УДК 004.42:351.74

П. В. Савіцький
К. О. Стахміч
А. О. Богданова
С. О. Жуков

ІНФОРМАЦІЙНО-АНАЛІТИЧНА СИСТЕМА «GOVHUB» ДЛЯ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У СФЕРІ ГРОМАДСЬКОЇ БЕЗПЕКИ

Вінницький національний технічний університет

Анотація

У роботі розв'язується актуальна науково-практична задача підвищення ефективності управління громадською безпекою шляхом створення інформаційно-аналітичної системи «GovHub». Запропоновано архітектуру інформаційно-аналітичної системи, яка призначена для інформаційної підтримки прийняття рішень при оперативній взаємодії громадян, силових структур та комунальних служб. Особливістю розробленої системи є інтеграція різних потоків даних: відеомоніторингу з БПЛА, геолокаційних даних та результатів NFC-ідентифікації особи. Реалізація архітектури виконана з використанням сучасного технологічного стеку (Kotlin, Swift, Python, PostgreSQL), що забезпечує надійність збереження даних та високу швидкість обробки запитів. Система дозволяє автоматизувати процеси виявлення правопорушень та мінімізувати час реагування на інциденти.

Ключові слова: громадська безпека, інформаційно-аналітична система, GovHub, прийняття рішень, відеомоніторинг БПЛА, NFC-ідентифікація, автоматизація, оперативне реагування.

Abstract

The paper addresses a relevant scientific and practical problem of improving public safety management through the development of the «GovHub» information and analytical system. The proposed architecture of the system is designed to provide decision-making support during operational interaction between citizens, law enforcement agencies, and utility services. A key feature of the developed system is the integration of diverse data streams: UAV video monitoring, geolocation data, and NFC-based personal identification results. The architecture is implemented using a modern technology stack (Kotlin, Swift, Python, PostgreSQL), ensuring data storage reliability and high-speed request processing. The system enables the automation of offense detection processes and minimizes response time to incidents.

Keywords: public safety, information and analytical system, GovHub, decision support, UAV monitoring, NFC identification, data integration, incident response.

Вступ

У сучасних реаліях глобальної цифровізації побудова ефективної взаємодії між державним апаратом та суспільством є одним із пріоритетних завдань національної стратегії безпеки. Попри стрімкий розвиток цифрових сервісів, спостерігається критична розпорошеність існуючих платформ, що призводить до відсутності оперативної комунікації між громадянами, правоохоронними органами та комунальними службами. Це призводить до затримок у прийнятті критично важливих рішень під час реагування на надзвичайні події.

Актуальність даної роботи зумовлена необхідністю розробки уніфікованої архітектури інформаційно-аналітичної системи, яка дозволить автоматизувати процеси ідентифікації та моніторингу правопорядку. Метою роботи є проєктування та реалізація системи «GovHub», яка інтегрує інструменти моніторингу (включно з керуванням дронами), засоби верифікації (NFC) та захищені канали комунікації в єдину екосистему. Такий підхід дозволяє оптимізувати процеси забезпечення правопорядку за рахунок прозорості даних та автоматизації рутинних операцій.

Результати дослідження

У процесі розроблення екосистеми «GovHub» було проведено комплексне дослідження, спрямоване на визначення ключових потреб громадян у сфері цифрової безпеки та оптимізацію протоколів взаємодії із силовими структурами. Отримані результати стали фундаментом для розроблення відмовостійкої архітектури, що базується на принципах максимального захисту персональних даних та оперативності

реагування. Було проаналізовано ряд існуючих рішень у сфері державних послуг, зокрема додаток «Дія» та окремі відомчі портали. Під час аналізу виявлено суттєві недоліки: розпорошеність функцій між різними ресурсами, застарілі інтерфейси, відсутність прямого каналу зв'язку між свідками подій та патрульними екіпажами, а також критичний брак інтеграції мобільних пристроїв із апаратними комплексами спостереження, такими як безпілотні літальні апарати. Отож, виникла потреба у створенні єдиного інструменту, який би поєднував функції ідентифікації, подачі екстрених заявок та оперативного моніторингу в одному захищеному середовищі. Основні можливості користувачів описані на рис. 1.

