Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Оцінка ризиків для IoT: системна оцінка розумних будинків

Виконав: студент VI курсу, групи СНм-61
спеціальності 122 Комп’ютерні науки
(шифр і назва спеціальності)

_____ Радчук Д.А.
(підпис) (прізвище та ініціали)

Керівник _____ Мацюк О.В.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Мацюк О.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ Микитишин А.Г.
(підпис) (прізвище та ініціали)

Тернопіль
2021

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«___» _____ 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

Студенту Радчуку Дмитрію Антоновичу
(прізвище, ім'я, по батькові)

1. Тема роботи Оцінка ризиків для IoT: системна оцінка розумних будинків

Керівник роботи Мацюк Олександр Васильович, к.т.н., доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «28» жовтня 2021 року № 4/7-908

2. Термін подання студентом завершеної роботи 07.12.2021

3. Вихідні дані до роботи Наукові публікації про інтернет речей, розумні будинки

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Аналіз наукових публікацій по темі кваліфікаційної роботи 2 Оцінка ризиків для IoT та системна оцінка розумних будинків 3. Охорона праці та безпека в надзвичайних ситуаціях. Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Приймак М.В., професор		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор		

7. Дата видачі завдання 27 вересня 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	27.09.2021-29.09.2021	*Виконано*
2.	Підбір наукових джерел по темі кваліфікаційного -	30.09.2021-03.10.2021	*Виконано*
	роботи		
3.	Опрацювання наукових джерел по темі	04.10.2021-10.10.2021	*Виконано*
	кваліфікаційного роботи		
4.	Виконання дослідження щодо оцінки ризиків для IoT	11.10.2020-17.10.2021	*Виконано*
	та системна оцінка розумних будинків		
5.	Оформлення розділу «Аналіз наукових публікацій по	18.10.2021-24.10.2021	*Виконано*
	темі кваліфікаційної роботи		
6.	Оформлення розділу «Оцінка ризиків для IoT та	22.02.2021-01.03.2021	*Виконано*
	системна оцінка розумних будинків	25.10.2021-07.11.2021	
7.	Виконання завдання до підрозділу «Охорона праці»	08.11.2021-11.11.2021	*Виконано*
8.	Виконання завдання до підрозділу «Безпека в	12.11.201-14.11.2021	*Виконано*
	надзвичайних ситуаціях»		
9.	Оформлення кваліфікаційної роботи	15.11.201-24.11.2021	*Виконано*
10.	Нормоконтроль	25.11.2021-28.11.2021	*Виконано*
11.	Перевірка на плагіат	30.11.2021	*Виконано*
12.	Попередній захист кваліфікаційної роботи	07.12.2021	*Виконано*
13.	Захист кваліфікаційної роботи		

Студент _____ Радчук Д.А.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Мацюк О.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Оцінка ризиків для IoT: системна оцінка розумних будинків // Кваліфікаційна робота освітнього рівня «Магістр» // Радчук Дмитрій Антонович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кафедра комп’ютерних наук, група СНм-61 // Тернопіль, 2021 // С.60, рис. – 5, табл. – 4, додат. – 1, бібліогр. – 49.

Ключові слова: розумні будинки; Інтернет речей (IoT); оцінка ризику безпеки, інформаційні технології

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 будинку 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.

Ретельна оцінка ризиків безпеки повинна передувати будь-якому впровадженню безпеки, щоб гарантувати, що всі відповідні основні проблеми спочатку будуть виявлені.

ANNOTATION

Risks estimation for IoT: system of smart houses assessment // Qualification work of the educational level "Master" // Radchuk Dmytrii Antonovych // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and Software Engineering, Department of Computer Science, SNnm-61 group // Ternopil, 2021 // P. 60, fig. - 5, tables - 4, annexes - 1, references. - 49.

Key words: smart homes; Internet of Things (IoT); security risk assessment, information technology.

The use of IoT technology in smart homes opens up both opportunities and security risks. IoT-based smart homes are very vulnerable to various security threats both inside and outside the home. If the security of a smart home or smart device is compromised, privacy, personal information and even the security of the user will be compromised. Therefore, it is necessary to take appropriate measures to make smart homes safer and habitable.

A thorough assessment of security risks should precede any security implementation to ensure that all relevant underlying issues are identified first.

ПЕРЕЛІК СКОРОЧЕНЬ І ТЕРМІНІВ

ІТ	–	Інформаційні технології
ОС	–	Операційна система
ПЗ	–	Програмне забезпечення
ПК	–	Персональний комп’ютер
БД	–	База даних
API	–	(англ. Application Programming Interface) Прикладний програмний інтерфейс.
IoT	–	(англ. Internet of Things) Інтернет речей.
RFID	–	(англ.Radio Frequency Identification) радіочастотна ідентифікація
GPS	–	(англ.Global Positioning System) глобальна система позиціонування
Bluetooth LE		(англ.Bluetooth Low Energy) Bluetooth з низьким енергоспоживанням
RF		(англ. Radio Frequency) Радіочастоти

ЗМІСТ

ВСТУП

Актуальність теми. За останні кілька років технологічний аспект швидко змінюється і започаткував нову еру інформаційної революції, а саме революцію Інтернету речей (IoT). Однак цей прогрес разом із обіцяними вигодами у покращенні якості життя та створенні величезних економічних можливостей також створив потенційні непередбачені нові ризики; головне з них – нові потенційні виклики для порушень безпеки.

Інтернет речей — це нова парадигма, яка зосереджується на з'єднанні пристроїв, об'єктів чи «речей» один з одним, Інтернетом і користувачами. Очікується, що технологія IoT стане важливою вимогою для розробки розумних будинків, оскільки вона забезпечує зручність та ефективність мешканцям будинків, щоб вони могли досягти кращої якості життя. Застосування моделі IoT у розумних будинках, підключаючи об'єкти до Інтернету, ставить нові проблеми безпеки та конфіденційності з точки зору конфіденційності, автентичності та цілісності даних, які сприймаються, збираються та обмінюються об'єктами IoT. Ці проблеми роблять розумні будинки надзвичайно вразливими до різних типів атак на безпеку, в результаті чого розумні будинки на основі IoT є небезпечними, тому необхідно визначити можливі ризики безпеки, щоб скласти повну картину стану безпеки розумних будинків.

В кваліфікаційній роботі мною застосовано методологію оцінки критичних загроз, активів і вразливості, відому як OCTAVE Allegro, для оцінки ризиків безпеки розумних будинків. Метод зосереджується на інформаційних ресурсах і розглядає різні інформаційні контейнери, такі як бази даних, фізичні документи та люди.

Мета кваліфікаційної роботи – висвітлити різні вразливості безпеки розумних будинків на основі IoT, представити ризики для мешканців будинків та запропонувати підходи до пом'якшення виявлених ризиків.

Для досягнення поставленої мети було потрібно виконати наступні завдання:

–проаналізувати стан досліджень в даній предсметній області;

– проведено комплексну оцінку ризиків безпеки;

– запропонувати відповідні контрзаходи для зменшення ризиків до прийнятного рівня;

– зосередитися виключно на ідентифікації загроз безпеки, впливу або ризиків, а також відповідних контрзаходів для розумних будинків на основі IoT;

– визначити напрямки подальших досліджень.

Об’єкт дослідження системи розумного будинку.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає в проведені комплексної оцінки розумного будинку.

Практичне значення одержаних результатів. Результати дослідження можуть бути використані як основа для покращення вимог безпеки розумних будинків на основі IoT.

Апробація результатів кваліфікаційної роботи. Основні результати проведених досліджень обговорювались на IX науково-технічній конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя (м. Тернопіль, 2021 р.).

Публікації. Основні результати кваліфікаційної роботи опубліковано у двох працях конференції (Див. додаток А).

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури з 49 найменувань та 1 додатку. Загальний обсяг кваліфікаційної роботи складає 60 сторінки, з них 54 сторінки основного тексту, який містить 5 рисунків та 4 таблиці.

1 АНАЛІЗ НАУКОВИХ ПУБЛІКАЦІЙ ПО ТЕМІ КВАЛІФІКАЦІЙНОЇ РОБОТИ

1.1 Огляд наукових публікацій

Інтернет речей (IoT) – це нова парадигма, що з'являється завдяки широкому розвитку інформаційних та комунікаційних технологій (ІКТ). Інклюзивна інфраструктура IoT містить мережу пристроїв або об'єктів, таких як вбудовані комп'ютери, керовані давачі та мітки радіочастотної ідентифікації (RFID), на додаток до шлюзу IoT і віддаленого сервера [1].

Архітектура загальної системи IoT поділяється на три рівні: рівень сприйняття, мережевий рівень і рівень додатків. Спосіб групування компонентів у трьох рівнях загальної системи IoT показано на рис.1.1. З іншої точки зору, термін «речі» в моделі IoT охоплює як кіберсвіт (суб'єкти, кібер-дії, кіберподії та послуги), так і фізичний світ (об'єкти, поведінка, тенденції та фізичні події) [2].

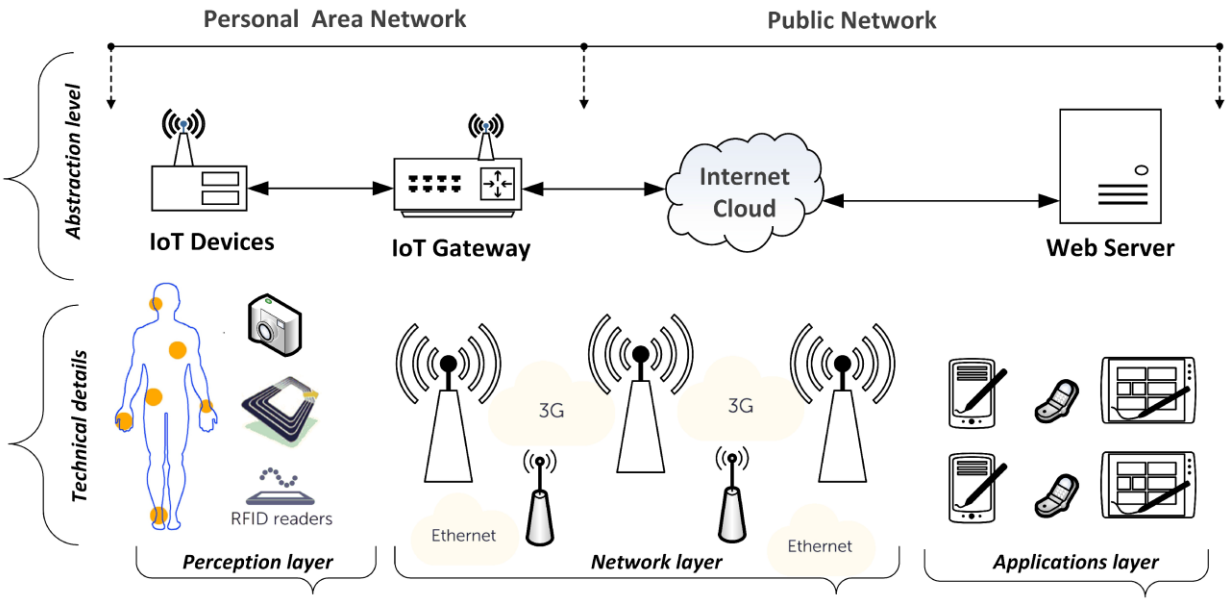

Рисунок 1.1 – Загальна архітектура системи IoT включає пристрої IoT, шлюз і веб-сервер.

На рис.1.1 показані внутрішня і зовнішня сторони системи. Рисунок 1.1 взято і змінено з [1].

Метою IoT є розширення функцій першої версії Інтернету за рахунок збільшення можливості підключення численних об’єктів. Використовуючи модель IoT, користувачі можуть ділитися як інформацією, наданою поведінкою користувача, так і інформацією, зібраною підключеними речами у фізичному світі [2].

