властивості загрози.
- Нарешті, виділено конкретні загрози, які можуть негативно вплинути на безпеку активів.

ПРОФІЛЮВАННЯ ЗАГРОЗ ТА ОЦІНКА РИЗИКІВ. ФАЗА ПОМ'ЯКШЕННЯ РИЗИКУ

- На етапі пом'якшення ризику ризики кібер та фізичної безпеки щодо інформаційних активів визначаються шляхом визначення того, як сценарії загроз можуть вплинути на систему розумного дому. Оцінка здійснюється шляхом аналізу впливу або наслідків цих загроз на середовище розумного дому. Нарешті, для кожного з виявлених ризиків визначається стратегія пом’якшення. Ризики аналізуються і присвоюється якісне значення, щоб описати ступінь впливу на користувачів розумного дому. Значення впливу виводиться з критеріїв оцінки ризику, а інформація про оцінку використовується для ранжирування ідентифікаторів ризиків і визначення пріоритетності пропонованих дій з пом'якшення.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Інформаційний об'єкт	Інформація, зібрана пристроями (датчиками)
Сфера занепокоєння	1) Зміна показників датчика газу може призвести до хибного реагування на наявність газу в приміщенні, що може позначитись на здоров'ї та житті мешканців 2) Отримання даних із датчика руху можна використати для визначення присутності мешканців будинку. 3) Зчитування стану замків дверей та систем сигналізації можна використати, щоб визначити, коли розумний будинок зайнятий. 4) DoS атаки на рівень сприйняття (компрометація каналу зв'язку) систем розумного будинку продукує не можливість сприйняття фізичних параметрів датчиками, що тим самим унеможливлює виявлення таких ризиків, як пожежа, повінь, несподівані рухи тощо.
Дійова особа. Хто здійснюватиме вплив на інформаційний об'єкт створюючи загрозу безпеці?	Зловмисник (хакер, недобросовісний постачальник програмних та апаратних засобів).

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Інформаційний об'єкт	Інформація, зібрана пристроями (датчиками)		
Засоби. Яким чином дійова особа здійснить це? Що вони повинні зробити для цього?	Засоби взлому. Вразливості в апаратному забезпеченні.		
Мотив. Який виграш отримає дійова особа здійснивши порушення безпеки?	Фінансова вигода, задоволення персональних амбіцій.		
Результат. Яким чином це відобразиться на інформаційному об'єкті?	○ Розкриття • Зміна	○ Знищення • Переривання	
Вимоги безпеки. Яким чином будуть порушені вимоги безпеки інформаційного об'єкту?	Лише авторизовані члени розумного будинку повинні мати доступ до цієї інформації та змінювати її.		
Імовірність. Яка імовірність відтворення подібного впливу?	• Висока	○ Середня	○ Низька

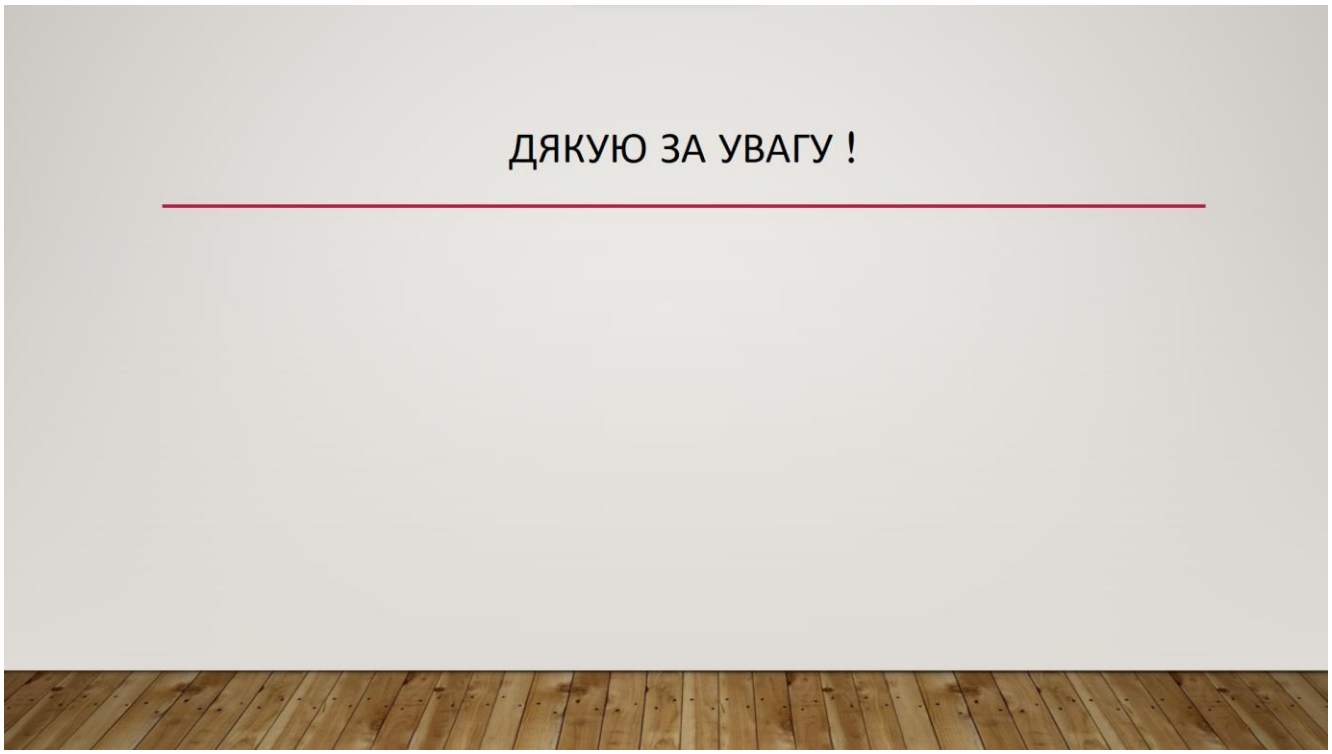
РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Наслідки. **Які будуть наслідки для організації або власника інформаційного об'єкта при порушенні вимог безпеки?**	**Важкість.** **Наскільки серйозними є ці наслідки для організації чи власника об'єкту в залежності від зони впливу?**		
У випадку порушення вимог безпеки для цього інформаційного об'єкту система розумного будинку не в змозі буде відстежувати та контролювати критично важливі показники давачів, що може призвести до негативних наслідків, пов'язаних як із фізичною природою (пожежа, підтоплення), так із людським фактором (проникнення, крадіжка речей). В обох випадках прояви негативних наслідків можуть призвести до великих фінансових втрат.	Зони впливу	Значення	Оцінка
	Репутація та довіра клієнтів	Висока	4 * 3 = 12
	Фінансова	Висока	9
	Продуктивність	Низька	2
	Життя, здоров'я, безпека	Висока	15
	Штрафи та юридичні санкції	Низька	1
		Відносне значення оцінки ризику	39