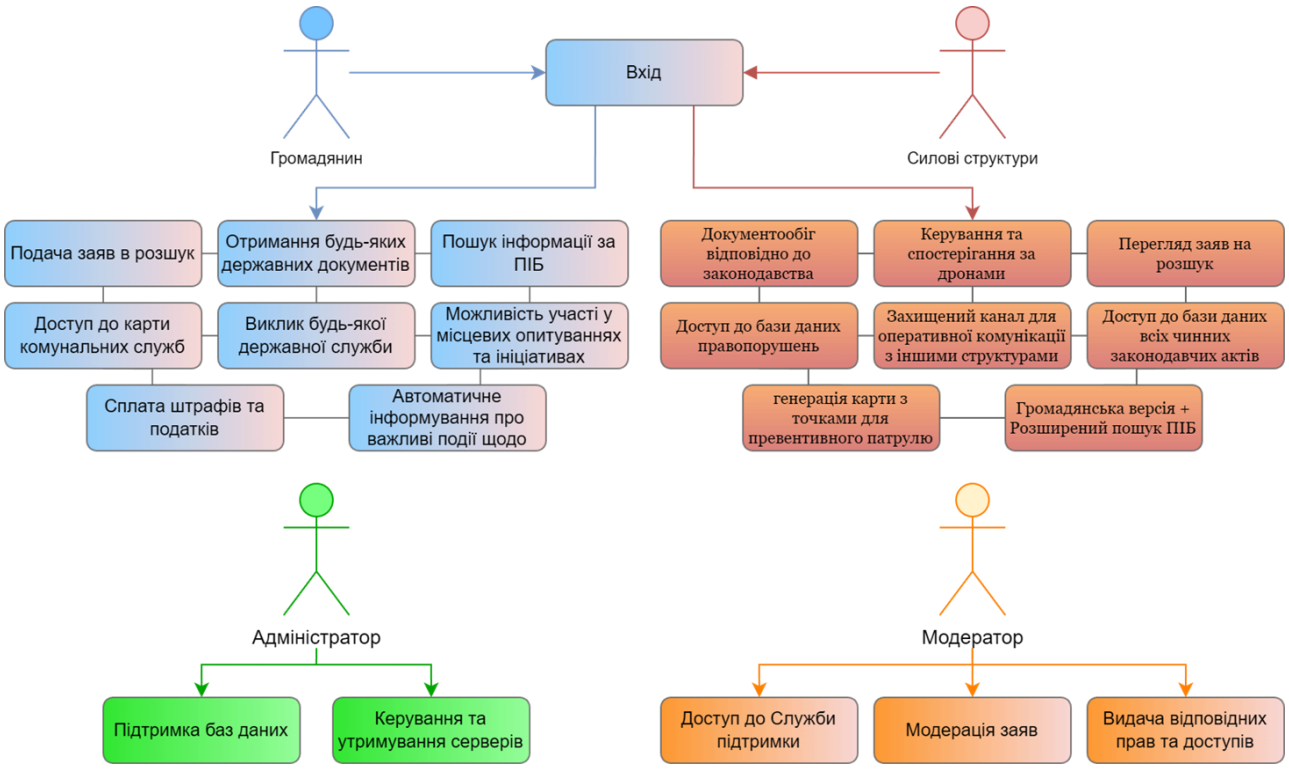

Рисунок 1. Use case діаграма

Робота застосунку «GovHub» розпочинається з проходження процедури багатофакторної авторизації через інтегровані державні реєстри, що є фундаментом безпеки всієї системи. Після успішного підтвердження особи система в автоматичному режимі проводить верифікацію статусу користувача та, згідно з ієрархією доступу, активує відповідний рівень функціональних модулів: від стандартного інтерфейсу для цивільних осіб до розширеного інструментарію для представників спецслужб. Для підтримання стабільності при масових зверненнях система використовує складні алгоритми динамічного розподілу потоків даних, що дозволяє мінімізувати затримки та забезпечити високу швидкість відгуку при будь-яких запитах, незалежно від навантаження на серверний контур. Важливою технологічною перевагою є можливість здійснення миттєвої ідентифікації осіб через вбудований NFC-модуль смартфона, який у поєднанні з біометричними документами зводить ризик фальсифікації даних до нуля та дозволяє проводити пошук за ПІБ у реальному часі. Таке поєднання криптографічного захисту та інтелектуальної маршрутизації даних дозволяє «GovHub» виступати не просто як сервіс, а як високоефективний цифровий інструмент оперативного реагування.

