Міністерство науки і освіти України
Національний університет “Львівська політехніка”

ЖОВНІР ЮРІЙ ІВАНОВИЧ

УДК 004.056:004.45:728.2

МЕТОДИ ТА ЗАСОБИ ПОБУДОВИ ІНТЕЛЕКТУАЛЬНОЇ ПРОГРАМНОЇ СИСТЕМИ БЕЗПЕКИ ЖИТЛОВИХ КОМПЛЕКСІВ

01.05.03.- математичне та програмне
забезпечення обчислювальних машин і
систем

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Львів – 2025

Дисертацією є рукопис

Роботу виконано в Національному університеті “Львівська політехніка” Міністерства освіти і науки України

Наукові керівники:	кандидат фізико-математичних наук, доцент **Захарія Любов Михайлівна** Національний університет “Львівська політехніка”, доцент кафедри інформаційних систем та мереж
	доктор технічних наук, професор **Пасічник Володимир Володимирович** Національний університет “Львівська політехніка”, професор кафедри інформаційних систем та мереж
Офіційні опоненти:	доктор технічних наук, професор **Глибовець Андрій Миколайович** Національний університет «Києво-Могилянська академія», м. Київ, декан факультету інформатики
	доктор технічних наук, професор **Угрин Дмитро Ілліч** Чернівецький національний університет імені Юрія Федьковича, м.Чернівці, доцент кафедри комп’ютерних наук

Захист відбудеться “___” _____ 2025 р. о ____ на засіданні спеціалізованої вченої ради Д 35.052.05 у Національному університеті “Львівська політехніка” (79013, м. Львів, вул. Степана Бандери, 12, 226 ауд. головного корпусу).

З дисертацією можна ознайомитися у науково-технічній бібліотеці Національного університету “Львівська політехніка” (79013, м. Львів, вул. Професорська 1)

Автореферат розіслано “___” _____ 2025 р.

Вчений секретар
спеціалізованої вченої ради,
доктор технічних наук, професор Ростислав БУНЬ

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Враховуючи виклики сучасності, дослідження в галузі інтелектуальних програмних систем безпеки має високу актуальність. У межах цього дослідження основну увагу зосереджено на гарантуванні безпеки в контексті побудови інтелектуальних систем для потреб мешканців багатоквартирних будинків та житлових комплексів. З огляду на те, що житлові комплекси стають дедалі масштабнішими та популярнішими, постає питання розроблення та впровадження високотехнологічних інтелектуальних програмних систем управління безпекою та підвищення їх ефективності.

Зростання загроз для житлових комплексів включає кібератаки на IoT-пристрої, що можуть призвести до порушення приватності мешканців, фінансових втрат та фізичної небезпеки, компрометацію персональних даних мешканців, а також атаки типу DDoS, які можуть вивести з ладу критичні системи безпеки.

Житлові комплекси є складними системами, де фізична безпека повинна бути інтегрована з інформаційними технологіями, що вимагає створення захищених каналів зв'язку, надійного управління доступом і постійного моніторингу кіберзагроз. Сучасні інтелектуальні системи безпеки повинні мати можливість прогнозувати загрози за допомогою прогностичних моделей та реагувати на них до того, як вони стануть критичними.

Соціальна значущість теми полягає у забезпеченні довіри мешканців до новітніх технологій, захисті їхньої приватності, створенні комфортного і безпечного середовища для життя. Ефективні методи підтримання належного рівня безпеки також дозволяють запобігти потенційним фінансовим втратам і зменшити витрати на реагування на інциденти. Таким чином, розроблення та впровадження методів і засобів побудови інтелектуальної програмної системи безпеки житлових комплексів є актуальною та життєво важливою задачею.

Використання інтелектуальних сенсорів, камер спостереження, зчитувачів та інших IoT пристроїв з мережевими інтерфейсами дає змогу інтегрувати їх у єдиній інтелектуальній системі безпеки. Розроблення такої програмної системи безпеки з урахуванням ситуаційної обізнаності присвячене дисертаційне дослідження. У цій роботі запропоновано використовувати інфраструктуру інтернет-провайдерів (в даному випадку йдеться про Львівського регіонального інтернет провайдера - компанію АСТРА-ЛЬВІВ), зокрема, існуючу кабельну мережу, серверні кластери, інструменти методології DevOps, бази даних користувачів, персоналу для розгортання та супроводу інтелектуальної програмної системи безпеки житлового комплексу.

Задача створення інтелектуальної програмної системи безпеки житлових комплексів залишається актуальною через фрагментарність рішень, недостатню інтеграцію та адаптивність існуючих систем. Для її вирішення необхідно впроваджувати методи та засоби інтеграції фізичної та інформаційної безпеки, використовувати інструменти штучного інтелекту і застосовувати проактивні методи захисту. Таким чином, дослідження за цією тематикою має як науково-методичне, так і практично-прикладне значення для комерційного впровадження та широкого використання.

Зв'язок роботи з науковими програмами, планами, темами. Задачі, що вирішуються у дисертаційній роботі, випливають із завдань у сфері науки і техніки, сформульованих у Законі України № 2519-VI від 09.09.2010 р. «Про внесення змін до Закону України «Про пріоритетні напрямки розвитку науки і техніки», також у Постанові Кабінету міністрів України від 30 квітня 2024 р. за № 476 «Про затвердження переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 31 грудня року, наступного після припинення або скасування воєнного стану в Україні». Результати наукових досліджень і практичних напрацювань, що наведені в дисертації, тісно пов’язані з напрямами науково-технічної діяльності кафедри інформаційних систем та мереж Національного університету «Львівська політехніка» – «Розроблення

інтелектуальних агентів пошуку релевантної інформації в мережі Інтернет та її опрацювання з метою автоматичного наповнення баз даних та баз знань», «Розроблення системи підтримки прийняття рішень на основі онтологічних знань та технологій машинного навчання».

Мета і задачі дослідження. Метою дисертаційної роботи є розроблення нових та вдосконалення існуючих методів та засобів побудови та супроводу інтелектуальних програмних систем безпеки для житлових комплексів і формування високотехнологічного, безпечного та комфортного середовища проживання.

Завдання дослідження:

- Провести аналіз підходів, методів та засобів для побудови інтелектуальних програмних систем безпеки багатоквартирних будинків та житлових комплексів.
- Сформувати комплекс методів для реалізації процесів розроблення та супроводу інтелектуальних програмних систем безпеки на основі технологій IoT.
- Спроектувати доменно-орієнтовану онтологію для програмної системи безпеки з ситуаційною обізнаністю на основі конструктивів базової чотиривимірної онтології GFO та сформувати обернено-адитивну метрику для її оцінювання.
- Сформувати структуру та архітектуру інтелектуальної програмної системи безпеки з ситуаційною обізнаністю для житлових комплексів та розробити її концептуальну модель.
- Розробити процедури побудови інтерфейсів інтелектуальних програмних систем безпеки житлового комплексу, системно поєднавши методи персон та випадкового лісу.
- Розробити програмну систему безпеки з ситуаційною обізнаністю житлового комплексу «АСТРА. Безпечний ЖК» та провести її тестові випробування.

Об'єктом дослідження є проектування прикладних програмних систем гарантування безпеки мешканців та майна в житловому комплексі.

Предметом дослідження є методи та засоби розроблення інтегрованих програмних систем безпеки з ситуаційною обізнаністю для житлових комплексів.

Методи дослідження. Для вирішення поставлених у дисертаційній роботі завдань використано такі методи дослідження: метод аналізу ієрархій - для визначення кращих програмно-апаратних платформ на основі технологій IoT та формування комплексів програмних інструментів методології розроблення і супроводу програмної системи безпеки; SWOT аналіз сприяв обранню методології управління IT проектами; методи онтологічного моделювання для проектування бази знань інтелектуальної системи безпеки; методи та засоби штучного інтелекту для створення програмної системи безпеки з ситуаційною обізнаністю; методи теорії графів при побудові обернено-адитивної метрики для оцінювання онтологічної близькості; методи структурного аналізу та концептуального моделювання для побудови структури та архітектури прикладної програмної системи безпеки з ситуаційною обізнаністю для житлових комплексів; метод персон в поєднанні з методом випадкового лісу для формування користувацьких інтерфейсів; методи об'єктно-орієнтованого програмування та системного аналізу для розроблення інтелектуальної програмної системи безпеки житлових комплексів.

Наукова новизна. Наукова новизна роботи полягає у розв'язанні важливої наукової задачі побудови інтелектуальної програмної системи безпеки житлових комплексів. У результаті розв'язання цієї задачі одержано такі наукові результати.

Вперше:

- Сформовано модель бази знань інтелектуальної програмної системи безпеки житлових комплексів у вигляді доменно-орієнтованої онтології, яка враховує просторово-часові, структурні і поведінкові аспекти взаємодії компонентів системи, та побудовано обернено-адитивну метрику для її оцінювання, зокрема ступеню зв'язності її елементів, що в сукупності підвищило ефективність аналізу критичних взаємозв'язків та структурної організації компонентів, а також адаптивність системи до потенційних змін середовища.

Удосконалено

- Методи прогнозування розвитку подій у інтелектуальних безпекових системах, які базуються на типових сценаріях і моделях поведінки, сформованих як результати аналізу історичних даних ситуоїдів, що дало змогу підвищити точність і оперативність прогнозування потенційних загроз, забезпечити своєчасне виявлення аномальних ситуацій та підвищити адаптивність системи до нових викликів завдяки гнучкому врахуванню змін у поведінкових патернах.

Отримало подальший розвиток:

- Метод аналізу ієрархій - для визначення кращих програмно-апаратних платформ на основі технологій інтернету речей та формування комплексів програмних інструментів методології розроблення та супроводу програмної системи безпеки, що дало змогу обґрунтовано вибирати оптимальні програмно-апаратні платформи з урахуванням ключових критеріїв ефективності, надійності та масштабованості, а також забезпечити цілісність і узгодженість програмних інструментів для розроблення та супроводу інтелектуальних систем безпеки.