Процес розгортання Інтернету речей включає різні технології, такі як бездротові сенсорні мережі (WSN), RFID, Bluetooth, зв’язок ближнього поля (NFC), Інтернет-протокол (IP), електронний код продукту (EPC), бездротова точність (Wi-Fi), давачі і виконавчі механізми [3], [4].

Ключова мета парадигми IoT полягає в тому, щоб дозволити користувачам однозначно ідентифікувати, позначати, отримувати доступ та контролювати речі в будь-який час і в будь-якому місці через Інтернет [5]. Мережі взаємопов’язаних пристроїв можуть створювати численні інтелектуальні та автономні програми та послуги, які пропонують особисті та економічні вигоди для суспільства [6].

Хоча існує кілька визначень розумних будинків, з технічної точки зору, загальною концепцією є підключення давачів, побутової техніки та розумних пристроїв через Інтернет для досягнення віддаленого моніторингу, віддаленого доступу та віддаленого керування житловим середовищем [7].

Тому розумні середовища націлені на багаті комбінації невеликих обчислювальних засобів для виявлення та надання персоналізованих послуг користувачам, які взаємодіють та обмінюються інформацією з середовищем [5].

Розумний будинок також можна визначити як будинок, який автоматизований завдяки застосуванню парадигми IoT і здатний реагувати на вимоги своїх мешканців, забезпечуючи комфорт і безпеку [8].

З соціальної точки зору середовище розумного будинку називають навколишнім інтелектом, який є чутливим і адаптивним до сучасних людських і соціальних потреб [9].

Домени додатків IoT дуже важливі і з часом будуть збільшуватися, оскільки вони пропонують потужні засоби для допомоги та підтримки особливих потреб літніх людей та людей з обмеженими можливостями [10], дозволяючи користувачам контролювати та контролювати навколишнє середовище.

Основними цілями розумного будинку є підвищення рівня автоматизації будинку, спрощення управління енергією та зменшення викидів у навколишнє середовище [11]. Крім того, рівень споживання енергії та комфорт мешканців є ключовими факторами при проектуванні будь-якого розумного будинку.

Розумний будинок зосереджується на автоматизації та керуванні екологічними послугами, такими як системи денного освітлення, опалення, вентиляції та кондиціонування повітря, моніторинг і контроль, безпека та енергозбереження. Приклад контрольованих екологічних послуг розумного будинку показано на рис.1.2.

Технічно система домашньої автоматизації складається з п’яти будівельних блоків: керованих пристроїв, давачів і виконавчих механізмів, мережі керування, контролера та пристроїв дистанційного керування [12]. Повна картина компонентів IoT, постачальників послуг, різних рівнів IoT та їх можливих проблем безпеки представлена на рис.1.3.

З точки зору пропонованих послуг існують різні види послуг розумного будинку, такі як розумні будинки для безпеки, розумні будинки для охорони здоров’я, розумні будинки для догляду за людьми похилого віку, розумні будинки для догляду за дітьми та розумні будинки для енергоефективності [13].

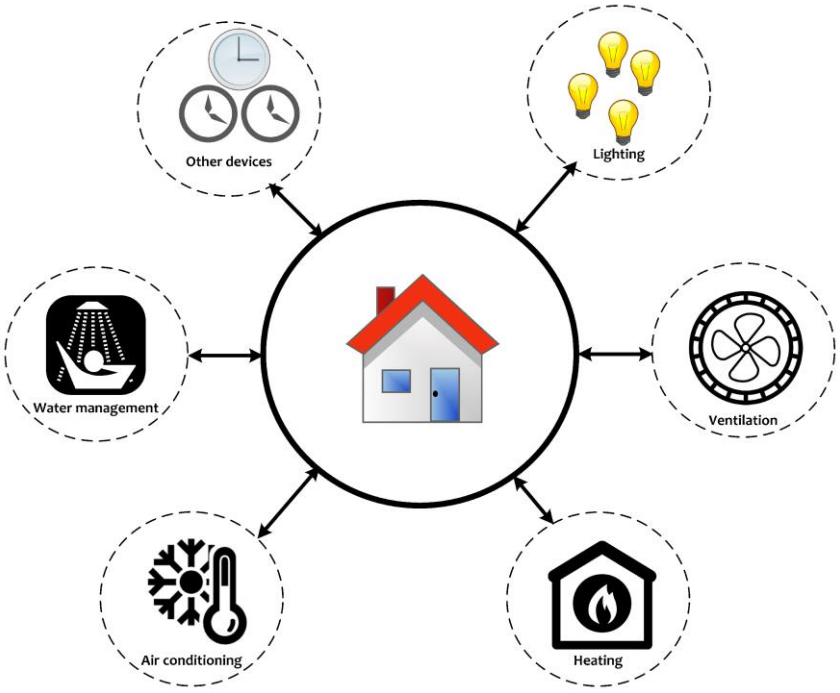

Рисунок 1.2 – Приклади деяких контрольованих екологічних послуг у розумних домах.

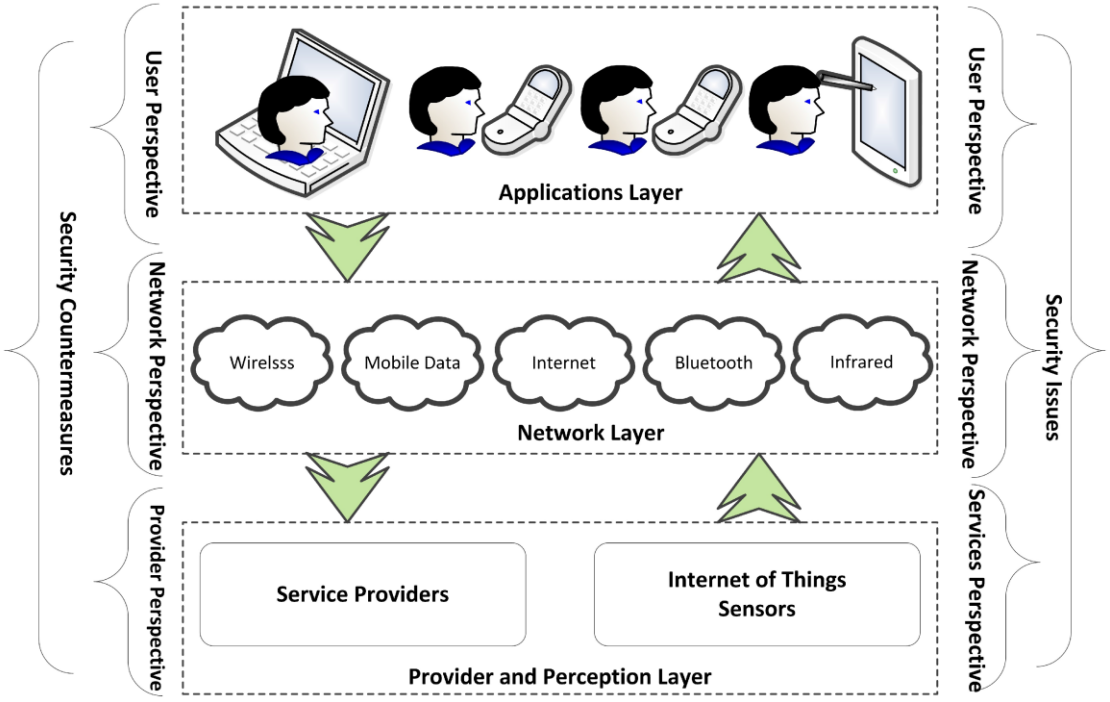

Рисунок 1.3 – Система IoT з точки зору постачальника, мережі та користувача.

На рис.1.3 висвітлені слабкі місця систем, що відповідають рівням IoT.

Системи домашньої автоматизації можна розділити на дві основні категорії: локально керовані або дистанційно керовані. Системи з локальним керуванням використовують внутрішній контролер для здійснення процесу автоматизації. Ці системи пропонують мешканцям повноцінного використання систем будинку зсередини свого будинку через стаціонарний або бездротовий інтерфейс.

Системи автоматизації з дистанційним керуванням використовують підключення до Інтернету, щоб запропонувати користувачам повний контроль зі свого персонального комп'ютера або мобільного пристрою. Система може працювати через інтеграцію з існуючою системою домашньої безпеки та нею можна керувати за допомогою смартфона через постачальника послуг домашньої безпеки [14].

Розгортання технології IoT для побудови розумних будинків, що стосується процесів автоматизації та контролю, створює нові проблеми безпеки. Таким чином, розумні будинки на основі IoT вимагають нового рівня вимог безпеки, оскільки середовище розумного дому міститиме важливу, конфіденційну та конфіденційну інформацію.

Оскільки технологія IoT відкриває можливості та створює ризики, розумний дім на основі IoT чутливий до вразливостей безпеки IoT і дуже вразливий до атак через Інтернет. Якщо розумний будинок або розумний пристрій зламано, зловмисник може вторгнутися в конфіденційність користувача, викрасти особисту інформацію та стежити за користувачами в середовищі розумного будинку [15].

Кількість пристроїв Інтернету речей швидко зросла, за останніми оцінками, у 2010 році було 12,5 мільярдів пристроїв, підключених до Інтернету, і, за прогнозами, до 2022 року кількість пристроїв збільшиться до 50 мільярдів [16].

Впроваджуючи технологію IoT у наші будинки, існує компроміс між зручністю, контролем, безпекою та конфіденційністю. Питання конфіденційності та безпеки слід розглядати з високим ступенем гнучкості, як стверджується в [17]. Тому безпека є однією з сфер, якій слід приділяти найвищий пріоритет при впровадженні технології розумного дому.

У цій кваліфікаційній роботі розглядається проблема ризиків безпеки розумного будинку на основі IoT.

Дослідницький внесок:

- по-перше, це дослідження застосовує методологію оцінки операційно-критичних загроз, активів і вразливості (OCTAVE), відому як методологія оцінки ризиків OCTAVE Allegro, щоб визначити ризики безпеки, що виникають як всередині, так і ззовні розумних будинків.
- по-друге, він розглядає цілісне уявлення про ризики кібер- та фізичної безпеки в домені розумного дому на основі IoT.
- по-третє, дослідження пропонує декілька контрзаходів для пом’якшення виявлених ризиків безпеки. Ці внески мають покращити існуючі політики безпеки для розумних будинків на основі IoT.

1.2 Огляд стану сучасних досліджень

Бездротові розумні давачі 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

(1) доступністю послуг (атаки переливання, заглушення та повторне відтворення),

(2) мережевою маршрутизацією (несанкціоноване оновлення маршрутизації та атаки на червоточину)

(3) автентифікацією вузлів (підслуховування та атаки імітації) [18].

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 [19].

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 інтерфейсу зв'язку.

Наприклад, маніпулювання цінами на електроенергію може призвести до зменшення рахунку супротивника за рахунок користувача (тобто рахунок користувача збільшується).

У дослідженні [20] запропоновано методику, яка може бути використана для ефективного виявлення маніпулювання цінами на електроенергію.

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 поширені атаки, швидше за все, будуть спрямовані на продукти групи контролюючих систем, оскільки вони найбільш схожі на існуючі цілі та підключені майже до будь-якого іншого розумного домашнього пристрою.

У дослідженні [21] було зроблено висновок, що супротивник 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 за допомогою інтерактивного цифрового телебачення або незаконно отримати доступ до телевізора за допомогою інших засобів контролю побутової техніки.

У [22] автори описали типи атак, які зазвичай спрямовані на WSN, і систему виявлення вторгнень, яку можна використовувати для запобігання від них.

Автори описали кібератаки, які відбуваються в бездротових сенсорних мережах, а саме: атаки відмови в обслуговуванні (DoS), неправильне спрямування, вибіркове пересилання, атаки, атаки Sybil, атаки на червоточини та атаки HELLO flood.

