Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ПРОГРАМНИЙ АСИСТЕНТ ФАХІВЦЯ З КРИМІНАЛІСТИЧНОГО АНАЛІЗУ КІБЕРЗЛОЧИНІВ»

Виконав: студент 2 курсу, групи 1БС-24 м
спеціальності 125 – Кібербезпека та захист інформації
_____ Микола ТАРАСЮК

Керівник: д. ф. н., доц. каф. ЗІ
_____ Леонід МАЙДАНЕВИЧ
«16» грудня 2025 р.

Опонент: к.т.н., доц. каф. ПЗ
_____ Олександр ХОШАБА
«16» грудня 2025 р.

Допущено до захисту
Во. Завідувач кафедри ЗІ
д.т.н., проф.
_____ Володимир ЛУЖЕЦЬКИЙ
«16» грудня 2025 р.

Вінниця ВНТУ – 2025 рік

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти II (магістерський)
Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека та захист інформації
Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ,
д.т.н., проф.
____Володимир ЛУЖЕЦЬКИЙ
«___» __вересня__ 2025 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Тарасюку Миколі Борисовичу

1. Тема роботи: «Програмний асистент фахівця з криміналістичного аналізу кіберзлочинів»
Керівник роботи: Майданевич Леонід Олександрович, к. ф. н., доц. каф. ЗІ, затверджені наказом ректора ВНТУ від 24 вересня 2025 року № 313.

2. Строк подання студентом роботи : 16 грудня 2025 року

3. Вихідні дані до роботи:
- операційна система – Windows та MacOS;
- середовище розробки – Visual Studio Code;
- мова програмування – Python;
- фреймворк – Flet.

4. Зміст текстової частини: Вступ. 1. Аналіз джерел і нормативно-правової бази у сфері розслідувань кіберзлочинів. 2. Модель системи підтримки процесу розслідування кіберзлочинів. 3. Практична реалізація програмного асистента фахівця 4. Економічна частина. Висновки. Список використаних джерел. Додатки.

5. Перелік ілюстративного матеріалу: UML-діаграма взаємодії складових програмного асистента фахівця з криміналістичного аналізу кіберзлочинів (плакат А4), UML-діаграма активності процесу обробки запитів користувача (плакат А4), UML-діаграма послідовності для запиту довідки (плакат А4), UML-діаграма послідовності для запиту в чат (плакат А4), UML-діаграма потоків даних (плакат А4), Схема алгоритму запуску застосунку (плакат А4), Схема алго-

ритму запиту довідки (плакат А4), Схема алгоритму запиту в чат (плакат А4), Схема детального алгоритму генерування відповіді (плакат А4), Схема алгоритму завершення роботи (плакат А4), Схема модуля обробки мовлення (плакат А4), Схема модуля штучного інтелекту (плакат А4), Схема логічного модуля застосунку (плакат А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	доц. кафедри ЗІ, к. ф. н., Майданевич Л. О.	25.09.2025	18.12.2025
2	доц. кафедри ЗІ, к. ф. н., Майданевич Л. О.	25.09.2025	18.12.2025
3	доц. кафедри ЗІ, к. ф. н., Майданевич Л. О.	25.09.2025	18.12.2025
4	зав. каф. ЕПВМ, к. е. н., проф. Лесько О. Й.	18.12.2025	18.12.2025

7. Дата видачі завдання 24 вересня 2025 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	24.09.2025 – 26.09.2025	
2	Аналіз інформаційних джерел за напрямком магістерської кваліфікаційної роботи	27.09.2025 – 07.10.2025	
3	Науково-технічне обґрунтування	11.10.2025 – 22.10.2025	
4	Аналіз нормативно-правової документації, стандартів та інструментів в сфері криміналістичного аналізу кіберзлочинів	23.10.2025 – 26.10.2025	
5	Аналіз та формування вимог до програмного асистента фахівця з криміналістичного аналізу кіберзлочинів	27.10.2025 – 02.11.2025	
6	Розробка програмного асистента фахівця з криміналістичного аналізу кіберзлочинів	03.11.2025 – 10.11.2025	
7	Тестування та оцінювання програмного асистента фахівця з криміналістичного аналізу кіберзлочинів	10.11.2025 – 17.11.2025	
8	Розробка розділу економічного обґрунтування доцільності роботи	18.11.2025 – 22.11.2025	
9	Оформлення пояснювальної записки	23.11.2025 – 29.11.2025	
10	Попередній захист та доопрацювання МКР	29.11.2025 – 11.12.2025	
11	Перевірка на наявність текстових запозичень	12.12.2025 – 15.12.2025	
12	Представлення МКР до захисту, рецензування	16.12.2025 – 19.12.2025	
13	Захист МКР	19.12.2025 – 23.12.2025	

Студент _____ Микола ТАРАСЮК

Керівник роботи _____ Леонід МАЙДАНЕВИЧ

АНОТАЦІЯ

УДК 004.056

Тарасюк М. Б. Програмний асистент фахівця з криміналістичного аналізу кіберзлочинів. Магістерська кваліфікаційна робота зі спеціальності 125 – Кібербезпека та захист інформації, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2025. 97 с.

На укр. мові. Бібліогр.: 55 назв; рис.: 27 табл. 28.

Магістерська кваліфікаційна робота присвячена розробці програмного асистента для підтримки криміналістичного аналізу кіберзлочинів. У процесі виконання роботи проаналізовано нормативно-правове забезпечення розслідування кіберзлочинів в Україні та сучасний інструментарій цифрової криміналістики, що застосовується для дослідження комп'ютерних систем і цифрових даних. Розроблено теоретико-множинну модель програмного асистента фахівця з криміналістичного аналізу кіберзлочинів. На основі отриманих результатів розроблено архітектуру програмного асистента, створено логічні моделі його функціонування та алгоритми обробки користувацьких запитів із використанням методів машинного навчання та семантичного аналізу тексту. Реалізовано програмний застосунок та проведено тестування його точності в умовах різних формулювань опису правопорушень.

Ілюстративна частина складається з 13 плакатів з демонстрацією результатів розробки і проведених досліджень.

В економічному розділі здійснено оцінку витрат на розробку програмного застосунку.

Ключові слова: кіберзлочин, програмний асистент, цифрова криміналістика, штучний інтелект, обробка природної мови, семантичний аналіз, Кримінальний кодекс України.

ANNOTATION

UDC 004.056

Tarasiuk M. B. Program assistant of a specialist in the forensic analysis of cybercrimes. Master's thesis on specialty 125 – Cybersecurity and information protection, educational program – Security of information and communication systems. Vinnytsia: VNTU, 2025. – 97 p.

In Ukrainian. Bibliographer: 55 titles; fig.: 27 tabl. 28.

The master's thesis is devoted to the development of a software assistant to support the forensic analysis of cybercrimes. In the course of the work, the regulatory and legal support for the investigation of cybercrimes in Ukraine and the modern tools of digital forensics used for the study of computer systems and digital data were analyzed. A multi-theoretical model of a software assistant for a specialist in the forensic analysis of cybercrimes has been developed. On the basis of the obtained results, the architecture of the software assistant was developed, logical models of its functioning and algorithms for processing user requests were created using methods of machine learning and semantic text analysis. The software application was implemented and its accuracy was tested in the conditions of different formulations of the description of offenses.

The illustrative part consists of 13 posters with a demonstration of the results of development and conducted research.