- Системне поєднання методів персон та випадкового лісу у процесах побудови ефективних інтерфейсів інтелектуальних програмних систем, яке дозволяє враховувати індивідуальні характеристики і поведінкові особливості груп користувачів, та дало змогу підвищити рівень персоналізації інтерфейсів, забезпечити адаптивність систем до різних сценаріїв користувацької взаємодії та покращити загальний досвід користувачів шляхом оптимізації навігації, зручності використання та швидкості доступу до ключових функцій системи безпеки.

Практичне значення одержаних результатів. Проаналізовано та використано прогресивні підходи для розроблення і впровадження інтелектуальних систем безпеки на основі існуючої інфраструктури інтернет провайдера. Розроблені та реалізовані програмні компоненти, що можуть бути розширені і вдосконалені в наступних версіях системи безпеки, а також можуть адаптуватися до нових сценаріїв і реалізацій. Сформовано методологічний підхід, що системно реалізує метод персон та випадкового лісу для побудови інтерфейсів системи безпеки з урахуванням результатів аналізу складу мешканців та працівників житлових комплексів. Розроблено і апробовано методи розпізнавання загроз безпеці і потенційні інструменти з відповідними процедурами прийняття рішень згідно сценаріїв безпеки та можливістю навчання системи на основі бази знань. Одержані результати успішно імплементовано в програмній системі “АСТРА Безпечний ЖК”, що перебуває на етапі впровадження та дослідної експлуатації. Результати дисертаційного дослідження впроваджені в навчальний процес підготовки ІТ фахівців у ряді провідних ЗВО України.

Особистий внесок здобувача. Усі наукові результати, викладені в дисертації, отримані здобувачем особисто. У працях, опублікованих у співавторстві, здобувачеві належать: розроблення структури та архітектури інтелектуальної системи безпеки [1]; розроблення підходів до створення модуля, який розраховує вагові коефіцієнти для кожного моменту часу, визначаючи його важливість для поточного завдання [2]; аналіз архітектурних рішень для інтелектуальних будинків, проаналізовані останні розробки в сфері безпеки та управління правами доступу для інтелектуальних будинків [3]; проведення аналізу та обґрунтування доцільності використання обернено-адитивної метрики для онтологій інтелектуальних систем безпеки житлових комплексів [4]; вибір програмно-апаратних засобів для створення інтелектуальних систем безпеки з метою подальшого аналізу методом аналізу ієрархій, визначення основних критеріїв для проведення аналізу, таких як: гнучкість, вартість, легкість використання та підтримка різнотипових пристроїв і протоколів [5]; програмне та інформаційне забезпечення для застосування алгоритмів випадкового лісу та методу персон [6]; визначення функціональних областей інтелектуальної системи безпеки житлового комплексу, проектування концепції підсистеми відеоспостереження [7]; розроблення ряду базових програмно-алгоритмічних конструкцій моделюючого комплексу “Мультипроцесист”, в якому реалізовано основні базові принципи системи алгоритмічних алгебр з використанням принципів клонування знань [8]; розроблення безпекових сценаріїв для побудови доменно-

орієнтованої онтології, опис онтології мовою OWL [9]; побудова концептуальної моделі модуля відеоспостереження з використанням UML діаграм [10]; аналіз інструментарію методології DevOps, розроблення сценаріїв застосування DevOps в IT-інфраструктурі, зокрема опрацювання даних на периферійних та хмарних платформах, автоматизація управління інфраструктурою та забезпечення кібербезпеки [11], запропоновано метод створення комплексів інструментів та обрання кращого набору для реалізації методології DevOps в інформаційних системах[12]; проаналізовано роль DevOps в екосистемах IoT [13].

Апробація результатів дисертації. Результати дослідження доповідались і обговорювались на міжнародних наукових та науково-практичних конференціях: IEEE 19th Intern. Conf. on Computer Science and Information Technologies (CSIT-2024) (Львів, 2024, Scopus), V міжнар. наук.-практ. конф. «Current Trends in Scientific Research Development» (Бостон, США, 2024), 4 міжнар. наук.-практ. конф. «Science in the Modern World: Innovations and Challenges » (Торонто, Канада, 2024), I Міжнар. наук.-практ. конф. «European Congress of Scientific Discovery» (2024, Мадрид, Іспанія), II Міжнародній науково-практичній конференції «Future of science: innovations and perspectives» (Стокгольм, Швеція, 2024), на науковій конференції молодих вчених (2010, Львів), а також на наукових семінарах кафедри інформаційних систем та мереж Національного університету "Львівська політехніка".

Публікації. За результатами дисертаційного дослідження опубліковано 20 друкованих праць, з них 11 у виданнях, що включені МОН України до переліку фахових наукових видань та 2 у журналах, що індексується у наукометричній базі Scopus, 7 тез доповідей у матеріалах наукових та науково-практичних конференцій.

Структура роботи. Дисертаційна робота загальним обсягом 202 сторінки складається зі вступу, п'яти розділів, висновків, списку використаних джерел із 129 найменувань і додатків. Основний текст викладено на 142 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** наведено загальну характеристику роботи, обґрунтовано актуальність, сформульовано мету та основні задачі дослідження, структуровано подано пункти наукової новизни і характеристику практичної цінності роботи.

У **першому розділі** проведено аналіз етапів розвитку інтелектуальних систем для розумних будинків, актуального стану дослідження питань безпеки в контексті побудови інтелектуальної програмної системи безпеки житлових комплексів. Визначено основні терміни, подано чітке означення концепту житловий комплекс (ЖК), яким є утворенням, що виділене із житлового середовища, як самодостатня структурна одиниця, що включає взаємо поєднані житлові та нежитлові об'єкти, а також об'єкти інженерної інфраструктури. Визначено потреби в безпеці житлових комплексів, якими є відеоспостереження, контроль доступу, реагування на надзвичайні ситуації та ін. Акцентовано увагу на гострій необхідності побудови інтелектуальних програмних систем безпеки, зокрема, автоматичного доступу до укриттів, можливість виклику екстрених служб у випадку відсутності стандартних засобів зв'язку, урахування потреб людей з обмеженими можливостями, підвищення рівня кібербезпеки в такого роду системах.

Проаналізовано тенденції та сформовано рекомендації щодо трансформації функціональних вимог до сучасних інтелектуальних програмних систем безпеки, обґрунтовано вимоги до розроблення системи з урахуванням сучасних трендів їх розвитку, таких як: розпізнавання обличчя та об'єктів, авторизація з використанням безконтактної технології зв'язку та енергоефективних протоколів бездротового зв'язку, методів і засобів штучного інтелекту та алгоритмів машинного навчання.

Розглянуто еволюцію інформаційно-технологічних рішень в домені розумних будинків. Від найпростіших децентралізованих систем автоматизації в управлінні освітленням, енергоспоживанням, відеоспостереженням та ін. без функцій інтелектуального аналізу даних до інтелектуальних середовищ проживання, що можуть адаптуватися до поведінки мешканців, з можливостями локального опрацювання даних, їх інтелектуального

аналізу та прийняття оптимальних рішень. Проаналізовано мережеві топології інтелектуальних інформаційних систем та їх генезу від централізованих мереж до гібридно-кластерних рішень.

Проведено аналіз концепту традиційних та подано основні принципи сучасних архітектурних рішень: сервісно-орієнтованих архітектур з використанням блокчейну, методів та засобів штучного інтелекту, інтелектуальних програмних систем з ситуаційною обізнаністю, які характеризуються 5-ти рівневою структурою: збору даних, керування даними, формулювання контексту, генерування послуг та керування ними (рис. 1). Проаналізовано базові засади системи алгоритмічних алгебр з використанням принципів клонування знань, які в кінцевому рахунку є занадто складними з точки зору їх практичного використання. Проведено аналіз ряду базових 4-х вимірних онтологій та обрано онтологію GFO (General Formal ontology) для побудови проблемно-орієнтованої онтології, як основи створення інтелектуальної програмної системи безпеки житлових комплексів з ситуаційною обізнаністю. Проаналізовано метрики для мережевих та ієрархічних графових структур в контексті вимірювання параметрів онтологій.

У другому розділі проаналізовано підходи до обрання програмно-апаратних платформ, методологій реалізації проекту інтелектуальної програмної системи, комплексів програмних інструментів, проаналізовано системні переваги та недоліки використання методологій DevOps та DevSecOps при розробленні та впровадженні інтелектуальних систем безпеки житлових комплексів.

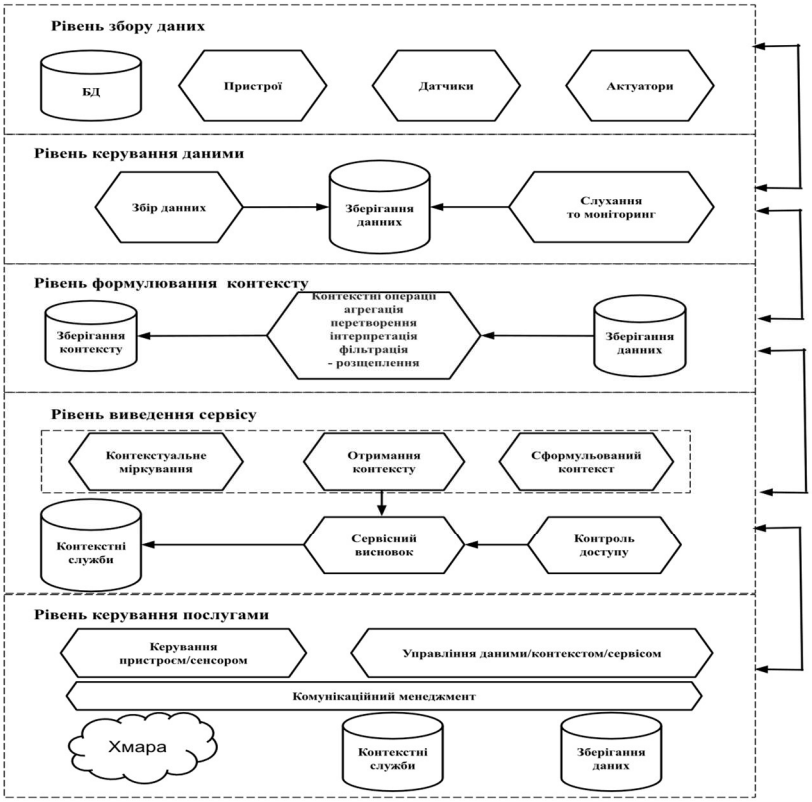


Рис. 1. Архітектура інформаційної системи «розумний будинок», що враховує контекст

Проведений порівняльний аналіз програмно-апаратних платформ на базі інформаційних технологій Інтернету речей за допомогою методу аналізу ієрархій дозволив визначити найбільш ефективні рішення, які можуть використовуватись при побудові такого роду систем. Для аналізу було обрано 8 платформ: Arduino, SmartThings, HomeAssistant, Hubitat, Vera, Google Home, Abode, OpenHab. На основі п’яти критеріїв, десятьма експертами було визнано кращою платформою Arduino, яка забезпечує високу гнучкість, широку

підтримку пристроїв та відносно низьку вартість, а також передбачає наявність належного рівня технічних знань, умінь та навичок для ефективного її використання.