Конфіденційність та відстеження є двома найважливішими питаннями безпеки, які виникають із технологією RFID, хоча варто згадати й деякі інші, такі як фізичні атаки, DoS-атаки, підробка, атаки підробки, підслуховування та перехоплення, збирання та збирання мережевого трафіку в реальному часі. аналіз.

У [23] автори представили аналіз ризиків розумного будинку за допомогою методу аналізу ризиків інформаційної безпеки (ISRA). Підданість

ризику Системи була перевірена з точки зору конфіденційності, цілісності та доступності. Процес аналізу проводився з використанням емпіричної інформації, зібраної на етапі розробки програмного забезпечення.

Аналіз ризиків розглядав п’ять системних компонентів, а саме: давачі в розумних будинках, хмарні сервери, внутрішні шлюзи, додатки для смартфонів та інтерфейси програмного забезпечення (API).

Виявлені ризики були згруповані в п’ять категорій, а саме: програмне забезпечення, апаратне забезпечення, інформаційні, комунікаційні та ризики, пов’язані з людиною.

Всього було досліджено 32 ризики: дев’ять ризиків класифіковано як низькі, чотири – високі, решта – помірні. У той час як дослідження в [24] зосереджено на кіберризиках, робота, проведена в цьому дослідженні, розглядає цілісне уявлення про розумні домашні середовища шляхом визначення вразливостей кібер- та фізичної безпеки за допомогою методології OCTAVE Allegro.

У літературі є кілька досліджень оцінки ризику, наприклад [25]. 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.

Щоб досягти кращої безпеки та безпеки для дистанційно контролюваних і керованих систем, у дослідженні [26] було запропоновано політику лише телефонного роз’єму та стратегію віртуального середовища.

Метою політики лише відключення телефону було забезпечити, щоб зв’язок між пристроями розумного дому та віддаленими користувачами ініціювався пристроями розумного дому лише з внутрішнього боку.

Запропонована система дозволила користувачеві легко контролювати та керувати мікрохвильовою піччю, камерою спостереження, системою центрального опалення та пральною машиною з будь-якого місця за допомогою мобільних телефонів.

Робота, проведена в [27], визнала основні атаки на середовище «розумного дому»:

(1) підслуховування,

(2) атаки DoS,

(3) викрадання інформації,

(4) атаки «воронки» та «червоточини».

Дослідження [28] представило модель безпеки для захисту інформаційного потоку в домашній мережі інтелектуальної мережі.

Запропонована модель була здатна ефективно керувати інформаційним потоком у домашній мережі, використовуючи політику конфіденційного та неконфіденційного потоку інформації, не впливаючи на нормальну функціональність домашньої мережі.

1.3 Висновок до першого розділу

Наведені вище дослідження щодо розумних будинків зосереджені головним чином на можливих проблемах безпеки, які можуть виникнути в розумних середовищах.

Немає жодного дослідження, яке охоплює всю архітектуру IoT як з кібернетичної, так і з фізичної точки зору.

Проте виявлені дослідження були зосереджені або на парадигмі IoT, або на деяких частинах систем розумного дому.

Це дослідження робить крок далі, проводячи оцінку ризиків безпеки розумних будинків із підтримкою IoT, враховуючи як кібернетичні, так і фізичні точки зору.

2 ОЦІНКА РИЗИКІВ ДЛЯ IoT ТА СИСТЕМНА ОЦІНКА РОЗУМНИХ БУДИНКІВ

2.1 Підхід до оцінки ризиків

Методологією, прийнятою для цього дослідження, є методологія OCTAVE Allegro [29]. Методологію оцінки ризиків було обрано, щоб забезпечити комплексну оцінку ризиків, що дає надійні результати, і зосереджена переважно на інформаційних активах. Підхід OCTAVE Allegro аналізує, як інформація використовується користувачами або пристроями в системі. Крім того, він розглядає інформаційні контейнери як місця, де існує інформація та як ця інформація піддається ризику. Інші важливі активи можна ідентифікувати та оцінити шляхом встановлення зв'язків із спочатку ідентифікованим інформаційним активом.

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 надає рекомендації, робочі таблиці та анкети для проведення процесу оцінки ризику. 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, як показано на рис.2.1 [30].

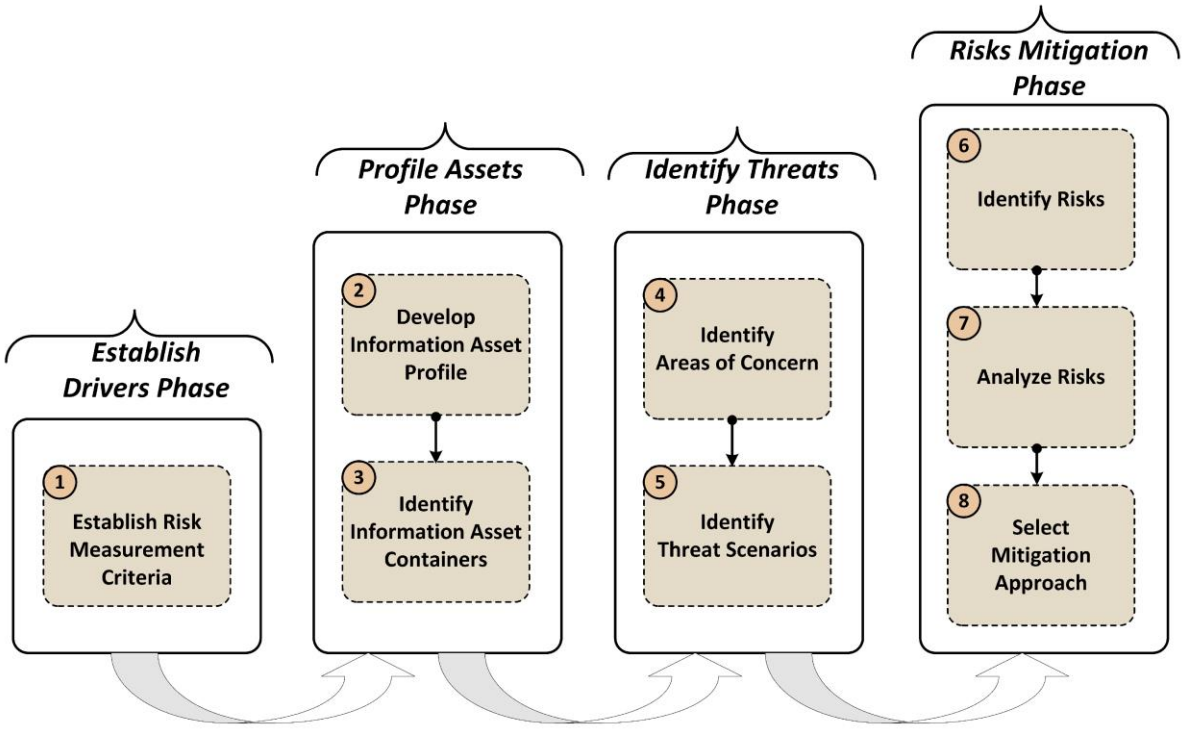

Рисунок 2.1 – Блок-схема методології OCTAVE Allegro з восьми кроків, які розділені на чотири великі групи.

Рисунок 2.1 було взято та змінено з [29].

Установіть фазу драйверів. Метою етапу встановлення драйверів є створення основи для оцінки ризику інформаційних активів шляхом розробки набору критеріїв вимірювання ризику для розумного будинку. Ці критерії дають можливість виміряти 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.

Фаза активів профілю. Під час фази профільних активів, яка включає кроки 2 і 3, показані на рис.2.1., спочатку визначаються критичні інформаційні активи, а потім їх профілюють. 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.

Визначте фазу загроз. На цьому етапі, який включає кроки 4 і 5, 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.

Фаза пом'якшення ризику. На етапі зменшення ризику, який включає кроки 6, крок 7 і крок 8, показані на рис.2.1, 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. 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.

2.2 Отримані результати

Результати цього дослідження представлені в табл.2.1 та табл.2.2, які дають кращий огляд виявлених загроз безпеці та потенційних ризиків у середовищі розумного дому на основі IoT. У двох таблицях показано інформаційні активи, які були ідентифіковані та використані в процесі оцінки ризиків, загрози, пов’язані з ними, а також наслідки чи потенційні впливи у вигляді конкретних ризиків та оцінок ризиків.

Таблиця 2.1 – Загрози безпеці, виявлені під час оцінки інформаційних ризиків з точки зору можливих загроз, пов'язаних з інформаційними активами.

№	Інформаційний актив	Можливі загрози безпеці
1	Облікові дані користувача	Видання себе за користувача Крадіжка особистих даних та облікових даних
2	Мобільні особисті дані та програми	Шкідливий код, введений у програми, встановлені на телефоні
3	Інформація, зібрана пристроями	Модифікація інформації Атаки відмови в обслуговуванні (DoS). Компрометація пристрою або давача
	Інформація про стан розумного будинку	Розкриття інформації Переривання функції
4	Структура розумного будинку Інформація про запаси	Отримайте доступ до інформації про запаси для пошуку конкретного пристрою з відомими вразливими місцями для атаки на розумні будинки
5	Інформація журналу	Отримайте доступ до даних журналів і отримайте корисну інформацію, що дозволить

		здійснити можливі атаки на систему розумного дому
6	Інформація, що передається через шлюз	Вкрасти інформацію з пакетів, переданих через шлюз
7	Інформація про налаштування розумного будинку	Модифікація інформації
8	Відеоканал з камер спостереження	Керуйте камерами, щоб стежити за користувачами та шпигувати за ними
9	Інформація про відстеження місцезнаходження	Спостереження за трафіком даних про місцезнаходження
10	Інформаційні ресурси (наприклад, зображення, документи та музика)	Зробіть збережені носії недоступними через апаратну несправність

Таблиця 2.2 – Ризики безпеки, виявлені під час виконання оцінки інформаційного ризику з точки зору можливих впливів та оцінки ризику.

№	**Можливі наслідки (ризики)**	**Оцінки ризику**
1	Несанкціонований доступ до основної системи розумного дому Несанкціоноване виконання операцій Втрата контролю над системою розумного дому	41
2	Зловмисник може фотографувати, записувати розмови та відстежувати місцезнаходження Зловмисник може дистанційно керувати смартфоном	41

	Зловмисник може здійснювати дзвінки та отримати доступ до мікрофона та камери телефону	
3	Зловмисник визначає найслабший пристрій із відомими вразливими місцями Зловмисник бере під контроль системи розумного дому Фінансові втрати	39
4	Вимірюваннями датчика маніпулюють, щоб проникнути в домашню систему Відстеження відсутності присутності призводить до проникнення в будинок Фінансові втрати	39
5	Зловмисник знаходить спосіб отримати доступ до основної системи Зловмисник змінює конфігурацію системи та додає задні двері Фінансові втрати	39
6	Системні ресурси вичерпуються за рахунок постійної самореплікації Можливість вивести систему з ладу, зробити її непридатною для використання Можливість введення в систему нових вразливостей безпеки	39
7	Труднощі в правильному налаштуванні системи розумного дому Неправильне використання систем SH з можливістю несправності Фінансові втрати	36
8	Порушення конфіденційності користувача Фінансові втрати	34
9	Порушення конфіденційності користувача	34

	Проникнення в розумний дім, якщо він вільний Фінансові втрати	
10	Порушення конфіденційності користувача Втрата інформації Шкода репутації	23

Таблиця 2.1 показує загрози, виявлені в результаті вивчення всієї системи розумного дому на основі IoT з точки зору кібер- та фізичної перспективи та відповідно до різних контейнерів активів. Виявлені ризики охоплюють аутентифікацію користувачів, поведінку користувачів, пристрої розумного дому та обмін даними між домашніми пристроями через Інтернет.

