УДК 004.4
DOI https://doi.org/10.32782/tnv-tech.2024.1.8

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ УПРАВЛІННЯ БЕЗПЕКОЮ РОЗУМНОГО БУДИНКУ

Савчук Т. О. *– доктор філософії, професор кафедри комп'ютерних наук*
Вінницького національного технічного університету
ORCID ID: 0000-0002-0061-6206

Капченко К. Г. *– студентка кафедри комп'ютерних наук*
факультету інтелектуальних інформаційних технологій та автоматизації
Вінницького національного технічного університету
ORCID ID: 0009-0006-8601-8237

Проведено аналіз сучасних програмних засобів управління безпекою розумного будинку, виявлено їх переваги та недоліки, в результаті чого було обгрунтовано необхідність створення інформаційної технології управління безпекою розумного будинку, яка забезпечить підвищення швидкості реакції на виявлену загрозу. Удосконалено математичну модель процесу управління безпекою розумного будинку за рахунок введення вектору факторів впливу на стан безпеки. Розроблено удосконалений алгоритм процесу управління безпекою розумного будинку, який забезпечить постійний аналіз безпеки розумного будинку та створення набору сценаріїв безпеки власником розумного будинку, що дозволить підвищити швидкість реакції на загрозу. Удосконалено алгоритм аналізу безпеки, який надасть можливість виявлення вразливостей безпеки розумного будинку, виявлення загрози, а також визначення її типу. Крім того, відповідно до узагальненого алгоритму, було сформовано структуру розроблюваної інформаційної технології управління безпекою розумного будинку, до якої входять модуль «Авторизація», модуль «Сценарії безпеки», модуль «Аналіз безпеки», модуль «Аналітика безпеки» та модуль «Виконання сценарію безпеки».

Розроблено алгоритми функціонування модулів «Аналіз безпеки», «Сценарії безпеки» та «Виконання сценарію безпеки». Запропоновано інформаційну технологію управління безпекою розумного будинку, яка дозволила підвищити швидкість реакції на виявлену загрозу, за рахунок можливості створення власником індивідуальних сценаріїв безпеки та постійного аналізу безпеки. Крім того проведено тестування запропонованої інформаційної технології управління безпекою розумного будинку, в результаті якого визначено, що швидкість забезпечення безпеки розумного будинку підвищилась на 20%, за рахунок застосування удосконаленого аналізу безпеки розумного будинку, який надає можливість створення власником будинку сценаріїв безпеки.

Ключові слова: *розумний будинок, інформаційна технологія, автоматизація, безпека, управління безпекою, сценарії безпеки, аналіз безпеки, реакція на загрозу.*

Savchuk T. O., Kapchenko K. G. Information technology for smart home security management

An analysis of modern software tools for managing the security of a smart home is carried out, their advantages and disadvantages are identified, as a result of which the need to create an information technology for managing the security of a smart home is substantiated, which will increase the speed of response to the identified threat. The mathematical model of the smart home security management process has been improved by introducing a vector of factors influencing the security status. An improved algorithm for the smart home security management process has been developed, which will provide continuous analysis of smart home security and the creation of a set of security scenarios by the smart home owner, which will increase the speed of response to the threat. The security analysis algorithm has been improved, which will make it possible to identify security vulnerabilities of a smart home, detect a threat, and determine its type. In addition, in accordance with the generalized algorithm, the structure of the developed information technology for managing the security of a smart home was formed, which includes the "Authorization" module, the "Security Scenarios" module, the "Security Analysis" module, the "Security Analytics" module, and the "Security Scenario Execution" module. The algorithms

for the functioning of the modules "Security Analysis", "Security Scenarios" and "Security Scenario Execution" have been developed. An information technology for managing the security of a smart home has been proposed, which made it possible to increase the speed of response to a detected threat by allowing the owner to create individual security scenarios and continuous security analysis. In addition, the proposed information technology for managing the security of a smart home was tested, as a result of which it was determined that the speed of ensuring the security of a smart home increased by 20%, due to the use of advanced security analysis of a smart home, which allows the owner to create security scenarios.