Відзначено, що у сучасних високотехнологічних проектних командах вибір методології розроблення та супроводу проектів відіграє ключову роль для досягнення успіху. Сьогодні в професійних середовищах IT фахівців є популярними методології Agile, DevOps, Waterfall, Lean, V-модель та Scrum. Для ухвалення обґрунтованого рішення щодо вибору методології використано SWOT-аналіз, з допомогою якого обрано методологію DevOps, яка найкраще відповідає цілям проекту зі створення інтелектуальної програмної системи безпеки. В контексті розроблення інтелектуальної програмної системи безпеки житлових комплексів були визначені інструменти та технології методології DevOps, які найчастіше використовуються в побудові інформаційних систем з використанням IoT технологій. Завдяки поєднанню методів аналізу ієрархій та експертного оцінювання сформовано комплекси програмних інструментів методології розроблення та супроводу програмної системи безпеки та обрано кращий серед них.

Визначено, що в IoT-застосунках для гарантування безпеки при імплементації методології DevOps використовуються методи - безпечного програмування, ідентифікації і управління доступом, шифрування даних, оновлення та патчингу, контейнеризації та ізоляції, безперервної інтеграції та безперервного постачання (CI/CD), планування і реагування на інциденти.

Відзначено, що в створеній інтелектуальній системі безпеки житлового комплексу використання методології DevOps ефективно реалізує функцію масштабованості такої IoT-системи, використовуючи процеси автоматизованого розгортання, розподілу навантаження, централізованого моніторингу та аналізу журналів.

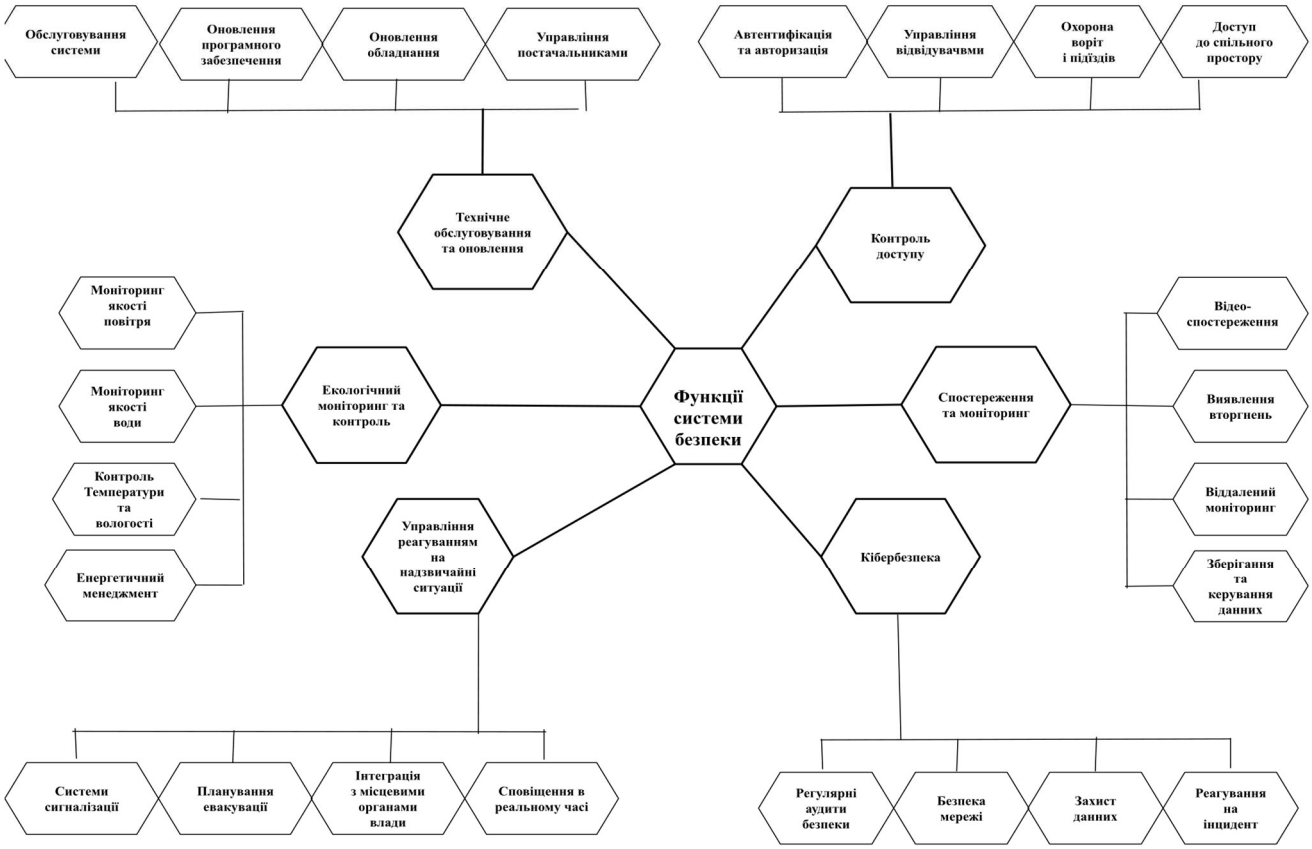


Рис. 2. Функції інтелектуальної системи безпеки житлового комплексу

З’ясовано, що впровадження інтелектуальної системи безпеки в житлових комплексах потребує складної та стійкої інфраструктури, в якій ефективно реалізовано керування численними точками доступу, комунальними об’єктами та великими фізичними

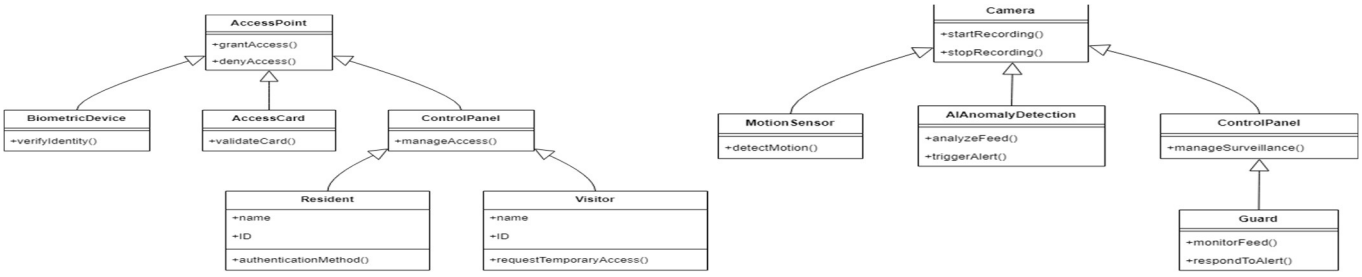
просторами. Це включає в себе інтеграцію різноманітних елементів безпеки, включаючи камери спостереження, механізми контролю доступу та сигналізації, розподілених по різних будівлях і спільних просторах. Визначено основні функціональні області інтелектуальної системи безпеки, які подані на рис. 2.

Розділ третій містить аналіз онтології GFO, як основи процесів формування та опрацювання бази знань інтелектуальної прикладної програмної системи безпеки житлових комплексів, обґрунтовано необхідність побудови обернено-адитивної метрики як інструменту вимірювання параметрів онтології.

Відзначено, що інтелектуальна програмна системи безпеки житлового комплексу розробляється як система, що враховує попередній досвід, аналізує ситуації та контекст з метою своєчасного виявлення загроз безпеки і виконання комплексів відповідних дій. Система покликана використовувати емпіричні знання, отримані з історичних контекстів, для процесів прийняття рішень. При цьому реалізуються проактивні заходи та процедури міркувань щодо потенційних подій у поточному сценарії. Вихідними умовами проекту інтелектуальної системи передбачено, що база знань постійно вдосконалюється та нарощує знаннєвий потенціал шляхом використання даних зворотного зв'язку, отриманих від різних давачів.

Визначено, що для підтримки чіткості та однозначності концептуальних визначень в межах інтелектуальної системи, вона повинна базуватися на спільній формальній концептуалізації (онтології). У загальному випадку така онтологія повинна містити як часові, так і просторові концептуалізації, обумовлюючи використання 4-вимірної онтології. В базовій GFO онтології використовуються поняття топоїдів, хроноїдів, конфігуроїдів для моделювання просторових, часових і структурних аспектів реальності. Ситуації та ситуоїди використовуються для подання контекстів.

При побудові онтології інтелектуальної програмної системи безпеки, було сформовано 20 базових сценаріїв. В процесі дослідження формалізовано основні структурні об'єкти GFO для інтелектуальної програмної системи безпеки, такі як фізичні і цифрові об'єкти, процеси, ролі, їхні відношення, а також проведено їх структурування з урахуванням часових аспектів.



а) б)

Рис.3 Шаблони онтології для інтелектуальної програмної системи безпеки житлового комплексу а) Шаблон автентифікації контролю доступу, б) Шаблон відеоспостереження

У процесі розроблення онтології виявлено ряд закономірностей, які представлені шаблонами, приклади яких наведені на рис. 3. Подано розроблені в процесі дослідження моделі передбачення та планування дій в середовищі ЖК та змодельована інтелектуальна програмна система безпеки як систему з ситуаційною обізнаністю, здатну виявляти, розпізнавати важливі ситуації, приймати щодо них рішення та вживати відповідних дій. Базові засади та формалізми доменно-орієнтованої онтології інтелектуальної програмної системи безпеки житлових комплексів, сформовані на основі концептів чотиривимірної онтології GFO.