У таблиці 2.2 можливі впливи або потенційні ризики визначені та пов'язані з активами та загрозами, зазначеними в таблиці 2.1.

У таблиці 2.1 (1) зловмисник намагається видавати себе за законного домашнього користувача та діяти від його імені. Для досягнення мети противника доступ до облікових даних мешканців зазвичай складається з ідентифікатора користувача та пароля.

Доступ до облікових даних користувачів можна здійснити за допомогою соціальної інженерії або шляхом перехоплення звичайних даних, які надають доступ до ресурсів Інтернету речей.

Соціальну інженерію можна пояснити як підхід до обману або впливу на людей, щоб вони розкрили конфіденційну інформацію. Шкідливий код може бути введений в програми, встановлені в системі IoT, що дає змогу зловмисникам виконувати шкідливі операції.

Загроза ін’єкції шкідливого коду призначається (2), і вона також пов’язана з видаванням себе за користувача в (1).

Загрози компрометації пристрою в таблиці 2.1 (3) можуть призвести до ситуацій, коли давачі не зможуть виявити фізичні ризики, такі як пожежа, повінь або будь-який дивний рух у будинку. Крім того, викравши інформацію, зібрану встановленими давачами, як зазначено в (6), зловмисник

може впровадити шкідливий код, вірус або хробак у мережевий трафік, а потім випустити його в систему або мобільні програми. Інтенсивне використання ресурсів системи через постійне саморозмноження, що призводить до того, що система не може завершити відповідну роботу та виводить систему з ладу, що в кінцевому підсумку робить систему розумного дому повністю непридатною для використання.

Отримавши доступ до даних про місцезнаходження з мобільних пристроїв або пристроїв із підтримкою GPS, як зазначено в (9), супротивник може зробити висновок, що мешканця розумного будинку немає вдома, що може призвести до більш серйозних наслідків, таких як фінансові втрати через пограбування будинку. У таблиці 2.3 наведено додаткові відомості та приклади з реального світу, пов’язані з можливими ризиками безпеки, зазначеними в таблиці 2.2.

Таблиця 2.3 – Реальні приклади, пов'язані з виявленими загрозами та ризиками безпеки від різних інформаційних активів.

№	**Реальні приклади**
1	Неавторизована особа отримує необхідні облікові дані та може увійти в основну систему розумного дому.
2	Законний користувач втрачає свій мобільний пристрій або його викрадають, а потім маніпулюють програмами, пов’язаними з розумним домом. Телефонним додатком можна керувати дистанційно, вводячи шкідливий код.
3	Інформаційний актив навмисно змінюється зловмисниками, щоб інтелектуальний лічильник джерела живлення показував високе споживання електроенергії. Заклинювання та втручання на фізичному рівні можуть перешкодити давачам виявити такі ризики, як пожежа, повінь та несподіваний рух. Злагоджений давач руху можна використовувати, щоб визначити, коли

	вдома є люди. Статуси дверних замків і сигналізації можна використовувати, щоб визначити, коли розумний будинок зайнятий.
4	Зловмисники можуть отримати доступ до цього інформаційного активу, отримавши незашифрований резервний носій або за допомогою атаки соціальної інженерії.
5	Цей актив можна отримати, якщо дані журналу легко доступні через незахищений канал.
6	Цей актив можна отримати, якщо шлюз не захищений належним чином, наприклад, відкрита мережа Wi-Fi. Зловмисник може захопити з’єднання Wi-Fi, ввести шкідливий код, а потім взяти під контроль систему розумного дому.
7	Цей актив можна отримати, якщо інформаційний актив зберігається як файл даних у системі розумного дому (наприклад, ПК) без надійних механізмів аутентифікації.
8	Цей актив можна отримати, якщо такі пристрої передані несерйозному (ненадійному) сторонньому постачальнику послуг.
9	Цей актив можна отримати, якщо така інформація надсилається із системи відстеження на пристрій прослуховування у вигляді відкритого тексту та перехоплюється зловмисником.
10	Цей актив можна знайти фізично або в цифровому вигляді, наприклад, на паперах, компакт-дисках, DVD-дисках, носіях резервного копіювання, ПК, комунікаційних мережах або базах даних. Неавторизовані особи можуть отримати доступ до інформації, якщо вона не зберігається належним чином і безпечно.

Можливі контрзаходи з метою захисту інформаційних активів і, отже, підвищення безпеки розумного дому наведені в табл.2.4. Ключовими концепціями запропонованих підходів до пом'якшення є правильна технічна конфігурація, надійна аутентифікація користувача та поінформованість про

безпеку мешканців будинку. Запропоновані контрзаходи співвідносяться із загрозами та ризиками безпеки.

Таблиця 2.4 – Пропоновані заходи протидії безпеці та ризикам, які слід застосовувати в середовищах розумного дому на основі IoT.

№	**Можливі підходи до пом'якшення**
1	Контролювати доступ до системи за допомогою ефективних біометричних ідентифікаторів Запровадити програму поінформованості користувачів, щоб вони дізналися про соціальну інженерію Впровадити багатофакторну аутентифікацію
2	Уникайте використання незахищеного Wi-Fi, який надає хакерам доступ до особистих даних Налаштуйте безпечну мережу перед використанням програми для домашньої автоматизації Пам’ятайте про вкрадені або втрачені пристрої
3	Використовуйте безпечний канал зв’язку, використовуючи захищену віртуальну приватну мережу (VPN) Обмежте мережевий трафік так, щоб він був доступний лише авторизованим користувачам Розробити програму навчання безпеці для мешканців розумного дому
4	Використовуйте систему виявлення вторгнень (IDS) / систему запобігання вторгненню (IPS) Використовуйте механізми шифрування для передачі даних безпеки Робіть часті резервні копії даних, щоб зберегти копії конфіденційних даних
5	Захистіть фізичне розташування встановлених пристроїв Забезпечте безпечний доступ до інтерфейсів конфігурації пристроїв Замініть конфігурацію зручності використання за замовчуванням для

	встановлених пристроїв
6	Використовуйте звичайне обладнання та програмне забезпечення для збору та дослідження мережевого трафіку Створіть резервні копії конфігурацій робочої системи Завжди відстежуйте роботу системи, шукайте інциденти неправильної поведінки
7	Застосуйте надійний механізм аутентифікації, такий як аутентифікація відбитків пальців Пропонуйте програми підвищення обізнаності та навчання щодо безпеки системи Переконайтеся, що конфігурації системи безпечні та виконані справжніми людьми
8	Обмежте фізичний доступ до пристроїв лише справжнім людям Уникайте передачі інфраструктури на аутсорсинг стороннім постачальникам послуг Змініть конфігурації пристрою за замовчуванням, щоб досягти кращого рівня безпеки
9	Вимкніть непотрібні служби відстеження місцезнаходження на мобільних пристроях Розвивайте добре розуміння проблем конфіденційності користувачів Відстежуйте поведінку системи, щоб виявити будь-який підозрілий витік конфіденційності
10	Використовуйте лише надійні та автентичні мережі (провідні чи бездротові) Діліться інформацією обережно та в обмеженому порядку Використовуйте лише перевірених постачальників для отримання технічної підтримки у разі збоїв обладнання в розумному домі

Використання надійного методу аутентифікації, такого як біометричні ідентифікатори, є першим запропонованим контрзаходом у табл.2.4 (1).

Біометричні ознаки включають, наприклад, відбитки пальців, геометрію руки, сканування сітківки та візерунки райдужної оболонки ока, а також підпис. На додаток до потужних можливостей аутентифікації для цивільних і судово-медичних застосувань, біометричний розглядається як ненав'язливий підхід, який підходить для людей з психічними розладами, які не можуть пам'ятати свої облікові дані [31]. Він також пропонує хороші можливості для реалізації на апаратних платформах. Найкращий спосіб забезпечити безпеку уваги користувачів – це пропонувати постійні програми поінформованості про безпеку та навчальні програми [32].

Багатофакторна автентифікація – це процес ідентифікації користувача шляхом перевірки двох або більше заяв, представлених користувачем, кожна з різних категорій факторів, які включають те, що ви знаєте, що у вас є, або те, чим ви є.

Використання безпечних з'єднань Wi-Fi у середовищах розумного дому (2) зупиняє зловмисника від злому мережевого посилання, а отже, зменшує можливість доступу до конфіденційних даних, перевіряючи мережевий трафік, що проходить через нього, або впроваджуючи шкідливі коди в систему. система [33]. Зловмисник бездротового з'єднання створює вразливість, через яку зловмисник може ввести шкідливий код, який може бути виконаний деякими мобільними додатками. Зловмисники можуть використовувати готові інструменти, такі як WebView API, для вбудовування веб-вмісту в мобільні програми[34].

У табл.2.4 (3), використовуючи захищені канали зв'язку, обмежуючи доступ до трафіку лише авторизованими користувачами та проводячи навчання з безпеки, можна уникнути зміни інформації, розкриття інформації та компрометації пристрою чи давача. Це має зменшити потенційні ризики маніпулювання пристроєм, а отже, і фінансові втрати. Такий же сценарій можна виконати для (6). Постійна перевірка мережевого трафіку, забезпечення доступу до конфігурацій системи та моніторинг поведінки системи повинні запобігти крадіжці інформації через мережі розумного дому.

У свою чергу, це має зменшити час простою системи, зменшити можливість виснаження ресурсів системи та зменшити можливість впровадження нових вразливих місць у систему розумного дому.

Часте резервне копіювання та архівування даних (4) зберігає копії конфіденційних даних і захищає їх як від фізичного, так і від технічного пошкодження. Захист носіїв резервних копій має бути забезпечений шляхом наявності та застосування політики безпеки, призначення прав доступу до програмного забезпечення для резервного копіювання лише уповноваженим особам, зберігання резервних копій за межами сайту, контролю фізичного доступу, де зберігаються резервні копії, використання вогнетривкого та носійного сейфу, а також використання захищених паролем і зашифрованих резервних копій.

Слід брати до уваги захист фізичного місцезнаходження та доступу до інтерфейсів конфігурації пристроїв. Запропонований підхід до пом’якшення (5) представляє цю проблему та рекомендує міркування щодо фізичної безпеки. Якщо підхід біометричної аутентифікації буде інтегровано в систему розумного дому, той самий підхід можна використовувати для застосування логічних і фізичних обмежень безпеки. Застосування того ж механізму аутентифікації для логічного та фізичного контролю доступу має підвищити економічну ефективність системи розумного дому.

Варто зазначити, що запропоновані підходи до пом'якшення не пропонують повного вирішення виявлених загроз і ризиків; натомість контрзаходи розглядаються як методи стримування загроз безпеці та зменшення ризиків та наслідків безпеки. Суворе застосування контрзаходів безпеки призведе до зниження зручності використання системи. Знову ж таки, у табл.2.4 (9), повне вимкнення служби відстеження місцезнаходження може захистити частину конфіденційності користувача, але це може різко зменшити зручність використання пристрою. Тому слід шукати гарний баланс між безпекою системи та зручністю використання. Базу для покращення безпеки та конфіденційності для мобільних пристроїв, подібну

до запропонованої в [35], можна розглядати як частину підходів до пом’якшення.

Вибір справжніх постачальників пристроїв IoT і компонентів системи є частиною підходів до пом’якшення, зазначених у табл.2.4 (10). Пристрої IoT, куплені у хижих постачальників, можуть містити шкідливі коди або неправильні конфігурації, які можуть поставити під загрозу будь-які реалізовані обмеження безпеки. Крім того, для підтримки функціонування та стійкості системи, регулярне технічне обслуговування, перевірка конфігурації та виправлення помилок має здійснюватися справжнім і добре навченим персоналом відповідно до юридичних контрактів.