Key words: *smart home, information technology, automation, security, security management, security scenarios, security analysis, threat response.*

Кожен аспект нашого життя стає все більш цифровим і технологічно насиченим, розумні будинки визначають новий рівень зручності та інновацій в сфері житлового будівництва. Завдяки швидкому розвитку технологій, все більше людей стають зацікавленими в використанні розумних систем для контролю за своїми будинками.

Безпека розумного будинку є одним з найважливіших аспектів його функціонування, а тому важливим кроком у цьому процесі є аналіз безпеки розумного будинку. Розумний будинок може бути оснащений системами відеоспостереження, давачами пожежі, витоку газу або води, а також системою безпеки з автоматичним оповіщенням [1]. Оскільки розумний будинок використовує високотехнологічні пристрої та системи, забезпечення його безпеки має велике значення.

Використання програмних додатків для управління безпекою розумного будинку відзначається зручністю перегляду відеозаписів з камер спостереження, отриманням сповіщень про управління освітленням та терморегулюванням [2]. Проте, для забезпечення повноцінної безпеки розумного будинку, необхідні удосконалення, як у самому додатку, так і у процесі аналізу безпеки.

Процес управління безпекою розумного будинку буде швидший та надійніший, якщо буде відбуватись на підставі виявлення не тільки загроз безпеці, а й вразливостей та визначення потенційних загроз, а також, за можливості, швидкої реакції на виявлену загрозу за рахунок завчасно розроблених сценаріїв безпеки власником будинку, що реалізовуватимуться при використанні відповідної інформаційної технології.

Таким чином, створення інформаційної технології управління безпекою розумного будинку, що забезпечить підвищення швидкості реакції на загрозу безпеці розумного будинку є актуальною задачею.

Ринок сучасних засобів управління безпекою розумного будинку постійно розширюється, і на ньому доступні різноманітні програмні засоби з різною функціональністю. Майже всі вони є універсальними, але мають певні недоліки. Серед популярних сучасних засобів для управління безпекою розумного будинку слід відзначити Samsung SmartThings та Google Home.

Додаток Samsung SmartThings, для управління розумним будинком, надає можливість керувати безпекою та його різними аспектами [3]. Перевагами Samsung SmartThings є можливість інтеграції з великою кількістю пристроїв та можливість розширюваності. SmartThings підтримує широкий спектр різних розумних пристроїв, включаючи освітлення, термостати, давачі, камери та інші. Це сприяє збільшенню автоматизації будинку та надає можливість керування різними пристроями. Проте, ця платформа має певні недоліки: нестабільна робота, помітні затримки або відмови працювати, що зменшує швидкість реакції, а також відсутнє забезпечення оновлень безпеки й відслідковування загроз.

Google Home – додаток управління безпекою розумного будинку від Google, що пропонує відеоспостереження, давачі руху, а також можливість керування розумним будинком через мобільний додаток або голосовими командами. Він інтегрується з іншими пристроями розумного будинку, такими як термостати і освітлення [4]. Перевагами цього додатку є те, що він повністю інтегрований з екосистемою Google, що означає, що ви можете використовувати його для доступу до різних послуг Google, а також можливість створення сценаріїв з голосовими командами, які полегшують управління пристроями розумного будинку. Серед недоліків можна виділити те, що додаток не має добре налаштованої і автоматизованої системи оновлень, яка регулярно перевіряє наявність нових загроз безпеці.

Результати аналізу сучасних засобів управління безпекою розумного будинку за основними характеристиками представлено в таблиці 1.

Таблиця 1

Характеристика програмних засобів управління безпекою розумного будинку

Характеристика	Samsung SmartThings	Google Home
Зрозумілий інтерфейс	+	+
Сумісність з іншими пристроями	+	+
Інтеграція з системами	+	+
Оновлення безпеки	-	-
Можливість створення сценаріїв безпеки	-	-
Автоматизація	-	-
Легкість налаштування	-	+

За результатами аналізу визначено, що засіб управління безпекою розумного будинку Google Home може бути використаний для процесу управління безпекою розумного будинку, але він потребує удосконалення, що забезпечить підвищення швидкості реакції на загрозу безпеці та розширення функціоналу. Таким чином, доцільним є створення програмного засобу, який надаватиме можливість користувачу створювати індивідуальний сценарій із заходами безпеки та забезпечить надійне управління безпекою розумного будинку за рахунок вчасного виявлення потенційних загроз та підвищення швидкості реакції на загрозу.