На рис. 2 зображена структура мобільного застосунку «GovHub».

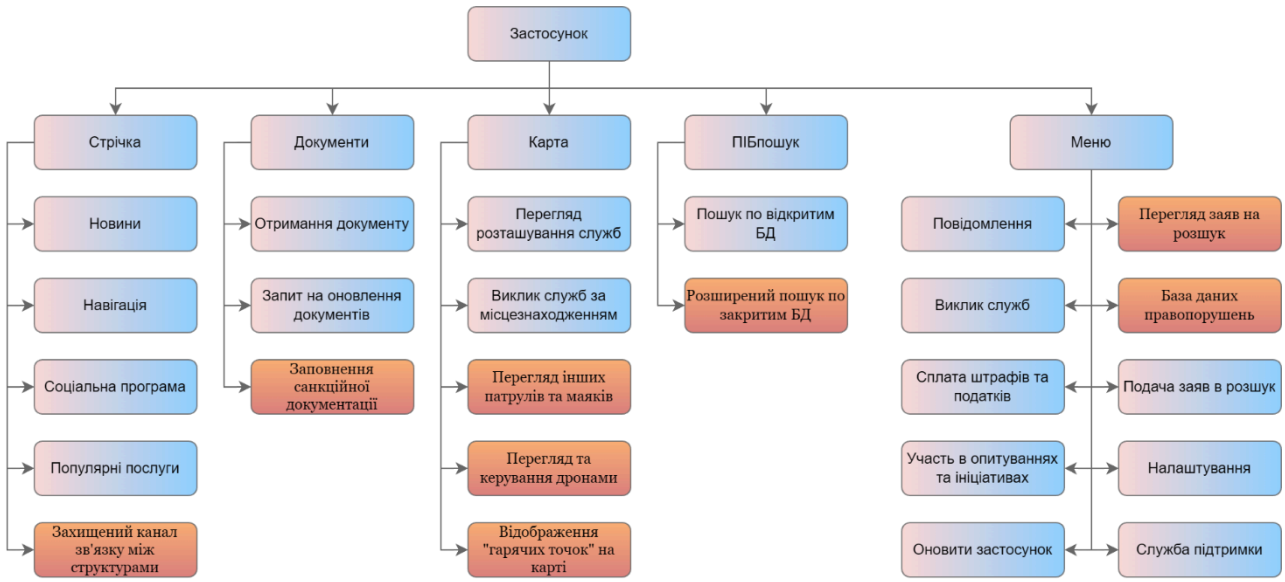

Рисунок 2. Структура застосунку

Структура «GovHub» побудована за модульним принципом, що забезпечує гнучкість системи при масштабуванні на загальнодержавний рівень. Головний екран містить інтуїтивно зрозумілу панель навігації, яка надає швидкий доступ до основних векторів: стрічки актуальних новин безпеки, електронних документів, інтерактивної карти інцидентів та інтелектуального пошуку. Модуль ідентифікації використовує технологію NFC для зчитування біометричних даних, що гарантує найвищий рівень захисту від підробок. Окремий функціональний блок призначений для представників спецслужб, що дозволяє авторизованим співробітникам здійснювати керування патрульними дронами в реальному часі та отримувати доступ до закритих баз правопорушень безпосередньо з мобільного пристрою. Застосунок підтримує інтеграцію з хмарною інфраструктурою через закритий контур, що забезпечує стабільну синхронізацію та зберігання даних під захистом енд-ту-енд шифрування державного зразка.

