DOI 10.31891/2307-5732-2025-347-26
УДК 004.942:004.9:004.6

КУНАНЕЦЬ НАТАЛІЯ
Національний університет «Львівська політехніка»
https://orcid.org/0000-0003-3007-2462
e-mail: nek.lviv@gmail.com
ЖОВНІР ЮРІЙ
Національний університет «Львівська політехніка»
https://orcid.org/0009-0006-6186-2861
e-mail: e-mail: zhovnir@astra.in.ua
ВЕРЕМЕЄНКО АНДРІЙ
Національний університет «Львівська політехніка»
https://orcid.org/0009-0000-1916-3254
e-mail: andriiverem@gmail.com
ПУЩАК СЕМЕН
Національний університет «Львівська політехніка»
https://orcid.org/0009-0009-8958-6522
e-mail: spushchak@astra.in.ua

КОНЦЕПТУАЛЬНЕ МОДЕЛЮВАННЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ З СИТУАЦІЙНОЮ ОБІЗНАНІСТЮ

Стаття присвячена концептуальному моделюванню системи відеоспостереження з ситуаційною обізнаністю, що базується на технологіях Інтернету речей. Запропоновано використовувати ситуаційно-обізнаний підхід, який інтегрує інтелектуальні пристрої, алгоритми машинного навчання та засоби аналітики для забезпечення ефективного моніторингу, виявлення загроз і автоматизованого реагування на інциденти. Основна увага приділяється концептуальній моделі на основі UML-діаграм, які використовуються для формалізації структури, функціональності та взаємодії компонентів системи.

У статті розглянуто основні компоненти системи: сенсори, камери, програмне забезпечення для ситуаційного аналізу, системи зберігання даних та візуалізації, а також модулі для прогнозування подій і управління ризиками. Діаграма прецедентів описує основні сценарії використання, зокрема моніторинг у реальному часі, аналіз архівних записів, реагування на аномалії. Діаграма послідовності демонструє взаємодію між компонентами системи в режимі реального часу, наприклад, при виявленні руху або загрози.

Окрему увагу приділено діаграмі класів, яка відображає структуру програмного забезпечення, включаючи класи для обробки даних, управління пристроями, модулів аналітики та візуалізації. Діаграма компонентів деталізує архітектуру системи, підкреслюючи інтеграцію між IoT-пристроями, серверними компонентами та хмарними сервісами. На діаграмі розгортання моделюється фізична інфраструктура системи, що охоплює камери, сенсори, мережеві пристрої, сервери та мобільні додатки.

Запропонований підхід забезпечує масштабованість, адаптивність і високу ефективність системи відеоспостереження, дозволяючи виявляти загрози в реальному часі, прогнозувати можливі ризики та оперативно реагувати на них. Використання концептуального моделювання сприяє створенню системи, яка відповідає сучасним вимогам безпеки, забезпечує інтеграцію з іншими інформаційними системами та враховує обмеження в енергоспоживанні IoT-пристроїв. Стаття демонструє важливість UML-діаграм у формалізації складних архітектурних рішень та плануванні їхньої реалізації.

Ключові слова: концептуальне моделювання, система відеоспостереження, ситуаційна обізнаність, Інтернет речей (IoT), UML-діаграми, діаграма прецедентів, діаграма активностей, діаграма послідовності, діаграма компонентів, діаграма розгортання, аналітика даних, масштабованість, безпека, прогнозування загроз, автоматизація.

KUNANETS NATALIIA
ZHOVNIR YURIY
VEREMEENKO ANDRII
PUSHCHAK SEMEN
Lviv Polytechnic National University

CONCEPTUAL MODELING OF A SITUATIONALLY AWARE VIDEO SURVEILLANCE SYSTEM BASED ON INTERNET OF THINGS TECHNOLOGY

The article is dedicated to the conceptual modeling of a situationally aware video surveillance system based on Internet of Things (IoT) technology. A situationally aware approach is proposed, integrating intelligent devices, machine learning algorithms, and analytical tools to enable effective monitoring, threat detection, and automated incident response. The focus is on a conceptual model using UML diagrams, which are employed to formalize the structure, functionality, and interactions of system components.

The article examines the key components of the system: sensors, cameras, situational analysis software, data storage and visualization systems, as well as modules for event forecasting and risk management. The Use Case Diagram describes the main usage scenarios, including real-time monitoring, archival data analysis, and anomaly response. The Sequence Diagram demonstrates the interaction between system components in real time, for example, during motion detection or a threat event.

Special attention is given to the Class Diagram, which represents the software structure, including classes for data processing, device management, and analytical and visualization modules. The Component Diagram details the system architecture, emphasizing the integration between IoT devices, server components, and cloud services. The Deployment Diagram models the physical infrastructure of the system, covering cameras, sensors, network devices, servers, and mobile applications.

The proposed approach ensures scalability, adaptability, and high efficiency of the video surveillance system, enabling real-time threat detection, risk prediction, and prompt response. The use of conceptual modeling facilitates the creation of a system that meets modern

security requirements, integrates with other information systems, and considers the energy consumption constraints of IoT devices. The article highlights the importance of UML diagrams in formalizing complex architectural solutions and planning their implementation.

Keywords: conceptual modeling, video surveillance system, situational awareness, Internet of Things (IoT), UML diagrams, use case diagram, activity diagram, sequence diagram, component diagram, deployment diagram, data analytics, scalability, security, threat prediction, automation.

Постановка проблеми у загальному вигляді
та її зв'язок із важливими науковими чи практичними завданнями

Сучасні системи відеоспостереження для багатоквартирних будинків стають складнішими, оскільки орієнтуються на можливість не лише спостерігати, але й опрацьовувати інформацію для автоматичного виявлення потенційних загроз та реагувати на них. У таких системах важливим компонентом є технологія ситуаційної обізнаності, адже вона забезпечує фіксацію, розуміння та прогнозування подій, що допомагає адміністраторам системи та службам безпеки ефективніше реагувати на потенційні загрози у режимі реального часу.

Аналіз досліджень та публікацій

Останні дослідження у сфері інформаційних систем з ситуаційною обізнаністю зосереджені на вдосконаленні методів опрацювання й представлення знань для підтримки процедури прийняття рішень у критичних і швидкозмінних середовищах. У праці [1] Гал Феллер та інші досліджують взаємодію когнітивних та зовнішніх факторів, які сприяють розвитку технології ситуаційної обізнаності, зокрема в умовах зміни клінічних ситуацій в медичній практиці. Автори демонструють, що розуміння ситуації дозволяє знизити частоту діагностичних та оперативних помилок, сприяючи безпеці пацієнтів та адаптивності медичних рішень у реальному масштабі часу, що є важливим для динамічних середовищ.

Для створення інформаційних систем із ситуаційною обізнаністю сучасні дослідники пропонують об'єднувати методи подання та опрацювання знань із новітніми методами штучного інтелекту та технологіями опрацювання великих даних, що дозволяє здійснювати автоматичне виявлення, інтерпретацію та прогнозування подій у динамічних середовищах. Дослідники розглядають ситуаційну обізнаність як здатність аналізувати й прогнозувати зміни в середовищі, що є важливим для прийняття рішень у військових, медичних та промислових системах Модель ситуаційної обізнаності, запропонована Ендслі [2], є фундаментальною в багатьох галузях, включаючи військові, медичні, промислові системи, а також системи моніторингу та безпеки. Вона виокремлює три рівні ситуаційної обізнаності: сприйняття інформації, розуміння ситуації та прогнозування майбутнього розвитку подій. Ця модель використовується для оцінки процесів у інформаційних системах відеоспостереження, «розумний будинок» та військових застосунках і підтримує прийняття рішень у реальному масштабі часу на основі комплексної оцінки ситуації.

Алгоритми штучного інтелекту значно підвищують ефективність використання технології ситуаційної обізнаності та опрацювання даних з різних джерел. В інформаційні системах відеоспостереження ситуаційна обізнаність досягається через об'єднання даних з різних джерел, таких як відеокамери, давачі звуку, температури та системи контролю доступу. Зокрема, моделі на основі нечіткої логіки дозволяють адаптуватися до нечіткості вхідних даних і забезпечувати високу точність оцінки ситуацій. Це особливо актуально для систем відеоспостереження, де технології ситуаційної обізнаності є важливим інструментом виявлення загроз та підтримки динамічного прийняття рішень [3].

Для досягнення ситуаційної обізнаності використовують інтеграцію кількох технологічних підходів, включаючи бази знань, алгоритми опрацювання даних та аналізу поведінки об'єктів, що дозволяє реагувати на зміни в реальному масштабі часу. Такий підхід використовується у критично важливих сферах, в яких можливість швидкого й точного оцінювання ситуацій є вирішальною для успішного функціонування, наприклад, у медичних або військових застосунках [4].