Ситуоїд Su та його часові зрізи – ситуації Sit – є центральними елементами моделі пропонованої системи. Ситуоїдам притаманні наступні характеристики: контекстний комплекс, часові та просторові межі, динамічні характеристики. Ситуоїд Su визначаємо

через його ціль Gl і розглядаємо як перехід між двома обмежуючими ситуаціями (Sit^{su}_{st} і Sit^{su}_{end}), а саме початковим станом і передбачуваним цільовим станом.

Робота інтелектуальної програмної системи безпеки організована навколо опрацювання взаємопов'язаних концептуальних моделей знань, таких як моделі середовища Cm_{env}, які побудовані на основі об'єктів, розпізнаних у середовищі, Контекстні/задачні моделі Cm_{con} зберігають дані, релевантні конкретному завданню, ситуації, меті. Вони формуються як підмножина $Cm'_{env} \subseteq Cm_{env}$ моделі середовища для поточного часу tc. з додатковими об'єктами, що стосуються наміру $Gl_{int,tc}$, наданими відповідним шаблоном із бази знань

$$Cm_{con,tc} = (Cm'_{env,tc}, Gl_{int,tc}, t_c). \quad (1)$$

Інтелектуальна програмна система безпеки використовує ситуоїди GFO для моделювання динаміки розвитку ситуацій. Процес виконання завдання моделюється як послідовність ситуацій $(Sit_{t1}, Sit_{t2}, \ldots, Sit_{tk})$ з відповідною послідовністю конфігурацій $(Cj_{t1}, Cf_{t2}, \ldots, Cf_{tk})$. Кожна конфігурація в послідовності подана у вигляді графа знань:

$$Cf_{ti} = (SV_{con}, SE_{rel}, t_i), \quad (2)$$

де SV_{con} — це набір вузлів, що відповідають об'єктам, а SE_{rel} — набір зв'язків, що використовуються в специфікації ситуації. І об'єкти, і зв'язки класифікуються відповідно до онтології системи. Конкретні конфігурації в послідовності конфігурацій можуть бути різними, що відображає динаміку конфігурацій ситуації в процесі виконання завдання. Переходи між ситуаціями моделюються з використанням досвіду як структура дій або подій, які викликають перехід. Кожен створений ситуоїд розглядається як єдине ціле в контексті виконання завдання. У кожному ситуоїді можна вказати поточну ситуацію, минулі ситуації та кількість прогнозованих ситуацій (Рис.4). Всі ці ситуації враховуються при прийнятті рішень для виконання завдання.

Система використовує емпіричні знання для виявлення ситуацій, планування та передбачення розвитку ситуації. Ці знання зберігаються контекстно, тобто ключем для пошуку є подібність контексту. Як основу для прогнозів використовуються досвідчені знання та функція подібності F_{sim}.

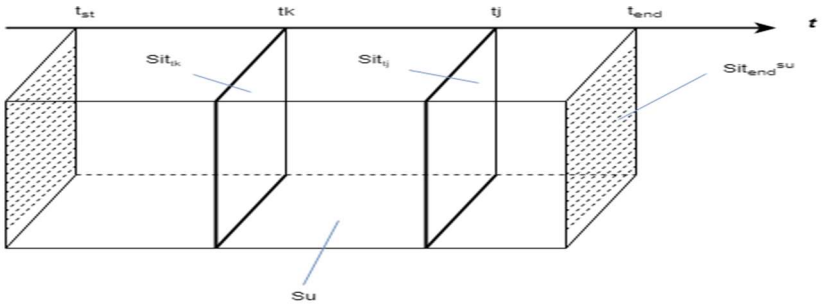


Рис. 4. Часові зрізи ситуоїда

Реалізовано функцію F_{sim}, що вимірює відстань між поточним контекстом (1) і ключовим контекстом $(Cm^{kb}_{env}, Gl^{kb}_{int})$ у базі знань. У процесі пошуку значення цієї функції мінімізуємо:

$$F_{sim}: \left(\left(Cm'_{env,tc}, Gl_{int,tc} \right), \left(Cm^{kb}_{env}, Gl^{kb}_{int} \right) \right). \rightarrow min \quad (3)$$

Формування бази знань з використанням зворотного зв'язку: Модель наміру Sit_{tg} для переходу на наступну ситуацію шукає в базі знань можливі дії, що призводять до цієї ситуації. На цьому етапі може бути побудовано декілька моделей $SSit_{tg} = \{Sit_{tg}\}$,, включаючи модель спостерігача або різні варіанти моделей наміру з використанням різних дій. Наслідки таких дій прогнозуються у вигляді траєкторій ситуації. Далі обирається найбільш ефективний варіант дії з використанням функції вибору F_{sel} і критеріїв вибору Cr.

$$F_{sel}: \left(SSit_{tg}, Cr \right) \rightarrow min. \quad (4)$$

Оцінюються відмінності між побудованими передбаченнями та реальними даними. У випадку, якщо вони не можуть бути компенсовані простою зміною параметрів шаблонів, що використовуються для передбачення, шаблони оновлюються, або створюється новий шаблон у базі знань для поточного контексту.

Для пошуку найкоротшого шляху між контекстами, застосовуються метрики, які використовуються для кількісного оцінювання моделей систем, а також, дозволяють визначити розмір системи та відстані між їх елементами. В дисертаційній роботі проаналізовано широкий набір метрик, які використовуються для вимірювання у різних типах онтологій, їхні переваги і недоліки, а також сформовано оригінальну обернено-адитивну метрику, яка забезпечує більш повний та комплексний аналіз онтологій для створюваної інтелектуальної програмної системи безпеки. Запропонована метрика, дозволяє оцінювати відстані між концептами в онтології, при наявності багатьох шляхів, від одного концепту до іншого, допускає дробові значення відстаней між вузлами орієнтованого графа онтології, та забезпечує достовірну оцінку відношень між концептами.

Позначимо Ni – кількість переходів від концепту A до концепту B по i-му шляху, i=1, …, K, де K – кількість різних шляхів, якими можна перейти по орієнтованому графу певної онтології від концепту A до концепту B.

Відстань d(A, B) між концептами A та B визначаємо таким чином:

$$\frac{1}{d(A,B)} = \sum_{i=1}^{K} \frac{1}{N_i}. \quad (5)$$

Метрика ґрунтується на понятті відстані. Відстань d (x, y) – однозначна, невід'ємна, дійсна функція $d: X \times X \to \mathbb{R}$, визначена для $\forall$ x, y $\in$ X, яка задовольняє трьом аксіомам метрики:

1) d (x, y) = 0 $\Leftrightarrow$ x ≡ y (аксіома тотожності)
2) d (x, y) = d (y, x) (аксіома симетрії)
3) d (x, z) ≤ d (x, y) + d (y, z) (аксіома трикутника)

Доведемо, що ці аксіоми справджуються для вказаної метрики.

Відзначено, що запропонована обернено-адитивна метрика для оцінювання сформованої доменно-орієнтованої онтології є зручним інструментом аналізу онтологій, сформованих на основі GFO.

У **четвертому розділі** проаналізовано та досліджено структуру та архітектуру інтелектуальної програмної системи безпеки житлового комплексу з ситуаційною обізнаністю.

Наголошено, що під структурою інтелектуальної програмної системи безпеки з ситуаційною обізнаністю розуміється організовану сукупність компонентів, що забезпечують інтелектуальні процедури моніторингу середовища, аналізу даних, і управління безпекою в реальному масштабі часу. Вона включає інтелектуальних агентів і давачі, служби внутрішнього програмного забезпечення, та центральний блок управління, які працюють разом для створення комплексного захисту житлового комплексу (Рис.5).

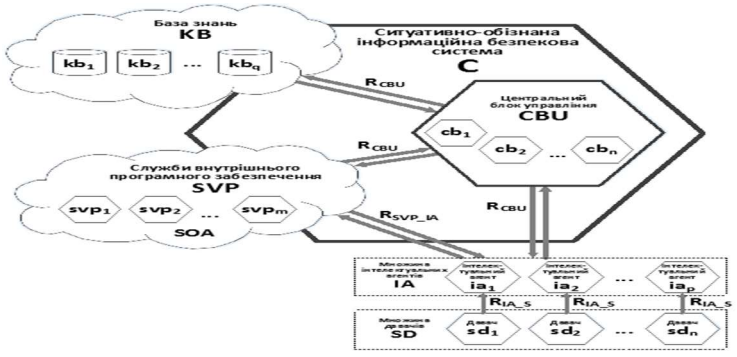


Рис. 5 Структура інтелектуальної програмної системи безпеки житлового комплексу з ситуаційною обізнаністю

Відзначено, що інтелектуальні автономні агенти, є ключовими компонентами інтелектуальної програмної системи безпеки житлового комплексу (рис.6). Вони є програмними або апаратними суб'єктами, здатними автономно діяти в середовищі, приймати рішення на основі отриманих даних, і виконувати завдання без втручання людини.

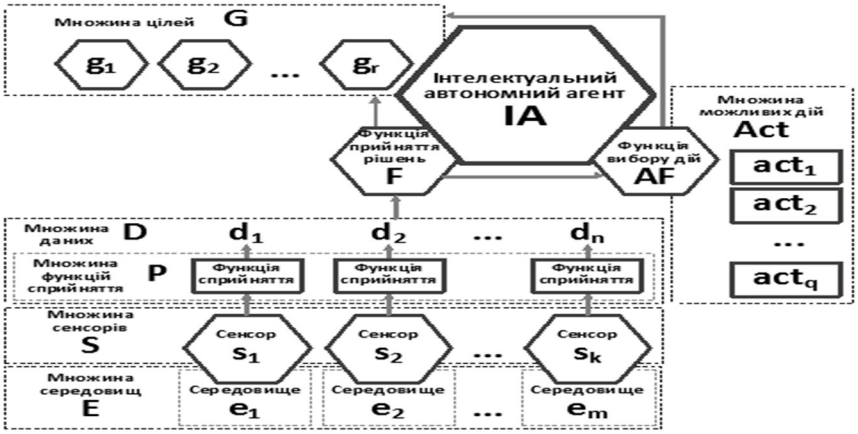


Рис. 6. Структура концепту «інтелектуальний автономний агент»

Концепт «інтелектуальний автономний агент» подано у формі кортежу:

$$IA=(S,E,D,P,F,Act,G,AF), \quad (6)$$

де S – множина сенсорів, які використовує агент для отримання інформації з середовища $S=\{s_1, s_2, \ldots, s_k\}$, E – середовище, або множина середовищ, у яких агенти функціонують $E=\{e_1,e_2,\ldots,e_m\}$, D – множина даних, зібраних агентом з середовищ для аналізу і прийняття рішень $D=\{d_1, d_2, \ldots, d_n\}$, P – функція сприйняття, яка визначає, як агент отримує інформацію з середовища: P:E→D. Множина функцій сприйняття P={p1,p2,…,pn} відповідає множині даних D, F – функція прийняття рішень, яка визначає, як агент опрацьовує дані для вибору дій: F:D→Act, Act – множина можливих дій, які може виконувати агент. Act={act1,act2,…,actq}, G – множина цілей, яких намагається досягти агент G={g1, g2, …, gr}, AF – функція вибору дій, яка визначає, яку дію виконує агент для досягнення мети на основі аналізу даних: AF:F→Act.