Для задоволення технічних вимог проєкту було обрано сучасний стек технологій. Фронтенд-частина розроблена на мовах Kotlin та Swift для відповідних платформ, що гарантує високу продуктивність інтерфейсу. База даних використовує PostgreSQL для надійного збереження реєстрів та історії звернень. Серверна логіка реалізована на Python, що дозволило ефективно інтегрувати модулі обробки відеопотоків із дронів та складні алгоритми фільтрації контенту. Для внутрішньої комунікації та розробки використовуються захищені середовища GitLab та Mattermost, що виключає витік інформації на етапі створення продукту. Для додаткових сервісів передбачено використання LiqPay API для миттєвої оплати адміністративних штрафів та державних мит у кілька кліків, що значно спрощує фінансові взаємодії громадян із державою.

Висновки

У результаті проведеного дослідження було розроблено та теоретично обґрунтовано концепцію інформаційно-аналітичної системи «GovHub», що є вагомим внеском у розвиток національної інфраструктури безпеки та цифровізації державних послуг.

Розроблено архітектуру інформаційно-аналітичної системи «GovHub» для підтримки прийняття рішень у сфері безпеки. Структура системи базується на модульному принципі, що дозволяє масштабувати її на загальнодержавний рівень та інтегрувати з існуючими реєстрами через захищені протоколи обміну даними.

Використання мов програмування Kotlin та Swift забезпечить високу продуктивність клієнтських додатків, а серверна частина на Python з базою даних PostgreSQL дозволить реалізувати ефективну логіку обробки запитів та зберігання історії інцидентів.

Створений застосунок забезпечує не просто надання адміністративних сервісів, а формує якісно новий стандарт оперативної взаємодії між громадянами та силовими структурами, де технології моніторингу, криптографічного захисту та автоматизованої ідентифікації працюють як єдиний

механізм. Впровадження таких інноваційних модулів, як пряме керування патрульними дронами зі смартфона авторизованого співробітника та миттєва NFC-верифікація біометричних документів, дозволяє значно знизити рівень бюрократизації, мінімізувати ризики підробки даних та критично підвищити швидкість реагування на правопорушення в реальному часі.

В подальших дослідженнях планується приділити розширенню інтелектуальних можливостей карти та впровадженню алгоритмів предиктивної аналітики для прогнозування потенційних інцидентів. Це дозволить трансформувати систему з інструменту реагування на інструмент попередження правопорушень шляхом прогнозування потенційних загроз на основі аналізу патернів поведінки та геопросторових даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Documentation for Kotlin development [Електронний ресурс] – URL: https://kotlinlang.org/docs/home.html
2. Swift Documentation. Apple Developer [Електронний ресурс] – URL: https://developer.apple.com/documentation/swift
3. PostgreSQL 15.0 Documentation [Електронний ресурс] – URL: https://www.postgresql.org/docs/15/index.html
4. Python 3.11.0 documentation [Електронний ресурс] – URL: https://docs.python.org/3/

Савіцький Павло Вікторович – студент групи 2ІСТ-25б, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м. Вінниця, e-mail: savickijpavel42@gmail.com

Стахміч Каріна Олександрівна – студентка групи 2ІСТ-25б, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м. Вінниця, e-mail: karinastahmic@gmail.com

Богданова Анастасія Олександрівна – студентка групи 2ІСТ-25б, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м. Вінниця, e-mail: noonex392@gmail.com

Жуков Сергій Олександрович – к.т.н., доцент кафедри системного аналізу та інформаційних технологій, Вінницький національний технічний університет, e-mail: sazhukov@gmail.com

Savickij Paul V. – student of group 2IST-25b, Faculty of Intellectual Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: savickijpavel42@gmail.com

Stahmich Karina O. – student of group 2IST-25b, Faculty of Intellectual Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: karinastahmic@gmail.com

Bogdanova Anastasia O. – student of group 2IST-25b, Faculty of Intellectual Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: noonex392@gmail.com

Zhukov Serhii O. – Ph.D., Assistant Professor of the Department of System Analysis and Information Technologies, Vinnytsia National Technical University, Vinnytsia, e-mail: sazhukov@gmail.com