У дослідженні [5] розглядається впровадження методів машинного навчання для підвищення ситуаційної обізнаності у інформаційних системах відеоспостереженні в житлових комплексах. Основний акцент зроблено на використанні комп'ютерного зору та візуалізації даних для ефективного моніторингу поведінки мешканців і відвідувачів. Дослідники вивчають можливості створення «глобальних ідентифікаторів» людей, що допомагають відстежувати їх пересування у межах будівлі, забезпечуючи тим самим точне розуміння ситуацій та підвищення безпеки через автоматизоване виявлення загроз у реальному масштабі часу.

Однією з ключових переваг використання машинного навчання та нейронних мереж у інформаційних системах з ситуаційною обізнаністю дослідники вважають їх здатність адаптуватися до змінних умов та навчатися на основі нових даних [6]. Це особливо важливо у динамічних середовищах, таких як багатоквартирні будинки, де ситуації можуть швидко змінюватися. Наприклад, система може навчатися на основі історичних даних про інциденти та адаптувати свої алгоритми для більш точного виявлення загроз у майбутньому. Це дозволяє забезпечити надійніший та ефективніший захист мешканців.

Розуміння поведінкових моделей мешканців та врахування соціальних факторів дозволяє інформаційним системам з ситуаційною обізнаністю не лише виявляти потенційні загрози, але й підтримувати комфортну та безпечну атмосферу для всіх мешканців. Сучасні інформаційні системи з ситуаційною обізнаністю використовують методи аналізу поведінки для виявлення аномалій, які можуть

свідчити про небезпеку або порушення. Застосування алгоритмів машинного навчання та штучного інтелекту дозволяє системам навчатися на основі історичних даних, розпізнавати типові поведінкові шаблони та оперативно реагувати на відхилення від норми. Соціальні аспекти СО включають врахування культурних, демографічних та психологічних характеристик мешканців. Розуміння соціальних стереотипів та упереджень є важливим для розробки систем, які не лише ефективно реагують на загрози, але й мінімізують ризик хибних спрацьовувань. Дослідження підкреслюють, що соціальні стереотипи можуть впливати на сприйняття та інтерпретацію поведінки, тому їх врахування є критичним для точності систем з ситуаційною обізнаністю [7].

Формалізація ситуаційної обізнаності є критично важливим кроком для побудови інтелектуальних систем, здатних до автоматизованого аналізу, прогнозування та прийняття рішень. Завдяки строгому математичному опису ситуаційної обізнаності можна створювати моделі, які інтегрують дані з різних джерел, описують складні взаємозв'язки між об'єктами та забезпечують високу точність оцінки поточних і майбутніх станів середовища.

Одна з найпоширеніших моделей ситуаційної обізнаності, розроблена Ендслі, визначає ситуаційну обізнаність як сукупність трьох рівнів:

$$[\,SA\ =\ \langle L_1, L_2, L_3\rangle]$$

де:

- (L_1) — сприйняття об'єктів і подій у середовищі,
- (L_2) — розуміння значення отриманої інформації,
- (L_3) — прогнозування майбутніх станів середовища.

Ця модель використовується для аналізу та побудови систем, які інтегрують дані про об'єкти, їхній стан і потенційні зміни. Наприклад, у системах відеоспостереження вона дозволяє послідовно переходити від виявлення осіб у межах житлового комплексу до оцінки їхньої поведінки та прогнозування потенційних загроз [2].

СО також формалізується через логічні моделі, які визначають ситуацію як сукупність об'єктів, їхніх станів і часу:

$$[\,SA(t) = \{(o_i, s_i, t) \mid i\ \in I\}\,]$$

де:

- $(\mathrm{o_i})$ — об'єкт (наприклад, особа, транспортний засіб, двері),
- $(\mathrm{s_i})$ — стан об'єкта (рух, відкриття, закриття),
- (t) — момент часу.

Ця модель дозволяє описувати ситуації як набір характеристик, що змінюються з часом. Її застосування до систем з ситуаційною обізнаністю забезпечує автоматичне визначення змін у поведінці об'єктів, що є основою для оперативного реагування [8].

Онтологічні моделі дозволяють формалізувати ситуаційну обізнаність через трійки:

$$[\,SA\ =\ \langle Entity, Relationship, Attributes\ \rangle]$$

де:

- $Entity$ — об'єкти середовища (наприклад, мешканці, ліфти, коридори),
- $Relationship$ — відносини між об'єктами (взаємодія, близькість, спільне перебування),
- $Attributes$ — характеристики об'єктів (висота, вага, швидкість руху).

Такі моделі є основою для опису складних сценаріїв, що інтегрують дані з численних сенсорів і пристроїв IoT. Наприклад, при виявленні особи, яка перебуває у забороненій зоні, онтологія дозволяє зіставити ці дані з іншими подіями (часом доби, рівнем освітлення), формуючи комплексне розуміння ситуації [9].

Формулювання цілей статті

Метою дослідження є розроблення концептуальної моделі системи відеоспостереження з ситуаційною обізнаністю, яка забезпечує інтеграцію сенсорних даних, інтелектуальних алгоритмів та автоматизованих механізмів аналізу для підвищення ефективності управління безпекою у середовищі житлового комплексу.

Завдання дослідження

- Дослідити існуючі концепції та технології у сфері відеоспостереження та ситуаційного аналізу з використанням IoT.
- Створити модель та правила ситуаційного аналізу у системі відеоспостереження.
- Сформувати концептуальну модель системи, яка включає основні компоненти, їх функціональні можливості, взаємозв'язки та способи інтеграції.
- Визначити ролі сенсорів, камер, хмарних сервісів та локальних хабів у забезпеченні безперервного збору й опрацювання інформації.

Виклад основного матеріалу

Використання інформаційних систем із ситуаційною обізнаністю для відеоспостереження у житлових комплексах є сучасним підходом, що значно підвищує ефективність безпеки та захищеності житлових об'єктів. Зазначені системи дозволяють забезпечити точне виявлення та оперативне реагування на загрози, завдяки спроможності виявляти, аналізувати й прогнозувати потенційно небезпечні ситуації.

Це особливо важливо в житлових комплексах, де рівень безпеки має прямий вплив на комфорт та довіру мешканців, що робить використання таких технологій актуальним та обґрунтованим.

Підсистема відеоспостереження є ключовим компонентом інформаційної безпекової системи багатоквартирного житлового комплексу. Вона забезпечує моніторинг, запис, зберігання і аналіз відеоданих для підвищення рівня безпеки, своєчасного реагування на загрози та контролю доступу.

Реалізація ситуаційної обізнаності у системі відеоспостереження передбачає об'єднання відеопотоків із камер спостереження з додатковими даними, такими як показники сенсорів руху, контролю доступу та інших інтелектуальних пристроїв. Це дозволяє створити комплексну картину ситуації, яка розширює можливості звичайного відеоспостереження. Інтеграція таких джерел даних дозволяє автоматично ідентифікувати підозрілу активність у режимі реального часу. Наприклад, якщо камера виявляє присутність особи вночі у забороненій зоні, а інші сенсори підтверджують підозрілу активність (звук або рух), інформаційна система може автоматично передати сигнал тривоги до служби безпеки.

Використання технологій ситуаційної обізнаності сприяє зменшенню впливу людського фактору, оскільки автоматизовані алгоритми здатні виконувати рутинний аналіз даних і виявляти аномалії з більшою точністю, ніж оператори спостереження. Наприклад, сучасні алгоритми на основі машинного навчання забезпечують опрацювання великих обсягів відеоданих, що дає можливість оперативно виявляти й інтерпретувати аномальні поведінкові шаблони. Одним із підходів є використання так званих «глобальних ідентифікаторів», які допомагають відслідковувати рухи конкретних осіб у межах усього об'єкта, дозволяючи здійснювати повне просторово-часове відстеження переміщень [5]. Це важливо для великих житлових комплексів, де одна особа може переміщуватися через різні зони спостереження, і необхідна можливість безперервного відстеження.

Дослідження також показують, що використання технології ситуаційної обізнаності у системі відеоспостереження підвищує загальний рівень безпеки через можливість запобігання загроз ще на ранніх етапах. Наприклад, використовується інформація від численних сенсорів і пристроїв IoT для автоматичного сповіщення про події, такі як несанкціоновані спроби входу. У цьому випадку оператор системи отримує повідомлення з аналітичним звітом про подію, що дозволяє визначити пріоритети реагування та забезпечити швидке відновлення безпеки об'єкта.

Окрім того, використання системи відеоспостереження з ситуаційною обізнаністю у житлових комплексах можуть працювати автономно, це дозволяє зменшити кількість необхідного персоналу, що знижує витрати на утримання служби безпеки. Сучасні платформи також дозволяють зберігати інформацію та створювати звіти, що полегшує подальше розслідування інцидентів та сприяє оптимізації операційної діяльності об'єктів. Розвиток таких інформаційних систем не лише підвищує рівень безпеки, але й оптимізує управлінські процеси, роблячи їх більш адаптивними та прозорими для мешканців.