Обґрунтовано висновки, що служби внутрішнього програмного забезпечення, є важливим компонентом інтелектуальної програмної системи безпеки житлового комплексу (рис.7). Вони реалізовані як хмарні сервіси, що виконують ресурсомісткі обчислення, та забезпечують виконання різноманітних завдань і відповідають за управління підсистемами та комунікацією між різними елементами системи безпеки. Формальний запис концепту «служба внутрішнього програмного забезпечення» як елемента структури інтелектуальної програмної системи безпеки житлового комплексу подано кортежем:

$$SVP=(N,F,R,M,V), \quad (7)$$

де N – набір сервісів, що реалізовані як хмарні обчислення та надають ресурси для системи, забезпечують виконання завдань, пов'язаних із безпекою $N=\{n_1,n_2,\ldots,n_m\}$, F – множина функцій, що виконуються службою, визначають, як служба реалізує опрацювання даних і виконання складних обчислень для забезпечення потрібних функцій безпеки. $F=\{f_1,f_2,\ldots,f_m\}$, R – набір ресурсів, які використовуються службою для виконання функцій (обчислювальна потужність, пам'ять тощо), включають інфраструктуру, що необхідна для роботи служби. $R=\{r_1,r_2,\ldots,r_p\}$, M – множина даних, що опрацьовуються та зберігаються службою для аналізу безпеки та прийняття рішень. $M=\{m_1,m_2,\ldots,m_q\}$, V – набір процедур і протоколів, правил, що забезпечують правильне функціонування служби в рамках інтелектуальної програмної системи. $V=\{v_1,v_2,\ldots,v_r\}$.

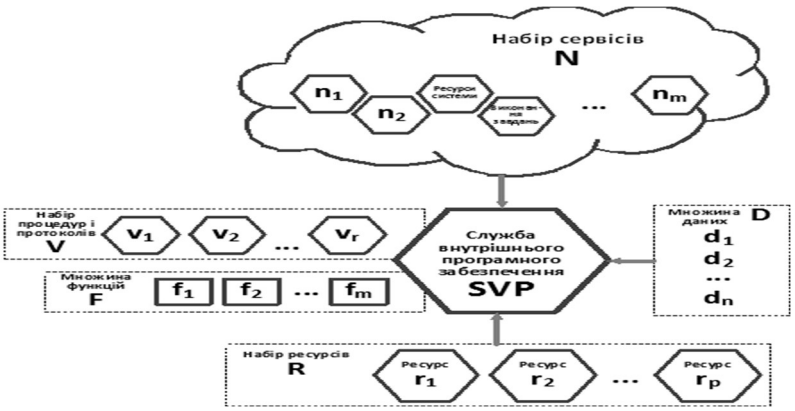


Рис. 7. Структура концепту «служба внутрішнього програмного забезпечення»

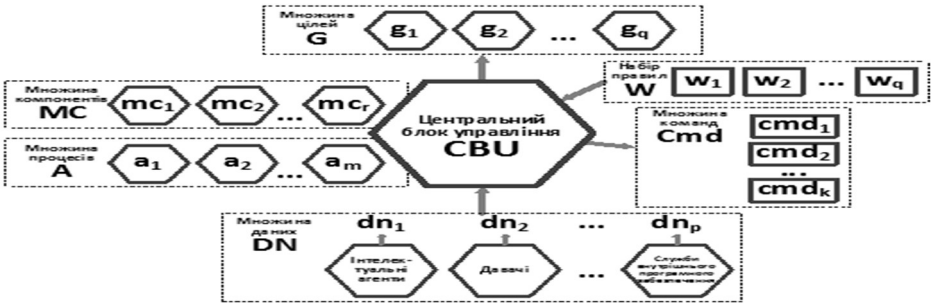


Рис. 8. Структура концепту «Центральний блок управління»

Концепт «Центральний блок управління» подано кортежем (рис.8):

$$CBU=(MC,DN,A,W,G, Cmd), \quad (8)$$

де MC – множина компонентів центрального блоку, які реалізують основні функції керування системою, забезпечують апаратну та програмну інфраструктуру для виконання процедур управління $MC=\{mc_1,mc_2,\ldots,mc_r\}$, DN – множина даних, що надходять від сенсорів, інтелектуальних агентів та служб внутрішнього програмного забезпечення, які використовуються для аналізу з метою формування загальної ситуаційної обізнаності $DN=\{dn_1,dn_2,\ldots,dn_p\}$, A – множина процесів, що виконуються для аналізу ситуації, зокрема опрацювання даних та виявлення аномалій, включаючи глибинний аналіз і виявлення загроз. A асоціює кожну команду з конкретним компонентом або підсистемою, яка повинна виконати дію $A=\{a_1,a_2,\ldots,a_m\}$, W – набір правил, що визначають логіку прийняття рішень на основі аналізу даних $W=\{w_1,w_2,\ldots,w_q\}$, G – множина цілей або стратегій, яких система намагається досягти для забезпечення безпеки, що визначають загальну мету системи, зокрема, забезпечення безпеки мешканців та реагування на потенційні загрози $G=\{g_1, g_2,\ldots, g_q\}$, Cmd – множина команд, що видаються для виконання дій, які визначені як результат аналізу і прийняття рішень $Cmd=\{cmd_1,cmd_2,\ldots,cmd_k\}$. Центральний блок управління, є ядром інтелектуальної програмної системи безпеки житлового комплексу, відповідає за загальний контроль, прийняття рішень і глибинний аналіз даних, управління політикою та стратегією, а також розподілом ресурсів. Загальна структура ситуаційно-обізнаної інтелектуальної програмної системи безпеки подана кортежем:

$$C=<IA,SVP,CBU, SD, KB>, \quad (9)$$

де C – структура інтелектуальної програмної системи безпеки з ситуаційною обізнаністю, IA – інтелектуальні агенти, множина автономних пристроїв, що орієнтовані на виконання певних завдань і використовують дані, отримані з сенсорів $IA=\{ia_1,ia_2,\ldots,ia_p\}$, SVP – служби внутрішнього програмного забезпечення, реалізовані як хмарні сервіси, що виконують

ресурсномісткі обчислення відповідно до вимог сервіс-орієнтованої архітектури $SVP=\{svp_1,svp_2,\ldots,svp_m\}$, CBU – центральний блок управління, що відповідає за формування загальної картини ситуації та аналіз інформації, отриманої від сенсорів, агентів і служб $CBU=\{cb_1,cb_2,\ldots,cb_n\}$, SD – множина сенсорів, що інтегровані з інтелектуальними агентами та подають дані щодо біжучої ситуацію $SD=\{sd_1,sd_2,\ldots,sd_n\}$, KB – база знань, яка використовується центральним блоком управління як експертні знання для аналізу ситуації та ухвалення відповідних рішень $KB=\{kb_1,kb_2,\ldots,kb_q\}$.

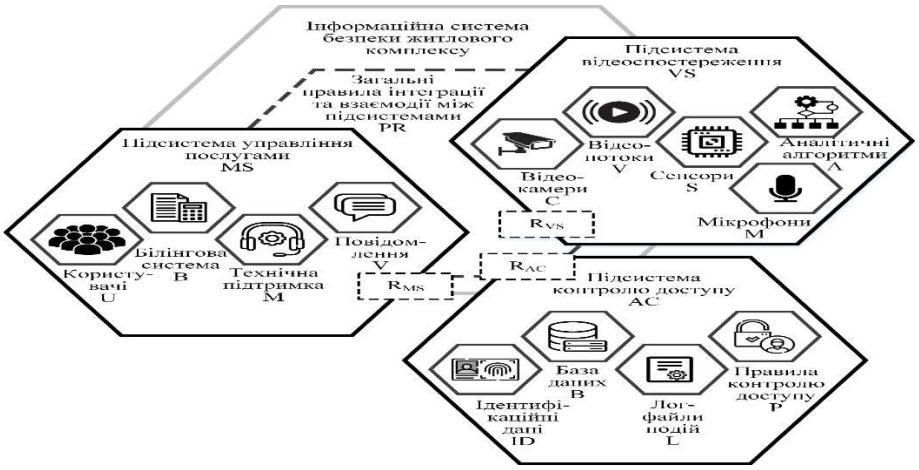


Рис. 9. Архітектура інтелектуальної
програмної системи безпеки житлового комплексу

Взаємодія компонентів інтелектуальної програмної системи безпеки передбачає інтелектуальні агенти збирають дані з давачів, та передають їх службам внутрішнього програмного забезпечення для подальшого опрацювання. Служби, реалізовані як хмарні сервіси, виконують ресурсомісткі обчислення, результати яких передаються до центрального блоку управління.