Застосування методології OCTAVE Allegro вимагає використання різних робочих таблиць для ідентифікації ризику та зменшення його наслідків. Включення до цього дослідження всіх розроблених робочих листів є складним завданням через обмеженість простору. Однак додаткові відомості щодо робочих таблиць і процесу оцінки ризику задокументовані в [36].

2.3 Ризики та підходи до зменшення впливу

Щодо рис.2.2, типове середовище розумного будинку на основі IoT включає широкий спектр пристроїв, послуг і постачальників. Пристрої розумного будинку та їх постачальників можна розділити на шість категорій, а саме: розподільники електроенергії, контролери розумного дому, будівельні програми, побутова техніка, комунікаційні пристрої, а також постачальники IT та телекомунікацій.

Архітектура розумного будинку на основі IoT розділена на три рівні; рівень пристрою або сприйняття, мережевий рівень і рівень додатків. На рис.2.2 представлено типове середовище розумного дому на основі IoT, а також показані виявлені ризики безпеки та відповідні протидії, зіставлені з

середовищем розумного дому. Насправді ризики безпеки можуть перетинати більше ніж один рівень IoT.

Наприклад, ризик несанкціонованого доступу можна знайти у доступі до основних конфігурацій системи, доступі до шлюзу IoT та входу до програм розумного дому. Тому в усіх цих пунктах необхідно впровадити надійний метод аутентифікації. Біометричні технології можуть бути вбудовані в багатофакторну аутентифікацію для створення надійного механізму аутентифікації користувачів.

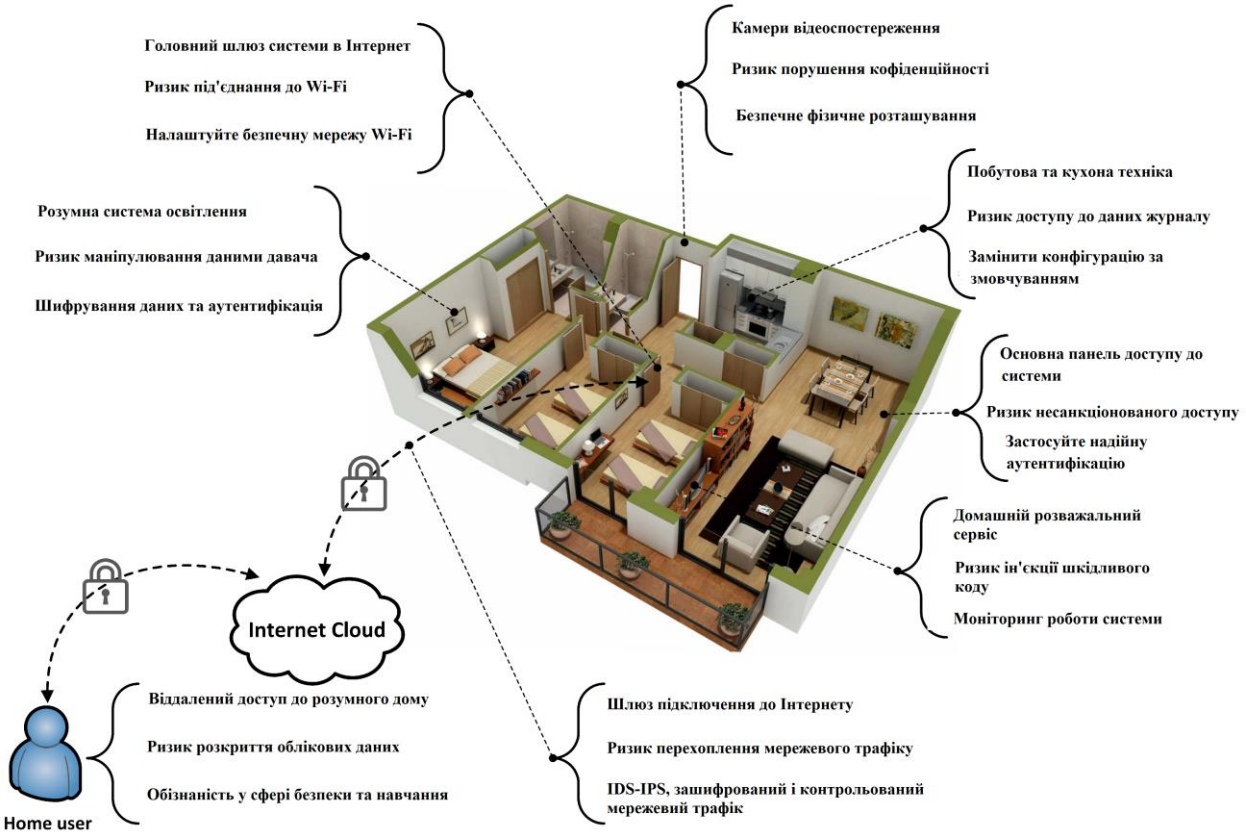

Рисунок 2.2 – Ризики безпеки та підходи до їх пом'якшення вказуються на реальне середовище розумного будинку.

План поверху був запозичений з Amazing Architecture [37].

Пристроям IoT, встановленим в розумних будинках, не вистачає високої обчислювальної потужності, великого простору для зберігання даних і великого розміру пам’яті. Тому впровадження інтенсивних рішень безпеки

може бути недоступним. Щоб запропонувати безпечне з'єднання між пристроями Інтернету речей і шлюзом в середовищі розумного дому, слід використовувати розподілений механізм шифрування або енергоефективне шифрування даних, наближене до алгоритму безпеки на основі трикутника, який використовує ефективне генерування ключів.

На межі мережевого рівня шлюз IoT працює як посередник між пристроями IoT і зовнішньою мережею. Шлюз IoT сприйнятливий до різних безпекових дій, таких як атака «людина посередині» та можливість збирати дані з пристроїв IoT. Таким чином, безпека шлюзу є важливою потребою для захисту потоку даних всередині та за межами середовища розумного дому. Захищений шлюз можна побудувати шляхом впровадження ефективних алгоритмів безпеки, таких як криптографія з еліптичною кривою та використання надійних підходів аутентифікації користувачів.

Щоб досягти високого рівня безпеки на всьому шляху передачі даних, від пристрою IoT до домашнього користувача на віддаленому боці, мережеве з'єднання з постачальником послуг Інтернету (ISP) має бути захищене. Загальні механізми безпеки мережі, такі як віртуальні приватні мережі (VPN), повинні бути реалізовані для надання зашифрованого посилання на провайдера. Розподілена система виявлення вторгнень (IDS) для мереж IoT має бути розгорнута. Крім того, для створення системи раннього попередження для виявлення будь-якої ненормальної поведінки в мережевому трафіку можна застосувати збір і моніторинг трафіку за допомогою стандартного обладнання та програмного забезпечення.

Розумні будинки на основі IoT дуже вразливі до атак через Інтернет. Якщо вся система розумного дому або розумний пристрій будуть скомпрометовані, зловмисник зможе вторгнутися в конфіденційність мешканців розумного дому, викрасти особисту або конфіденційну інформацію, контролювати систему розумного дому і навіть контролювати мешканців у середовищі розумного будинку. Оцінка ризику безпеки є початковим кроком до розуміння безпеки розумного дому, що дозволяє

виявити нові вразливості безпеки і, отже, полегшити встановлення відповідних вимог безпеки.

У цьому дослідженні було проведено комплексну оцінку ризиків безпеки з використанням OCTAVE Allegro та виявлено 10 критичних інформаційних активів. За допомогою оцінки ризиків було виявлено приблизно 15 ризиків безпеці з кібернетичної та фізичної точок зору, як зазначено в табл.2.1, які походять як всередині, так і за межами розумних будинків. Інтуїтивно, існують інші ризики, які не були зазначені через обмеження часу та збільшення кількості робочих аркушів у методі OCTAVE Allegro. Вплив ризиків безпеки описано в табл.2.2. Відповідні контрзаходи для пом’якшення ризиків до прийнятного рівня (оскільки 100% безпеки ніколи не досягнуто) запропоновані в таблиці 2.4.

Оцінка ризику має на меті визначити найсерйозніші потенційні небезпеки з даною оцінкою ризику, як показано в таблиці 2.2. Ризики фізичної безпеки відповідають пристроям і давачам. Ризики для обладнання стосуються крадіжки, дефектів, маніпуляцій та саботажу різних пристроїв всередині або за межами розумного будинку.

Найвищий показник ризику, який становить 41, пов’язаний з кібер-або інформаційними активами, такими як облікові дані користувачів, мобільні особисті дані та користувацькі програми. Усередині мережевого зв'язку, представленого мережевим рівнем на рисунках, основні ризики виникають через неадекватні механізми аутентифікації, відсутність безпечних каналів зв’язку та відсутність відповідних механізмів шифрування даних.

Надійні методи аутентифікації користувачів, такі як біометричні дані, слід розглянути та застосовувати до розумних будинків на основі IoT. Біометрична наука спрямована на ідентифікацію або перевірку людини на основі фізіологічних або поведінкових характеристик. Біометрія широко використовується як у цивільних, так і в судово-медичних дослідженнях. Завдяки своїй точності та надійності відбитки пальців як біометрична ознака можуть забезпечити високий рівень безпеки для кібер- та фізичного доступу

за короткий час обробки. Біометрія також має застосування в безпеці електронного здоров’я, яку можна використовувати для носних пристроїв розумного дому. Слід також розглянути протоколи аутентифікації для WSN та Інтернету речей.

Хоча в цьому дослідженні були запропоновані запобіжні заходи для пом’якшення ризиків безпеки, заходи обережності розглядаються на стороні кінцевого користувача. Виробники пристроїв і програмісти також повинні працювати над забезпеченням пристроїв із більшими можливостями безпеки та програм із безпечними та простими у налаштуванні інтерфейсами користувача. Урядові органи мають бути більш залученими, пропонуючи юридичну підтримку, стандарти безпеки та правоохоронну політику.

Запропоновані підходи до пом'якшення слід використовувати для зменшення загроз безпеці і, отже, для зменшення потенційних ризиків. Підвищення безпеки системи шляхом застосування більшої кількості рішень безпеки вплине на загальну зручність використання системи. Тому при використанні деяких із запропонованих контрзаходів необхідно збалансувати як безпеку системи, так і зручність використання. Крім того, інші фактори, які впливають на безпеку системи розумного дому, такі як рівень освіти мешканців та обізнаність щодо безпеки, слід брати до уваги при застосуванні контрзаходів безпеки в системах розумного дому на основі IoT.

Результати оцінки ризиків демонструють, що людський фактор є найбільшою причиною ризиків, оскільки не тільки адміністратори безпеки, але й люди різного віку з різним технічним досвідом можуть жити в розумних будинках, які представляють найбільший ризик. Мешканці розумного дому з обмеженими технічними знаннями більш вразливі до атак соціальної інженерії, а також до неправильного використання та неправильної конфігурації системи; таким чином, програма підвищення обізнаності в безпеці є обов’язковою в усіх випадках, щоб зменшити кількість ризиків безпеки та суму очікуваної шкоди.

Результати дослідження та запропоновані підходи до пом’якшення можуть дозволити всім зацікавленим сторонам, особливо кінцевим користувачам, знати про різні ризики безпеки та вжити відповідних заходів щодо пом’якшення безпеки для покращення безпеки в розумних будинках на основі IoT. Крім того, результати дослідження встановлюють корисні внески, які можна використовувати як основу для оновлення вимог безпеки в розумних будинках на основі IoT і для покращення існуючих політик безпеки.

2.4 Висновки до другого розділу

В другому розділі кваліфікаційної роботи проведено комплексну оцінку ризиків безпеки за допомогою методу OCTAVE Allegro та визначено 10 критичних кібер- та фізичних активів.

Як результат дослідження, було виявлено приблизно 15 ризиків безпеки, що виникають як всередині, так і за межами розумних будинків.