Використання інтелектуальних алгоритмів дозволяє автоматично аналізувати відеопотоки та генерувати тривожні сигнали лише у випадку виявлення підозрілої активності. Це дозволяє операторам зосередитися на більш важливих завданнях та швидше реагувати на загрози.

З огляду на значний обсяг та різноманітність даних, що генеруються сенсорами, камерами спостереження, контролерами доступу та іншими пристроями IoT, використання традиційних методів опрацювання стає недостатньо ефективним. Це зумовлює необхідність впровадження новітніх підходів для масштабованої, гнучкого та швидкого опрацювання інформації, таких як хмарні технології та розподілені обчислення.

Завдання підсистеми відеоспостереження інформаційної безпекової системи полягає у моніторинг ситуації у реальному часі, записі, зберіганні та опрацюванні відеоматеріалів, оповіщенні про виявлені загрози, виявленні та аналізі підозрілої активності, налагодженні двостороннього зв'язку між мешканцями і відвідувачами, контролі доступу до об'єктів та приміщень житлового комплексу.

Формула ситуаційної обізнаності у системі відеоспостереження може бути представлена у вигляді багатофакторної моделі, яка враховує ключові параметри збору, аналізу даних і прогнозування:

$SA=f(C,P,A,T)$

де C — контекстуальна інформація, яка включає дані, зібрані від сенсорів, камер і зовнішніх джерел, таких як геолокація, погодні умови або інші параметри середовища.

P — сприйняття, що відображає здатність системи ідентифікувати об'єкти, події або аномалії у відеопотоці чи сенсорних даних.

A — аналіз, який включає виявлення взаємозв’язків між подіями, розпізнавання шаблонів і побудову сценаріїв ситуаційного розвитку.

T — прогнозування, що визначає ймовірний розвиток ситуацій на основі поточних даних і історичних шаблонів.

Розширена формула може враховувати вагові коефіцієнти для різних компонентів залежно від специфіки системи:

$SA=w1\cdot C+w2\cdot P+w3\cdot A+w4\cdot T,$

де w1,w2,w3,w4 — вагові коефіцієнти, що визначають значимість кожного компонента у конкретній системі.

Формізовано описано, як різні аспекти інформації та її опрацювання взаємодіють для створення повного уявлення про ситуацію, що є критично важливим для прийняття рішень у системі відеоспостереження з ситуаційною обізнаністю.

Такий підхід є ефективним для багаторівневих систем відеоспостереження житлових комплексів, де необхідно поєднувати інформацію з різних джерел, таких як камери спостереження, системи контролю доступу, давачі руху чи температури.

Сучасний підхід до формалізації ситуаційної обізнаності інтегрує контекстні дані з джерел у реальному часі. Ситуація моделюється через динамічне опрацювання взаємозалежних об'єктів та контексту:

$$SA = \langle O, C, T, F \rangle$$

де O — об’єкти, що взаємодіють у середовищі, C — контекст (географічні, тимчасові або соціальні фактори), T — часова шкала подій, F — функція прогнозування, яка оцінює майбутні зміни.

Ситуаційна обізнаність відображається на UML-діаграмах через моделювання компонентів, функціональних можливостей, взаємодій і станів, які дозволяють системі аналізувати, прогнозувати й реагувати на зміни в середовищі.

Основні функції систем відеоспостереження можемо визначити як комплексне покриття території відеонаглядом, реєстрація та зберігання відео, виявлення руху та аналітика даних, надання дистанційного доступу та управління, забезпечення стійкості до зовнішніх умов, захисту від вандалізму, контролю доступу.

Система відеонагляду проводить моніторинг у реальному масштабі часу, забезпечуючи візуальне спостереження за територією житлового комплексу, зокрема входами, під'їздами, паркінгами, дитячими майданчиками та іншими ключовими зонами. У результати моніторингу зберігаються записи і архівуються відео, тобто проводиться неперервний запис відео з можливістю зберігання записів у хмарі чи на локальних серверах, налаштування часових інтервалів для запису (24/7 або в певні години). Використання сенсорів забезпечує фіксацію активності у визначених зонах, детекцію руху та автоматичне сповіщення про підозрілі рухи. Аналітика відеопотоків сприяє розпізнавання обличь, номерних знаків, підозрілої поведінки за допомогою алгоритмів штучного інтелекту.

В результаті взаємодії з системою контролю доступу, тривожною сигналізацією, давачами руху чи диму забезпечується можливість виклику охорони або автоматичного блокування входів/виходів. Контроль відеопотоків для мешканців, адміністрації чи охоронного персоналу можливий через мобільний додаток чи веб інтерфейс. Відображення ситуаційної обізнаності в UML-діаграмах дозволяє систематизувати функціональні можливості системи, забезпечити інтеграцію між компонентами та проєктувати алгоритми, які сприяють швидкому й точному реагуванню на зміни в середовищі.

Система відеоспостереження є ключовим елементом сучасної інформаційної безпекової системи і відіграє важливу роль у забезпеченні безпеки мешканців багатоквартирних житлових комплексів. Важливість концептуального моделювання інформаційної системи відеоспостереження полягає в забезпеченні систематичного підходу до її проєктування, розуміння ключових компонентів, їх функцій та взаємодій. Концептуальне моделювання дозволяє створити узгоджену архітектуру, що полегшує реалізацію, обслуговування та адаптацію системи до змін у середовищі. Основними аргументами на користь концептуального моделювання є систематизація проєктування, яка дозволяє структурувати процес проєктування, чітко визначивши компоненти системи, їх функціональність та взаємозв’язки, що знижує ймовірність помилок і недоліків на етапі розробки та впровадження. Візуалізація архітектури забезпечується використанням моделей, таких як UML-діаграми, які дають наочне уявлення про структуру системи, дозволяючи різним зацікавленим сторонам легко зрозуміти її роботу, компоненти та взаємодії. Аналіз вимог допомагає глибоко оцінити функціональні та нефункціональні вимоги системи, такі як масштабованість, безпека, пропускна здатність та інтеграція з іншими системами. Інтеграція компонентів забезпечується моделюванням, яке дозволяє об’єднати різнорідні елементи системи, такі як камери, датчики, сервери та панелі моніторингу, в єдину ефективну систему. Оптимізація процесів стає можливою завдяки виявленню неефективних або надлишкових процесів, які можна удосконалити для зменшення витрат на впровадження та експлуатацію. Прогнозування поведінки системи за допомогою моделей дозволяє передбачити її реакцію на різні сценарії, включаючи аномалії, атаки чи збої, що сприяє створенню надійної системи, здатної працювати стабільно навіть у критичних умовах. Підтримка прийняття рішень забезпечується завдяки концептуальній моделі, яка дозволяє аналізувати альтернативні варіанти реалізації, порівнювати їх ефективність та вибирати оптимальне рішення. Забезпечення масштабованості та адаптивності системи, яка повинна відповідати змінним умовам і вимогам, реалізується завдяки створенню архітектури, готової до майбутніх змін. Полегшення обслуговування та оновлення забезпечується чітким розумінням архітектури системи, досягнутим через моделювання, що спрощує впровадження оновлень і інтеграцію нових технологій. Підвищення рівня безпеки, яке є критично важливим для системи відеоспостереження, реалізується через врахування загроз, прогнозування ризиків та впровадження механізмів захисту на рівні архітектури системи. Таким чином, концептуальне моделювання є основою для успішного проєктування, впровадження та експлуатації системи відеоспостереження, забезпечуючи чітке бачення архітектури, функціональності та взаємодії компонентів, сприяючи створенню ефективної, надійної та адаптивної інформаційної системи.

Діаграма послідовності відображає взаємодію між об'єктами системи, зосереджуючись на їхній хронологічній послідовності. Вона моделює функціонування підсистеми відеоспостереження у сценаріях, таких як виявлення руху або запит відеозапису.

У сценарії "Виявлення руху та запис відео з камери" визначено такі актори та об'єкти: MotionDetector, який виявляє рух у зоні спостереження; Camera, що починає запис відео; VideoArchive, який зберігає відеозапис; SystemController, який координує взаємодію між компонентами системи; SecurityPersonnel, який отримує сповіщення про рух.

Послідовність подій у цьому сценарії починається з того, що MotionDetector виявляє рух і надсилає сигнал до SystemController. SystemController передає команду відповідній камері (Camera) для початку запису. Camera передає відеопотік до VideoArchive для збереження. Після цього SystemController надсилає сповіщення SecurityPersonnel з деталями події, такими як місце, час та камера. SecurityPersonnel має можливість переглянути відеозапис із VideoArchive.