In the economic section, an assessment of the costs of developing a software application was made.

Keywords: cybercrime, software assistant, digital forensics, artificial intelligence, natural language processing, semantic analysis, Criminal Code of Ukraine.

ЗМІСТ

ВСТУП

Актуальність теми. Фахівці з цифрової криміналістики часто працюють з великою кількістю нормативних документів, технічних описів, стандартів і рекомендацій, розкиданих по різних джерелах. Наявність програмного асистента, який об’єднує всі необхідні довідкові матеріали в одному додатку, суттєво підвищує ефективність роботи та скорочує час, витрачений на пошук потрібної інформації.

Особливої актуальності така система набуває у випадках, коли з цифровими інцидентами працюють фахівці без глибоких знань у сфері кримінального права, зокрема ІТ-спеціалісти, аналітики з кібербезпеки чи технічні експерти. У таких ситуаціях програмний асистент може надавати рекомендації щодо відповідних правових норм для попередньої кваліфікації події.

Метою дослідження є спрощення процедури аналізу кіберзлочинів шляхом розробки моделі системи підтримки процесу розслідування кіберзлочинів та програмного застосунку що реалізує її.

Для досягнення поставленої мети в магістерській роботі були сформульовані такі ***завдання***:

- проаналізувати предметну область і відкриті джерела на тему цифрової криміналістики;
- оглянути нормативно-правову базу щодо забезпечення кібербезпеки та цифрової криміналістики;
- провести порівняльний аналіз існуючих засобів криміналістичного аналізу;
- розробити теоретико-множинну модель програмного асистента;
- розробити архітектуру програмного асистента;
- розробити моделі процесів та алгоритми їх реалізації;
- провести варіантний аналіз та обґрунтування вибору засобів для реалізації програмного асистента фахівця з криміналістичного аналізу;
- реалізувати програмний асистент фахівця з криміналістичного аналізу;

- провести тестування розробленого програмного асистента для підтвердження його працездатності та ефективності;
- провести обґрунтування економічної доцільності розробки програмного асистента.

Об'єктом дослідження є процес криміналістичного аналізу кіберзлочинів.

Предметом дослідження є модель системи підтримки процесу розслідування кіберзлочинів та програмного застосунку що реалізує її.

Методи дослідження. При вирішенні завдань магістерської роботи використовувалися, зокрема: системний аналіз (при дослідженні інформації, рішень, відмінностей, критеріїв), структурно-функціональний аналіз (при розкритті функціональних проявів моделей, схем), теоретико- множинний підхід (при розробці моделей), міждисциплінарний та трансдисциплінарний підходи (як певні алгоритми дослідження).

Новизна одержаних результатів полягає в розробці моделі програмного асистента фахівця з криміналістичного аналізу кіберзлочинів.

Практична цінність даної магістерської роботи полягає в тому, що розроблений програмний асистент допомагає удосконалити методику криміналістичного розслідування кіберзлочинів.

Публікації результатів магістерської кваліфікаційної роботи.

Результати магістерської роботи доповідалися на таких конференціях:

1. Майданевич, Л. О., Тарасюк, М. Б., Комп'ютерно-технічна експертиза: основні аспекти підготовки до проведення, ВНТУ, 2025 [1].

2. Майданевич Л. О., Кирбят'єв О. О., Тарасюк М. Б., Алгоритм отримання електронних доказів в умовах потенційного самознищення електронних (цифрових) слідів, кримінальний аналіз і кібербезпека: об'єднання зусиль для нових викликів, Одеський державний університет внутрішніх справ, 23 травня 2025 року [2].

1 АНАЛІЗ ДЖЕРЕЛ І НОРМАТИВНО-ПРАВОВОЇ БАЗИ У СФЕРІ РОЗСЛІДУВАНЬ КІБЕРЗЛОЧИНІВ

1.1 Аналіз джерел інформації з питань розслідування кіберзлочинів

Стрімкий розвиток інформаційних технологій та глобалізація кіберпростору зумовили появу нової категорії протиправних дій, які здійснюються з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Такі діяння отримали загальну назву кіберзлочини. Їх виникнення стало закономірним наслідком цифровізації суспільства, адже зростання обсягів даних, поширення онлайн-сервісів і залежність бізнесу та державних структур від інформаційних систем створили нове середовище для злочинної діяльності.

Цифрова криміналістика є науковою та практичною дисципліною, спрямованою на виявлення, збереження, аналіз і представлення цифрових доказів у спосіб, прийнятний у суді. Вона сформувалася на перетині інформаційних технологій, криміналістики та права, і становить одну з ключових складових сучасного процесу розслідування кіберзлочинів [3].

На відміну від традиційної криміналістики, яка вивчає матеріальні сліди злочину (документи, об'єкти, речові докази), цифрова криміналістика оперує нематеріальними інформаційними об'єктами, що існують у формі цифрових даних. Саме ця особливість зумовила появу нових теоретичних категорій, понять і методів, спрямованих на інтерпретацію інформаційних процесів як об'єкта наукового дослідження.

Процедура проведення цифрової криміналістики складається з таких основних етапів [4]:

– *збір* (виявлення, маркування, фіксація та отримання даних із можливих джерел релевантної інформації з дотриманням процедур, що забезпечують цілісність цих даних);

- *дослідження* (форензична обробка зібраних даних із використанням комбінації автоматизованих і ручних методів, оцінювання та вилучення даних, що становлять особливий інтерес, при цьому зберігаючи їхню цілісність);
- *аналіз* (аналіз результатів дослідження із застосуванням юридично обґрунтованих методів і технік для отримання корисної інформації, яка відповідає на запитання, що стали підставою для проведення збору та дослідження);
- *звітність* (підготовка звіту за результатами аналізу, який може включати опис виконаних дій, пояснення вибору інструментів і процедур, визначення подальших дій, наприклад, проведення додаткової криміналістичної експертизи, усунення виявлених вразливостей, удосконалення існуючих засобів безпеки, а також надання рекомендацій щодо поліпшення політик, процедур, інструментів та інших аспектів криміналістичного процесу)

Цей процес може бути підтриманий програмними асистентами цифрового розслідування, які автоматизують частину аналітичних дій, підвищують точність виявлення слідів та мінімізують людський фактор.

Останні кілька років в Україні гостро постало питання розвитку цифрової криміналістики, форензики, антифорензики та суміжних наукових напрямів, пов’язаних із розслідуванням кіберзлочинів. Зростання кількості інцидентів у кіберпросторі, активізація кібератак на критичну інфраструктуру та поширення технологічно складних схем злочинів зумовили підвищену увагу до формування наукової та нормативно-правової бази у цій сфері.

Дослідники, практики та представники правоохоронних органів активно дискутують щодо необхідності впровадження єдиної термінології, узгодження визначень основних понять та створення системного підходу до цифрових доказів, процедур їх збирання, зберігання та аналізу на правовому рівні.

У своїй роботі Бараненко Р. В. проводить аналіз наукових досліджень інших авторів і вказує на те, що вітчизняні науковці не дійшли згоди щодо єдиного

визначення поняття «кіберзлочин» [5]. Автор дискутує щодо необхідності заміни термінів «кіберзлочин» та «комп'ютерний злочин» на більш широке поняття «кіберправопорушення». Інші дослідники, своєю чергою, пропонують такі визначення, як «злочини у сфері використання інформаційних технологій» [6], «злочини у сфері комп'ютерної інформації» [7] та інші.