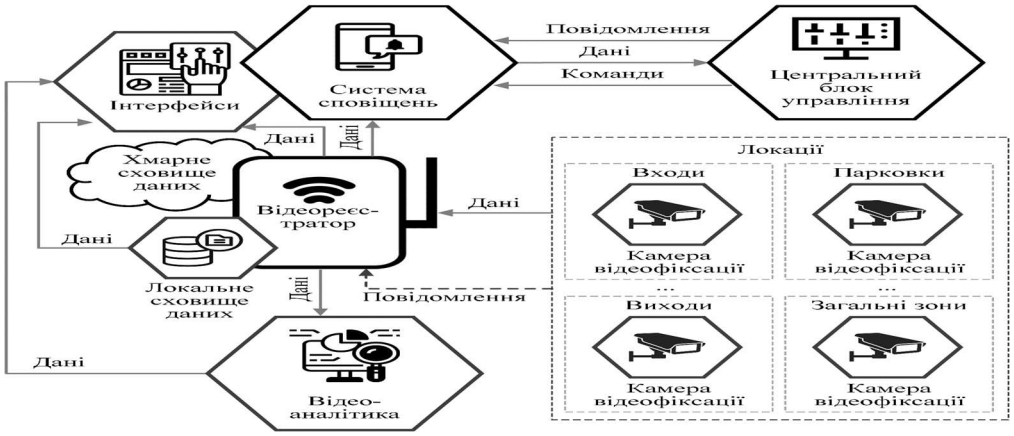


Рис. 10. Архітектура підсистеми відеоспостереження

Зазначено, що під архітектурою інтелектуальної програмної системи безпеки розуміється її концептуальну модель, в якій визначаються компоненти та їх взаємодії, функції, а також методи та засоби їх інтеграції із зовнішнім середовищем (рис.9). Формально архітектуру інтелектуальної програмної системи безпеки житлового комплексу подано кортежем множин, що задають окремі групи елементів в підсистемах і множин відношень заданими на них:

$$IS=(VS,AC,MS,PR), \quad (10)$$

де VS – підсистема відеоспостереження

$$VS=(C,M,S,A,V,R_{VS}), \quad (11)$$

де C – відеокамери, M – мікрофони, S – сенсори, A – аналітичні алгоритми (виявлення руху, розпізнавання обличь), V – відеопотоки, R_{VS} – правила взаємодії із центральним блоком. Підсистема відеоспостереження (VS) (рис.10) збирає дані з допомогою камер, опрацьовує їх за допомогою аналітичних алгоритмів, і взаємодіє з іншими підсистемами через центральний блок.

AC – підсистема контролю доступу:

$$AC=(ID,B,L,P,R_{AC}), \quad (12)$$

де ID – ідентифікаційні дані (картки, біометрія), B – база даних, L – лог файли, P – правила контролю доступу, R_{AC} – реакції на події (блокування). Підсистема контролю доступу (AC) регулює доступ до приміщень, зберігає журнали подій та може автоматично блокувати доступ у разі загрози.

MS – підсистема управління послугами:

$$MS=(U,B,T,N,RMS), \quad (13)$$

де U – користувачі, B – білінгова система, T – технічна підтримка, N – повідомлення, R_{MS} – правила керування послугами. Підсистема управління послугами оператора (MS) реалізує процеси управління користувачами, їхніми передплатами, обслуговуванням і надає інформаційні сервіси, зокрема повідомлення.

PR – загальні правила інтеграції та взаємодії між підсистемами.

$$PR = (PR_{VS}, PR_{AC}, PR_{MS}), \quad (14)$$

де RPVS, RPAC,RPMS – правила інтеграції та взаємодії кожної із підсистем. В архітектурі фіксується як компоненти системи взаємодіють між собою, як вони інтегруються з іншими системами і підсистемами, а також, як забезпечується реалізації функцій зручності використання, масштабованості, безпеки та ефективності роботи цілісної інтелектуальної програмної системи безпеки.

Підсистема відеоспостереження, забезпечує моніторинг території комплексу, включаючи входи, виходи, паркінги, дитячі майданчики та місця загального користування. Вона використовує мережу камер високої роздільної здатності, з можливістю запису та відтворення відеоматеріалів. Ця підсистема збирає дані через камери, опрацьовує їх за допомогою аналітичних алгоритмів, і взаємодіє з іншими підсистемами.

Підсистеми контролю доступу, регулює доступ до приміщень, зберігає журнали подій, та може автоматично блокувати доступ у разі загрози. Вона використовує електронні ключі, RFID-мітки або біометричні сканери.

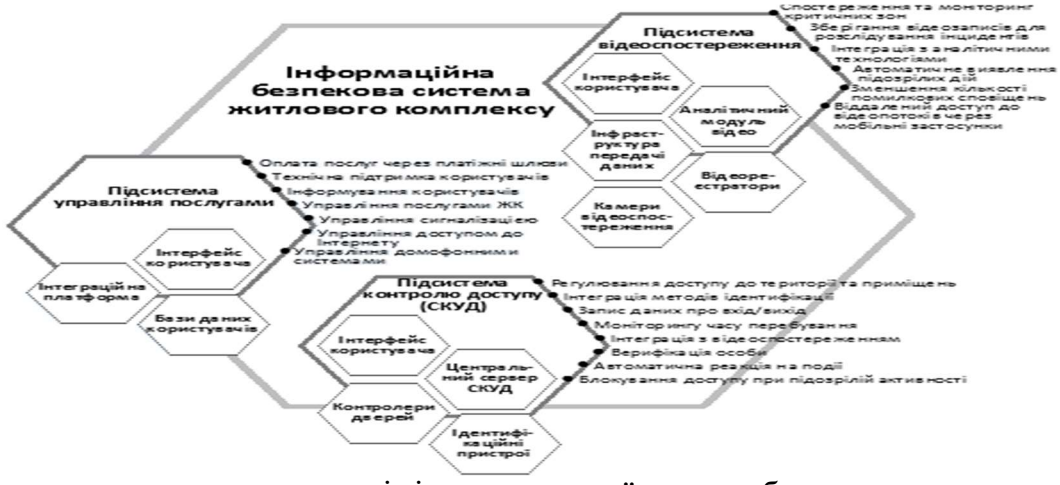


Рис. 11. Інтегроване подання компонентів інтелектуальної системи безпеки житлового комплексу

Підсистема управління послугами, керує користувачами, їхніми передплатами, зв'язками зі сторонніми службами, та надає інформаційні сервіси. Мешканці можуть обирати набір послуг через мобільний додаток, або веб-інтерфейс.

Відзначено, що підсистеми, працюють в єдиній екосистемі, використовуючи

центральний контрольний блок, який синхронізує їхню роботу (рис.11). Завдяки такій взаємодії, автоматизовано ряд процесів, наприклад: відкривання дверей після успішної ідентифікації за допомогою відео аналітики, або, автоматичне створення технічних заявок на основі даних з камер та давачів.

У п’ятому розділі подано відомості щодо реалізації інтелектуальної програмної системи безпеки АСТРА “Безпечний ЖК”.

Наголошено, що у першій версії програмного продукту, основна увага зосереджена на реалізації підсистем контролю доступу та відеоспостереження. Проаналізовано процес концептуального моделювання інформаційної системи безпеки житлового комплексу на прикладі підсистеми відеоспостереження, яка реалізує функцію відеоспостереження у всіх критичних зонах житлового комплексу: входах, виходах, ліфтах, паркінгах, прилеглих територіях та громадських зонах (Рис. 12).

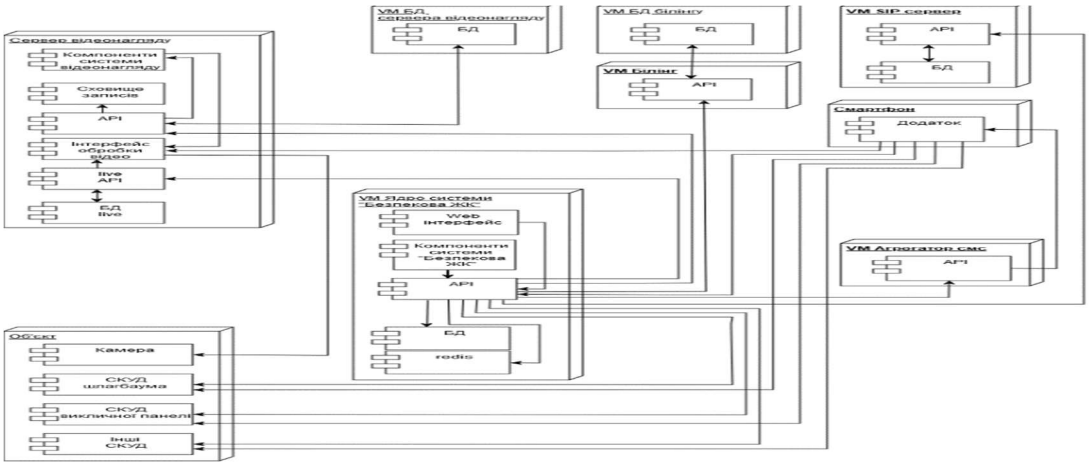


Рис. 12. UML діаграма розгортання інтелектуальної системи безпеки

Відзначено, що для розроблення бекенду, обрано та використано інформаційно-технологічну платформу Arduino та Django, що є веб платформою на основі мови Python, використовує архітектуру model-view-template. Основними її компонентами є моделі. Django ORM (Object-Relational Mapping), представлення, шаблони, URL-менеджер, проміжне програмне забезпечення, база даних, міграції. Як СУБД обрано PostgreSQL, яка дозволяє розширювати функціонал, додаючи нові типи даних, оператори та індекси, без необхідності змінювати вихідний код. Вона має потужний механізм опрацювання складних запитів, включаючи підтримку під-запитів, об’єднань, агрегатних функцій і багатовимірних масивів. Модуль відеоспостереження, реалізований наступним чином (Рис.13): відеопотік з камер, через веб-сервер Nginx транслює потокове відео, в паралель відеопотік конвертується до єдиного стандарту h264/aac, засобами ffmpeg та ffprobe, та зберігається в архіві zoneminder.