Елементи UML діаграми послідовності включають лінії життєвого циклу для об'єктів MotionDetector, SystemController, Camera, VideoArchive і SecurityPersonnel. Повідомлення включають: detectMotion() — викликається MotionDetector; alertController() — повідомлення від MotionDetector до SystemController; startRecording() — команда від SystemController до Camera; saveVideo() — збереження відео в архів; notifySecurity() — сповіщення охоронця про подію; retrieveVideo() — запит охоронця до VideoArchive для перегляду запису.

Графічне представлення діаграми містить вертикальні лінії життєвого циклу для кожного об'єкта, стрілки для повідомлень між об'єктами та нотацію для умов, таких як [motionDetected], або альтернативні сценарії (Alt). Ця діаграма ілюструє динамічну взаємодію між об'єктами в часі, допомагаючи зрозуміти потік даних і повідомлень між компонентами системи. Демонструє взаємодію між компонентами системи для досягнення ситуаційної обізнаності.

Розглянемо сценарій використання системи відеоспостереження візуалізований на діаграмі послідовності. Користувач встановлює застосунок на смартфон, відкриває його та вводить номер телефону для авторизації. Система відеоспостереження генерує код підтвердження авторизації і через агрегатор смс надсилає користувачу. Користувач вводить код підтвердження і натискає “Підтвердити”. Система звіряє код та у випадку відсутності розбіжностей видає повідомлення про успішну авторизацію. Після цього застосунок починає опитувати систему щодо наявності для нього зарезервованого акаунту, що призначений для відео/аудіо дзвінків. Спочатку пошук аккаунту відбувається в базі даних системи. Якщо відповідний акаунт знайдено, то система відправляє дані у застосунок. Якщо акаунт не знайдено, але послуга має бути доступною, то система резервує аккаунт на SIP сервері, записує дані аканту до себе в базу даних і видає застосунку.

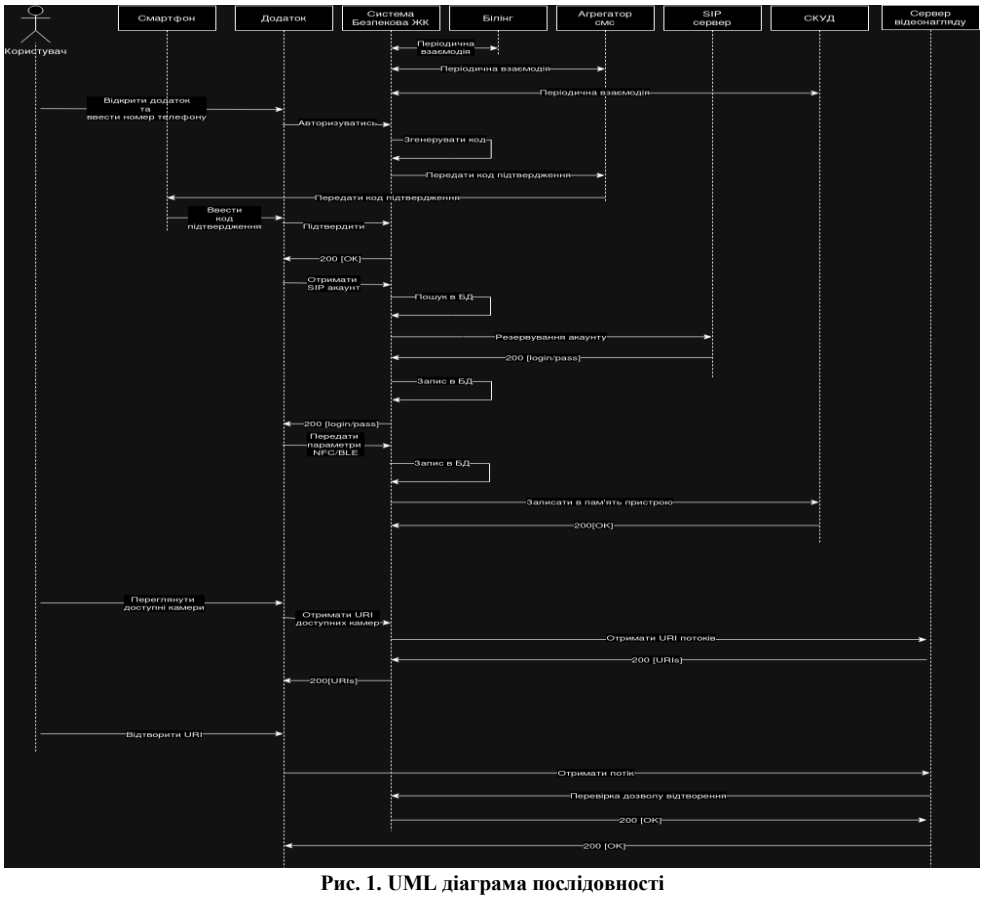

Рис. 1. UML діаграма послідовності

Застосунок без участі користувача авторизовує акаунт для прийому/здійснення дзвінків. Після завершення всіх запитів, що стосують акаунту, застосунок передає системі мітку NFC/BLE. Ця мітка записується в базу даних системи, а також надсилається системою на пристрої СКУД, до якого належить користувач і користувач має мати можливість взаємодіяти з ними.

Користувач при потребі може переглянути відомості про доступні камери. При переході на вкладку відеонагляду відправляється запит на отримання відомостей про доступні камери. Система робить додатковий запит до сервера відеонагляду, який повертає URL потоків. Після цього ці дані передаються на застосунок та прописуються. Коли користувач обирає певну камеру і надсилає запит на відтворення відеопотоку. Запит пересилається до сервера відеонагляду для отримання відеопотоку. Сервер відеонагляду перепитує систему дозвіл на відтворення відеопотоку. Після підтвердження видає застосунку дозвіл на його перегляд. Діаграма демонструє взаємодію між компонентами системи для досягнення ситуаційної обізнаності.

Діаграма компонентів системи відеоспостереження з ситуаційною обізнаністю демонструє елементи її архітектури, інтеграцію інтелектуальних пристроїв, програмних компонентів, системи аналізу даних і засоби взаємодії. Основними компонентами такої системи є IoT-пристрої, які включають давачі та сенсори для збору інформації про навколишнє середовище, наприклад, давачі руху, температури, вологості або звуку; розумні пристрої, такі як камери відеоспостереження, дверні замки та освітлювальні системи, якими можна централізовано керувати; актори, які виконують дії у відповідь на команди, наприклад, відкриття дверей або запуск сигналізації.

Центральний хаб опрацювання даних отримує дані від IoT-пристроїв, виконує їх попереднє опрацювання та передає до інших систем. Його інтерфейси включають прийом даних із сенсорів (receiveSensorData()) та управління пристроями (controlDevice(deviceID, command)). Система ситуаційного аналізу використовує алгоритми машинного навчання та штучного інтелекту для аналізу даних у реальному часі, забезпечуючи ідентифікацію аномалій, прогнозування загроз і аналіз сценаріїв безпеки через інтерфейси аналізу даних (analyzeData(dataStream)) і створення прогнозів (generatePrediction(scenario)).

Система керування подіями відповідає за виявлення подій, реагування на них і сповіщення користувачів. Її інтерфейси дозволяють створювати події (createEvent(eventType, details)) і керувати сповіщеннями (sendNotification(userID, message)). Система візуалізації та моніторингу надає зручний формат для операторів або користувачів, відображаючи зібрані дані та результати аналізу ситуації. Вона забезпечує візуалізацію потоків даних, доступ до історичних даних і панелі для управління ситуаціями через інтерфейси доступу до даних (viewData(criteria)) і взаємодії з користувачем (userInteraction(actions)).

База знань зберігає типові сценарії, шаблони поведінки, правила реагування та історичні дані про інциденти. Її інтерфейси включають запити до бази (queryKnowledge(criteria)) і оновлення даних (updateKnowledge(newData)). Система захисту даних забезпечує шифрування даних, автентифікацію пристроїв і користувачів, а також контроль доступу через інтерфейси автентифікації (authenticate(userID, credentials)) та шифрування (encryptData(data)).

Хмарні сервіси зберігають дані, забезпечують обчислювальні потужності для складних алгоритмів аналізу та резервування, надаючи інтерфейси для синхронізації даних (syncData(localData)) і хмарного аналізу (cloudAnalysis(dataBatch)).

Взаємозв’язки між компонентами включають передачу даних від IoT-пристроїв до Центрального хаба опрацювання даних, який надсилає їх до Системи ситуаційного аналізу та Системи керування подіями. Система ситуаційного аналізу використовує Базу знань для порівняння отриманих даних із типовими сценаріями. Система візуалізації отримує результати аналізу та дані з хмари для створення панелей моніторингу. Система захисту даних забезпечує безпеку всіх з'єднань та інтеграцій між компонентами. Ця діаграма демонструє, як підсистема відеоспостереження інтегрується з іншими системами для забезпечення ситуаційної обізнаності та підвищення рівня безпеки на основі IoT. Діаграма відображає модулі, які підтримують ситуаційну обізнаність та показує їх взаємозв’язок із сенсорами, камерами, системами сповіщень і користувачами.