Наслідки цих ризиків були описані, припускаючи, що загрози реалізовані.

Запропоновано відповідні контрзаходи для зменшення ризиків до прийнятного рівня.

Складність розумних послуг не входила в рамки цього дослідження, таким чином, не було створено жодної системи розумного будинку.

.

3 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

3.1 Охорона праці

3.1.1 Причини електротравм та умови ураження людини електричним струмом

Чинна класифікація причин електротравматизму не відрізняється від загальноприйнятої класифікації причин нещасних випадків. Найбільш поширеними серед груп причин електротравматизму є організаційні та технічні.

Серед технічних причин слід виділити такі, як недосконаліть конструкції електроустановки і засобів захисту, допущені недоліки при виготовленні, монтажу і ремонті електроустановки, невідповідність будови електроустановок і захисних засобів умовам їх застосування тощо.

Організаційні причини електротравматизму в першу чергу пов’язані з недостатньою кваліфікацією працівників, порушеннями правил безпеки, відсутністю нагляду та контролю за виконанням робіт в електроустановках, несвоєчасним опосвідчення технічного стану електроустановок, відсутністю чи невідповідністю вимогам безпеки засобів захисту, експлуатацією несправних електроустановок тощо.

Серед безпосередніх причин попадання людей під напругу слід виділити такі:

- поява напруги на корпусі електроустановки або на електрично зв'язаних з ним металоконструкціях (далі – корпусі) у результаті пошкодження основної ізоляції;
- поява напруги на ізольованих струмовідних частинах електроустановок у результаті пошкодження додаткової ізоляції;

- доступність неізольованих струмовідних частин електроустановок, які знаходяться під напругою, що призводить до випадкового (прямого) дотику до них;
- потрапляння в зону розтікання струму в землі;
- виникнення електричної дуги між струмовідними частинами і тілом людини.

Струм через тіло людини проходить, якщо вона торкається одночасно двох точок, між якими існує різниця потенціалів, і при цьому виникає замкнене коло. Величина цього струму залежить від схеми включення, тобто від того, яких частин електроустановки торкається людина, а також від параметрів електричної мережі. Серед різноманітних схем включення людини в електричне коло слід виділити такі:

- одночасний дотик до двох полюсів мережі постійного струму або до фази та нуля однофазної мережі чи двох фаз трифазної мережі змінного струму;
- дотик до одного з полюсів чи однієї з фаз мережі змінного струму, при якому коло струму замикається через людину та землю;
- дотик до корпусу електроустановки, який у результаті пошкодження основної ізоляції знаходиться під напругою, за умови, що коло струму замикається через людину та землю;
- одночасний дотик до двох точок на поверхні землі, які в результаті замикань на землю знаходяться під напругою.

Практично при всіх схемах (крім першої) складовим елементом кола струму через тіло людини є земля. Тому при аналізі небезпеки враження струмом у різних електричних мережах необхідно зрозуміти сутність явищ, які виникають при замиканні мережі на землю та розтіканні струму в землі.

Замикання на землю може відбутися внаслідок появи контакту між струмовідними частинами і заземленим корпусом, при падінні на землю обірваного проводу, при порушенні ізоляції устаткування тощо. У всіх цих випадках струм від частин, що знаходяться під напругою, проходить у землю

через елементи обладнання, що мають контакт з ґрунтом, або спеціальний металевий електрод, який прийнято називати заземлювачем.

Розміри та форма елементів обладнання та електродів можуть бути різними. Різні можуть бути і електричні властивості ґрунту, особливо за наявності в місті замикання кількох шарів ґрунту з різними питомими опорами.

3.1.2 Засоби та заходи з безпечної експлуатації електроустановок

При розробці системи засобів та заходів з безпечної експлуатації електроустановок у першу чергу враховується:

- особливості виробничого середовища;
- доступність електрообладнання;
- величина напруги мережі живлення, В;
- величина струму замкнення на землю, А;
- конструктивні особливості мережі живлення – кількість фаз і режим нейтралі;
- величина опору і стан ізоляції провідників відносно землі;
- протяжність і розгалуженість мережі живлення.

Усі засоби і заходи електробезпеки прийнято поділяти на три групи: технічні, організаційні та електрозахисні.

Технічних засоби і заходи з електробезпеки реалізуються в конструкції електроустановок при їх розробці, виготовленні і монтажі відповідно до чинних нормативів. За своїми функціями технічні засоби і заходи електробезпеки поділяються на дві групи:

- технічні заходи та засоби електробезпеки, що використовуються за нормального режиму роботи електроустановок;
- технічні заходи та засоби електробезпеки, що використовуються за аварійних режимів роботи електроустановок.

До основних технічних засобів і заходів першої групи відносяться:

- захист від випадкового (прямого) доторкання до струмовідних частин;
- блокувальні пристрої;
- засоби орієнтації та сигналізації;
- захисне розділення електричних мереж;
- застосування малої (зверхнизької) напруги;
- компенсація ємнісних струмів замикання на землю;
- вирівнювання потенціалів.

Залежно від призначення, умов експлуатації та конструкції в електроустановках можуть застосовуватись одночасно декілька з перелічених технічних засобів і заходів.

Технічні заходи електробезпеки, що використовуються за аварійних режимів роботи електроустановок включають:

- · захисне заземлення;
- · занулення;
- · захисне відключення;
- · подвійна ізоляція.

Електрозахисні засоби – це технічні вироби, що не є конструктивними елементами електроустановок і застосовуються під час виконання робіт в електроустановках з метою запобігання електротравм.

Організаційні заходи і засоби щодо попередження електротравм регламентуються НПАОП 0.00-1.21-98 «Правила безпечної експлуатації електроустановок споживачів». Вони включають професійний відбір, професійну підготовку, навчання і перевірку знань працівників з питань електробезпеки, організацію безпечного виконання та нагляду за роботами в електроустановках, обмеження доступу в електроустановки, огляд, профілактичні, протиаварійні, приймально-здавальні випробування електроустановок, опосвідчення діючих електроустановок тощо.

3.2 Безпека в надзвичайних ситуаціях

3.2.1 Вплив факторів трудового середовища на здоров’я та працездатність розробника програм

Кожній організації властива своє специфічне трудове середовище. Трудова діяльність розробника програм завжди здійснюється в певному просторі і в певний час, з використанням конкретних засобів виробництва (засобів праці і предметів праці). Крім того, в процесі конкретної трудової діяльності між працівниками складаються і певні соціально-трудові відносини, які також динамічні, і змінюються залежно від зміни умов протікання трудової діяльності людини. Тому трудова діяльність здійснюється в певному середовищі, що розуміється як сукупність умов і впливів, наявних в деякому оточенні.

Під трудовою середовищем розуміються кошти, умови праці та взаємини людей, що беруть участь у трудовому процесі. Трудове середовище включає, як фізичні фактори (тобто санітарно-гігієнічні умови праці в широкому сенсі), так і техніко-технологічні чинники (засоби праці, предмети праці, технологічний процес).

Засоби праці представляють собою знаряддя праці, з допомогою яких люди впливають на предмети праці і, видозмінюючи їх, надають їм корисні властивості, здатні задовольняти певні потреби. До засобів праці відносяться машини й устаткування, інструменти і пристосування, виробничі будівлі та споруди, всі види транспорту, лінії електропередач, засоби зв'язку та сигналізації, засоби захисту працівників.

Основна роль в засобах праці належить саме знарядь виробництва, оскільки саме з їх допомогою людина перетворює предмети природи. Засоби праці та предмети праці у своїй сукупності складають засоби виробництва. Але, як відомо, самі по собі засоби виробництва функціонувати не можуть. Провідну роль поєднанні засобів праці і предметів праці, тобто

функціонування засобів виробництва належить людині. Тому вирішальним фактором процесу виробництва є робоча сила людини.

Засоби праці, предмети праці і люди в трудовій організації знаходяться в постійній взаємодії. Елементи фізичної трудового середовища схильні до постійних змін. Ці зміни відбуваються швидше серед елементів фізичної трудового середовища, що є продуктом людської праці, і породжують цілий ряд соціальних наслідків. Зміна матеріальних елементів фізичної трудового середовища, що є частиною природи, відбувається повільніше і до певного моменту з меншими соціальними наслідками. Положення людини в трудовому середовищі може бути різним, і залежить від того, переважають чи у фізичній трудової середовищі матеріальні фактори, що є частиною природи, або матеріальні чинники, є продуктом людської праці.

Відносини, в які вступають люди в процесі трудової діяльності, утворюють соціальну трудову середу. З соціологічної точки зору, праця, в першу чергу, являє собою відносини, що виникають між конкретними людьми – учасниками процесу праці. В ході трудової діяльності люди вступають у суспільні відносини, і в рамках цих суспільних відносин формуються міжособистісні відносини, взаємна поведінка індивідів. Характер міжособистісних відносин у трудовому середовищі, визначається соціальним статусом і роллю індивіда в трудовій організації, і має суттєвий вплив на поведінку людини в трудовому середовищі, і досягнення ефекту трудової діяльності.

На поведінку працівників у трудовій середовищі впливають: форми організації та оплати праці, психологічний клімат, виробничо-побутові умови, життєве оточення працівників, позавиробнича діяльність людей.

3.2.2 Умови праці, що впливають на виникнення зорового дискомфорту користувача ЕОМ

При організації праці, що пов'язана з використанням ВДТ ЕОМ і ПЕОМ, для збереження здоров'я працюючих, запобігання професійним захворювання і підтримки працездатності слід передбачити внутрішньозмінні регламентовані перерви для відпочинку.

Внутрішньозмінні режими праці і відпочинку мають передбачати додаткові нетривалі перерви в періоди, що передують появі об'єктивних і суб'єктивних ознак стомлення і зниження працездатності.

При виконанні протягом дня робіт, що належать до різних видів трудової діяльності, за основну роботу з ВДТ ЕОМ і ПЕОМ слід вважати таку, що займає не менше 50 % часу впродовж робочої зміни мають передбачатися:

- перерви для відпочинку і вживання їжі (обідні перерви);
- перерви для відпочинку і особистих потреб (згідно з трудовими нормами);
- додаткові перерви, що вводяться для окремих професій з урахуванням особливостей трудової діяльності.

Тривалість обідньої перерви визначається чинним законодавством про працю і Правилами внутрішнього трудового розпорядку підприємства (Організації, установи).

Внутрішньозмінні режими праці і відпочинку при роботі з ВДТ ЕОМ і ПЕОМ розроблено з урахуванням характеру трудової діяльності, напруженості і важкості праці диференційовано для кожної професії.

За характером трудової діяльності виділено три професійні групи згідно з діючим класифікатором професій ДК 003-95 і Зміна № 1 до ДК 003-95:

- розробники програм (інженери-програмісти) – виконують роботу переважно з відеотерміналом та документацією при необхідності і інтенсивного обміну інформацією з ЕОМ і високою частиною прийняття

рішень. Робота характеризується інтенсивною розумовою творчою працею з підвищеним напруженням зору, концентрацією уваги на фоні нервово-емоційного напруження, вимушеною робочою позою, загальною гіподинамією, періодичним навантаженням на кисті верхніх кінцівок. Робота виконується в режимі діалогу з ЕОМ у вільному темпі з періодичним пошуком помилок в умовах дефіциту часу;

− оператори електронно-обчислювальних машин – виконують роботу яка пов'язана з обліком інформації одержаної з ВДТ за попереднім запитом, або тієї, що надходить з нього, супроводжується перервами різної тривалості, пов'язана з виконанням іншої роботи і характеризується як робота з напруженням зору, невеликими фізичними зусиллями, нервовим напруженням середнього ступеня та виконується у вільному темпі;

− оператор комп'ютерного набору – виконує одноманітні за характером роботи з документацією та клавіатурою і нечастими нетривалими переключеннями погляду на екран дисплея, з введенням даних з високою швидкістю, робота характеризується як фізична праця з підвищеним навантаженням на кисті верхніх кінцівок на фоні загальної гіподинамії з напруженням зору (фіксація зору переважно на документи), нервово-емоційним напруженням.