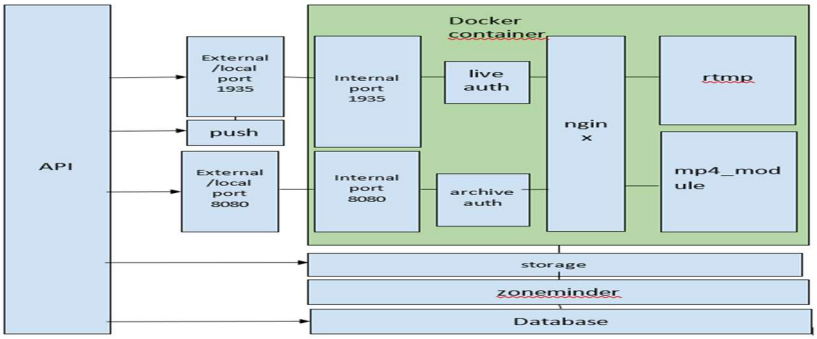


Рис. 13. Структура модуля відеоспостереження інтелектуальної системи безпеки

Для автоматизації розгортання, використовується docker container, який вже і містить API для взаємодії з іншими компонентами системи. Користувацький інтерфейс, розроблено з використанням бібліотеки react.js, який використовує мови програмування TypeScript, візуальні компоненти інтерфейсу реалізовано на основі Ant Design. Відзначено, що в інтелектуальній системі безпеки житлового комплексу, передбачено реалізацію багатокористувацьких інтерфейсів, які формуються індивідуально для кожного ЖК. Для їх побудови, використано системне поєднання методу персон та методу випадкового лісу. З використанням методу персон сформовано множину протоперсон, які функціонально відображають різні типи користувацьких груп інтелектуальної системи безпеки на основі їх демографічних, психографічних, та поведінкових характеристик. Наведемо метод визначення особливостей протоперсон:

Крок 1. Збір даних та ідентифікація потенційних критеріїв.

Крок 2. Аналіз даних для кожної протоперсони.

Крок 3. Вибір ключових критеріїв для класифікації.

Крок 4. Використання обраних критеріїв для навчання моделі.

Модель випадкового лісу будується на основі навчального набору даних, що містить критерії та мітки класів, та складається з множини дерев рішень, кожне з яких навчено на випадковій вибірці даних з навчального набору. Із застосуванням методу випадкового лісу проведено навчання моделі для оцінювання важливості ознак класифікування протоперсон. Кожне дерево в лісі обирає підмножину даних для навчання (із заміною) і випадковим чином - підмножину функцій для кожного розбиття. Нехай N – кількість дерев у лісі, n – кількість точок даних у підмножині, m – кількість об’єктів у підмножині. Вибирається випадкова підмножина даних D_k розміру n та випадкова підмножина функцій F_k розміру m. Дерево рішень будується за допомогою Dk і Fk. Класифікація відбувається з використанням дерева для нового спостереження. Усереднюють показники або використовується метод регресії для всіх дерев, щоб отримати остаточний результат. Результат класифікації $\hat{y}$ для об’єкта x можна подати як:

$$\hat{y}=\frac{1}{N}\sum_{k=1}^{N} N_k\,(x), \tag{15}$$

де $yk(x)$ – результат класифікації від k-дерева. Цей підхід гарантує, що наша модель випадкового лісу може впоратися зі складністю та мінливістю даних користувачів

$$\hat{y} = \text{mode}(\hat{y}_1, \hat{y}_2, \ldots \hat{y}_k), \tag{16}$$

де $\hat{y}_k$ – результат, отриманий з дерева k, а режим – це функція, яка повертає значення, яке найчастіше зустрічається серед них. Конкретні параметри, такі як кількість дерев у лісі, критерії вибору ознак тощо, можуть змінюватися залежно від конкретної реалізації та потреб процедур аналізу даних мешканців ЖК.

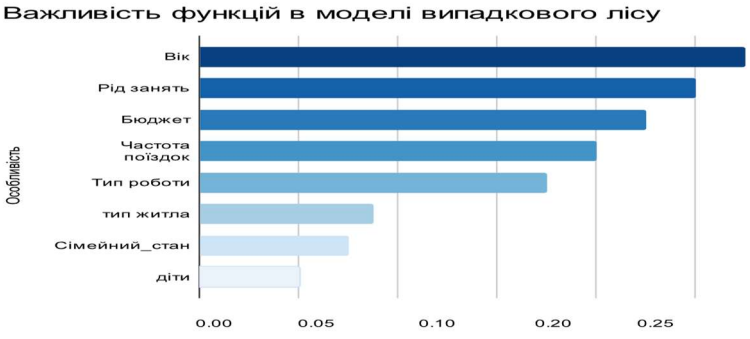


Рис. 14. Графік значущості ознак для класифікації

Для кожного ЖК на основі анкетних даних, отриманих від ОСББ навчаємо модель на визначення ключових критеріїв та класифікації мешканців. Для перевірки, модель була застосована в ЖК, де було зібрано 1000 анкетних даних. Навчальна вибірка склала - 70% (700 записів) і тестова вибірка - 30% (300 записів). Загальна точність отриманих результатів:

$$\text{Accuracy}=\frac{\text{Кількість правильних передбачень}}{\text{Загальна кількість передбачень}}=\frac{267}{300}\approx 0{,}89. \quad (17)$$

Результат важливості критеріїв представлений на (Рис. 14)

На основі отриманих даних важливості критеріїв, сформовано набір протоперсон, які відрізняються віком, родом занять, та бюджетом. Для формалізації та структурування об'єктів інтелектуальної програмної системи безпеки, розроблено набір UML діаграм, які дозволили верифікувати повноту та цілісність пропонованої інтелектуальної програмної системи.

Висновки

У дисертаційній роботі розв’язано важливу наукову задачу підвищення ефективності, надійності та адаптивності систем безпеки житлових комплексів шляхом розроблення та інтеграції інтелектуальних методів аналізу, прогнозування загроз і прийняття рішень на основі опрацювання великих обсягів даних, просторово-часових характеристик і поведінкових моделей користувачів. У дисертації одержано такі результати:

Проаналізовано широкий спектр наукових праць у галузі систем безпеки, в яких подані оригінальні методи та засоби їх побудови, розглянуто їхню застосовність у контексті житлових комплексів. Проведено аналіз архітектурних рішень для побудови таких інформаційних систем.

Використовуючи метод аналізу ієрархій, визначено кращу платформу для реалізації інформаційної системи безпеки житлового комплексу. Проведений SWOT аналіз методологій управління IT проектами сприяв обранню методології DevOps, як базової, що забезпечує ефективну реалізацію функцій безперервної інтеграції, тестування та доставки. Завдяки поєднанню методів аналізу ієрархій та експертного оцінювання сформовано комплекси програмних інструментів методології DevOps та обрано кращий серед них.

Використовуючи метод аналізу ієрархій, визначено кращу IT платформу для реалізації інформаційної системи безпеки житлового комплексу. Проведений SWOT аналіз методологій управління IT проектами сприяв обранню методології DevOps, як базової, що забезпечує ефективну реалізацію функцій безперервної інтеграції, тестування та доставки. Завдяки поєднанню методів аналізу ієрархій та експертного оцінювання сформовано комплекси програмних інструментів методології DevOps та обрано кращий серед них.

Сформовано структуру інформаційної системи безпеки, яка складається з інтелектуальних агентів та давачів, внутрішнього ПЗ та блоку управління, а також архітектуру, яка містить підсистеми відеоспостереження, контролю доступу і управління послугами та керується центральним блоком.

З використанням ситуоїдного об’єкта GFO розроблено моделі прогнозування та передбачення на основі баз знань. Визначено адитивно-обернену метрику, як один з інструментів обчислення відстаней між концептами онтології.

Досліджено, опрацьовано і структуровано значну кількість безпекових сценаріїв, на основі яких спроектовано відповідні ситуоїди, які подано конструкціями мови OWL та у вигляді патернів

Проведено аналіз результатів опитування мешканців ряду житлових комплексів з метою їх кластеризації з використанням демографічних, психографічних та поведінкових критеріїв. Використовуючи методи персон та випадкового лісу, сформовано класи протоперсон, які представляють відповідні ролі в інформаційній системі безпеки житлового комплексу.

Досліджено основні аспекти та інструментарії методології DevOps та їхню застосовність при розробці інтелектуальної інформаційної системи безпеки житлового комплексу та сформовано доцільні групи інструментів, які використано при розробленні систем.

Розроблено архітектурну модель інформаційної системи безпеки, побудовано UML діаграми, які відображають функціональну складову системи, проаналізовано і використано сучасні інформаційні технології відеоспостереження, цифрової ідентифікації та задач розпізнавання.

Реалізовано підсистеми контролю доступу, відеоспостереження, управління послугами та інтерфейси для користувачів і адміністраторів інформаційної системи безпеки житлового комплексу «АСТРА. Безпечний ЖК», яка враховує потреби громади в безпеці житлового комплексу, об'єднує в єдину інформаційну еко-систему IoT рішення безпеки ЖК (відеоспостереження, контроль доступу, інформаційні послуги), є незалежною від конкретних виробників давачів, враховує вітчизняні реалії сьогодення і проходить етап тестових випробувань.

Імплементація інформаційної системи безпеки ЖК на функціональному полі інтернет-провайдера, додало їй наступних переваг: використання кабельної інфраструктури провайдера на території ЖК для швидкого і раціонального розгортання, використання серверної інфраструктури провайдера, інструментарію методології DevOps, для моніторингу, інтеграції, захисту від кібератак та оперативного масштабування.

База знань інформаційної системи формується із врахуванням вимог подальшої інтеграції та розбудови функцій ситуаційної обізнаності в наступних версіях програмного комплексу.

Список опублікованих праць за темою дисертації

Статті, опубліковані у періодичних виданнях, індексованих міжнародною наукометричною базою даних Scopus

1. Zhovnir Y., Kunanets N., Burov Y., Duda O., Pasichnyk V. Development of the structure and architecture of situational awareness security information systems for residential complexes // Eastern-European Journal of Enterprise Technologies. 2025. № 1(133). P. 63-98.
2. Vladov S., Avkurova Zh., Lytvyn V., Zhovnir Yu. Analytical neural network system for the helicopter turboshaft engines operating modes classification // International Journal of Computing. 2024. Vol. 23, No. 3. P. 342–359.