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Пом'якшення ризиків. **Виходячи з загальної оцінки цього ризику, які дії слід вжити?**			
○ Прийняти	○ Відкласти	• Пом'якшити	○ Передати

Щодо ризиків, які було вирішено пом'якшити, слід виконати наступні дії.	
Якого контейнера будуть стосуватись дії?	**Який адміністративний, технічний та фізичний контроль слід застосували до цього контейнера? Який залишковий ризик все ще буде прийнято організацією?**
Технічний	Обмежити доступність мережевого трафіку лише для авторизованих користувачів; використання протоколів передачі даних із шифруванням (наприклад, SSL/TLS) а також використовувати захищену віртуальну приватну мережу (VPN).
Фізичний	Зберігайте всі фізичні дані в надійному місці. Регулярне оновлення апаратного забезпечення; створення резервних копій всієї важливої інформації.
Люди	Інформування мешканців стосовно безпечного управління розумним будинком а також розробка програми навчання безпеці для мешканців розумного будинку.


ДЯКУЮ ЗА УВАГУ !

ДОДАТОК Б

(обов'язковий)

Копія публікації

INTERNATIONAL SCIENTIFIC JOURNAL
«COMPUTER SYSTEMS AND INFORMATION TECHNOLOGIES»

UDC 004.92
DOI: 10.31891/CSIT-2021-5-11

OLGA MOROZOVA, ARTEM TETSKYI,
National Aerospace University "Kharkiv Aviation Institute"
ANDRII NICHEPORUK, DENUS KRUVAK,
Khmelnytskyi National University
VITALII TKACHOV
Kharkiv National University of Radio Electronics

SMART HOME SYSTEM SECURITY RISK ASSESSMENT

The concept of the Internet of Things became the basis of the fourth industrial revolution, which allowed to transfer the processes of automation to a new saber. As a result, automation systems, such as smart homes, healthcare systems and car control systems, have become widespread. The developers of such systems primarily focus their efforts on the functional component, leaving safety issues in the background. However, when designing and operating IoT systems, it is equally important to assess potential bottlenecks and develop complete and comprehensive strategies to mitigate and eliminate the negative effects of cyberattacks.

The purpose of this study is to identify possible cyber threats and assess their impact on critical information objects in the smart home system. To achieve this goal, the three-level architecture of the smart home system is considered and a review of known cyber threats for each level is conducted. The critical information objects in the smart home system are the containers in which the information objects are stored, the risk assessment criteria and the cyber threat scenarios. The information security risks of the smart home system were assessed using the OCTAVE Allegro methodology for the information object that presents the information collected by the smart home sensors.