Встановлюються такі внутрішньозмінні режими праці та відпочинку при роботі з ЕОМ при 8-годинній денній робочій зміні в залежності від характеру праці:

− для розробників програм із застосуванням ЕОМ, слід призначати регламентовану перерву для відпочинку тривалістю 15 хвилин через кожну годину роботи за ВДТ;

− для операторів із застосування ЕОМ, слід призначати регламентовані перерви для відпочинку тривалістю 15 хвилин через кожні дві години;

У всіх випадках, коли виробничі обставини не дозволяють застосувати регламентовані перерви, тривалість безперервної роботи з ВДТ

не повинна перевищувати 4 години. При 12-годинній робочій зміні регламентовані перерви повинні встановлюватися в перші 8 годин роботи аналогічно перервам при 8-годинній робочій зміні, а протягом останніх 4-х годин роботи, незалежно від характеру трудової діяльності, через кожну годину тривалістю 15 хвилин.

З метою зменшення негативного впливу монотонності є доцільним застосовувати чергування операцій усвідомленого тексту і числових даних (зміна змісту роботи). Чергування вводу даних та редагування текстів.

Для зниження нервово-емоційного напруження, стомлення зорового аналізатору, поліпшення мозкового кровообігу, подолання несприятливих наслідків гіподинамії, запобігання втомі доцільні деякі перерви використовувати для виконання комплексу вправ.

В окремих випадках – при хронічних скаргах працюючих з ВДТ ЕОМ і ПЕОМ на зорове втому незважаючи на дотримання санітарно-гігієнічних вимог до режимів праці і відпочинку, а також застосування засобів локального захисту очей – допускаються індивідуальних підхід до обмеження часу робіт з ВДТ, зміни характеру праці, чергування з іншими видами діяльності, не пов'язаними з ВДТ.

Активний відпочинок має полягати у виконанні комплексу гімнастичних вправ, спрямованих на зняття нервового напруження, м'язове розслаблення, відновлення функцій фізіологічних систем, що порушуються протягом трудового процесу, зняття втоми очей, поліпшення мозкового кровообігу і працездатності.

3.3 Висновок до третього розділу

В третьому розділі кваліфікаційної роботи освітнього рівня «Магістр» розглянуто причини електротравм та умови ураження людини електричним струмом та засоби та заходи з безпечної експлуатації електроустановок.

Описано фактори трудового середовища на здоров’я та працездатність розробника програм, я також звернено увагу на умови праці, що впливають на виникнення зорового дискомфорту користувача ЕОМ

ВИСНОВКИ

1) Проведено комплексну оцінку ризиків безпеки за допомогою методу OCTAVE Allegro та визначено 10 критичних кібер- та фізичних активів. Було виявлено приблизно 15 ризиків безпеки, що виникають як всередині, так і за межами розумних будинків. Наслідки цих ризиків були описані, припускаючи, що загрози реалізовані
2) Запропоновано відповідні контрзаходи для зменшення ризиків до прийнятного рівня. Це дослідження було зосереджено виключно на ідентифікації загроз безпеки, впливу або ризиків, а також відповідних контрзаходів для розумних будинків на основі IoT.
3) Дослідження було зосереджено виключно на ідентифікації загроз безпеки, впливу або ризиків, а також відповідних контрзаходів для розумних будинків на основі IoT.
4) Складність розумних послуг не входила в рамки цього дослідження; таким чином, не було створено жодної системи розумного будинку.
5) В подальшому необхідно розробляти структури для усвідомлення та оцінки ризиків безпеки в розумних будинках на основі IoT.

ПЕРЕЛІК ДЖЕРЕЛ

1. King, J.; Awad, A.I. A Distributed Security Mechanism for Resource-Constrained IoT Devices. Informatica (Slovenia) 2016, 40, 133–143.

2. Ning, H. Unit and Ubiquitous Internet of Things; CRC Press, Inc.: Boca Raton, FL, USA, 2013.

3. Miller, M. The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities are Changing the World; Que Publishing: Indianapolis, Indiana, 2015.

4. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Commun. Surv. Tutor. 2015, 17, 2347–2376.

5. Suryadevara, N.K.; Mukhopadhyay, S.C. Smart Homes: Design, Implementation and Issues; Springer: Cham, Switzerland, 2015.

6. Khan, R.; Khan, S.U.; Zaheer, R.; Khan, S. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. In Proceedings of the 10th International Conference on Frontiers of Information Technology, Islamabad, India, 17–19 December 2012; pp. 257–260.

7. Fabi, V.; Spigliantini, G.; Corgnati, S.P. Insights on Smart Home Concept and Occupants' Interaction with Building Controls. Energy Procedia 2017, 111, 759–769.

8. Harper, R. (Ed.) Inside the Smart Home: Ideas, Possibilities and Methods. In Inside the Smart Home; Springer: London, UK, 2003; pp. 1–13.

9. Aarts, E.; Marzano, S. The New Everyday: Views on Ambient Intelligence; 010 Publishers: Rotterdam, The Netherlands, 2003.

10. Nunes, R.J.C.; Delgado, J.C.M. An Internet Application for Home Automation. In Proceedings of the 10th Mediterranean Electrotechnical Conference, Lemesos, Cyprus, 29–31 May 2000; Volume 1, pp. 298–301.

11. Al-sumaiti, A.S.; Ahmed, M.H.; Salama, M.M.A. Smart Home Activities: A Literature Review. Electr. Power Compon. Syst. 2014, 42, 294–305. .

12. Kyas, O. How to Smart Home; Key Concept Press: Wyk auf Föhr, Germany, 2013.

13. De Silva, L.C.; Morikawa, C.; Petra, I.M. State of the Art of Smart Homes. Eng. Appl. Artif. Intell. 2012, 25, 1313–1321.

14. Shen, B.; Lin, Y.; Wang, X. Research on Data Mining Models for the Internet of Things. In Proceedings of the 2010 International Conference on Image Analysis and Signal Processing, Zhejiang, China, 9–11 April 2010; pp. 127–132.

15. Kang, B.; Liu, F.; Yun, Z.; Liang, Y. Design of an Internet of Things-based Smart Home System. In Proceedings of the 2011 2nd International Conference on Intelligent Control and Information Processing, Harbin, China, 25–28 July 2011; Volume 2, pp. 921–924.

16. Evans, D. The Internet of Things: How the Next Evolution of the Internet is Changing Everything; Cisco Internet Business Solutions Group (IBSG): San Jose, CA, USA, 2011.

17. 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, Ankara, Turkey, 26–28 June 2011; Özcan, A., Zizka, J., Nagamalai, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 288–296.

18. 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, Las Vegas, NV, USA, 9–13 January 2008; pp. 1–4.

19. Chaqfeh, M.A.; Mohamed, N. Challenges in Middleware Solutions for the Internet of Things. In Proceedings of the 2012 International Conference on Collaboration Technologies and Systems (CTS), Denver, CO, USA, 21–25 May 2012; pp. 21–26.

20. Liu, Y.; Hu, S.; Ho, T.Y. Vulnerability Assessment and Defense Technology for Smart Home Cybersecurity Considering Pricing Cyberattacks. In

Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, CA, USA, 2–6 November 2014; pp. 183–190.

22. Yoo, D.Y.; Shin, J.W.; Choi, J.Y. Home-network Security Model in Ubiquitous Environment. Proc. World Acad. Sci. Eng. Technol. 2007, 26. Available online: http://waset.org/publications/2785 (accessed on 6 March 2018).

23. Can, O.; Sahingoz, O.K. A Survey of Intrusion Detection Systems in Wireless Sensor Networks. In Proceedings of the 2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), Istanbul, Turkey, 27–29 May 2015; pp. 1–6.

24. Jacobsson, A.; Boldt, M.; Carlsson, B. A Risk Analysis of a Smart Home Automation System. Future Gener. Comput. Syst. 2016, 56, 719–733.

25. Rubio-Loyola, J.; Sala, D.; Ali, A.I. Accurate Real-time Monitoring of Bottlenecks and Performance of Packet Trace Collection. In Proceedings of the 33rd IEEE Conference on Local Computer Networks (LCN2008), Montreal, QC, Canada, 14–17 October 2008; pp. 884–891.

26. Wu, T.; Zhao, G. A Novel Risk Assessment Model for Privacy Security in Internet of Things. Wuhan Univ. J. Nat. Sci. 2014, 19, 398–404.

27. Yang, L.; Yang, S.H.; Yao, F. Safety and Security of Remote Monitoring and Control of Intelligent Home Environments. In Proceedings of the 2006 IEEE International Conference on Systems, Man and Cybernetics, Taipei, Taiwan, 8–11 October 2006; Volume 2, pp. 1149–1153.

28. Mantoro, T.; Ayu, M.A.; Mahmod, S.M.B. Securing the Authentication and Message Integrity for Smart Home using Smart Phone. In Proceedings of the 2014 International Conference on Multimedia Computing and Systems (ICMCS), Marrakech, Morocco, 14–16 April 2014; pp. 985–989.

29. Tong, J.; Sun, W.; Wang, L. An Information Flow Security Model for Home Area Network of Smart Grid. In Proceedings of the 2013 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, Nanjing, China, 26–29 May 2013; pp. 456–461.

30. Караллі, Р.А.; Стівенс, Дж.Ф.; Янг, Л.Р.; Wilson, WR. Представляємо Octave Allegro: покращення процесу оцінки ризиків інформаційної безпеки; Технічний звіт CMU/SEI-2007-TR-012, ESC-TR-2007-012; Інститут програмної інженерії: Піттсбург, Пенсильванія, США, 2007.

31. Караллі, Р.; Стівенс, Дж.; Янг, Л.; Wilson, W. The OCTAVE Allegro Guidebook, v 1.0 ; Сертифікаційна програма; Інститут програмної інженерії: Піттсбург, Пенсильванія, США, 2007.

32. Awad, A.I.; Hassanien, A.E. Impact of Some Biometric Modalities on Forensic Science. In Computational Intelligence in Digital Forensics: Forensic Investigation and Applications; Muda, A.K., Choo, Y.H., Abraham, A.N., Srihari, S., Eds.; Springer: Cham, Switzerland, 2014; Volume 555, pp. 47–62. .

33. Stallings, W.; Brown, L. Computer Security: Principles and Practice, 3rd ed.; Prentice Hall Press: Upper Saddle River, NJ, USA, 2014.

34. Yoo, D.Y.; Shin, J.W.; Choi, J.Y. Home-network Security Model in Ubiquitous Environment. Proc. World Acad. Sci. Eng. Technol. 2007, 26. Available online: http://waset.org/publications/2785 (accessed on 6 March 2021).

35. Luo, T.; Hao, H.; Du, W.; Wang, Y.; Yin, H. Attacks on WebView in the Android System. In Proceedings of the 27th Annual Computer Security Applications Conference, Orlando, FL, USA, 5–9 December 2011; ACM: New York, NY, USA, 2011; pp. 343–352.

36. Krupp, B.; Sridhar, N.; Zhao, W. SPE: Security and Privacy Enhancement Framework for Mobile Devices. IEEE Trans. Dependable Secur. Comput. 2017, 14, 433–446.

37. Bako, A. Internet of Things Based Smart Homes: Security Risk Assessment and Recommendations. Master’s Thesis, Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden, 2016. Available online: http://www.diva-portal.org/smash/get/diva2:1032194/FULLTEXT02.pdf (accessed on 6 March 2021).