Для удосконалення математичної моделі процесу управління безпекою розумного будинку введемо додаткові характеристики.

Нехай $S_i(t)$ це *i*-й стан безпеки будинку в момент часу *t*.

Тоді, стан безпеки можна описати з використанням двійкової логіки, а саме: $S_i(t) = 1$, якщо є потенційна загроза, та $S_i(t) = 0$, якщо загрози немає. $Sensor(t) \{Sensor_1(t), Sensor_2(t), ..., Sensor_n(t)\}$ – вектор значень давачів, необхідних для аналізу стану безпеки, де $Sensor_i(t)$ представляє вимірювання *i*-го давача в момент часу *t*.

Таким чином, вектор факторів безпеки $V_i(t)$ у *i*-му стані безпеки може бути визначений як функція від значень різних давачів, які впливають на стан безпеки засобу:

$$V_i(t) = f(Sensor_1(t), Sensor_2(t), ..., Sensor_n(t)).$$

Тоді, задача управління безпекою розумного будинку зводиться до визначення:

$$F(F_j(S_i(t))),$$

де $F(F_j(S_i(t)))$ – це множина сценаріїв безпеки за i-м станом $S_i(t)$.

Кожна функція $F_j(S_i(t))$ визначає конкретний j-й сценарій або набір дій, які користувач встановлює для управління безпекою розумного будинку за i-м станом $S_i(t)$ в разі виявлення потенційної загрози.

Нехай $A(S_i(t))$ буде алгоритмом аналізу стану безпеки в момент часу t. Він визначає, чи є потенційна загроза в системі на основі отриманих даних. Таким чином, реакція на події залежить від аналізу, проведеного алгоритмом $A(S_i(t))$, і налаштувань користувача. Якщо $A(S_i(t))$ виявляє загрозу, і якщо користувачі налаштували сценарій $F_j(S_i(t))$, то відбувається відповідна реакція на загрозу.

Стан безпеки $S_i(t)$ може оновлюватися в момент часу $(t + dt)$, де dt – це інтервал часу протягом якого оновлюється стан безпеки на основі отриманих даних та виконаних сценаріїв.

Отже в кожний наступний момент часу з урахуванням факторів впливу g та відповідно обраних сценаріїв безпеки розумного будинку за i-м станом $S_i(t)$, визначатиметься як:

$$S_i(t+dt) = g(V_i(t), F_1(S(t)), F_2(S(t)), ..., F_n(S(t))),$$

де $g(V_i(t), F_1(S(t)), F_2(S(t)), ..., F_n(S(t)))$ – вектор факторів впливу на стан безпеки.

Ця удосконалена математична модель дозволяє визначити взаємозв'язок між станом безпеки, користувацькими сценаріями та алгоритмом аналізу, а введені формули надають точну характеристику того, як сенсори та інші фактори впливають на стан безпеки системи розумного будинку. Зокрема, вона враховує багатоаспектність безпеки, оскільки стан безпеки визначається не лише одним, але різними давачами.

Існуючі засоби з управління безпекою розумного будинку в основному використовують ряд основних функцій, таких як:

1. Аналіз безпеки, який передбачає відстеження та оцінку стану безпеки розумного будинку, що дозволяє виявляти загрози безпеці.

2. Відображення інформації про виявленні загрози, що передбачає інформування користувачів про виявлені загрози та їхній стан.

Ці функції допомагають забезпечувати ефективне управління безпекою розумного будинку, надання користувачам інформації, а також контроль над станом безпеки [5].

Для розширення функціоналу засобів управління безпекою розумного будинку доцільно надати користувачеві можливість створення індивідуальних сценаріїв безпеки, які б зберігались в базі даних, та виконувались за умови виявлення загрози, а також забезпечити проведення аналізу безпеки розумного будинку, який дасть можливість виявлення вразливостей систем розумного будинку, виявлення загрози та визначення її типу. Після проведення аналізу безпеки розумного будинку та за умови ідентифікації певної загрози, буде виконуватись відповідний сценарій безпеки.