Keywords: security risk assessment, smart home, critical information object, threats

ОЛЬГА МОРОЗОВА, АРТЕМ ТЕЦЬКИЙ
Національний аерокосмічний університет ім. М.Є. Жуковського "Харківський авіаційний інститут"
АНДРІЙ НІЧЕПОРУК, ДЕНИС КРИВАК
Хмельницький національний університет
ВІТАЛІЙ ТКАЧОВ
Харківський національний університет радіоелектроніки

ОЦІНКА РИЗИКІВ БЕЗПЕКИ СИСТЕМИ РОЗУМНОГО БУДИНКУ

Концепція Інтернету речей стала основою четвертої промислової революції, що дозволило перевести на новий щабель процеси автоматизації. Наслідком цього стало широке поширення систем автоматизації зокрема, розумних будинків, систем у сфері охорони здоров'я та систем керування автомобілем. Розробники таких систем в першу чергу фокусують власні зусилля на функціональній складовій, залишаючи питання безпеки на другий план. Проте, при проектуванні та експлуатації систем Інтернету речей не менш важливим завданням є оцінка потенційних "вузьких" місць та розроблення повних та вичерпних стратегій по пом'якшенню та усуненню негативних впливів кібератак.

Метою даного дослідження є визначення можливих кіберзагроз та оцінка їх впливів на критичні інформаційні об'єкти в системі розумного будинку. Для досягнення мети у роботі розглянуто трьохрівневу архітектуру системи розумного будинку та проведено огляд відомих кіберзагроз для кожного рівня. Визначено критичні інформаційні об'єкти в системі розумного будинку контейнери, в яких зберігаються інформаційні об'єкти, критерії оцінки ризиків та сценарії кіберзагроз. Проведено оцінку ризиків інформаційної безпеки системи розумного будинку із залученням методології OCTAVE Allegro для інформаційного об'єкту, що представляє інформацію, зібрану датчиками розумного будинку. Проведений процес оцінки ризиків дозволяє проаналізувати інформаційні об'єкти в системі розумного будинку, які є критичними з точки зору безпеки, провести аналіз ризиків та їх впливів на об'єкти, та запропонувати можливі контрзаходи з метою захисту інформаційних об'єктів та створення системи розумного дому більш безпечним.

Перспективним напрямком подальших досліджень є формування комплексної оцінки ризиків інформаційної безпеки системи розумного будинку та реалізації програмної системи, що дозволить автоматизувати процес формування оцінки ризиків не тільки для системи розумного будинку, а й для інших систем, що імплементують принцип Інтернету речей.

Ключові слова: оцінка ризиків безпеки, розумний будинок, критичний інформаційний об'єкт, загрози.

Introduction

The growing popularity of the Internet of Things (IoT) provides ample opportunities to improve, plan and automate our lives. IoT allows you to network and manage multiple devices that provide data collection, analysis and transmission. The scope of IoT continues to expand every year, covering new areas of life, from smart homes, cities to healthcare.

However, along with the obvious benefits and conveniences of using IoT, the concept of the Internet of Things leaves a number of potential security bottlenecks for attackers. Users' personal data collected by smart devices is always of value to hackers and hijackers of confidential information. In addition, a cyberattack on an Internet of Things solution has the potential to damage physical services and physical infrastructure. When designing and operating Internet of Things systems, an important task is to assess these potential bottlenecks and develop complete and comprehensive strategies to mitigate and eliminate the negative effects of cyberattacks. Therefore, *the purpose of this study* is to identify possible cyber threats and assess their impact on critical information objects in the smart home system.

Three-level architecture of home automation systems and attacks on its components

The architecture of the Internet of Things system, and in particular the smart home, can be represented through three logical levels (fig. 1): the level of perception, the network level and the level of applications [1, 2]. Let's take a closer look at each level of the smart home system and analyze known cyber threats that violate the integrity, availability and confidentiality of information at the appropriate level.