Діаграма розгортання ілюструє фізичну архітектуру підсистеми, включаючи розташування апаратних вузлів, програмного забезпечення та їх взаємозв’язки. Моделює фізичне розташування компонентів, які забезпечують ситуаційну обізнаність, розміщення сенсорів, серверів для обробки даних та аналізу, інтерфейсів для доступу користувачів. Основними компонентами є вузли, комунікаційні зв’язки та програмні модулі.

Серед вузлів виділяються камери спостереження, які захоплюють відео та передають дані до центрального сервера. Камери встановлюються на території комплексу та оснащені вбудованим програмним забезпеченням для опрацювання відео та мережевого підключення. Центральний сервер розташований у серверній кімнаті та забезпечує координацію роботи системи, зберігання архівів і управління доступом. Програмне забезпечення сервера включає систему управління відеоспостереженням та базу даних для архівів відео і логів подій. Сенсори руху встановлюються у ключових зонах спостереження та забезпечують виявлення руху з передачею сигналу до камери або сервера. Мобільні пристрої користувачів слугують для доступу до відеоархіву, перегляду потоків у

реальному масштабі часу та отримання сповіщень. Вони оснащені мобільним застосунком або вебінтерфейсом. Мережеве обладнання, включаючи роутери, комутатори та мережеві камери, забезпечує передачу даних між вузлами.

Комунікаційні зв'язки системи передбачають підключення камер до центрального сервера через локальну мережу, передачу сповіщень мобільним пристроям через захищені інтернет-з'єднання і підключення сенсорів руху до камер або сервера через дротові чи бездротові зв'язки.

Програмні компоненти включають систему керування подіями, яка опрацьовує сигнали від сенсорів руху; модуль запису та зберігання відео, що зберігає файли у визначеному форматі; та модуль сповіщень, який надсилає сигнал тривоги охоронцям або користувачам.

Сценарій розгортання описує процеси роботи системи відеоспостереження: камери спостереження передають відеопотік до центрального сервера; сервер опрацьовує сигнали від сенсорів руху, ініціює запис і зберігає відео в архіві; сповіщення про події надходять на мобільні пристрої охоронців чи мешканців; користувачі отримують доступ до архіву чи переглядають потоки в реальному часі через мобільний застосунок.

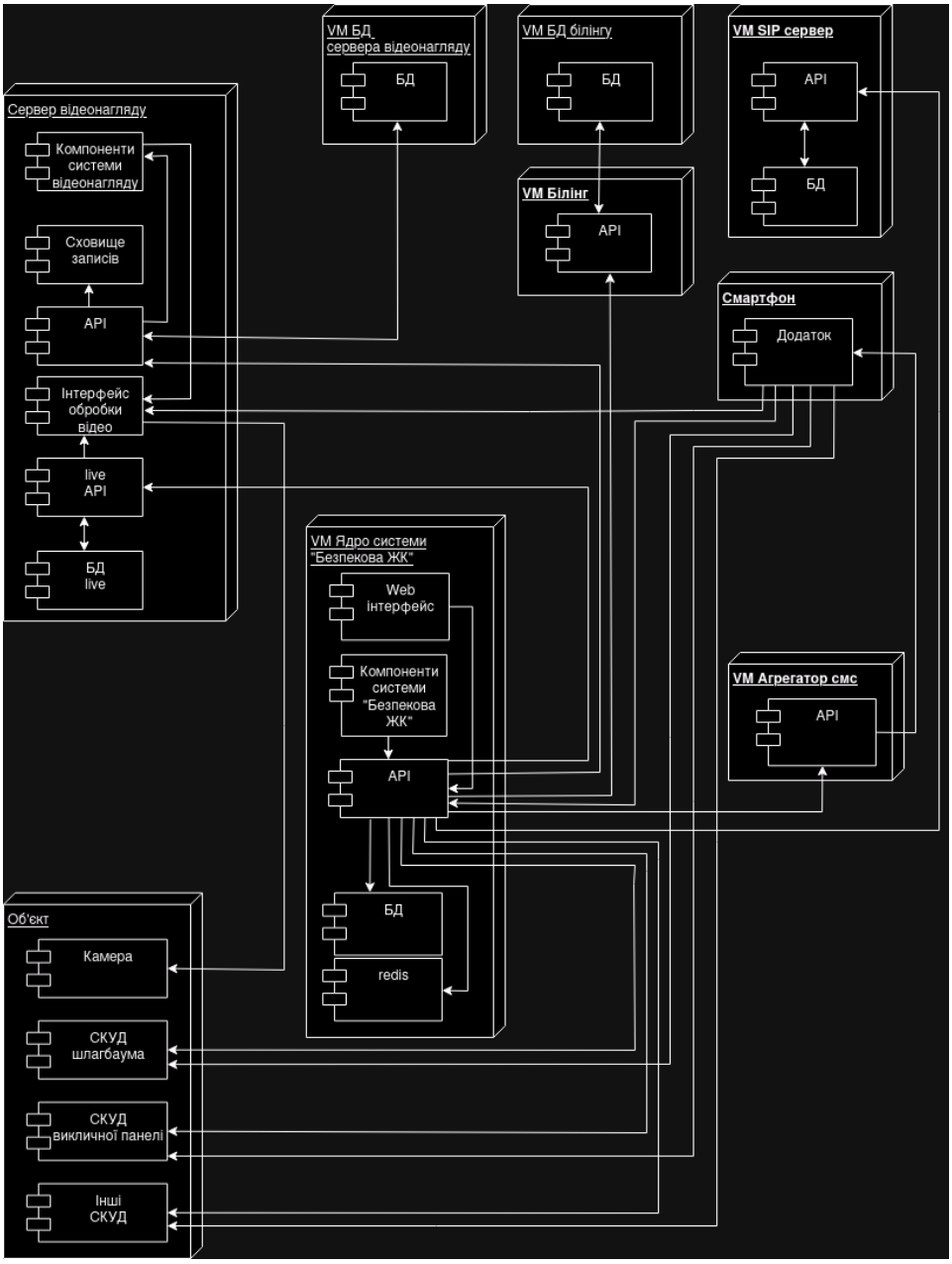

Рис.2. UML діаграма розгортання

Графічно діаграма містить прямокутні вузли, що представляють фізичне обладнання (камери, сервери, пристрої), компоненти програмного забезпечення, які працюють на цих вузлах, та лінії зв'язку, що відображають мережеві підключення. Вона показує фізичне розміщення компонентів системи на вузлах і є важливою для проєктування апаратної частини системи відеонагляду.

Система відеоспостереження складається з ядра та додаткових підсистем, які взаємодіють із ядром через API. Основні підсистеми включають сервер відеонагляду, білінг, СКУД панелей і шлагбаумів, агрегатор смс і застосунок. Сервер відеонагляду містить API для роботи з компонентами системи та записами, live API, інтерфейс опрацювання відео (видача архіву та потоків), дві бази даних (для записів і live) та компоненти системи відеонагляду (сервіси, процеси). Білінг забезпечує взаємодію з базою даних через API. Агрегатор смс використовується для відправки повідомлень. Застосунок слугує інструментом для взаємодії кінцевого користувача із системою відеоспостереження та іншими підсистемами.

Діаграма компонентів (Component Diagram) демонструє структуру програмних і апаратних компонентів системи, їхні взаємозв'язки та функціональність, відображаючи логічну архітектуру системи відеоспостереження. Основними компонентами є система керування камерами, яка відповідає за контроль роботи камер. Вона має інтерфейси для запуску та зупинки запису (startRecording(), stopRecording()) та отримання статусу камер (getCameraStatus()) і взаємодіє з фізичними камерами через API або драйвери.

Архів відео (Video Archive) зберігає відеозаписи, маючи інтерфейси для збереження відео (saveVideo(data: VideoStream)), пошуку записів (retrieveVideo(criteria: Query)) та автоматичного видалення старих записів (deleteOldVideos(policy: RetentionPolicy)). Детектор руху (Motion Detector Module) виявляє рух у зоні спостереження, має інтерфейси для перевірки активності (detectMotion()) та надсилання тривожного сигналу (sendAlert()) і інтегрується з камерами для активації запису.

Система сповіщень (Notification System) інформує користувачів про події через інтерфейси, що дозволяють надсилати повідомлення (sendNotification(user: User, event: Event)) та налаштовувати тривоги (configureAlerts(settings: AlertConfig)). Інтерфейс користувача (User Interface) забезпечує доступ до функціоналу системи через веб-інтерфейс або мобільний додаток, включаючи перегляд відеопотоку в реальному часі (viewLiveStream(cameraID: String)), доступ до архіву (accessVideoArchive(criteria: Query)) та зміну налаштувань (manageSettings(settings: SystemConfig)).