Статті, опубліковані у періодичних виданнях, які входять до переліку наукових фахових видань України

3. Жовнір Ю., Буров Є. Еволюція архітектурних рішень для розумних будинків // Computer Systems and Information Technologies. 2024. Вип.3. С. 74–85.
4. Григорович А., Григорович В., Жовнір Ю., Грибовський О. Формування обернено-адитивної семантичної метрики для аналізу онтологій безпекових систем багатоквартирних будинків // Комп’ютерно-інтегровані технології: освіта, наука, виробництво. 2024. Вип. 56. С. 12-30.
5. Жовнір Ю., Грибовський О. Порівняльний аналіз програмно-апаратних інструментальних засобів для створення безпекової системи багатоквартирного будинку // Herald of Khmelnytskyi National University. Technical Sciences. 2024. Вип. 339(4). С.344-358.
6. Жовнір Ю., Грибовський О., Пасічник С., Бобик І. Створення інтерфейсів безпекових систем багатоквартирних будинків з використанням методу Персон // Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі. 2024. Вип. 16. С. 145–166.
7. Burov E., Zhovnir Y., Zakhariya O. The vision and implementation of intelligent security system // Herald of Khmelnytskyi National University. Technical Sciences. 2024. Is. 341(5). 497-509.

8. Цейтлін Г.Е., Захарія Л.М., Захарія О.В., Жовнір Ю.І Екологічні аспекти подання знань засобами алгебри алгоритміки // Проблеми програмування. 2010. № 2–3. С. 369-375.
9. Burov Y., Zhovnir Y., Zakharia O. Designing the ontology for intelligent security system of residential community // Scientific Journal of the Ternopil Ivan Puluj National Technical University. 2024. Vol. 116, no 4. P. 111-124.
10. Кунанець Н., Жовнір Ю., Веремеєнко А., Пущак С. Концептуальне моделювання системи відеоспостереження з ситуаційною обізнаністю // Herald of Khmelnytskyi National University. Technical Sciences. 2025. №1. С. 189-202.
11. Жовнір Ю. І., Грибовський О. М., Орлов М. В., Дуда О. М., Кунанець Н. Е. Методологія розроблення та супроводу інформаційних систем, базованих на технології інтернету речей // Управління розвитком складних систем. 2024. Вип. 60. С. 56-71.
12. Орлов М.В., Дуда О.М., Жовнір Ю.І., Грибовський О.М. Інструменти методології DevOps в інформаційних системах на основі технологій IoT // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2024. Вип. 57. С. 128-139.
13. Орлов М. В., Грибовський О.М., Жовнір Ю.І., Дуда О.М. Від концепції до реальності: роль DevOps в екосистемах IoT // Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2024. Т. 35(74), № 6, Ч.2. С. 157-164.

Праці та тези доповідей у збірниках матеріалів конференцій

1. Vaskiv R., Veretennikova N., Nebesnyi R., Bilovus H., Zhovnir Y. Formation of an IT project team by analogy with a flock // IEEE 19th International Conference on Computer Science and Information Technologies (CSIT). 2024.
2. Жовнір Ю.І., Кунанець Н.Е., Захарія О.В. Вимоги до інформаційних систем безпеки житлового кварталу // Proceedings the 5th International Scientific and Practical Conference "Current Trends in Scientific Research Development", (December 12-14, 2024). Boston, 2024. P. 298–303.
3. Жовнір Ю.І., Кунанець Н.Е., Захарія О.В., Орлов М.В. Використання методологій devops та devsecops у IT проєктах // Proceedings the 4th International Scientific and Practical Conference "Science in the Modern World: Innovations and Challenges", (December 19-21, 2024). Toronto, 2024. P. 228-233.
4. Жовнір Ю.І., Кунанець Н.Е., Захарія О.В., Пасічник С.О. Формування бекенду та фронтенду інформаційної системи безпеки з ситуаційною обізнаністю // Proceedings I International scientific and practical conference «European Congress of Scientific Discovery» (December 29-31, 2024). Madrid, 2024. P. 244-252.
5. Жовнір Ю.І., Кунанець Н.Е., Захарія О.В., Орлов М.В. Планування та прогнозування ситуації в інтелектуальній інформаційній системі безпеки // Proceedings II International scientific and practical conference "Future of Science: Innovations and Perspectives", (December 23-25, 2024). Stockholm, 2024. P. 163-169.
6. Жовнір Ю., Захарія Л., Захарія Ю. Формалізація та породження знань засобами алгебри алгоритміки // Комп'ютерні науки та інженерія: матеріали наукової конференції молодих вчених, 25-27 листопада 2010 р. Львів, 2010. С. 118-120.
7. Жовнір Ю., Ваків М., Захарія Л. Віртуальна аудиторія як система електронного навчання інвалідів // Комп'ютерні науки та інженерія: матеріали наукової конференції молодих вчених, 25-27 листопада 2010 р. Львів, 2010. С. 126-128.

АНОТАЦІЇ

Жовнір Ю.І. Методи та засоби побудови інтелектуальної програмної системи безпеки житлових комплексів. На правах рукопису**.** Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 01.05.03 - математичне та програмне забезпечення обчислювальних машин і систем. Національний університет «Львівська політехніка», Міністерство освіти і науки України, Львів, 2025.

Дисертація присвячена розробленню інтелектуальної програмної системи безпеки житлових комплексів з ситуаційною обізнаністю. Зазначені системи є складною областю для розроблення, впровадження та супроводу. За своєю природою вони є динамічними системами, які усвідомлюють зміни, що відображають в навколишньому середовищі та спроможні розумно реагувати на них. Онтологія забезпечує загальний словник, основу для специфікації об'єктів, включених у систему, та їх взаємодії. Розглянуто онтологію, як програмний документ, який розробляється синхронно із системою безпеки. У цьому сенсі локальна онтологія відображає поточну версію програмного продукту. Для багаторазового використання програмний документ побудовано на основі фундаментальної онтології GFO, що дозволяє моделювати просторову, часову та ситуаційну динаміку. Онтологія для інтелектуальної програмної системи безпеки побудована на основі сценаріїв, які підтримуються системою. У дисертації запропоновано основу для передбачення та планування лій на основі онтології GFO. Кожне завдання або проблема розглядається як ситуоїд, що має ряд проміжних ситуацій. Контекстно організована база досвідних знань використовується для отримання інформації про можливі сценарії розвитку подій і використовується для планування та прогнозування. Процес планування та передбачення працює в умовах неповної інформації та непередбачених зовнішніх подій, оскільки прогнози постійно оновлюються з використанням зворотного зв'язку від даних давачів та узгодження цієї інформації з прогнозованою моделлю. Запропоновано метрику, яку використано для оцінювання параметрів проблемно-орієнтованої онтології системи безпеки житлового комплексу. Обґрунтовано необхідність введення цієї метрики. Розроблено структуру та архітектуру для інтелектуальної програмної системи безпеки з ситуативною обізнаністю. Досліджено процеси створення персоналізованих інтерфейсів безпекових систем на основі поєднання методу персон та методу випадкового лісу для класифікації потенційних користувачів системи. Розглянуто сучасні інструменти реалізації методології DevOps при розробленні та супроводженні інтелектуальної програмної системи безпеки. На основі отриманих результатів реалізовано та передано в дослідну експлуатацію першу черга інтелектуальної програмної системи безпеки з ситуаційною обізнаністю АСТРА "Безпечний ЖК", на базі регіонального провайдера Інтернет послуг «АСТРА-ЛЬВІВ». Результати дисертаційного дослідження впроваджено у навчальний процес підготовки ІТ фахівців у ряді провідних ЗВО України.

Ключові слова: інтелектуальна програмна система безпеки, онтологія, загальна формальна онтологія (GFO), мова веб-онтології, структура опису ресурсів, мова шаблонів, ситуаційна обізнаність, просторова та часова динаміка, житловий комплекс, ситуаційна обізнаність, аналіз ситуації, ситуоїд, обернено-адитивна метрика, метод Персон, метод випадкового лісу, інтернет речей (IoT), DevOps.

Zhovnir Y.I. Methods and tools for developing an intelligent software security system for residential complexes. On the rights of the manuscript. Dissertation for obtaining the scientific degree of candidate of technical sciences in the specialty 01.05.03 - mathematical and software support of computing machines and systems. Lviv Polytechnic National University, Ministry of Education and Science of Ukraine, Lviv, 2025.

The dissertation is devoted to the development of an intelligent software security system with

situational awareness. Intelligent security systems represent a complex area for implementation, as they are inherently dynamic systems that perceive changes in the environment and respond intelligently. Ontology provides a common vocabulary and a foundation for specifying objects included in the system and their interactions. Ontology is considered a software document developed alongside the security system. In this sense, it is a localized ontology reflecting the current version of the application. However, for reusability, the software document is based on the General Formal Ontology (GFO), which enables modelling of spatial, temporal, and situational dynamics. The ontology for the intelligent software security system is built upon scenarios supported by the system. The dissertation proposes a framework for forecasting and planning based on the GFO ontology. Each task or problem is treated as a "situoid," comprising a series of intermediate situations. The structure focuses on analysing changes between situations resulting from anticipated actions or events. A contextually organized experiential knowledge base is used to derive information about possible event scenarios, which supports planning and evaluation. The model enables the construction and comparison of configuration change trajectories for specific objects, situations, or situoids. The planning and forecasting process operates under conditions of incomplete information and unpredictable external events, with forecasts being continuously updated using feedback from sensor data and aligning this information with the predictive model. A metric is proposed for developing effective intelligent systems using ontologies for knowledge representation, especially in the design of residential community security systems. The proposed metric is analysed and substantiated. The structure and architecture of an intelligent software security system with situational awareness have been developed. The process of creating interfaces for security systems is studied using a combination of the Persona method and the Random Forest method for user classification. Modern approaches to integrating DevOps methodology into the development and maintenance of Internet of Things (IoT)-based solutions are considered and implemented. A comparative analysis of some of the most popular software and hardware tools for creating an intelligent security platform for a residential community has also been conducted. Based on the obtained results, an intelligent software security system with situational awareness, ASTRA "Safe Residential Community," has been implemented, currently undergoing testing and deployment.

Keywords: intelligent software security system, ontology, General Formal Ontology (GFO), Web Ontology Language, Resource Description Framework, template language, situational awareness, spatial and temporal dynamics, residential community, situational awareness, situation analysis, situoid, reverse-additive metric, Persona method, Random Forest method, Internet of Things (IoT), DevOps.