Бараненко Р. В. визначає «кіберзлочинність» як сукупність «кіберправопорушень», що дозволяє спростити термінологію. Натомість інші автори під поняттям «кіберзлочинність» об'єднують усі види кримінальних правопорушень, вчинених в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси та інформаційна техніка можуть виступати предметом або метою злочинних посягань, середовищем, у якому відбуваються правопорушення, або засобом і знаряддям вчинення кримінального правопорушення [8].

На сьогоднішній день із наукових праць українських дослідників можна узагальнити, що кіберзлочини – це суспільно небезпечні діяння, спрямовані на порушення роботи комп'ютерних систем, незаконне втручання в інформаційні ресурси, знищення, блокування чи модифікацію даних, а також використання інформаційних технологій як знаряддя вчинення злочину.

Таким чином, кіберзлочин має подвійну природу – технічну (оскільки реалізується через інформаційні технології) та правову (оскільки посягає на суспільні відносини, що охороняються законом).

Для визначення цифрової криміналістики більшість авторів посилаються на Колодіну А. С. та Федорову Т. С., які в своєму дослідженні охарактеризували її наступним чином: «цифрова криміналістика (форензіка, комп'ютерна криміналістика, розслідування кіберзлочинів) – прикладна наука про розкриття злочинів, пов'язаних з комп'ютерною інформацією, про дослідження цифрових доказів, методи пошуку, отримання і закріплення таких доказів.» [9].

Дане визначення, незважаючи на свою простоту, охоплює основні завдання цифрової криміналістики. У своєму дослідженні Степанюк Р. Л. та Перлін С. І. також розглядають інші визначення цифрової криміналістики, запропоновані

вітчизняними науковцями [10]. Деякі автори пропонують розглядати цифрову криміналістику як складову загальної криміналістики [11], тоді як інші вважають її самостійною науковою дисципліною [12]. Степанюк Р. Л. та Перлін С. І. наголошують, що цифрова криміналістика та застосування цифрових технологій у криміналістиці не є тотожними поняттями.

На міжнародному рівні це обговорення триває вже протягом тривалого часу. Провідні країни світу розробляють стандарти цифрової криміналістики, формують спеціалізовані інституції та гармонізують законодавство для забезпечення ефективної співпраці під час розслідування кіберзлочинів, що мають транскордонний характер.

Зарубіжні фахівці переважно розглядають цифрову криміналістику як складову частину ширшої системи судових наук [13]. У їхніх працях цифрова криміналістика визначається як комплекс наукових методів, засобів і процедур, спрямованих на збереження, виявлення, фіксацію, збирання, перевірку, ідентифікацію, аналіз, інтерпретацію, документування та представлення цифрових доказів, отриманих із цифрових джерел [14]. Головна мета цих процесів – забезпечення достовірного доказового матеріалу для розслідування подій, переважно кримінального або іншого протиправного характеру.

На міжнародному рівні, так само як і у вітчизняному науковому дискурсі, тривають дискусії щодо визначення базової термінології та потреби її чіткого закріплення у правовому полі [15]. Відсутність уніфікованих дефініцій ускладнює інтеграцію цифрової криміналістики в судово-експертну практику, а також створює труднощі у взаємодії між спеціалістами правової та технічної сфер. Останні, як правило, володіють глибокими знаннями лише у своїй галузі, що призводить до комунікаційних бар’єрів та непорозумінь під час спільного розслідування кіберінцидентів [16].

Отже, можна зробити висновок, що цифрова криміналістика є відносно молодою, динамічною галуззю, яка перебуває на етапі активного формування власної методології, системи понять та нормативно-правового підґрунтя. Сучасні наукові дослідження зосереджені на розробленні універсальних підходів

до класифікації цифрових доказів, стандартизації процесів їх збирання та аналізу, а також на гармонізації технічних і юридичних аспектів у межах судово-експертної діяльності. Така інтеграція сприятиме підвищенню якості доказової бази, ефективності розслідувань і зміцненню правової визначеності у сфері кібербезпеки.

1.2 Огляд нормативно-правової бази щодо забезпечення кібербезпеки та цифрової криміналістики

Міжнародні правові акти у сфері кібербезпеки відіграють ключову роль у формуванні глобальної системи протидії кіберзлочинності та забезпеченні ефективного розслідування інцидентів у цифровому середовищі. Вони забезпечують уніфікацію термінології та процедур збору цифрових доказів, що сприяє узгодженості підходів різних держав під час проведення кіберрозслідувань. Такі акти також сприяють розвитку механізмів взаємної допомоги та обміну інформацією між країнами, створюючи правові підстави для співробітництва у сфері кібербезпеки. Важливим аспектом міжнародного регулювання є встановлення балансу між вимогами безпеки та захистом прав людини у цифровому просторі. Крім того, міжнародні нормативні документи становлять основу для розробки та вдосконалення національного законодавства у сфері кіберзахисту, сприяючи його гармонізації із загальновизнаними міжнародними стандартами.

Найбільш значущим і комплексним документом у цій галузі є Конвенція Ради Європи про кіберзлочинність, відома як Будапештська конвенція [17]. Вона є першим міжнародним договором, спрямованим на уніфікацію кримінально-правових підходів до боротьби з комп’ютерними злочинами та на створення правових механізмів співпраці держав.

Основними положеннями Конвенції є:

- криміналізація діянь, пов’язаних із незаконним доступом до комп’ютерних систем, перехопленням даних, втручанням у роботу систем або зловживанням пристроями;
- визначення правил збору, збереження та передачі електронних доказів;
- створення механізмів міжнародного співробітництва, включно з екстрадицією, взаємною правовою допомогою та оперативним обміном інформацією.

Будапештська конвенція стала фундаментом для національного законодавства більшості країн світу, у тому числі України. Вона також слугує основою для гармонізації процесів цифрової криміналістики та уніфікації термінології.

У відповідь на нові виклики кіберзлочинності у 2022 році був прийнятий Другий додатковий протокол , який посилює співпрацю у сфері електронних доказів [18]. Він регламентує порядок прямого доступу до даних у провайдерів послуг, взаємодію між правоохоронними органами та приватним сектором, а також забезпечення захисту персональних даних під час транскордонного обміну інформацією.

Цей документ актуалізує необхідність створення швидких процедур обміну електронними доказами без надмірних бюрократичних бар’єрів, що особливо важливо у випадках кіберінцидентів, які мають короткий часовий слід.

ООН (Організація Об’єднаних Націй) відіграє ключову роль у формуванні глобальної політики кібербезпеки. Резолюції Генеральної Асамблеї, зокрема № 57/239 «Створення глобальної культури кібербезпеки» (2002 р.) [19] та № 64/211 «Створення глобальної культури кібербезпеки та захисту критичної інформаційної інфраструктури» (2009 р.) [20], визначають стратегічні напрями міжнародної співпраці.

ООН закликає держави впроваджувати національні стратегії кібербезпеки, створювати центри реагування на інциденти (CERT/CSIRT) та розвивати міжнародний обмін інформацією про кіберзагрози. Крім того, у межах

Міжнародного союзу електрозв'язку (ITU) розроблено стандарти та рекомендації, що сприяють підвищенню стійкості кіберінфраструктур.