Сервер бази даних (Database Server) зберігає інформацію про камери, архіви, події та користувачів, забезпечуючи виконання запитів (queryData(request: Query)) та збереження даних (storeData(record: Record)).

Взаємозв'язки між компонентами включають взаємодію Camera Management System із Motion Detector Module для активації запису при виявленні руху. Camera Management System передає відеозаписи до Video Archive. Video Archive та Notification System отримують дані від Database Server. User Interface звертається до Video Archive для відображення даних користувачам, а Notification System надсилає повідомлення користувачам через налаштовані канали. Сценарій роботи системи передбачає, що при виявленні активності детектор руху сповіщає Camera Management System, камера починає запис і передає дані до Video Archive. Notification System інформує користувача про подію, а користувач через User Interface може переглянути запис або прямий відеопотік. Графічно діаграма включає прямокутники для компонентів із назвами та інтерфейсами, лінії з'єднання між компонентами для демонстрації взаємодії, а також умовні символи, що позначають залежності від апаратного обладнання, наприклад, камер і сенсорів. Ця діаграма відображає структуру та взаємозв'язки між програмними компонентами системи, забезпечуючи розуміння програмної архітектури та інтеграції компонентів. Користувач авторизується в застосунку, вводячи номер телефону та код підтвердження. Застосунок взаємодіє через API із інформаційною безпековою системою житлового комплексу. Користувач отримує доступ до акаунта для дзвінків, перегляду камер і записів, а також можливість замовлення послуг і зв'язку з технічною підтримкою, за умови підключених послуг.

Діаграма прецедентів цієї системи відеоспостереження ілюструє взаємодію користувачів (акторів) із системою та відображає основні функціональні можливості. Основними акторами є адміністратор системи, який відповідає за налаштування, моніторинг, обслуговування та управління доступом до системи; охоронний персонал, який використовує систему для моніторингу відео в реальному часі та реагування на інциденти; мешканець, що має доступ до перегляду відео з певних камер, зокрема у своєму під'їзді чи біля квартири; та система контролю доступу, яка інтегрується з підсистемою для автоматизації процесів доступу до території. Актори, взаємодіють із системою через прецеденти, які забезпечують ситуаційну обізнаність. Основні функціональні можливості системи відображені через такі прецеденти. Моніторинг відео в реальному масштабі часу, який доступний адміністраторам і охоронному персоналу, дозволяє здійснювати візуальне спостереження за територією в реальному масштабі часі через монітори або мобільний застосунок. Перегляд архівних записів, доступний адміністраторам, охоронцям і мешканцям, дає змогу отримувати доступ до записів подій, що сталися раніше. Налаштування системи, яке виконується адміністраторами, охоплює конфігурацію параметрів камер, таких як якість запису, тривалість зберігання, зони детекції руху тощо. Функція детекції руху, що виконується системою контролю доступу і використовується охоронним персоналом, забезпечує автоматичне фіксування руху в зоні спостереження та надсилання сповіщень. Інтеграція з системою контролю доступу дозволяє перевіряти відео у разі спрацювання доступу, наприклад, під час відкриття дверей.

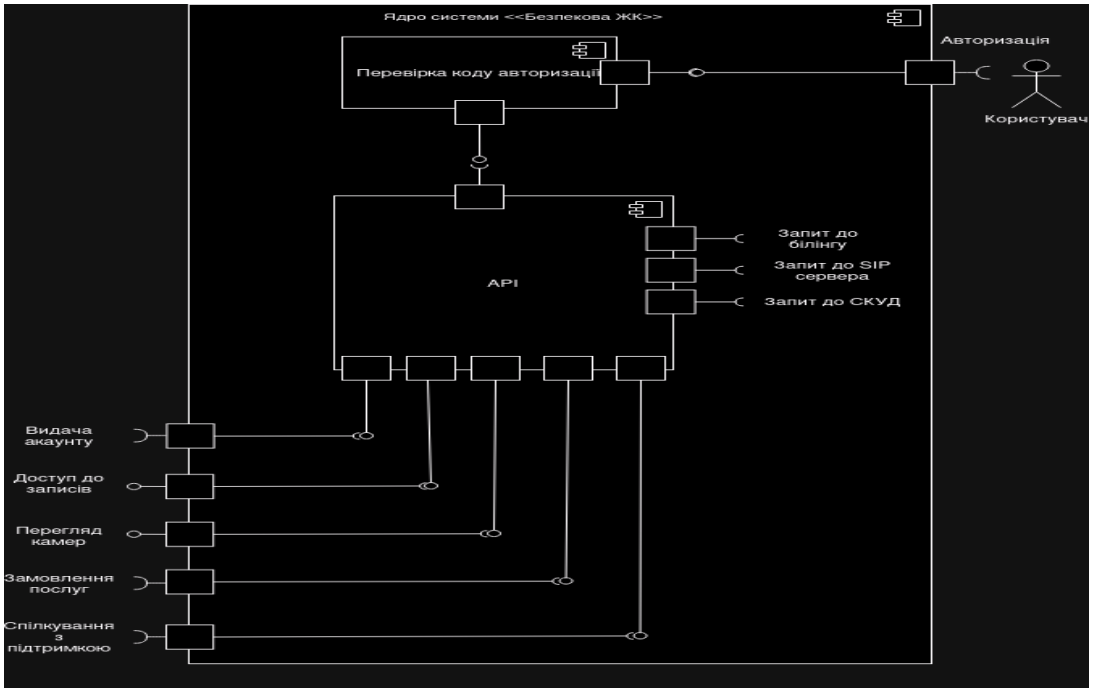

Рис. 3. UML діаграма компонентів

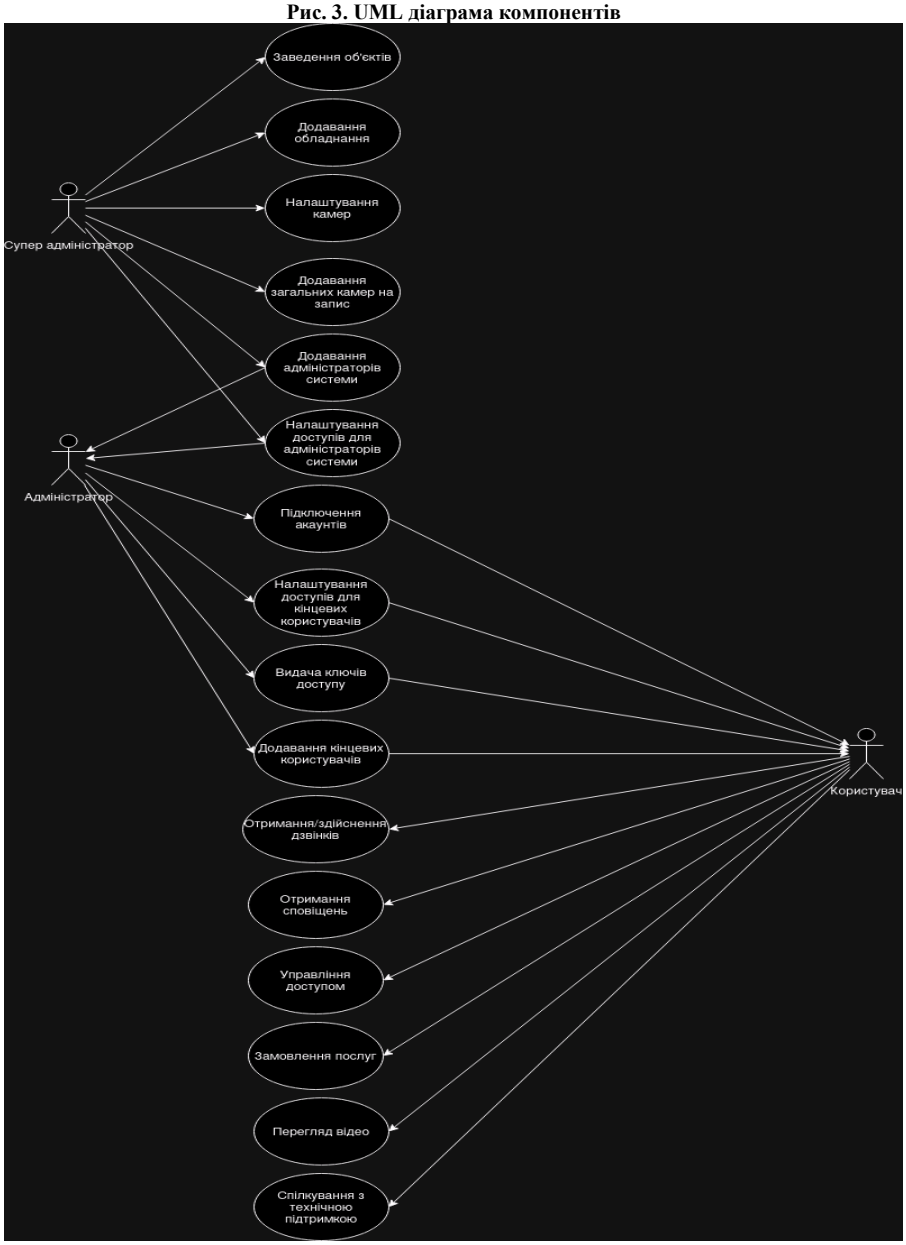

Рис. 4. UML діаграма прецедентів

Формування звітів про події, яке здійснюється адміністратором, дає змогу генерувати звіти про інциденти, перегляди камер або зони активності. Дистанційний доступ, доступний мешканцям і адміністраторам, забезпечує можливість користування системою через мобільний застосунок чи вебінтерфейс. Діаграма відображає сценарії використання, які пов'язані з ситуаційною обізнаністю, такі як виявлення аномалій, автоматичне реагування на загрози або прогнозування ризиків.