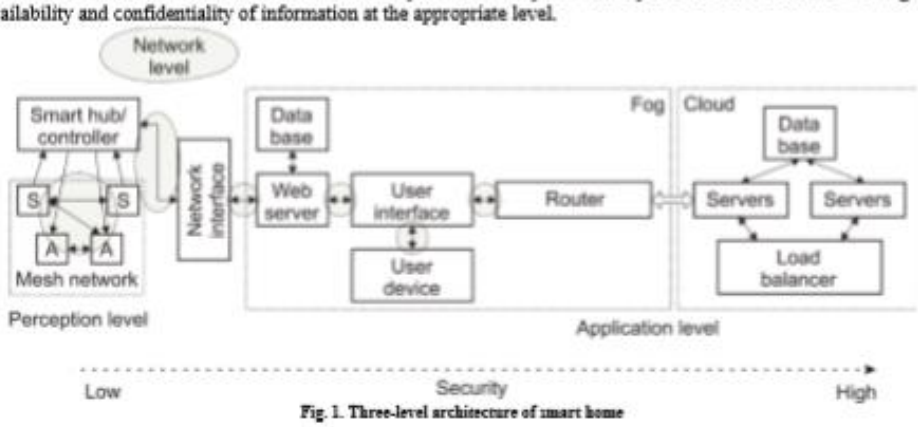


Fig. 1. Three-level architecture of smart home

Perception level

The closest level to the physical environment in the architecture of a smart home is the level of perception. The main functions of this level are the collection of information about the state of the physical environment and the implementation of mechanisms for influencing it. The assigned functions are implemented using multiple sensors and actuators, respectively. The information collected by the sensors depends on the nature of the physical environment and may relate to location, changes in the air and environment, movement, vibration, and so on. Actuators implement the principle of conversion of electrical energy transmitted through conductors into other types of energy. Examples of actuators are various types of motors, relay modules and automated cranes. The security of this level in the smart home system is the lowest, which «attracts» attackers to carry out attacks on the smart home device. The most common security threats to this level of perception are:

Eavesdropping. Eavesdropping is an unauthorized attack that violates the privacy of real-time information in which an attacker intercepts private messages, such as phone calls, text messages, fax transmissions, or video conferencing. Ehe main purpose of the eavesdropping attack is to violate the confidentiality of information. An unsecured data channel is used to access the information that is sent and received.

Fake node. This is an attack in which an attacker adds a new node to the system and fills the network with fake data. The main purpose of this attack is to stop the transmission of information from real network nodes. A node added by an attacker consumes the energy of real nodes and potentially controls it to destroy the network.

Node Capture. In this attack, an attacker gains full control of a key node, such as a gateway node. It can transmit all information, including the connection between the sender and the recipient, the key used to ensure secure communication and the information stored in memory.

Timing attacks: This is a type of passive attack aimed at devices with limited computing resources. During the attack, an attacker discovers vulnerabilities and obtains secrets that are stored in the security of the system, tracking how long it takes the system to respond to various requests.

Replay attack. This is an attack in which an attacker eavesdrops on security between the sender and the recipient and takes authentic information from the sender. The attacker sends the victim the same authenticated information that was already received during his communication, demonstrating proof of his identity and authenticity. The message is encrypted, so the recipient can consider it as a valid request and take the actions desired by the attacker.

Network level

The network layer performs a transport function for transmitting information within a smart home and is a bridge between the level of perception and the level of applications. It transmits information collected from physical objects using sensors. It also takes responsibility for connecting smart things, network devices and networks to each other. The presence of a communication component makes this level sensitive to attacks by attackers. It has noticeable [3, 4] security issues regarding the integrity and authentication of information transmitted over the network. Common security threats and problems for network layers are [5, 6]:

Expoloit: A type of attack that is implemented using a piece of software code or a sequence of commands that exploit vulnerabilities in software. The purpose of the attack can be both to seize control of the system and to disrupt its operation.

«Man in the middle» attack: A Man in the middle is a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other. One example of a MItM attack is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

Denial of Service (DoS) attack: This is an attack whose primary purpose is to prevent legitimate users from accessing devices or other network resources. This is usually accomplished by filling the target devices or network resources with redundant requests in order to prevent or complicate the use of some or all legitimate users.

Data Warehouse Attack: User information is stored on storage devices or in the cloud. An attacker could attack both storage devices and the cloud, and user information could be changed to incorrect information, thereby violating the integrity and confidentiality of data.

Application level

The application layer is the highest level in the logical smart home hierarchy and defines all applications that use smart home technology or in which smart home is deployed. Its main purpose is to provide services to applications. Services may be different for each program, as services depend on the information collected by the sensors. At the application level, there are many issues where security is a key issue. In particular, when the Internet of Things is used to create a smart home, it creates many threats and vulnerabilities inside and out. One of the main problems in implementing smart security in a smart home based on the Internet of Things is that the devices used in smart homes have low computing power and low memory. Common security threats and application level problems are [1, 7]:

Malicious code attack: This is code in any part of the software, the main purpose of which is to violate the confidentiality, availability and integrity of information, as well as damage to the system. Malicious software can implement its own code into the body of a user application, or exist separately in memory as a standalone software code, etc.

Cross-site scripting: This is an injection attack that allows an attacker to insert a client-side malicious code script, such as a web page viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. By performing such actions, an attacker can completely change the content of the program according to their needs and use the original information in an illegal way.

Smart home system security risk assessment

An important task in the design and operation of smart home systems is to identify cyber threats, assess their impact on potentially "bottlenecks" in the system and develop complete and comprehensive strategies to mitigate and eliminate the negative effects of cyberattacks. Moreover, the sooner the assessment is carried out and appropriate measures are taken, the greater the likelihood of ensuring the integrity, accessibility and confidentiality of information. Consider the process of assessing the risks of information security of the smart home system. To assess the risks, we use the OCTAVE Allegro methodology [9].

OCTAVE Allegro is a methodology that allows you to streamline and optimize the process of assessing information security risks, allowing the organization to obtain sufficient results in a small amount of time, human and other limited resources. The main focus of the OCTAVE Allegro methodology is to consider people, technology and tools in the context of their relationship to the information and business processes and services they support.