Європейський Союз активно формує власну систему регулювання у сфері кібербезпеки. Серед ключових актів варто відзначити:

– Директиву NIS2 (Network and Information Security Directive, 2023) – документ, який зобов'язує держави-члени ЄС впроваджувати національні стратегії кібербезпеки, забезпечувати безпеку критичної інфраструктури та встановлює вимоги до звітності про кіберінциденти [21];
– Регламент (ЄС) 2019/881 (Cybersecurity Act), який створює систему сертифікації кібербезпеки продуктів, послуг і процесів на рівні ЄС [22];
– Регламент (ЄС) 2016/679 (GDPR), що встановлює норми захисту персональних даних, у тому числі під час обробки їх у рамках цифрових розслідувань [23].

Міжнародні організації постійно докладають зусиль для своєчасного оновлення правової бази з метою ефективної протидії кіберзагрозам. З огляду на стрімкий розвиток технологій та зростання кількості кіберінцидентів, такі структури, як ООН, Європейський Союз, Інтерпол, Ради Європи та НАТО, розробляють і вдосконалюють міжнародні стандарти, конвенції та рекомендації у сфері кібербезпеки. Особливе значення має Будапештська конвенція про кіберзлочинність, яка залишається основним міжнародним документом у цій галузі та постійно доповнюється новими протоколами. Такі ініціативи сприяють уніфікації термінології, гармонізації законодавства різних країн і зміцненню міжнародної співпраці у боротьбі з кіберзлочинністю.

Система правового регулювання у сфері протидії кіберзлочинності в Україні формується під впливом міжнародних норм та стандартів, зокрема положень Будапештської конвенції про кіберзлочинність (2001 р.), яку Україна ратифікувала у 2005 році [24]. Відповідно до цього міжнародного документа, національне законодавство поступово адаптується до європейських вимог, передбачаючи комплексну відповідальність за правопорушення у сфері

інформаційних технологій, а також визначаючи процедури розслідування таких злочинів.

Основні положення щодо інформаційної безпеки закріплені у Конституції України, де статті 31, 32 і 40 гарантують право на приватність, таємницю листування й недоторканність особистого життя [25]. Ці норми визначають базові принципи, якими мають керуватися органи досудового розслідування під час роботи з цифровими доказами, забезпечуючи баланс між безпекою держави та правами людини.

Безпосередня кримінальна відповідальність за кіберзлочини встановлена Кримінальним кодексом України (ККУ), у якому розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» містить такі основні статті (табл. 1.1) [26].

Ці статті формують правову основу для кваліфікації кіберзлочинів та проведення криміналістичних досліджень цифрових слідів.

Таблиця 1.1 – Зміст розділу XVI Кримінального кодексу України

№ статті	Назва статті	Суть правопорушення
361	Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку	Незаконне втручання в роботу комп'ютерних систем або мереж, що призводить до порушення їх роботи чи витоку інформації.
361-1	Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут	Розробка, розповсюдження або продаж вірусів, троянів чи інших засобів, призначених для несанкціонованого доступу або пошкодження інформації.
361-2	Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації	Незаконне розповсюдження конфіденційних даних, до яких було отримано доступ без дозволу.

Продовження таблиці 1.1

362	Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації	Незаконне копіювання, зміна, знищення або блокування інформації без дозволу власника.
363	Порушення правил експлуатації електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється	Недотримання встановлених правил експлуатації або безпеки, що призвело до пошкодження систем чи витоку даних.
363-1	Перешкоджання роботі електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку	Атаки типу DoS/DDoS – перевантаження системи через масову розсилку повідомлень з метою блокування її роботи.

Ключовим нормативно-правовим актом у сфері кібербезпеки є Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [27]. Він визначає правові та організаційні основи забезпечення кібербезпеки держави, встановлює повноваження суб'єктів системи кібербезпеки та регламентує координацію їхньої діяльності.

Документ також визначає необхідність взаємодії державного та приватного секторів у питаннях обміну інформацією про кіберінциденти, створення національної системи реагування (CERT-UA) [28] та впровадження міжнародних стандартів інформаційної безпеки.

Згідно з цим Законом, основними суб'єктами системи кібербезпеки є (табл. 1.2):

Таблиця 1.2 – Основні суб'єкти системи кібербезпеки України

Орган	Повна назва	Основні функції у сфері кібербезпеки
Держспецзв'язку	Державна служба спеціального зв'язку та захисту інформації України	Формує та реалізує державну політику у сфері кіберзахисту, криптографічного та технічного захисту інформації; координує діяльність національної системи кібербезпеки.
СБУ	Служба безпеки України	Здійснює контррозвідувальні заходи у сфері кібербезпеки, виявляє, запобігає та розслідує кіберзлочини, що загрожують національній безпеці.

Продовження таблиці 1.2

Національна поліція України	Департамент кіберполіції Національної поліції України	Розслідує кіберзлочини, проводить оперативно-розшукові дії, забезпечує взаємодію з міжнародними правоохоронними органами у сфері кібербезпеки.
НБУ	Національний банк України	Забезпечує кіберзахист банківської та фінансової інфраструктури, встановлює вимоги до безпеки платіжних систем і фінансових установ.
Інші органи	Органи державної влади та суб'єкти критичної інформаційної інфраструктури	Відповідають за захист власних інформаційних систем, впроваджують політику кіберзахисту на рівні своїх секторів (енергетика, транспорт, охорона здоров'я тощо).

В таблиці 1.3 наведено інші законодавчі акти які належать до нормативно-правової бази, що регламентує протидію кіберзлочинності.

У сукупності наведені нормативно-правові акти формують концептуальну основу національної системи протидії кіберзлочинності та забезпечення інформаційної безпеки. Вони визначають як фундаментальні права учасників інформаційних відносин, так і механізми кримінально-правового впливу на осіб, що вчиняють правопорушення у кіберпросторі.

Попри наявність достатньо розвиненої нормативно-правової бази у сфері протидії кіберзлочинності, в Україні на сьогоднішній день все ще відсутня чітка класифікація та систематизація понять, пов'язаних із цифровою криміналістикою, форензикою та суміжними галузями. Законодавство визначає основні принципи захисту інформації та відповідальність за кіберзлочини, однак не містить уніфікованих термінів і критеріїв, що регламентують діяльність з виявлення, збору, збереження та аналізу цифрових доказів. Це ускладнює правозастосовну практику, створює неоднозначність у тлумаченні термінів і гальмує розвиток національної системи цифрової криміналістики як складової кібербезпеки держави.

Таблиця 1.3 – Спеціальні нормативно-правові акти в законодавстві України

№	Нормативно-правовий акт	Рік ухвалення	Основний зміст / призначення
1	Закон України «Про інформацію»[29]	1992	Визначає правовий режим інформації, її види, принципи доступу та захисту, права і обов'язки суб'єктів інформаційних відносин.
2	Закон України «Про захист інформації в інформаційно-комунікаційних системах»[30]	1994	Регламентує технічні, організаційні та правові засади забезпечення інформаційної безпеки в ІТС; встановлює вимоги до захисту інформації від несанкціонованого доступу.
3	Закон України «Про захист персональних даних»[31]	2010	Визначає порядок обробки та захисту персональних даних; гармонізує українське законодавство з положеннями GDPR.
4	Закон України «Про електронну ідентифікацію та електронні довірчі послуги»[32]	2017	Визначає правові засади використання електронного підпису, печатки, часових міток та електронної ідентифікації; забезпечує довіру до електронних транзакцій.
5	Стратегія кібербезпеки України до 2025 року (Указ Президента № 447/2021) [33]	2021	Визначає стратегічні цілі державної політики у сфері кіберзахисту: розвиток цифрової криміналістики, підвищення кіберстійкості, посилення можливостей правоохоронних органів.