Одним з основних функціоналів інформаційної технології управління безпекою розумного будинку є створення акаунту власника розумного будинку та ідентифікація користувача. Важливим функціоналом є створення індивідуальних сценаріїв безпеки та перегляду існуючих. Не менш важливим функціоналом є проведення аналізу безпеки розумного будинку, який відповідає за отримання

інформації про стан системи розумного будинку та ідентифікує можливу загрозу. Також важливим є відображення результатів актуальної аналітики безпеки та виконання певного сценарію безпеки.

На основі описаного функціоналу сформовано узагальнений алгоритм процесу управління безпекою розумного будинку, UML-діаграма активності якого наведена на рисунку 1.

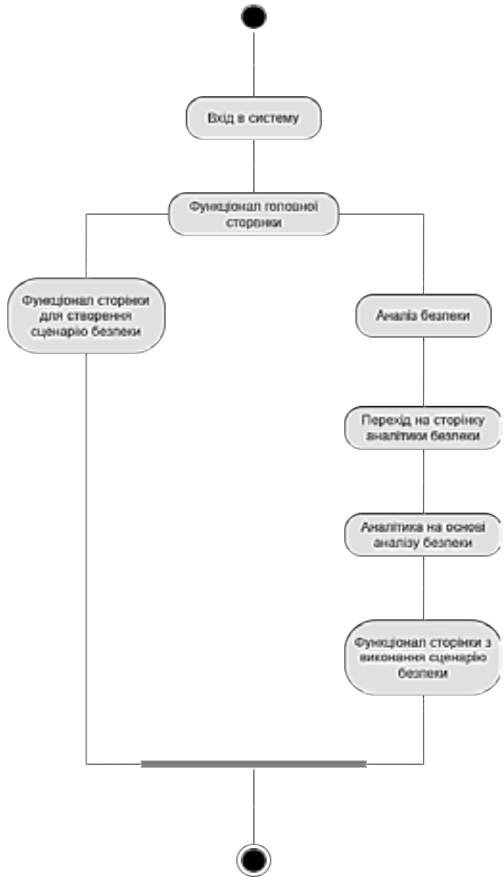

Рис. 1. UML-діаграма активності процесу управління безпекою розумного будинку

Запропонований узагальнений алгоритм для управління безпекою забезпечить постійний аналіз безпеки та пришвидшення реакції на виявлену загрозу, завдяки створення набору сценаріїв безпеки.

Реалізація запропонованого алгоритму для управління безпекою розумного будинку можлива за наявністю у складі інформаційної технології таких модулів: модуль «Авторизація», модуль «Аналіз безпеки», модуль «Сценаріїв безпеки», модуль «Аналітики безпеки», модуль «Виконання сценарію безпеки».

Модуль авторизації отримує першочергову інформацію про користувача, який хоче здійснити вхід та перевіряє чи є він поточним користувачем, відповідно до чого дає доступ до основного функціоналу або повертає помилку. Модуль сценаріїв безпеки дозволяє додавати сценарії безпеки шляхом отримання інформації

від користувача через користувацький інтерфейс, редагувати та видаляти їх за потреби. Модуль аналізу безпеки отримує інформацію про поточний стан систем розумного будинку та проводить аналіз вразливостей. А також ідентифікує наявні загрози безпеці за рахунок отримання інформації з відповідних давачів або камер. Модуль аналітики безпеки отримує дані про стан безпеки та формує звіт за певний проміжок часу, а також надає оцінку критичності небезпеки у разі її виявлення. Модуль виконання сценарію безпеки отримує інформацію про оцінку критичності небезпеки, відповідно до чого запускає алгоритм дій прописаний в відповідному сценарію безпеки.

Структура інформаційної технології управління безпекою розумного будинку наведена на рисунку 2.