The OCTAVE Allegro methodology defines eight successive stages, organized in 4 phases (Fig. 2): definition of criteria, profiling of objects, identification of threats, identification and mitigation of risks. With the help of OCTAVE Allegro tables, it is possible to record the results of each assessment step risk and use them as input for the next steps. Individual steps apply to each individual information object. To assess safety risks, we use the OCTAVE Allegro template, which is presented in [9, 10].

During the research, we were inspired by work [10], and presented our own vision of the problem. Consider in more detail the application of the OCTAVE Allegro methodology to assess the security risks of a smart home system.

Definition of risk assessment criteria

The purpose of this step is to determine what may be the consequence of the risk to the business strategy and objectives or critical success factors (commercial stakeholders) and to the occupants of the smart home (non-commercial stakeholders). This step consists of two sub-step. The first sub-step involves defining a set of qualitative and quantitative measures to assess the impact of risks on the identified critical information objects in the smart home system. In the process of the second activity, the zone of influence is prioritized according to their importance for the owner of the smart home or stakeholders.

Criteria for evaluating the OCTAVE Allegro methodology include the following categories: customer reputation and trust; life, health, safety; fines and legal sanctions; financial losses; productivity.

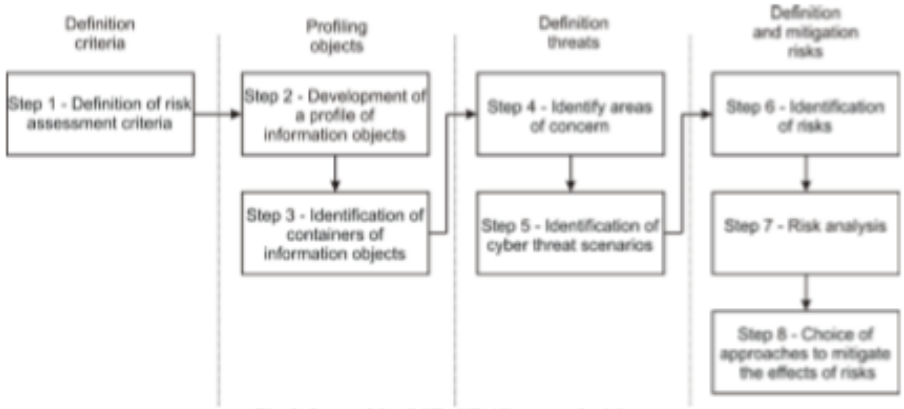


Fig. 2. Steps of the OCTAVE Allegro methodology

Before filling in the OCTAVE Allegro tables, it is necessary to determine who are the stakeholders for whom the risk assessment in the smart home system is carried out. The following stakeholders can be identified for the smart home system: non-commercial stakeholders represented by the end users of the smart home system and commercial stakeholders - software and hardware manufacturers, private and public companies involved in the installation and deployment of home automation systems, etc. Table 1 provides examples of risk assessment criteria, in particular for the categories of life, health, safety and fines and legal sanctions, as well as their priority.

Table 1

Risk assessment criteria

	Low	Middle	High
Criterion	Risk assessment criteria - life, health, safety (priority - 5)		
Life (non-commercial stakeholders)	No loss or significant threat to the lives of end users	Users' lives are in danger, but after receiving medical care, they recover	Loss of human life
Health (non-commercial stakeholders)	The deterioration is minimal and can be treated immediately with recovery within a few days	Temporary deterioration of users' health	Significant violation of the health of users. The recovery period is more than one month. Acquisition of chronic diseases.
Safety (non-commercial stakeholders)	The safety of the final consumer is in question	Minimal impact on end-user safety. The presence of an administrative offense	End-user safety is compromised. The presence of a criminal offense
...	...	...	...
Criterion	Risk assessment criterion - fines and legal sanctions (priority - 1)		
Fines (commercial stakeholders)	Collection of fines in the amount of less than UAH 100,000	Collection of fines in the amount of 100 to 300 thousand UAH.	Collection of fines in the amount of more than UAH 300,000.
Lawsuits (commercial stakeholders)	Registration of lawsuits in the amount of less than UAH 100,000	Registration of lawsuits in the amount of less than 100 to 300 thousand UAH	Registration of lawsuits in the amount of more than 300 thousand UAH.
Investigations (commercial stakeholders)	No inquiries from the government or other investigative agencies	Request for information from the government or other investigative body	The government or other investigative agency is launching an in-depth investigation against the stakeholders

Thus, the criterion for assessing the risks to life, health and safety is set at 5 (highest), for reputation - 4, for financial losses - 3, for productivity - 2. The lowest priority is the category of fines and legal sanctions with the appropriate level priority 1.

