67-72-21/2
28.03.2025

ВІДГУК
офіційного опонента
доктора технічних наук, професора,
доцента кафедри комп'ютерних наук
Чернівецького національного університету імені Ю. Федьковича
Угрина Дмитра Ілліча
на дисертаційну роботу Жовніра Юрія Івановича на тему "Методи та засоби побудови інтелектуальної програмної системи безпеки житлових комплексів", подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 01.05.03 - математичне та програмне забезпечення обчислювальних машин і систем.

Актуальність теми дослідження

Проблематика гарантування безпеки житлових комплексів на основі сучасних інформаційних технологій є надзвичайно актуальною в умовах швидкої урбанізації та зростання кіберзагроз. В сучасному світі, де зростає роль автоматизації та цифрових технологій, необхідність створення ефективних систем безпеки для житлових комплексів стає ще більш нагальною. Традиційні методи гарантування безпеки, які базуються на фізичному патрулюванні, системах контролю доступу та відеоспостереження, поступово втрачають свою ефективність через зростання складності загроз та необхідність інтеграції різних аспектів безпеки в єдину інтелектуальну систему.

Особливої актуальності набуває використання IoT-рішень, методів штучного інтелекту, які дозволяють прогнозувати загрози, автоматизувати процеси управління безпекою та покращувати рівень реагування на потенційні інциденти. Застосування таких підходів сприяє створенню адаптивних систем безпеки, які здатні не лише ідентифікувати загрози в реальному часі, а й аналізувати історичні дані для прогнозування та попередження потенційних небезпек. Слід відзначити, що підвищена урбанізація призводить до концентрації великої кількості людей в межах одного житлового комплексу, що ускладнює процес гарантування безпеки. Зростає також кількість IoT-пристроїв, які взаємодіють між собою, що створює нові виклики, пов'язані з кібербезпекою та управлінням інформаційними потоками. Важливим аспектом є захист персональних даних мешканців, оскільки будь-які витоки інформації можуть призвести до серйозних наслідків.

Дисертаційна робота Жовніра Ю.І. спрямована на розроблення комплексної інтелектуальної програмної системи безпеки житлових комплексів, що поєднує фізичні та цифрові аспекти захисту, є актуальною як з наукової, так і з практичної точки зору. Робота має значний внесок у розвиток методів автоматизованого управління безпекою житлових об'єктів, забезпечуючи ефективний контроль доступу, ситуаційну обізнаність та адаптивність системи до змінюваних умов.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій

Дисертаційна робота базується на ґрунтовному аналізі сучасних методів побудови інтелектуальних систем безпеки. Автор застосував широкий спектр наукових підходів, які забезпечили комплексний підхід до вирішення поставленої проблеми. Зокрема, використані методи аналізу ієрархій, що дозволило визначити найбільш ефективні програмно-апаратні платформи для реалізації інтелектуальної системи безпеки житлового комплексу; SWOT-аналіз, який допоміг оцінити сильні та слабкі сторони впроваджуваних технологій у сфері безпеки житлових комплексів; онтологічного моделювання, застосований для проектування бази знань інтелектуальної системи, що дозволило структуровано представити взаємозв'язки між різними об'єктами безпеки; випадкового лісу, який використаний для формування персоналізованих користувацьких інтерфейсів. Застосування таких методів забезпечило високий рівень обґрунтованості отриманих наукових положень, висновків та рекомендацій. Крім того, автором проведено тестування розробленої системи на реальних даних, що підтверджує практичну ефективність запропонованих підходів.

Наукова новизна отриманих результатів

Наукова новизна роботи полягає у розробленні інтелектуальної програмної системи безпеки житлових комплексів з ситуаційною обізнаністю. Зокрема, автором:

Вперше:

- Розроблено модель бази знань інтелектуальної програмної системи безпеки житлових комплексів у вигляді доменно-орієнтованої онтології, яка інтегрує просторово-часові, структурні та поведінкові аспекти взаємодії

компонентів системи. Запропоновано обернено-адитивну метрику для оцінювання онтологій, що дозволяє визначати ступінь зв'язності елементів. Це сприяло підвищенню ефективності аналізу критичних взаємозв'язків, оптимізації структурної організації компонентів, а також адаптивності системи до можливих змін у середовищі.

Удосконалено:

- Методи прогнозування розвитку подій у інтелектуальних системах безпеки на основі типових сценаріїв та моделей поведінки, що формуються в результаті аналізу історичних даних ситуоїдів. Це дозволило підвищити точність і швидкість прогнозування загроз, своєчасно виявляти аномальні ситуації та покращити адаптивність системи до нових викликів шляхом гнучкого врахування змін у поведінкових патернах.