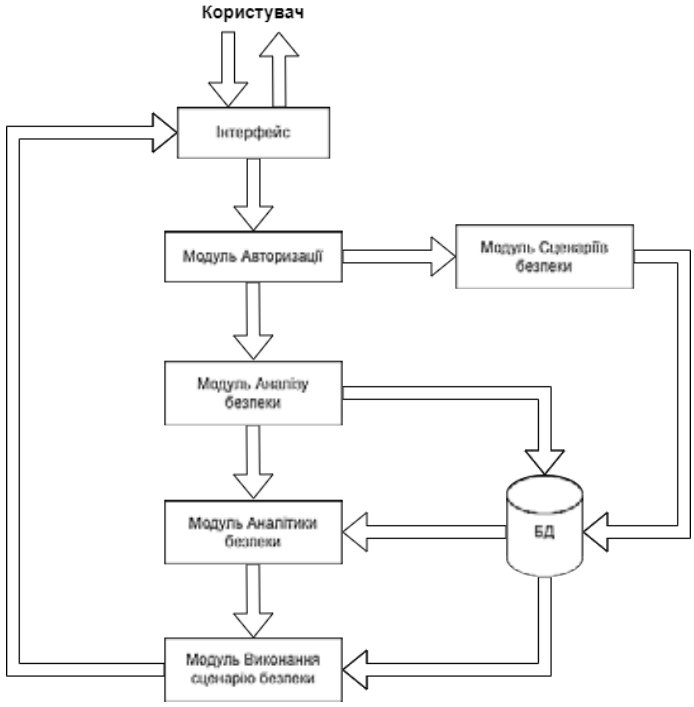

Рис. 2. Структура інформаційної технології управління безпекою розумного будинку

Взаємодія користувача з певним модулем відбувається через зрозумілий інтерфейс. Першим модулем з яким взаємодіє користувач є модуль «Авторизації» У користувача є можливість зареєструватись та увійти до інформаційної технології. Після входу користувач має можливість взаємодіяти з такими модулями: модуль «Сценаріїв безпеки», у якому необхідно створити власні сценарії безпеки, модуль «Аналіз безпеки», за допомогою якого буде відбуватись аналіз безпеки розумного будинку та виявлення можливих вразливостей систем розумного будинку та потенційних загроз безпеці, модуль «Аналітики безпеки», який буде надавати можливість спостерігати за аналітичними даними зібраними в ході роботи інформаційної технології, а також модуль «Виконання сценарію безпеки». Модулі «Сценарії безпеки», «Аналіз безпеки» та «Аналітика безпеки» будуть взаємодіяти з базою даних для відправки та отримання певних необхідних даних.

Таким чином, запропонована структура інформаційної технології управління безпекою розумного будинку дозволить розширити функціонал в існуючих додатках з управління безпекою розумного будинку, а також забезпечить швидку реакцію на виявлену загрозу безпеці розумного будинку, за рахунок наявності модулів «Сценарії безпеки», «Аналіз безпеки» та «Виконання сценарію безпеки».

Створення удосконаленого алгоритму аналізу безпеки розумного будинку є актуальним завданням, оскільки модуль «Аналіз безпеки» є одним з основних модулів інформаційної технології управління безпекою розумного будинку.

Удосконалений алгоритм аналізу безпеки розумного будинку базується на зниженні ризиків несанкціонованого доступу або виходу з ладу систем таких, як відеоспостереження, давачі пожежі і тд., та забезпеченні надійного захисту будинку. Основою для аналізу безпеки розумного будинку є використання статистичних методів, що дозволяють об'єктивно оцінити стан безпеки будинку і знизити вплив суб'єктивних факторів.

Алгоритм аналізу безпеки розумного будинку складатиметься з таких кроків:

Крок 1. Отримання інформації про поточний стан безпеки розумного будинку у вигляді технічних характеристик та функціональних можливостей компонентів розумного будинку, що пов'язані з безпекою, такі як відеокамери, давачі руху, системи тривоги, давачі пожежі, тощо та визначення їх поточного стану.

Крок 2. Аналіз вразливостей – виявлення потенційних вразливостей систем розумного будинку, за рахунок визначення поточного стану компонентів розумного будинку та отримання списку потенційних вразливостей таких, як слабкі місця у захисті будинку, незахищеність мережі, слабкі паролі, несправність давачів чи відеоспостереження і т. д.

Крок 3. Розробка заходів безпеки у вигляді набору заходів безпеки для запобігання та мінімізації виявлених загроз і вразливостей. Це може включати встановлення сильних паролів, шифрування комунікацій, використання двофакторної аутентифікації, оновлення програмного забезпечення, та регулярну перевірку на наявність вразливостей. А також набор сценаріїв при виявлені певної загрози безпеці, створений власником у додатку.