Development of a profile of information objects

In this step, critical information objects should be identified and profiled. In the process of profiling, we will define clear boundaries for the object in the smart home system, its safety requirements and identify all places where the object is stored, transported and stored. These steps will identify vulnerabilities in critical information objects.

The first step in the process of developing information object profiles is the actual identification of these objects. It should be noted that the level of applications will not be considered due to its greater security of information objects [8]. For the level of perception and network level of a smart home (Fig. 1), the following critical information objects can be distinguished [2]: information collected by sensors; video surveillance camera data; user credentials

(username and password); information resources (documents, user files); information on setting up a smart home; structure of a smart home (information about devices); information about the event log (information about the state of the smart home); user devices; location information. Table 2 shows the profile of the critical information object «information collected by devices»

Identification of containers of information objects

After describing the profiles of critical information objects, according to the OCTAVE Allegro methodology, the containers of information objects are identified. An information object container is a place where information is located. Containers can be technical (software, software, servers and communication networks), physical (paper, flash media, CDs) or people (who knows about the information). They can also be both internal and external to the organization. Let's analyze (technical, physical and human) containers for the critical information object «information collected by devices». Table 3 shows the containers of the information object «information collected by devices».

Table 2

Critical Information Object Profile "Information Collected by Devices (Sensors)"

(1) Critical object *What is a critical information object?*	**(2) Justification of the choice** *Why is this information important for the organization?*	**(3) Description** *What is the general description of this information object?*
Information collected by devices	This information object is an important component in the functioning of the smart home system and is the main source of input data on the state of the environment. Compromise of this information object may result in system malfunction and risks associated with, for example, fire or flood.	This information object determines the output from the devices, for example, it determines what actions the actuators will perform. This information determines the safety and convenience of the smart home, which are the main goals of the smart home system.
(4) Owner (s) *Who owns this information object?*		
The owner of this information object is the smart home system, which has the main responsibility for this information		
(5) Security requirements *What are the security requirements for this information object?*		
Confidentiality	Only authorized employees can view this information resource:	Only residents of the smart home have access to this information facility. This information may also be required by service providers for provision of appropriate services in accordance with contracts
Integrity	Only authorized users can modify this information object:	Only residents have the right to manipulate this information object.
Accessibility	This information object must be available to these users within 24 hours, 7 days a week.	This facility should be ready for use when residents or other related systems need it. This information facility must be available around the clock to ensure the operation of the smart home system. A short shutdown should not disrupt the operation of the system, while a long interruption (more than 8 hours) would cause significant problems.
(6) The most important safety requirements *What is the most important security requirement for this information object?*		
• Confidentiality	• Integrity	• Accessibility

Identify areas of concern

In this step the identify problem areas in previously identified information objects is carried out. For each identified information object, specific problems are identified that may adversely affect the security of this object. This step describes the potential impacts, if any, of the threat and the conditions that cause the event. The description, which is based on the storage locations of the information objects defined, provides a detailed understanding of where the information object may start a security breach.

Identification of cyber threat scenarios

The next step is to build threat scenarios for each identified information object. A threat scenario includes one or more objects, an actor (actor), means, motives, and a list of undesirable outcomes. An actor can be both natural (storm, flood, fire or other disaster), automated (malicious software) and intelligent (criminal, activist or other person who intends to cause school to a smart home). The means is the vulnerability used by the entity against the information object. The motive is the actor's desire to apply the means to the information object. An undesirable result is damage to the information object (it can be disclosure, alteration, interruption or destruction). This step allows to identify threat scenarios that can be implemented to a greater extent. Threats are identified using containers in which object are stored or transferred.

Table 3

Containers of the information object "information collected by devices (sensors)"

№	Description of the container	Owner
Technical information containers		
Internal		
1 2 3	Database: The information resource is located on database servers and web servers The internal network of a smart home User's devices	Smart home owner / residents
External		
5	Internet	–
Physical information containers		
Internal		
1 2	Paper media Storage devices	Smart home owner / residents
External		
–	–	–
Human information containers		
Internal		
1	Family members	residents
External		
2 3	Guests Service man	Guests Service man

Identification of risks

Risk is the possibility of causing damage or loss (data, software, hardware) and consists of event, consequence and uncertainty. The threat can have many potential negative consequences for the organization. For example, a breach of an organization's e-commerce system can affect an organization's reputation with customers as well as its financial position. In order to determine the risks for each information object, a threat scenario is applied to its components, provided that the threat scenario is implemented and the impact on the stakeholders of the smart home is assessed.

Risk analysis

At this stage, the identified risks in step 6 are assessed using the assessment criteria established in the first step. These scores are used to prioritize risks, and as a result, to mitigate the impact of risks on the smart home system. Thus, for each risk of the information object, the following actions should be performed: assign values "high", "medium" and "low" in the field Value (Table 4) taking into account the risk assessment criteria (Table 1); calculate the score for each impact zone by multiplying the impact area priority by the impact value (high = 3, medium = 2, low = 1). After writing the result in the evaluation column, a final evaluation is formed, which is a relative indicator of risk.