Діаграма прецедентів графічно відображає основні функції системи у вигляді овальних фігур, які представляють ключові можливості, такі як моніторинг, запис, налаштування та інші. Актори, позначені прямокутниками з фігурками, взаємодіють із цими функціями через лінії зв'язків, які показують взаємозв'язки між акторами та прецедентами.

Діаграма класів системи відеоспостереження моделює структуру системи, відображаючи класи, їх атрибути, методи та зв'язки між ними, що дозволяє зрозуміти взаємодію компонентів і функції, які вони виконують. Основними класами є:

Camera. Атрибути: cameraID (унікальний ідентифікатор камери), location (місце розташування камери), resolution (роздільна здатність, наприклад Full HD, 4K), status (активність камери: увімкнена/вимкнена), recordingMode (режим запису: 24/7 або за детекцією руху). Методи: startRecording() (запуск запису), stopRecording() (зупинка запису), adjustSettings(settings) (зміна параметрів).

VideoArchive. Атрибути: archiveID (ідентифікатор архіву), startTime (час початку запису), endTime (час завершення запису), filePath (шлях до файлу запису). Методи: saveVideo(video) (збереження відео в архів), retrieveVideo(timeRange) (отримання записів за заданим часовим проміжком).

MotionDetector. Атрибути: detectorID (ідентифікатор сенсора), sensitivity (рівень чутливості), status (стан: увімкнено/вимкнено). Методи: detectMotion() (перевірка наявності руху), sendAlert() (надсилання сповіщення).

User. Атрибути: userID (ідентифікатор користувача), role (роль: Адміністратор, Охоронець, Мешканець), accessRights (права доступу, наприклад, доступ до певних камер). Методи: login(credentials) (авторизація), requestVideo(cameraID) (запит відео).

SystemController. Атрибути: systemID (ідентифікатор системи), status (статус системи: активна/неактивна). Методи: monitorSystem() (контроль стану компонентів), generateReport() (створення звіту про події).

Відношення між класами:

Асоціація: Camera пов'язаний із VideoArchive, оскільки камери створюють відеозаписи, які зберігаються в архіві; MotionDetector пов'язаний із Camera для активації запису при виявленні руху; User взаємодіє із SystemController для доступу до функціоналу.

Композиція: SystemController містить список камер (Camera), детекторів руху (MotionDetector) та архівів (VideoArchive).

Наслідування: Administrator, SecurityPersonnel і Resident є підкласами класу User, маючи різні права доступу.

Графічне представлення діаграми включає прямокутники для кожного класу, розділені на три секції: назва класу, атрибути, методи, а також лінії між класами для позначення зв'язків (асоціація, композиція, наслідування).

Переваги підсистеми відеоспостереження включають профілактику злочинів завдяки постійному моніторингу, що знижує ймовірність незаконних дій, створення доказової бази, оскільки записи можуть бути використані у випадку розслідування злочинів, забезпечення комфорту та безпеки мешканцям для створення спокійного середовища, а також економічність, завдяки використанню сучасних камер з енергоефективними технологіями, які знижують витрати на обслуговування.

Можливі виклики та недоліки підсистеми включають проблеми приватності, які потребують чіткого регулювання доступу до записів та дотримання законодавства; вразливість до атак, що вимагає захисту через шифрування даних та регулярне оновлення програмного забезпечення; а також високу вартість, адже первинна установка та регулярне обслуговування можуть бути дорогими.

Розроблені UML діаграми позитивно вплинули на процес розроблення інформаційної системи відеоспостереження, забезпечуючи структурований і зрозумілий підхід до проєктування, впровадження та підтримки системи. Вони дозволяють створити наочне уявлення про структуру системи, її компоненти, функціональність і взаємозв'язки, що допомогло зацікавленим сторонам, включаючи замовників, розробників і користувачів, мати однакове розуміння системи. Наприклад, діаграма прецедентів ілюструє, як користувачі взаємодіють із системою, які ключові функції вона виконує і які сценарії передбачено. UML діаграма прецедентів структурує розроблення інформаційної системи, дозволяючи розділити її на етапи: визначення вимог, проєктування архітектури, моделювання взаємодій і впровадження.