У сфері цифрової криміналістики важливе значення має дотримання міжнародних стандартів та рекомендацій, що забезпечують єдині вимоги до процесів збору, збереження, аналізу та документування цифрових доказів. Стандартизація цих процесів гарантує правову допустимість отриманих результатів, підвищує якість експертиз і сприяє взаємодії між державними, правоохоронними та приватними структурами в межах розслідувань кіберінцидентів.

Міжнародний стандарт ISO/IEC 27037 визначає принципи та найкращі практики для ідентифікації, збору, отримання та збереження цифрових доказів [34]. Його метою є забезпечення цілісності, достовірності та відтворюваності цифрових даних, що можуть бути використані у кримінальному провадженні.

Основні положення стандарту включають:

- визначення ролей і відповідальності осіб, які здійснюють цифрову криміналістику;
- вимоги до процедур фіксації та маркування носіїв;
- принципи дотримання ланцюга зберігання доказів (chain of custody);
- забезпечення мінімального впливу на первинні дані під час збору;
- опис інструментів і технічних засобів, які повинні бути сертифікованими та перевіреними.

Таким чином, ISO/IEC 27037 формує базову основу для побудови процесів цифрової криміналістики відповідно до міжнародних вимог.

Документ NIST Special Publication 800-86, розроблений Національним інститутом стандартів і технологій США (NIST), спрямований на інтеграцію цифрової криміналістики в процеси реагування на інциденти безпеки [35].

Основні елементи рекомендацій NIST включають:

- створення структурованого підходу до збору та аналізу цифрових артефактів;
- визначення етапів: підготовка – виявлення – аналіз – документування – реагування;
- рекомендації щодо збереження метаданих, створення образів дисків та логів мережевого трафіку;
- забезпечення повторюваності результатів при застосуванні різних інструментів та методів;
- важливість правового супроводу кожного етапу розслідування, з урахуванням національних норм.

NIST SP 800-86 має практичний характер і часто використовується як методологічна основа для побудови внутрішніх процедур цифрової криміналістики у державних і корпоративних структурах.

Інші стандарти які мають відношення до кібербезпеки та інформаційних технологій наведено в таблиці 1.4.

Таблиця 1.4 – Стандарти в сфері кібербезпеки та інформаційних технологій

№	Документ / Стандарт	Рік	Основний зміст та призначення	Ключові положення
1	ISO/IEC 27041:2015 – Guidance on assuring suitability and adequacy of incident investigative methods[36]	2015	Визначає методологію оцінювання ефективності та достовірності інструментів і процедур цифрової криміналістики.	– Гарантує надійність результатів розслідування. – Містить критерії оцінки методів, процесів і програмних засобів. – Сприяє стандартизації судово-технічного аналізу даних.
2	ISO/IEC 27042:2015 – Guidelines for the analysis and interpretation of digital evidence[37]	2015	Присвячений аналізу та інтерпретації цифрових доказів після їх збору.	– Визначає принципи оцінки достовірності, повноти та контексту даних. – Регламентує вимоги до відтворюваності результатів. – Встановлює правила документування висновків для суду.
3	ISO/IEC 27043:2015 – Incident investigation principles and processes[38]	2015	Формує загальні принципи та етапи розслідування кіберінцидентів.	– Визначає послідовність етапів: підготовка, виявлення, збір, аналіз, документування, звітування. – Рекомендує координацію між технічними й правовими підрозділами. – Узгоджує дії під час реагування на кіберінциденти.
4	RFC 3227 – Guidelines for Evidence Collection and Archiving (IETF) [39]	2002	Технічне керівництво для збору та архівування цифрових доказів у мережевих системах.	– Визначає порядок збору даних під час кіберінцидентів. – Забезпечує принципи збереження цілісності доказів. – Містить рекомендації щодо пріоритетності джерел (RAM, журнали, файлові системи).

Агентство з кібербезпеки та безпеки інфраструктури США (CISA) є одним із ключових міжнародних джерел методичних матеріалів у сфері цифрової криміналістики та кіберзахисту [40].

CISA не є стандартом у формальному розумінні, однак її керівництва та практичні інструкції широко застосовуються як галузеві рекомендації. Вони включають:

- CISA Incident Response Playbooks – покрокові алгоритми дій під час кіберінцидентів;
- CISA Forensics Guidance – принципи збору, аналізу та збереження цифрових даних;
- Best Practices for Evidence Handling – рекомендації щодо зберігання носіїв, логів та артефактів системної діяльності;
- Guides for Collaboration with Law Enforcement – опис процесів взаємодії з правоохоронними органами при розслідуванні кіберзлочинів.

Документи CISA мають переважно прикладний характер і орієнтовані на оперативне реагування, що робить їх важливим доповненням до більш формалізованих стандартів ISO та NIST.

Серед міжнародних стандартів цифрової криміналістики важливе місце займає сертифікаційна програма SANS GIAC (Global Information Assurance Certification), яка підтверджує професійні знання та практичні навички фахівців у сфері розслідування кіберінцидентів [41].

GIAC, створена SANS Institute [42], стандартизує рівень кваліфікації експертів з цифрової криміналістики та реагування на інциденти. Основні сертифікати у напрямі цифрової криміналістики:

- GCFE – збір, збереження та аналіз цифрових доказів;
- GCFA – аналіз інцидентів безпеки та відновлення подій;
- GNFA – дослідження мережевого трафіку;
- GASF – криміналістика мобільних пристроїв.

Сертифікації GIAC узгоджуються з міжнародними стандартами ISO/IEC 27037 та NIST SP 800-86, сприяючи уніфікації методів цифрової криміналістики. Вони визнаються правоохоронними органами та приватними компаніями у США, ЄС та інших країнах, забезпечуючи практичну перевірку знань і достовірність результатів розслідувань.

1.3 Інструментарій цифрової криміналістики та сучасні підходи до їх застосування

Цифрова криміналістика, як комплексна дисципліна на межі права та інформаційних технологій, спирається на широкий набір інструментів і програмних засобів, призначених для виявлення, збору, аналізу, відновлення та документування цифрових доказів. В таблиці 1.5 наведено категорії інструментів цифрової криміналістики, їх приклади та сфери застосування.