38. Zadran, H. Amazing Architecture, 2017. Available online: http://amazingarchitecture.net/2017/05/19/elegant-home-plan-design-ideas/ (accessed on 6 March 2021).

39. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПІН 3.3.2.007-98 «Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» [Електронний ресурс] // Міністерство охорони Здоров'я України Головне санітарно-епідеміологічне управління. – 1998. – Режим доступу до ресурсу: https://zakon4.rada.gov.ua/rada/show/v0007282-98.

39. Охорона праці в галузі [текст] : навчальний посібник / П. С. Атаманчук, В. В. Мендерецький, О. П. Панчук, Р. М. Білий - К. : «Центр учбової літератури», 2017. - 322 с.

40. Зацарний В. В. Конспект лекцій з дисципліни Основи охорони праці / В. В. Зацарний. – Київ: НТУУ "КПІ", 2016. – 74 с.

41. Гандзюк М. П. Основи охорони праці: Підручник. / М. П. Гандзюк, Є. П. Желібо, М. О. Халімовський. – Київ: Каравела, 2011. – 384 с.

42. Жидецький В. Ц. Основи охорони праці / В. Ц. Жидецький, В. С. Джигирей, О. В. Мельников. – Львів: Афіша, 2000. – 348 с.

43. Березуцький В. В. Основи охорони праці / В. В. Березуцький, Т. С. Бондаренко, Г. Г. Валенко. – Харків: Факт, 2007. – 480 с.

44. Грибан В. Г. Охорона праці / В. Г. Грибан, О. В. Негодченко. – Київ: Центр учбової літератури, 2011. – 280 с.

45. Охорона праці (питання та відповіді) / В. М.Москальова, В.А. Батлук, С. Л. Кусковець, В. Л. Филипчук.–Львів: Магнолія 2006, 2011.– 452 с.

46. Безпека життєдіяльності людини [Електронний ресурс] – Режим доступу: https://pidruchniki.com/15021119/bzhd/meta_tsivilnogo_zahistu/ – (дата звертання 15.11.2021).

47. Кодекс цивільного захисту України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/5403-17/ – (дата звертання 25.113.2021).

48. ПОЖЕЖНА БЕЗПЕКА [Електронний ресурс] – Режим доступу: https://pidruchniki.com/15130616/bzhd/pozhezhna_bezpeka/ – (дата звертання 02.12.2021).

49. Основні поняття та визначення пожежної безпеки [Електронний ресурс] – Режим доступу: https://pidruchniki.com/1373051938220/bzhd/pozhezhna_bezpeka/ – (дата звертання 09.12.2021).

ДОДАТКИ

Додаток А

Тези конференції

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

IX НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

8–9 грудня 2021 року

ТЕРНОПІЛЬ
2021

УДК 004.6
О.О. Ліщук, Д.А. Радчук – ст.гр. СНм-61, Т.Б. Зощук –ст.гр.СТм-61
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗУМНІ МІСТА ТА ІНТЕРНЕТ РЕЧЕЙ

UDC 004.6
O.O. Lishchuk, D.A. Radchuk, T.B. Zoshchuk

SMART CITIES AND THE INTERNET OF THINGS

Концепція розумних міст, що формується, стає вагомим прикладом того, як інформаційні технології можуть покращити якість життя при оптимізації міської діяльності. Оскільки понад половина світового населення проживає в містах та стрімкий ріст населення в країнах із економікою, що розвивається, існує вплив на перепланування існуючих міст та проектування нових міст з нуля, щоб стати зеленими та ефективними, забезпечивши транспортні системи, енергетичні мережі та державні служби, які забезпечать життєдіяльність мешканців міст.

Існує ряд сучасний технологій, еволюція та розгортання яких справяє зростанню розумних міст. Розвиток розумних міст зосереджено на конкретних потребах інфраструктури, наприклад, зменшенні втрат води через старіння інфраструктури труб, підвищення ефективності перевезень тощо. Різні регіони мають різні потреби: Однак основні технологічні тенденції не відрізняються, і тому виникає необхідність застосування інформаційних технологій для задоволення потреб міста.Потрібно визначати свою роль в системі рішень розумного міста та працювати над розвитком партнерських відносин, які дозволять колективно пропонувати рішення для міст.Міста можуть запровадити проміжне програмне забезпечення та хмарні системи для збору та використання даних, які відбираються з різноманітних давачів встановлених на території міста. Зазначимо, що сьогодні мало хто з міст збирає та всебічно аналізує дані міст.

Конфіденційність – це ще одна важлива проблема. Багато громадян турбуються про конфіденційність розумних лічильників. Менше споживання енергії може означати, що мешканець не перебуває вдома. Електронні медичні записи є величезним ризиком конфіденційності, як показав досвід healthcare.gov. Набагато більше зусиль щодо розбудови довіри на основі захисту конфіденційності та безпеки даних має відбутися до того, як розумні міста отримають одобрення громадян.

Позитивним є те, що концепція розумного міста, схоже, набуває визнання, принаймні у державних та технологічних компаніях. Прогнози вагомі, але деякі дослідники стверджують, що це новаторство програми інтелектуальних ІКТ не можуть автоматично створити розумне місто.

Література.

1. Дуда О. М., Куцанець Н. Е., Мацюк О. В., Пасічник В. В. Системні комплекси інформаційних технологій у проектах «Розумне місто» // Системний аналіз та інформаційні технології: матеріали 18-І Міжнародної науково-технічної конференції SAIT 2016 / Київ: НТК «ІПСА», 2016. – С. 215–216.
2. Дуда О. М., Куцанець Н. Е., Мацюк О. В., Пасічник В. В. Концепт «розумне місто» та інформаційні технології BigData // Матеріали V науково-технічної конференції „Інформаційні моделі, системи та технології ", Тернопіль, 2018. – С. 30.

УДК 004.6
Д. Корж – ст. гр. СНмз-61, Д. Радчук, М. Тимків – ст. гр. СНм-61, А. Колесник, Т. Зощук - ст. гр. СТм-61,
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РІЗНИЦЯ МІЖ «ТРАДИЦІЙНИМИ» ТА «РОЗУМНИМИ» МІСТАМИ

UDC 004.6
D. Korzh, D. Radchuk, M. Tymkiv, A. Kolesnyk, T. Zoshchuk

THE DIFFERENCE BETWEEN "TRADITIONAL" AND "SMART" CITIES

У роботі [1] концептуалізують відмінності між «традиційними містами» та «розумними містами» на основі теорії систем. Відповідно, системи - це «сукупність взаємодіючих або взаємозалежних складових частин, що утворюють складне ціле. Кожна система окреслена своїми просторовими та тимчасовими межами, оточена і піддається впливу навколишнього середовища, описується її структурою та призначенням і виражається в її функціонуванні».

Автори [1] стверджують: «Систему можна розділити на підсистеми. Підсистема є відокремленим і ідентифікованою частиною (компонент, елемент) системи». Отже, термін «місто» можна визначити під цим поняттям як «велике і постійне людське поселення, що складається зі складних підсистем»

У цій концептуальній структурі «традиційні міста» з пов'язаними з ними підсистемами розглядаються як незалежні системи, які не здатні спілкуватися зі своїм власним безпосереднім оточенням. На відміну від цього, «розумні міста» характеризуються міськими системами та підсистемами, які взаємодіють та обмінюються інформацією з іншими системами та підсистемами відповідно. Наприклад, транспортні (підсистеми) можуть спілкуватися та обмінюватися даними чи інформацією з постачальником енергії або інтелектуальною мережею. Отже, концепція «розумного міста» може включати принаймні технологічну перспективу та підхід, що враховує взаємозв'язки міських систем і підсистем.

Інше визначення терміну «місто» дано в [2], стверджуючи, що місто було б «найдраматичнішим проявом людської діяльності на навколишньому середовищі».

Щоб дослідити цю взаємодію, ми повинні розглядати міста як «міські екосистеми», іншими словами, «міські екологічні простори», з їхніми біологічними та фізичними складностями, які взаємодіють один з одним. Міська екосистема – це динамічний організм, який складається з природного, побудованого та соціально-економічного середовища». Цю концепцію міста можна вважати дуже корисною для дебатів про розумне місто, оскільки вона акцентує на фізичні основи життя в містах.

Література.

1. Lom, M., Pribyl, O. (2020). Smart city model based on systems theory. International Journal of Information Management. DOI 10.1016/j.ijinfomgt.2020.102092.
2. Dizdaroglu, D., Yigitcanlar, T. (2014). A parcel-scale assessment tool to measure sustainability through urban ecosystem components: the MUSIX model. Ecological Indicators, 41, 115-130.
3. Дуда О. М., Куцанець Н. Е., Мацюк О. В., Пасічник В. В. Концепт «розумне місто» та інформаційні технології BigData // Матеріали V науково-технічної конференції „Інформаційні моделі, системи та технології ", Тернопіль, 2018. – С. 30.

УДК 004.6
Д. Корж – ст. гр. СНмз-61, Д. Радчук, О. Ліщук – ст. гр. СНм-61, А. Колесник, Т. Зощук – ст.гр. СТм-61,
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗУМНА СИСТЕМА ЕЛЕКТРОННОГО ЗДОРОВ'Я ДЛЯ ВІДСТЕЖЕННЯ ТА МОНІТОРИНГУ ПАЦІЄНТІВ, ПЕРСОНАЛУ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ

UDC 004.6
D. Korzh, D. Radchuk, O. Lishchuk, A. Kolesnyk, Zoshchuk T.

SMART ELECTRONIC HEALTH SYSTEM FOR TRACKING AND MONITORING OF PATIENTS, PERSONNEL IN REAL TIME

Охорона здоров'я в Україні відстає від розвинених країн світу через недостатню кількість медичних працівників та відсутність застосування інформаційних технологій відстеження та моніторингу. Ця спричинило такі проблеми, як неправильна ідентифікація пацієнтів, довгий час очікування пацієнтів та неможливість ефективно використовувати медичне обладнання.

Україна повинна адаптуватися до вимог сучасної охорони здоров'я. Аналіз публікацій показав, що системи інформаційних технологій почали впроваджуватися в деякі лікарні, але навіть у цих лікарнях ці технології використовуються недостатньо.

Метою цієї публікації є надання відповідного вибору технології відстеження та моніторингу в реальному часі в охороні здоров'я у формі інтегрованої системи RFID/ZigBee. Така система має цілісну структуру для закладів охорони здоров'я, якої слід дотримуватися для індивідуальних рішень для підвищення ефективності та продуктивності персоналу, а також для кращого догляду за пацієнтами та мінімізації довгострокових витрат.

Структура включає в себе контекстуальні елементи як із трикутника стратегії інформаційної системи (ISST), так і з систем факторів відповідності людини, організації та технології (HOT-fit), таким чином, що нова структура враховує технологічні, організаційні, людські та бізнесові фактори.

Були проаналізовані різні випадки, щоб покращити робочий процес лікарень, використовуючи запропоновану технологію, включаючи такі процеси, як переміщення персоналу та медичних засобів. Це призвело до необхідності візуалізація та управління знаннями для підтримки аналізу даних у реальному часі для прийняття рішень бізнес-аналітики.

Кінцевою метою цього аналізу є надання інтерактивних платформ для медичного персоналу для підвищення ефективності та продуктивності.

Результатом цих удосконалень буде забезпечення кращого догляду за пацієнтами, скорочення часу очікування пацієнтів, зниження витрат на медичне обслуговування та надання більше часу персоналу для надання покращеної допомоги, орієнтованої на пацієнта, у секторі охорони здоров'я.

Література.

1. Hameed, R.T., Mohamad, O.A. & Ţăpuş, N. (2016). Health Monitoring System Based on Wearable Sensors and Cloud Platform. 20th International Conference on System Theory, Control and Computing (ICSTCC). p.pp. 543–548.