Крок 4. Тестування безпеки за допомогою аудиту безпеки, основна ідея якого полягає в систематичному скануванні розумного будинку з метою виявлення потенційних вразливостей. Може включати: перевірку мережевої безпеки, перевірку наявності захисту від хакерських атак, перевірку справності давачів безпеки та інших компонентів системи. Це допоможе виявити потенційні слабкі місця і вразливості, які можуть бути використані зловмисниками.

Крок 5. Ідентифікація загроз – визначення потенційних загроз безпеці будинку за рахунок отримання сповіщень про загрозу. Це можуть бути фізичні загрози (наприклад, крадіжки, пожежі) або цифрові загрози (наприклад, хакерські атаки, злам системи). Ідентифікація загрози відбуватиметься з використанням алгоритмів машинного навчання із урахуванням попереднього аналізу вразливостей систем розумного будинку та зібраних даних з давачів безпеки та відеоспостереження.

Крок 6. Механізм реагування на виявлену загрозу. Реагування відбуватиметься з урахуванням сценаріїв. При виявлені загрози, власнику будинку та службі моніторингу безпеки надійде сповіщення, що демонструватиме потенційну загрозу, а також буде виконано відповідний сценарій для забезпечення безпеки.

Таким чином, запропонований алгоритм аналізу безпеки розумного будинку, дасть можливість виявлення вразливості безпеки розумного будинку, виявлення і визначення її загроз.

Для розширення функціоналу засобів управління безпекою розумного будинку, необхідно реалізувати функціонал модуля сценаріїв безпеки. Цей модуль дозволить користувачам створювати, налаштовувати та керувати різними сценаріями безпеки в їхньому розумному будинку. Сценарії безпеки можуть включати в себе різні дії та реакції на події, такі як відкриття дверей або вікон, виявлення диму або витоку газу тощо. Щоб забезпечити користувача можливістю виконання певних дій по управлінню сценаріями безпеки, необхідно щоб даний модуль забезпечував виконання таких функцій:

1. Створення нового сценарію.
2. Отримання переліку наявних сценаріїв.
3. Отримання певного сценарію.
4. Редагування та видалення сценарію.

Процес управління сценаріями безпеки в інформаційній технології управління безпекою розумного будинку забезпечується функціонуванням модуля сценаріїв безпеки, UML-діаграма активності якого зображена на рисунку 3.

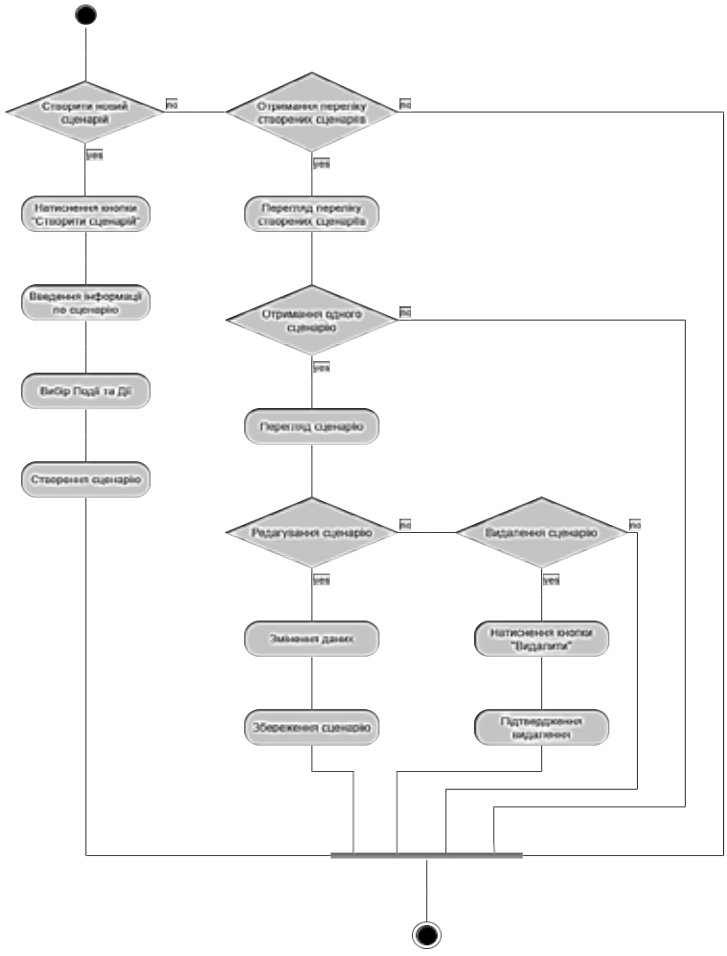

Рис. 3. UML-діаграма активності модуля сценаріїв безпеки

З метою забезпечення вчасного доступу власника розумного будинку до інформації про загрозу безпеці, інформаційна технологія управління безпекою будинку повинна передбачати цей крок у наперед створеному ним сценарію.