Таблиця 1.5 – Класифікація інструментів цифрової криміналістики

№	Категорія інструментів	Призначення	Приклади	Основні можливості
1	Інструменти збору та збереження цифрових доказів	Виявлення, копіювання та збереження інформації без порушення цілісності даних	FTK Imager, EnCase Forensic, dd / dc3dd	Створення точних копій носіїв (disk imaging), підтримка принципу Chain of Custody
2	Інструменти аналізу цифрових артефактів	Дослідження файлових систем, реєстру, журналів, поштових клієнтів тощо	Autopsy / The Sleuth Kit, X-Ways Forensics, Magnet AXIOM	Аналіз структур дисків, збір артефактів із соцмереж, месенджерів, браузерів, відновлення дій користувача
3	Інструменти відновлення даних	Відновлення видалених або пошкоджених файлів і баз даних	R-Studio, Recuva, DMDE, UFS Explorer	Відновлення даних після видалення, форматування або пошкодження носія
4	Інструменти мережевої криміналістики	Виявлення, аналіз і реконструкція подій у мережевому середовищі	Wireshark, NetworkMiner, Xplico	Аналіз мережевого трафіку, реконструкція сесій, визначення джерела атаки
5	Інструменти мобільної криміналістики	Вилучення даних зі смартфонів, планшетів, SIM-карт, флеш-пам’яті	Cellebrite UFED, Oxygen Forensic Suite, MOBILedit Forensic Express	Аналіз дзвінків, чатів, геолокацій, історії браузера
6	Інструменти аналізу шкідливого ПЗ	Дослідження заражених систем, виконуваних файлів, поведінки шкідливого ПЗ	IDA Pro, Ghidra, Cuckoo Sandbox, Volatility	Декомпіляція, динамічний аналіз, аналіз пам’яті
7	Інструменти для звітування	Формування структурованих звітів для судових або адміністративних органів	Belkasoft Evidence Center, FTK, EnCase	Автоматичне створення звітів, експорт у PDF, HTML, збереження структури доказів

Інтелектуальні експертні системи та системи підтримки розслідувань посідають особливе місце серед інструментів цифрової криміналістики, адже вони належать радше до правової, ніж технічної площини. На відміну від класичних засобів, що безпосередньо досліджують цифрові докази, ці системи не здійснюють технічного аналізу носіїв чи даних. Їх головне завдання – підтримка процесу розслідування, допомога експертам та слідчим у прийнятті рішень, інтерпретації результатів, оцінці доказів і формуванні правових висновків.

Такі програмні рішення базуються на законах, стандартах, знаннях експертів, логічних правилах і базах прецедентів, що дозволяє моделювати хід розслідування, перевіряти гіпотези та прогнозувати можливі сценарії подій. Таким чином, інтелектуальні експертні системи та системи підтримки розслідувань виступають важливим інструментом інтеграції цифрової криміналістики з юридичними аспектами розслідування, підвищуючи обґрунтованість і ефективність прийнятих рішень.

Правові та нормативні експертні системи призначені для забезпечення доступу до законодавчих актів, коментарів, судової практики та нормативних документів. Вони допомагають слідчим і експертам швидко зіставляти ознаки злочину з відповідними статтями закону та застосовувати прецеденти. Такі інструменти дозволяють автоматизувати пошук законодавчих норм, оцінювати ознаки правопорушення та пропонують, які статті Кримінального кодексу можуть бути застосовані у конкретному випадку. Приклади таких систем наведені в таблиці 1.6.

Системи підтримки розслідувань допомагають організувати, відстежувати та координувати розслідування кримінальних справ. Вони інтегрують дані з різних джерел, дозволяють будувати логіку подій і взаємозв’язки між учасниками, а також підтримують планування дій слідчого. Такі інструменти забезпечують ефективне управління справами, ведення електронних досьє та побудову аналітичних моделей злочинів. Приклади таких систем наведені в таблиці 1.7.

Таблиця 1.6 – Правові та нормативні експертні системи

Приклад системи	Призначення
LexisNexis / Westlaw / LIGA:ZAKON (Україна)	Пошук законодавства, судової практики, коментарів до нормативних актів
Caselex / Juris	Пошук схожих справ і застосування правових прецедентів
Експертні системи кримінального права (академічні прототипи)	Аналіз ознак діяння та пропозиція відповідних статей КК

Таблиця 1.7 – Системи підтримки розслідувань

Приклад системи	Призначення
COPLINK	Аналітична система для поліції США; поєднує дані з різних джерел і підказує напрями розслідування
i2 Analyst’s Notebook	Аналіз зв’язків між учасниками злочину, побудова сценаріїв подій
NICE Investigate / IBM iBase	Керування повним циклом розслідування – від фіксації події до судового розгляду
Crime Scene Management Software	Фіксація місця події, побудова карти слідів, контроль послідовності дій

Інтелектуальні та експертні системи це програми, що використовують технології штучного інтелекту та моделі знань для надання рекомендацій або прийняття рішень у процесі розслідування. Вони можуть працювати на основі правил (rule-based), статистичних моделей (Bayesian) або сучасних підходів машинного навчання. Такі системи допомагають аналізувати ознаки злочину, прогнозувати розвиток подій, виявляти зв’язки між підозрюваними, а також моделювати ситуації на місці події. Приклади таких систем наведені в таблиці 1.8.

Процедурні довідники та шаблони надають стандартизовані інструкції, алгоритми дій і шаблони документів, необхідні для правильного проведення розслідування. Вони допомагають дотримуватися процесуальних вимог і послідовності дій під час огляду місця події, збору доказів, проведення експертиз і складання звітів. Такі рішення можуть бути реалізовані у вигляді цифрових посібників, чек-листів або інтерактивних систем. Приклади таких систем наведені в таблиці 1.9.

Таблиця 1.8 – Інтелектуальні та експертні системи

Приклад системи	Призначення
Rule-based Expert Systems (прототипи)	Аналіз ознак злочину і рекомендація потенційних статей Кримінального кодексу
Bayesian & AI Models	Побудова логічних імовірнісних моделей для відновлення послідовності подій
Virtual Crime Scene Simulators	Імітація місця події для навчання та підтримки дій слідчого в реальних умовах

Таблиця 1.9 – Процедурні довідники та шаблони

Приклад системи	Призначення
Checklists for Investigators	Покроковий порядок дій на місці події (фіксація, фото, збір відбитків, опитування свідків)
Standard Operating Procedures (SOPs)	Цифрові системи, які ведуть слідчого через етапи розслідування
AI-guided assistants	Інтелектуальні помічники, що інтегрують законодавство, SOP і практику; підказують, які статті КК враховувати, які докази зібрати та які експертизи призначити

Розвиток технологій штучного інтелекту (ШІ) суттєво впливає на еволюцію цифрової криміналістики, відкриваючи нові можливості для автоматизації, прискорення та підвищення точності розслідувань кіберзлочинів. В умовах постійного зростання обсягів цифрових даних ШІ стає ключовим інструментом, що дозволяє виявляти закономірності, встановлювати приховані зв’язки між подіями та прогнозувати дії зловмисників.

Найбільш перспективними напрямами використання є машинне навчання, обробка природної мови, інтелектуальні системи підтримки рішень і технології візуалізації даних (табл. 1.10).

Таблиця 1.10 – Перспективи застосування ШІ у цифровій криміналістиці

Напрям	Приклад застосування	Очікуваний ефект
Машинне навчання	Класифікація кіберінцидентів, виявлення аномалій, аналіз трафіку	Підвищення точності та швидкості аналізу доказів
NLP (обробка природної мови)	Аналіз електронної переписки, логів, звітів	Виявлення загроз, автоматичне вилучення ключових даних
Експертні системи	Rule-based системи підтримки рішень	Рекомендації для слідчих та експертів
Візуалізація та реконструкція	3D-моделі подій, відтворення мережевих процесів	Зрозуміла презентація доказів для суду

Попри значний потенціал, використання ШІ у цифровій криміналістиці стикається з низкою викликів. Найсуттєвішими серед них є обмежений доступ до реальних криміналістичних даних, відсутність уніфікованих наборів для навчання, а також етичні та правові бар'єри (табл. 1.11).