Подальший розвиток отримали:

- Метод аналізу ієрархій для вибору оптимальних програмно-апаратних платформ на основі технологій Інтернету речей та розробки комплексів програмних інструментів для створення та супроводу програмної системи безпеки. Це дало змогу обґрунтовано обирати ефективні, надійні та масштабовані платформи, а також забезпечити узгодженість та цілісність програмних інструментів для розроблення і підтримки інтелектуальних систем безпеки.
- Синергетичне поєднання методу персон та алгоритму випадкового лісу в процесі створення ефективних інтерфейсів інтелектуальних програмних систем. Це дозволило враховувати індивідуальні характеристики та поведінкові особливості користувачів, що підвищило рівень персоналізації інтерфейсів, забезпечило адаптивність системи до різних сценаріїв взаємодії та покращило загальний досвід користувачів завдяки оптимізації навігації, підвищенню зручності використання та швидкому доступу до основних функцій системи безпеки.

Практичне значення результатів дослідження

Результати дисертаційної роботи мають значний практичний потенціал, оскільки створена інтелектуальна програмна система безпеки "АСТРА.

Безпечний ЖК" пройшла тестові випробування та впроваджується в реальні житлові комплекси. Це підтверджує її ефективність та адаптованість до реальних умов експлуатації. Впровадження системи дозволяє суттєво підвищити рівень безпеки мешканців, оптимізувати витрати на фізичну охорону, а також автоматизувати процеси контролю доступу та відеоспостереження. Додатково, система забезпечує інтеграцію з інфраструктурою інтернет-провайдерів, що дає змогу використовувати вже існуючі мережеві ресурси для розгортання рішень без значних додаткових інвестицій.

Практичне застосування розроблених методів та алгоритмів сприяє формуванню нових підходів до кібербезпеки житлових об'єктів, включаючи виявлення та протидію кібератакам на рівні IoT-пристроїв. Використання методології DevOps у розробці системи дозволяє забезпечити безперервну інтеграцію, тестування та оперативне оновлення безпекових модулів без втручання користувачів. Система також може бути адаптована для використання в інших сферах, таких як безпека комерційних центрів, офісних будівель, а також об'єктів критичної інфраструктури. Це відкриває широкі можливості для подальшого розвитку та масштабування розробленого рішення.

Повнота викладення матеріалів у публікаціях

За результатами дисертаційного дослідження автором опубліковано 20 наукових праць, включаючи 2 статті у фахових виданнях, що індексовані у базі даних Scopus та 7 тез доповідей у матеріалах наукових і науково-практичних конференцій.

Це свідчить про достатній рівень апробації та наукового визнання результатів дослідження.

Зміст та структура роботи

Дисертаційна робота складається з п'яти розділів, які послідовно розкривають поставлену проблему, обґрунтовують вибір методів дослідження, демонструють отримані результати та аналізують їх ефективність.

Перший розділ присвячений аналізу сучасних підходів до розробки інтелектуальних систем безпеки житлових комплексів. У ньому розглянуто основні принципи гарантування безпеки в розумних житлових середовищах,

виявлено актуальні проблеми та визначено напрямки дослідження. Проведено аналіз існуючих рішень у сфері автоматизованих систем безпеки, розглянуто їх переваги та недоліки. Визначено ключові вимоги до створення ефективної системи безпеки з використанням сучасних технологій. Виявлено прогалини у поточних підходах до управління безпекою житлових комплексів. Обґрунтовано необхідність інтеграції різних компонентів безпеки в єдину інтелектуальну систему. Сформульовано головні завдання, що вирішуються в межах дисертаційної роботи.

У *другому* розділі проведено аналіз підходів до вибору програмно-апаратних платформ, методологій реалізації проєкту та комплексів програмних інструментів. Розглянуто особливості застосування методологій DevOps та DevSecOps у процесі розроблення інтелектуальних систем безпеки житлових комплексів.

У ході дослідження було проведено порівняльний аналіз програмно-апаратних інструментальних засобів, використання яких є доцільним при створенні інтелектуальної системи безпеки житлового комплексу. Використання методу аналізу ієрархій дозволило структуровано оцінити та систематизувати різні інструментальні засоби, що забезпечило можливість ухвалення обґрунтованих рішень щодо оптимальних програмно-апаратних рішень при проєктуванні системи безпеки житлових кварталів. Проведений дисертантом SWOT-аналіз методологій управління IT-проєктами сприяв вибору методології DevOps, оскільки вона забезпечує ефективну реалізацію процесів безперервної інтеграції, тестування та доставки програмних систем. Ці функції є критично важливими для розгортання та експлуатації динамічних IoT-систем, що включають велику кількість компонентів і пристроїв. Впровадження DevOps та DevSecOps дозволило максимально адаптувати IoT-систему до функціональних вимог, забезпечити неперервний розвиток, а також підтримувати розширення функціональності без порушення стабільності роботи. Дисертантом обґрунтовано, що застосування методології DevOps у процесі розроблення інтелектуальної системи безпеки на основі IoT-технологій сприяє підвищенню ефективності, безпеки та надійності проєктних рішень. Це дозволяє системі

гнучко адаптуватися до змін, а також стабільно функціонувати у розгалужених мережах із великою кількістю різнотипових підключених пристроїв. На основі проведеного порівняльного аналізу з використання методу аналізу ієрархій було визначено оптимальний набір DevOps-інструментів для розроблення інтелектуальної системи безпеки.