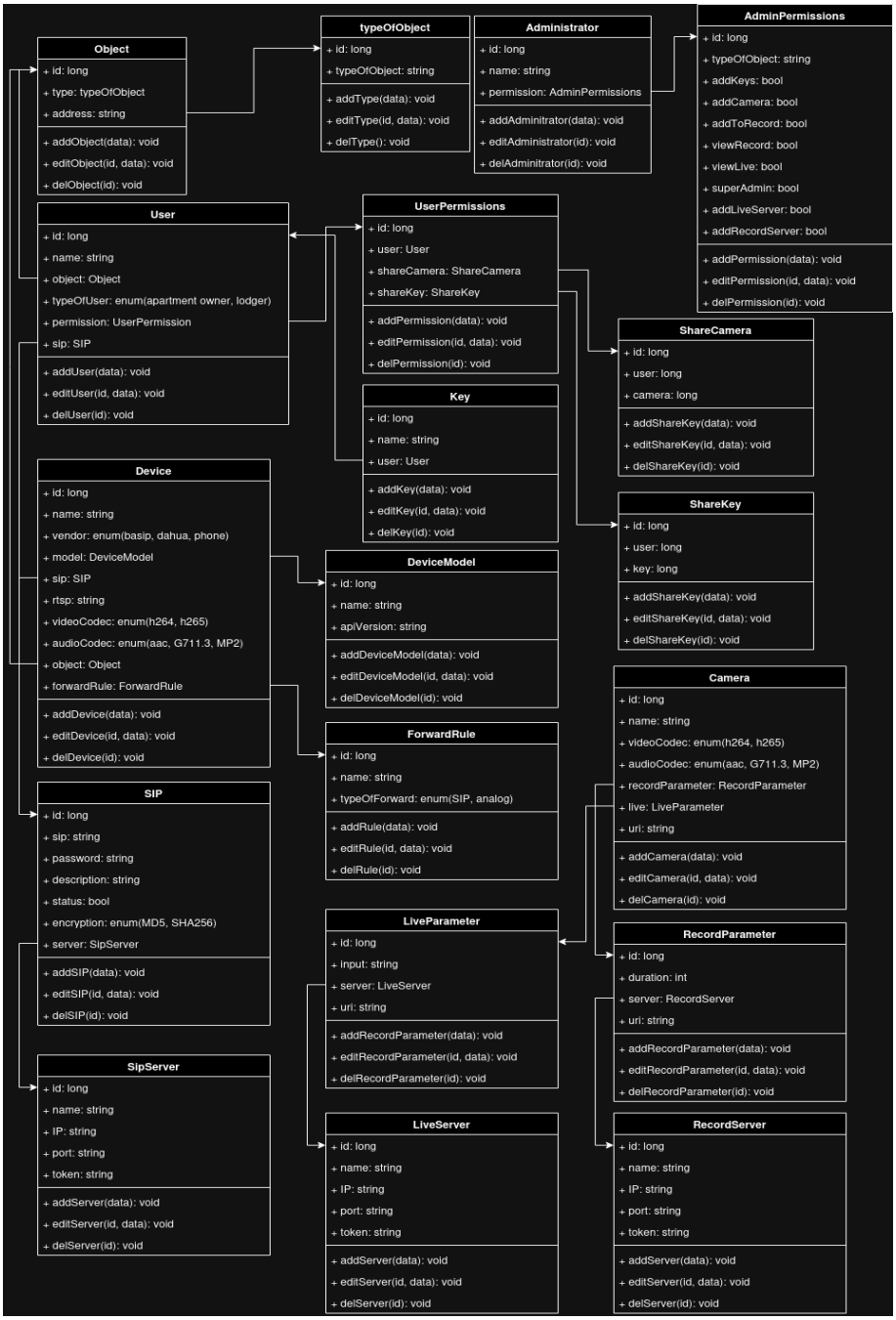

Рис. 5. UML діаграма класів

Діаграма класів визначає ключові класи, їх атрибути, методи і зв'язки, що дозволяє структурувати програмний код і забезпечити повторне використання компонентів, а діаграма компонентів описує модулі системи, полегшуючи планування інтеграції та розподілу завдань між командами. Діаграма активностей допомагає пояснити бізнес-процеси, які підтримує система, та узгодити їх із замовником, тоді як діаграма послідовності моделює взаємодії між компонентами, що дозволяє узгодити логіку роботи системи. Діаграма розгортання моделює фізичне розташування серверів, камер, баз даних, мережевого обладнання, що важливо для планування інфраструктури, а діаграма станів дозволяє моделювати поведінку системи в різних умовах, наприклад, реакцію на виявлення руху або збої. UML діаграма дозволяє моделювати альтернативні сценарії реалізації, оцінювати їх переваги та недоліки ще до впровадження, що знижує ризик помилок. Вони допомагають визначити найкритичніші функції системи, оптимізувати їх і створити резервні сценарії на випадок відмов. UML діаграма дозволила створити тестові сценарії, які охоплюють всі можливі сценарії взаємодії між компонентами та користувачами. Діаграми активностей та послідовності дозволяють моделювати дії користувачів і перевіряти, чи відповідає реальна система запланованим сценаріям. Завдяки цим UML діаграмам можна передбачити майбутні зміни або розширення системи, моделюючи додавання нових компонентів, функцій чи сценаріїв. Діаграми компонентів дозволили легко додавати нові модулі до існуючої архітектури, зберігаючи її узгодженість. UML діаграми допомогли моделювати механізми безпеки системи, такі як автентифікація, шифрування, контроль доступу. Діаграми класів та розгортання

дозволили моделювати взаємодії між компонентами, включаючи захищені канали зв'язку. UML діаграма сприяла створенню продуманої архітектури системи, враховуючи всі важливі аспекти. UML діаграми виступають універсальною мовою спілкування між аналітиками, розробниками, архітекторами, тестувальниками. Отже, UML діаграми є ключовим інструментом, що дозволив оптимізувати процес розроблення інформаційної системи відеоспостереження, забезпечити її ефективність, масштабованість, безпеку та адаптивність до змін.

Висновки з даного дослідження
і перспективи подальших розвідок у даному напрямі

Використання IoT пристроїв у системі відеоспостереження забезпечує багатофункціональність і автоматизацію процесів моніторингу. Сенсори, камери та актори, об'єднані в єдину мережу, створюють основу для високої ефективності та адаптивності системи. Інтеграція ситуаційного аналізу сприяє швидкому виявленню, прогнозуванню та реагуванню на потенційні загрози. Алгоритми аналізу даних у реальному часі дозволяють ідентифікувати аномалії та формувати відповідні сценарії реагування. Використання UML-діаграм у процесі концептуального моделювання забезпечує чітке визначення компонентів системи, їхніх функцій та взаємозв'язків, знижуючи ризики на етапах проєктування та реалізації. Створена концептуальна модель підтримує можливість масштабування системи шляхом додавання нових IoT-пристроїв та функціональних модулів, дозволяючи адаптувати систему до змінних вимог користувачів та умов середовища. Моделювання траєкторій змін та впровадження системи на основі знань підвищують якість прийняття рішень, дозволяючи системі порівнювати сценарії розвитку подій та обирати оптимальні стратегії для запобігання інцидентам. Інтеграція системи з іншими компонентами безпеки забезпечує комплексний підхід до захисту об'єктів і територій, роблячи систему здатною вчасно реагувати на критичні ситуації. Запропонована модель слугувала основою для розроблення сучасної системи відеоспостереження, зорієнтованої на забезпечення інформаційної безпеки в умовах розумних міст, житлових комплексів або промислових зон. Для досягнення максимальної ефективності системи вдосконалювалися алгоритми аналізу даних, оптимізовалися енергоспоживання IoT-пристроїв та забезпечувалися відповідність законодавчим вимогам щодо опрацювання персональних даних.

Подальші дослідження можуть бути спрямовані на розроблення більш точних алгоритмів аналізу даних у реальному масштабі часу, включаючи технології глибокого навчання для покращення розпізнавання об'єктів, ідентифікації аномалій і прогнозування поведінки, а також моделей інтеграції системи відеоспостереження з іншими системами безпеки, такими як контроль доступу, пожежна сигналізація, медичні та аварійні служби для створення комплексної інформаційної платформи.

Література

1. Feller, S., Feller, L., Bhayat, A., Feller, G., Khammissa, R. A. G., & Vally, Z. I. (2023). Situational awareness in the context of clinical practice. *Healthcare, 11*(23), 3098. https://doi.org/10.3390/healthcare11233098

2. Endsley, M. (2000). Theoretical underpinnings of situation awareness: A critical review. In M. R. Endsley & D. J. Garland (Eds.), *Situation awareness analysis and measurement* (pp. 3–32). Lawrence Erlbaum Associates.

3. Munir, A., Aved, A., & Blasch, E. (2022). Situational awareness: Techniques, challenges, and prospects. *AI, 3*(1), 55–77. https://doi.org/10.3390/ai3010005

4. Smith, K., & Hancock, P. A. (1995). Situation awareness is adaptive, externally directed consciousness. *Human Factors, 37*(1), 137–148. http://dx.doi.org/10.1518/001872095779049444

5. Ardabili, B. R., Yao, S., Pazho, A. D., Bourque, L., & Tabkhi, H. (2023). Enhancing situational awareness in surveillance: Leveraging data visualization techniques for machine learning-based video analytics outcomes. *arXiv*. https://doi.org/10.60097/ACIG/190341

6. Burov, Y. (2021). Knowledge based situation awareness process based on ontologies. In *Proceedings of the International Conference on Computational Linguistics and Intelligent Systems (COLINS)* (Vol. 2, pp. 45–55). Lviv Polytechnic Publishing House.

7. Ehrlinger, J., Readinger, W. O., & Kim, B. (2016). Decision-making and cognitive biases. In H. S. Friedman (Ed.), *Encyclopedia of mental health* (2nd ed., Vol. 1, pp. 191–202). Academic Press. http://dx.doi.org/10.1016/B978-0-12-397045-9.00206-8

8. Kokar, M. M., Matheus, C. J., & Baclawski, K. (2009). Ontology-based situation awareness. *Information Fusion, 10*(1), 83–98.

9. Steinberg, A. N., Bowman, C. L., & White, F. E. (1999). Revisions to the JDL data fusion model. In *Sensor Fusion: Architectures, Algorithms, and Applications III* (Proc. SPIE 3719). https://doi.org/10.1117/12.341367

References

1. Feller, S., Feller, L., Bhayat, A., Feller, G., Khammissa, R. A. G., & Vally, Z. I. (2023). Situational awareness in the context of clinical practice. Healthcare, 11(23), 3098. https://doi.org/10.3390/healthcare11233098

2. Endsley, M. (2000). Theoretical underpinnings of situation awareness: A critical review. In M. R. Endsley & D. J. Garland (Eds.), Situation awareness analysis and measurement (pp. 3–32). Lawrence Erlbaum Associates.

3. Munir, A., Aved, A., & Blasch, E. (2022). Situational awareness: Techniques, challenges, and prospects. AI, 3(1), 55–77. https://doi.org/10.3390/ai3010005

4. Smith, K., & Hancock, P. A. (1995). Situation awareness is adaptive, externally directed consciousness. Human Factors, 37(1), 137–148. http://dx.doi.org/10.1518/001872095779049444

5. Ardabili, B. R., Yao, S., Pazho, A. D., Bourque, L., & Tabkhi, H. (2023). Enhancing situational awareness in surveillance: Leveraging data visualization techniques for machine learning-based video analytics outcomes. arXiv. https://doi.org/10.60097/ACIG/190341

6. Burov, Y. (2021). Knowledge based situation awareness process based on ontologies. In Proceedings of the International Conference on Computational Linguistics and Intelligent Systems (COLINS) (Vol. 2, pp. 45–55). Lviv Polytechnic Publishing House.

7. Ehrlinger, J., Readinger, W. O., & Kim, B. (2016). Decision-making and cognitive biases. In H. S. Friedman (Ed.), Encyclopedia of mental health (2nd ed., Vol. 1, pp. 191–202). Academic Press. http://dx.doi.org/10.1016/B978-0-12-397045-9.00206-8

8. Kokar, M. M., Matheus, C. J., & Baclawski, K. (2009). Ontology-based situation awareness. Information Fusion, 10(1), 83–98.

9. Steinberg, A. N., Bowman, C. L., & White, F. E. (1999). Revisions to the JDL data fusion model. In Sensor Fusion: Architectures, Algorithms, and Applications III (Proc. SPIE 3719). https://doi.org/10.1117/12.341367