Таблиця 1.11 – Основні проблеми застосування ШІ у цифровій криміналістиці

Проблема	Суть проблеми	Наслідки
Обмежений доступ до реальних даних	Криміналістичні матеріали конфіденційні	Неможливість навчання моделей на реалістичних кейсах
Відсутність уніфікованих датасетів	Дані не стандартизовані, охоплюють лише окремі сценарії	Низька узагальнювальна здатність моделей
Етичні та юридичні ризики	Порушення конфіденційності або прав осіб	Неможливість легітимного використання результатів
Технічні обмеження	Overfitting, bias, помилкові спрацьовування	Ненадійність аналітичних висновків

Для подолання зазначених труднощів дослідники пропонують створення безпечних механізмів обміну даними, розробку стандартів анонімізації, а також використання нових підходів до навчання моделей (табл. 1.12).

Таким чином, інтеграція штучного інтелекту у цифрову криміналістику має значний потенціал для підвищення ефективності розслідувань. Водночас її успішна реалізація потребує збалансування між технічними можливостями, правовими обмеженнями та етичними принципами.

Таблиця 1.12 – Можливі шляхи вирішення проблем

Рішення	Суть підходу	Потенційний результат
Генерація синтетичних даних (GANs, симуляції)	Створення штучних даних, подібних до реальних кейсів	Забезпечення конфіденційності при навчанні моделей
Федеративне навчання	Моделі навчаються без передачі самих даних	Збереження приватності та підвищення точності
Міжсекторальна співпраця	Обмін даними між державою, наукою та бізнесом	Розширення доступу до репрезентативних даних
Стандарти анонімізації	Розробка правових і технічних норм	Законне використання криміналістичних даних у дослідженнях

Автоматизація процесів цифрової криміналістики розглядається як необхідний етап еволюції галузі, що має забезпечити підвищення ефективності, швидкості та об’єктивності розслідувань. Водночас упровадження автоматизованих систем і алгоритмів у криміналістичну практику супроводжується низкою суттєвих проблем – як технічних, так і організаційно-правових.

Однак упровадження автоматизованих систем супроводжується низкою проблем технічного, організаційного та правового характеру. Вони стосуються як обмежень самих алгоритмів, так і питань безпеки, верифікації результатів і підготовки фахівців (табл. 1.13).

Отже, автоматизація процесів криміналістичного аналізу має значний потенціал підвищення ефективності розслідувань, але потребує комплексного вирішення ряду проблем – від забезпечення якості даних і прозорості алгоритмів до створення нормативно-правової бази для їх офіційного використання. Тільки за умови дотримання принципів надійності, відтворюваності та безпеки автоматизовані рішення можуть стати повноцінним інструментом у цифровій криміналістиці.

Таблиця 1.13 – Основні проблеми автоматизації цифрової криміналістики

№	Проблема	Суть	Наслідки
1	Обмеженість універсальних алгоритмів	Кожне розслідування має унікальний контекст і тип даних	Ризик хибних висновків у нетипових випадках
2	Якість і достовірність вхідних даних	Неавтентичні або спотворені артефакти призводять до помилок	Неправильні результати аналізу, вплив на судові рішення
3	Відсутність стандартизації	Алгоритми працюють як «чорні скриньки» без пояснення логіки	Труднощі верифікації та прийняття результатів судом
4	Нестача навчальних і тестових даних	Реальні дані недоступні через конфіденційність і правові обмеження	Зниження точності моделей і достовірності висновків
5	Загроза кібербезпеці автоматизованих систем	Системи можуть стати об’єктом атак або підміни даних	Компрометація результатів аналізу
6	Недостатня кваліфікація фахівців	Робота з автоматизованими платформами вимагає нових знань	Потреба у спеціальній підготовці кадрів

1.4 Постановка завдання

Проведений аналіз джерел за темою засвідчив, що кіберзлочини мають виражений міждисциплінарний характер, у межах якого поєднуються технічні, правові та криміналістичні аспекти. Така особливість обумовлює істотну проблему: фахівці, відповідальні за розслідування кримінальних правопорушень, нерідко не володіють достатніми знаннями щодо технічного функціонування комп'ютерних систем і технологій, тоді як експерти з інформаційної безпеки та цифрових технологій часто не мають належного розуміння юридичних вимог і кваліфікуючих ознак складів злочину. Внаслідок цього формування правильної криміналістичної оцінки діяння є складним та ресурсоємним процесом, що потребує залучення широкого кола спеціалістів.

Аналіз нормативно-правових актів показав, що законодавче визначення кіберзлочинів у Кримінальному кодексі України подається в абстрактній формі, без конкретизації технічних умов та проявів правопорушення. Це призводить до того, що відповідні норми є малозрозумілими для осіб без юридичної освіти, ускладнюючи кваліфікацію інцидентів на ранніх етапах. Додатково виявлено розрив між правовими вимогами та практичними методами роботи з цифровими доказами: більшість сучасних інструментів цифрової криміналістики є зорієнтованими виключно на технічний аналіз – вилучення даних, дослідження артефактів, відновлення інформації, ідентифікацію мережевої активності тощо.

Таким чином, у сфері цифрової криміналістики наявним є дефіцит інтелектуальних систем, здатних забезпечити інтеграцію юридичних знань і технічних особливостей кіберзлочинів, спростити процес криміналістичної інтерпретації ознак правопорушення та підтримати ухвалення рішень слідчими та експертами. Вказане обґрунтовує потребу у створенні програмних рішень, що забезпечуватимуть автоматизований аналіз складу злочину на основі текстових описів та сприятимуть підвищенню ефективності розслідування кіберзлочинів.

В другому розділі магістерської роботи варто здійснити такі наукові розвідки: розробити теоретико-множинну модель програмного асистента

фахівця з криміналістичного аналізу кіберзлочинів, розробити архітектуру програмного асистента фахівця з криміналістичного аналізу кіберзлочинів, розробити моделі процесів та алгоритми їх реалізації для програмного асистента фахівця з криміналістичного аналізу кіберзлочинів.

В третьому розділі магістерської роботи варто здійснити такі наукові розвідки: обґрунтувати засоби розробки програмного асистента фахівця з криміналістичного аналізу кіберзлочинів, реалізувати програмний застосунок, протестувати та оцінити розроблений програмний застосунок.

В четвертому розділі варто здійснити такі наукові розвідки: обґрунтувати економічну доцільність розробки та впровадження програмного асистента фахівця з криміналістичного аналізу кіберзлочинів.

2 МОДЕЛЬ ПРОГРАМНОГО АСИСТЕНТА ФАХІВЦЯ З КРИМІНАЛІСТИЧНОГО АНАЛІЗУ КІБЕРЗЛОЧИНІВ

2.1 Теоретико-множинна модель програмного асистента фахівця з криміналістичного аналізу кіберзлочинів

У контексті поставленого завдання розроблювана система передбачає комплексну взаємодію користувача із програмним забезпеченням через графічний інтерфейс, що забезпечує доступ до довідкових розділів та чатового функціоналу. Для ефективної роботи система використовує базу даних, в якій зберігається довідкова інформація, історія повідомлень та профілі користувачів. Введені користувачем текстові запити проходять обробку на рівні природної мови, після чого передаються алгоритмам штучного інтелекту для генерації відповідей. Взаємозв’язки між користувачем, інтерфейсом, даними, мовними об’єктами та алгоритмами моделюються через чітко визначені функції і відношення, що забезпечує послідовність обробки інформації та коректність роботи системи.