Такий підхід дозволяє забезпечити стабільну роботу IoT-системи, оптимізувати розгортання та масштабування її компонентів, а також підвищити захищеність та ефективність управління в умовах безперервного розвитку й експлуатації.

Третій розділ містить детальний аналіз розроблених алгоритмів та методів прогнозування загроз. Запропонований дисертантом фреймворк забезпечує аналіз ситуацій та прогнозування потенційних загроз, що здійснюється на основі емпіричних шаблонів, які динамічно оновлюються шляхом узгодження з реальними даними. Для моделювання часових та просторових змін використовується онтологія GFO, а ситуоїди дозволяють описувати еволюцію ситуацій. Дисертант слушно відзначає, що використання штучного інтелекту забезпечує навчання системи на реальних даних, розпізнавання закономірностей та адаптацію до змін у середовищі. У дисертаційній роботі запропоновано обернено-адитивну метрику для глибшого аналізу онтологій та їх порівняння.

Четвертий розділ присвячений розробленню архітектури та структури інтелектуальної програмної системи безпеки з ситуаційною обізнаністю. Дисертантом розроблено структуру інтелектуальної системи безпеки, яка об'єднує ключові компоненти в єдину адаптивну мережу. Її основою є IoT-інфраструктура, що забезпечує інтеграцію сенсорних пристроїв із центральним блоком управління. Слід відзначити її унікальність, яка полягає у інтеграції інтелектуальних агентів із центральним блоком управління, яка дозволяє реалізувати не лише централізоване, а й децентралізоване управління процесами. Інтелектуальні агенти значно знижують навантаження на центральний блок управління, виконуючи первинний аналіз даних та ухвалення рішень у реальному масштабі часу. Це дозволяє поєднувати виконання різних завдань в інформаційній системі безпеки з урахуванням поточних ситуацій та динамічно

розподіляти обчислювальні ресурси між агентами та сервісами. Служба внутрішнього програмного забезпечення сприяє інтеграції всіх компонентів та автоматизацію процесів безпеки. Використання попередньої фільтрації даних агентами дозволяє прискорити централізоване ухвалення рішень. Водночас, гнучке налаштування поведінки підсистем підвищує адаптивність системи до змінних умов експлуатації.

На відміну від традиційних систем безпеки, які базуються переважно на централізованому управлінні, запропонована інформаційна система поєднує переваги централізованого та децентралізованого підходів. Це дозволяє мінімізувати затримки у прийнятті рішень та підвищити стійкість системи до відмов окремих її компонентів.

Заслуговує уваги розроблена дисертантом архітектура інтелектуальної системи, яка інтегрує підсистеми відеоспостереження, контролю доступу та управління послугами оператора в єдиний центр опрацювання даних. Запропонована архітектура забезпечує одночасне керування підсистемами в реальному масштабі часу, що раніше було складно реалізувати через обмеження сумісності відомих рішень. Досягнення такої інтеграції стало можливим завдяки стандартизації протоколів передачі даних та впровадженню спеціалізованих алгоритмів управління IoT-мережами. Більшість сучасних підходів не враховують варіативність множин відношень між компонентами, зосереджуючись лише на окремих аспектах взаємодії. У розробленій інтелектуальній системі використано системний підхід до моделювання, який охоплює повний спектр можливих сценаріїв взаємодії функціональних підсистем, що підвищує її гнучкість і надійність.

П'ятий розділ висвітлює практичні аспекти впровадження запропонованої системи. Дисертантом на прикладі підсистеми відеоспостереження проведене концептуальне моделювання інформаційної програмної системи житлового комплексу, що сприяло чіткому визначенню компонентів системи, їхніх функцій та взаємозв'язків, що дозволило мінімізувати ризики на етапах проєктування та реалізації. Створена концептуальна модель передбачає масштабованість системи

завдяки можливості додавання нових IoT-пристроїв і функціональних модулів, що забезпечує її адаптацію до змінних потреб користувачів і умов експлуатації.