Реагування на загрозу буде відбуватися таким чином:

1. Пошук відповідного сценарію безпеки в базі даних (БД), а саме при виникненні загрози виконується пошук в базі даних сценарію з відповідною подією. При цьому, в БД зберігаються створені власником розумного будинку сценарії безпеки, які містять інструкції, що виконуються в разі ідентифікації певної загрози.

2. Виконання дії за сценарієм безпеки, а саме множини відповідних інструкцій за сценарієм, таких як:

– активація системи сигналізації та сповіщення служб безпеки або власника будинку;

– запуск відеоспостереження та запис подій;

– закриття та блокування дверей або вікон для запобігання несанкціонованому доступу;

– вимикання або ізоляція певних систем для запобігання подальшим загрозам;

– повідомлення власника будинку чи інших авторизованих осіб.

UML-діаграма активності модуля виконання сценарію безпеки представлена на рисунку 4.

Рис. 4. UML-діаграма активності модуля виконання сценарію безпеки

Під час тестування запропонованої інформаційної технології управління безпекою розумного будинку кожен з 30 користувачів створив від 5 до 7 сценаріїв безпеки для понад 10 видів загроз. Отримані результати тестування наведені в таблиці 2.

З таблиці видно, що запровадження інформаційної технології сприятиме підвищенню швидкості реакції на загрозу, а також забезпеченню безпеки розумного будинку. результати тестування вказують на підвищення швидкості реакції на загрозу в інформаційній технології управління безпекою розумного будинку

Таблиця 2

Результати тестування інформаційної технології управління безпекою розумного будинку

Критерій	Інформаційна технологія	Google Home
Середній час від виявлення загрози до реакції на загрозу, с	0,5–3,0	5,0–8,0
Час забезпечення безпеки розумного будинку, с	16,0	20,0

в порівнянні з аналогом Google Home, понад 50%. Таким чином, за використання інформаційної технології управління безпекою розумного будинку підвищується швидкість забезпечення безпеки розумного будинку на 20%, за рахунок можливості створення власником сценаріїв безпеки та удосконаленого аналізу безпеки.

Висновки. Використання інформаційної технології управління безпекою розумного будинку надає можливість його власнику створювати множину сценаріїв безпеки, серед яких обирається сценарій за наявними факторами впливу, що дало можливість, порівняно із аналогами, підвищити швидкість реакції на виявлену загрозу більше, ніж на 50%, та забезпечити безпеку розумного будинку на 20% швидше.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Розумний будинок. URL: https://oxorona.com/smart-home/.
2. Автоматизація дому. URL: https://homesmart.com.ua/domashniaia-avtomatyzatsyia-10-sposobov-upravlenyia-umnym-domom/
3. Samsung SmartThings [Електронний ресурс]. URL: http://smartandyoung.com.ua/smart-things-shho-ce-za-programa-v-samsung
4. Google home. URL: https://home.google.com/welcome/.
5. Безпека. URL: https://www.smarthouse.ua/ua/bezopasnost.html.

REFERENCES:

1. Smart home [Electronic resource]. Access mode to the resource: https://oxorona.com/smart-home/.
2. Home automation [Electronic resource]. Access mode to the resource: https://homesmart.com.ua/domashniaia-avtomatyzatsyia-10-sposobov-upravlenyia-umnym-domom/
3. Samsung SmartThings [Electronic resource]. Access mode to the resource: http://smartandyoung.com.ua/smart-things-shho-ce-za-programa-v-samsung.
4. Google home [Electronic resource]. Access mode to the resource: https://home.google.com/welcome/.
5. Security [Electronic resource]. Access mode to the resource: https://www.smarthouse.ua/ua/bezopasnost.html.