Choice of approaches to mitigate the effects of risks

In the latter, the risks analyzed in the previous step are used to develop a strategy to mitigate the potential impact of risks on the information objects of the smart home system. Thus, in this step, the approach is chosen to deal with each threat according to their priority. There are several approaches to the choice: accept, reduce, transfer, postpone. After identifying the risks and assessing the risks, a mitigation checklist can be defined to avoid or limit the identified risks and the negative consequences arising from them. We perform a risk assessment for the information object «information collected by devices» (Table 4).

These steps of the OCTAVE Allegro methodology are performed for each critical information object. The conducted risk assessment process allows to analyze information objects in the smart home system that are critical from the point of view of safety, to analyze risks and their effects on objects, and to suggest possible countermeasures to protect information objects and create a smart home system more safer.

Conclusions

As a result of the study, the architecture of a smart home was considered as a system consisting of three logical levels: perception, network and application level. A review of known cyber threats was conducted for each level. In particular, critical information objects in the smart home system, risk assessment criteria and cyber threat scenarios have been identified. The information security risks of the smart home system were assessed using the OCTAVE Allegro methodology for the information object that presents the information collected by the smart home sensors. Further research is the formation of a comprehensive risk assessment of information security of the smart home system and the implementation of the software system, which will automate the process of risk assessment not only for the smart home system, but also for other systems that implement the Internet of Things.

Table 4

Risk assessment for the information object «information collected by devices»

Information object	Information collected by devices

		Area of concern	1) Changing the gas sensor can lead to a wrong response to the presence of gas in the room, which can affect the health and lives of residents 2) Obtaining data from the motion sensor can be used to determine the presence of occupants of the house. 3) Reading the status of door locks and alarm systems can be used to determine when a smart home is busy. 4) DoS attacks on the smart home system do not produce the ability to perceive the physical parameters of the sensors, which makes it impossible to detect such risks as fire, floods, unexpected movements, and so on			
		(1) Actor *Who will influence the information object creating a security threat?*	Intruder (hacker, unscrupulous supplier of software and hardware)			
		(2) Means *How will the protagonist do this? What should they do for this?*	Hacking tools Vulnerabilities in hardware			
		(3) Motive *What benefit does the protagonist gain from a security breach?*	Financial benefit, satisfaction of personal ambitions.			
		(4) The result *How will this be reflected in the information object?*	○ **Disclosure** ○ **Destruction** • **Modification** • **Interruption**			
		(5) Safety requirement *How will the security requirements of the information object be violated?*	This information should only be available to smart home owners			
		(6) Probability *What is the probability of reproducing such an effect?*	• **High**	○ **Medium**	○ **Low**	
	(7) Consequences *What will be the consequences for the organization or owner of the information object in case of violation of security requirements?*		**(8) Difficulty** *How serious are these consequences for the organization or owner of the facility, depending on the area of influence?*			
	In case of violation of safety requirements for this information object, the smart home system will not be able to monitor and control critical indicators of sensors, which can lead to negative consequences related to both the physical nature (fire, flooding) and the human factor. (penetration, theft of things). In both cases, the manifestations of negative consequences can lead to large financial losses		**Impact area**	**Value**	**Score**	
			Customer reputation and trust (4)	Middle (2)	4*2 = 8	
			Financial losses (3)	High (3)	9	
			Productivity (2)	Low (1)	2	
			Life, health, safety (5)	High (3)	15	
			Fines and legal sanctions (1)	Low (1)	1	
Relative value of risk assessment						15
(9) Risk mitigation Based on an overall assessment of this risk, what actions should be taken?						
○ **Accept**	○ **Defer**	• **Mitigate**	○ **Transfer**			
The following steps should be taken to mitigate the risks that have been identified						
Which container will the action apply to?	*What administrative, technical and physical controls should be applied to this container? What residual risk will the organization still accept?*					
Technical	Restrict the availability of network traffic only to authorized users; use of encrypted data transfer protocols (e.g. SSL / TLS)					
Physical	Store all physical data in a safe place. Regular hardware updates; back up all important information.					
People	Informing residents about the safe management of a smart home					

References

1. Burhan M. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey / M. Burhan, R.A. Rehman, B. Khan, B.S.Kim // Sensors (Basel) – 2018. – 18(9):2796.

2. Sethi P. Internet of Things: Architectures, Protocols, and Applications / P. Sethi, S.R. Sarangi // Journal of Electrical and Computer Engineering. – 2017. – 25 p.

3. Al-Garadi M. A. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security / M.A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, M. Guizani // arXiv:1807.11023. – 2018.

4. Apthorpe N. A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic / N. Apthorpe, D. Reisman, N. Feamster // arXiv:1705.06805. – 2017.