Дисертантом слушно відзначено, що ефективна взаємодія між серверною та клієнтською частинами відіграє ключову роль у розробленні веб-застосунків. Використання Django Rest Framework (DRF) для побудови RESTful API дозволило оптимізувати опрацювання запитів, а застосування React у поєднанні з TanStack Query та Axios забезпечило швидку та безперебійну інтеграцію API.

При розробленні інтерфейсів систем безпеки для житлових кварталів дисертантом успішно використаний метод персон, який сприяв глибшому розумінню потреб різних категорій користувачів та дозволив створити інтуїтивно зрозумілі та персоналізовані рішення, які враховують специфічні вимоги кожної групи користувачів. Персоналізація функціональності у системах безпеки дозволяє підвищити ефективність управління, забезпечити зручний користувацький досвід і збільшити рівень безпеки. Використання методу випадкового лісу дозволило ефективно опрацьовувати великі наборами ознак, що дозволило досягати високої точності класифікації мешканців для створення протоперсон. Аналіз важливості ознак дозволив визначити вплив різних факторів на процес класифікації, що сприяло подальшому вдосконаленню алгоритмів безпеки.

Зауваження та рекомендації

Хоча дисертація має високий рівень наукової новизни, хотілося б звернути увагу на такі аспекти:

1. У дисертаційній роботі відсутній перелік умовних скорочень.

2. Не описано архітектуру інформаційної системи, що заснована на моделі ієрархічних цілей та не описано рис. 1.3.

3. Дослідження першого розділу фокусується на певних інструментах (IoT, DevOps), але не аналізує альтернативи, наприклад, використання блокчейн-технологій для безпеки або нейронних мереж для аналізу поведінки мешканців. Це могло б розширити можливості для подальших досліджень.

4. Використання DevOps у другому розділі аргументовано лише теоретично, без експериментального підтвердження його переваг. Було б корисно

надати емпіричні результати, такі як швидкість розгортання системи, рівень автоматизації оновлень або вимірювання продуктивності, що дозволило б обґрунтувати вибір методології більш переконливо.

5. Не розглянуто альтернативні методи аналізу знань, оскільки, крім онтологій, існують інші підходи до структуризації знань (наприклад, графові бази даних або алгоритми кластеризації поведінкових патернів). Варто було б коротко порівняти їх із запропонованим методом.

6. Автор міг би більш детально розглянути питання масштабованості запропонованої системи для великих житлових комплексів з різними рівнями доступу. Було б корисно показати, чи можна її розширювати, чи є межі продуктивності, які можуть стати проблемою.

7. У дисертаційному дослідженні представлені різні підходи: метод випадкового лісу та метод персон. Проте не здійснено їх порівняння з альтернативними методами та не проаналізовано можливі недоліки. Це ускладнює оцінку їхньої доцільності та ефективності у контексті розробленої системи.

8. У роботі зустрічаються граматичні та стилістичні неточності, зокрема на с. 21 «Помилка! Джерело посилання не знайдено», на с. 45 «методу аналізу ієрархій (АНР)», на с. 46 «на основі наданих у статті порівняльних характеристик» та ін.

Проте зазначені зауваження носять рекомендаційний характер і не зменшують загальне позитивне враження від дисертаційної роботи.

Висновок.

Дисертаційна робота Жовніра Ю.І. є завершеним науковим дослідженням, спрямованим на розв'язання актуального завдання підвищення рівня безпеки житлових комплексів шляхом впровадження інтелектуальних програмних систем. Робота містить науково обґрунтовані результати, які мають як теоретичне, так і практичне значення. Зміст дисертації, отримані наукові результати та обрана тема дослідження відповідають спеціальності 01.05.03 – «Математичне та програмне забезпечення обчислювальних машин і систем», за

якою роботу подано до захисту. Стиль викладу наукових положень та отриманих результатів відповідає вимогам наукового стилю.

За результатами аналізу змісту поданої дисертаційної роботи вважаю, що дисертаційна робота «Методи та засоби побудови інтелектуальної програмної системи безпеки житлових комплексів» широко охоплює і повністю розв'язує поставлене наукове завдання. Робота за рівнем наукової новизни отриманих результатів, їх практичної значущості, якістю проведених досліджень та стилем викладення задовольняє усі вимоги МОН України, які ставляться до кандидатських дисертацій, а її автор Юрій Іванович Жовнір заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю за спеціальністю 01.05.03. – «математичне та програмне забезпечення обчислювальних машин і систем».

Офіційний опонент
доктор технічних наук, професор,
доцент кафедри комп'ютерних наук
Чернівецького національного університету
імені Юрія Федьковича Дмитро УГРИН

Підпис Угрина Д. засвідчую
Учений секретар Чернівецького національного
університету імені Юрія Федьковича
Мирловська
"18" березня

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ЧЕРНІВЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА * Код 02071240