5. Nicheporyk A.O. A method of detecting DDoS attacks on an IoT network / O.A. Nicheporyk, A.A. Nicheporyk, O.V. Fegir, A.D. Kazantsev, Ю.O. Nicheporyk // Bulletin of Khmelnytsky National University. Series: Technical Sciences. Khmelnytskyi. – 2020. – № 1. – P.156-164 [in Ukrainian].

6. Lee I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet. 2020; 12(9):157. https://doi.org/10.3390/fi12090157

7. Zhao S. Computational Intelligence Enabled Cybersecurity for the Internet of Things / S. Zhao, S. Li, L. Qi and L. D. Xu, // Proceedings of IEEE Transactions on Emerging Topics in Computational Intelligence. – vol. 4. – № 5. – P. 666-674.

8. Sarrab M. / Critical Aspects Pertaining Security of IoT Application Level Software Systems / M. Sarrab and S. M. Alnaeli, // Proceedings of 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). – 2018. – P. 960-964.

9. Caralli R.A. Octave allegro: Improving the information security risk assessment process / R.A. Caralli, J.F. Stevens, L.R. Young, W.R. Wilson // Technical report. – Software Engineering Institute, CMU/SEI-2007-TR-012, 2007.

10. Ali B. Internet of Things based Smart Homes: Security Risk Assessment and Recommendations / B. Ali // Master's Thesis, Luleå University of Technology, Department of Computer Science, Electrical and Space Engineering, 2016, 98 p.

UNICHECK

Ім'я користувача:
Кафедра КІ

ID перевірки:
1011006864

Дата перевірки:
30.04.2022 08:22:09 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
30.04.2022 08:22:49 EEST

ID користувача:
100005591

Назва документа: **Система профілювання вразливостей при керуванні розумним будинком**

Кількість сторінок: **82** Кількість слів: **14223** Кількість символів: **118243** Розмір файлу: **827.19 KB** ID файлу: **1010910421**

2.55%
Схожість

Найбільша схожість: **0.85%** з джерелом з Бібліотеки (ID файлу: **1010865618**)

1.67% Джерела з Інтернету	11	Сторінка 84
1.75% Джерела з Бібліотеки	63	Сторінка 84

0% Цитат

Не знайдено жодних цитат

Не знайдено жодних посилань

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	4

Sat Apr 30 07:32:05 EEST 2022, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 1.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 6%**

ID: 103216 Название: Система профілювання вразливостей при керуванні розумним будинком Добавлено в БД: 2022-04-30 Авторы: Кривак Д.М. Руководители: Нічепорук А.О. Консультанты: Оппоненты:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	94187	750	1045 (1%)	13 (2%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА ДИПЛОМНУ РОБОТУ

Дипломник: Кривак Денис Михайлович

Тема: Система профілювання вразливостей при керуванні розумним будинком

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг дипломної роботи:

Кількість листів креслень – ; кількість сторінок записки 90

1. Короткий зміст роботи та прийнятих рішень У роботі запропоновано систему профілювання вразливостей при керуванні розумним будинком

2. Висновок про відповідність роботи дипломному завданню Дипломна робота відповідає виданому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проведено аналіз існуючих відомих методів, моделей та системи профілювання загроз та вразливостей для систем що використовують IOT. У другому розділі досліджено та проаналізовано архітектуру та функціональні можливості автоматизованих систем керування розумним будинком. У третьому розділі запропоновано модель побудови профілів загроз при керуванні розумним будинком. У четвертому розділі проведено оцінку ризиків безпеки середовища розумного будинку.

4. Позитивні сторони роботи: Запропонована система профілювання загроз в середовищі розумного будинку дозволяє провести аудит вразливостей та кіберзагрозагроз, а також сформулювати основні напрямки пом'якшення та протидії таким викликам.

5. Негативні сторони роботи: В роботі не простежується зв'язок між системою профілювання загроз в середовищі розумного будинку та формалізацією

моделі інформаційної системи.

6. Оцінка графічного оформлення та пояснювальної записки роботи: –

7. Відгук про роботу в цілому: В загальному робота виконана на достатньому рівні.

8. Інші зауваження: –

9. Оцінка дипломної роботи:

Розглянувши позитивні та негативні сторони представленої дипломної роботи вважаю, що робота заслуговує оцінки «добре» 4,25 (B)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Мартинюк Валерій Володимирович, зав. каф. АКІТ ХНУ

"4" 05 2022р.

Завідувачу кафедри КІС
д-р.техн.наук, проф. Говорущенко Т. О.

Кривак Денис Михайлович
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-20-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіатоповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

30.04.2022
дата

підпис

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система профілювання вразливостей при керуванні розумним будинком

Автор: Кривак Денис Михайлович

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: освітньо-наукова

Науковий керівник: Нічепорук Андрій Олександрович, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 2.55% і адресується до 74 першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ А. О. Нічепорук

Гарант ОП _____ О. С. Савенко

Завідувач кафедри КІІС _____ Т. О. Говорущенко