Згідно з поставленим завданням система повинна мати такі компоненти:

1. Користувачі (U) – множина користувачів, які взаємодіють із програмним забезпеченням. Кожен користувач може виконувати певні дії: перегляд довідкової інформації, надсилання запитів до системи, отримання відповідей у чаті.
2. Інтерфейс (I) – множина елементів графічного інтерфейсу, за допомогою яких користувач здійснює взаємодію із системою. До інтерфейсу входять: кнопки переходу до довідкових розділів, поле введення повідомлення, вікно чату для відображення діалогу.
3. Дані (D) – множина інформаційних об’єктів, що зберігаються в базі даних. Вона охоплює довідкову інформацію, історію чатів, користувацькі профілі та службові записи.

4. Мовні об’єкти (L) – множина текстових запитів користувача та відповідей системи, представлених у вигляді природної мови. Цей компонент використовується для обміну інформацією між користувачем і ШІ-моделлю.

5. Алгоритми (A) – множина процедур і процесів, які реалізують функціонування системи. Сюди належать алгоритми обробки подій інтерфейсу, алгоритми обробки природної мови, генерації відповідей і роботи з базою даних.

6. Функції взаємодії (F) – множина відображень, які описують взаємозв’язки між компонентами системи, зокрема передачу інформації від користувача до моделі та назад.

7. Відношення (R) – множина відношень між компонентами, які відображають логічні зв’язки між користувачем, інтерфейсом, даними та алгоритмами системи.

Тоді теоретико-множинна модель застосунку буде мати такий вигляд:

$$S = \langle U, I, D, L, A, F, R \rangle , \tag{2.1}$$

де S – система програмного засобу;
U – множина користувачів системи;
I – множина елементів інтерфейсу користувача;
D – множина даних, що зберігаються та обробляються у системі;
L – множина мовних об’єктів (запити й відповіді);
A – множина алгоритмів, що забезпечують функціонування застосунку;
F – множина функцій взаємодії між компонентами;
R – множина відношень між основними множинами системи;

Основні функції взаємодії між компонентами можна визначити таким чином:

$$\begin{cases} f_1 : U \times I \rightarrow E, & \text{(взаємодія користувача з інтерфейсом)} \\ f_2 : E \rightarrow D, & \text{(подія створює або змінює дані)} \\ f_3 : D \rightarrow L, & \text{(дані подаються у мовній формі)} \\ f_4 : L \rightarrow A, & \text{(мовні об’єкти обробляються алгоритмами)} \\ f_5 : A(L) \rightarrow D, & \text{(результати роботи алгоритмів зберігаються в базі даних)} \end{cases}$$

Таким чином, система S описує повний цикл функціонування застосунку – від дій користувача через інтерфейс до генерації відповіді штучним інтелектом і збереження результатів у базі даних.

2.2 Архітектура програмного асистента фахівця з криміналістичного аналізу кіберзлочинів

На основі теоретико-множинної моделі можна визначити ключові блоки програмного асистента фахівця з криміналістичного аналізу кіберзлочинів, які забезпечують його функціонування та взаємодію між користувачем, даними та алгоритмами обробки інформації:

1. Інтерфейс користувача забезпечує зручну графічну взаємодію користувача із застосунком. Він містить кнопки для доступу до довідкових розділів, поле для введення повідомлень та вікно чату для відображення відповідей. Через інтерфейс користувач ініціює події, такі як натискання кнопок або надсилання повідомлень, а також отримує результати обробки, що надсилаються логічним модулем.

2. Логічний модуль виступає центральним контролером системи, координуючи всі процеси та взаємодію між блоками. Він обробляє події від користувача, визначає подальші дії, звертається до модуля обробки мовлення для підготовки запитів до модуля ШІ та отримує відповіді, які відображаються у чаті. Крім того, логічний модуль забезпечує двосторонню взаємодію з базою даних для збереження і отримання інформації, включаючи довідкові матеріали.

3. Модуль обробки мовлення відповідає за перетворення введеного користувачем тексту на структуровані дані, зрозумілі для моделі ШІ. Він виконує нормалізацію тексту, виділення ключових слів та аналіз намірів користувача. Модуль забезпечує проміжний рівень між логікою застосунку та модулем ШІ, передаючи структуровані запити для генерації відповідей.

4. Модуль штучного інтелекту генерує відповіді на основі оброблених запитів користувача. Він отримує структуровані дані від модуля обробки мовлення та створює змістовну текстову відповідь, яку передає назад у логіку застосунку для відображення у чаті. Модуль ШІ не взаємодіє безпосередньо з інтерфейсом або базою даних, його робота ізольована через логічний модуль та модуль обробки мовлення.

5. База даних слугує сховищем довідкової інформації. Вона забезпечує двосторонню взаємодію з логікою застосунку, надаючи необхідні дані для обробки запитів та зберігаючи результати роботи системи. База даних не взаємодіє безпосередньо з іншими блоками, всі запити проходять через логічний модуль.

Описані взаємодії між блоками структури програмного асистента фахівця з криміналістичного аналізу кіберзлочинів відображені на UML-діаграмі взаємодії на рисунку 2.1.

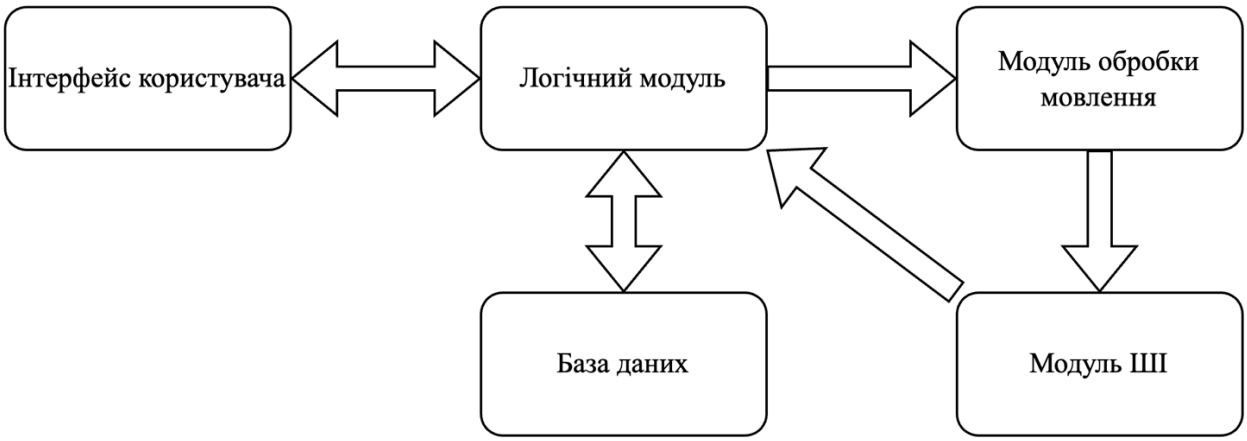


Рисунок 2.1 – UML-діаграма взаємодії складових програмного асистента фахівця з криміналістичного аналізу кіберзлочинів

2.3 Моделі процесів та алгоритми їх реалізації для програмного асистента фахівця з криміналістичного аналізу кіберзлочинів

Відповідно до теоретико-множинної моделі, було розроблено моделі процесів, які відображають роботу системи на різних рівнях абстракції. Моделі процесів описують взаємодію користувача з інтерфейсом, обробку запитів у логіці застосунку, обробку природної мови модулем обробки мовлення, генерацію відповідей моделлю штучного інтелекту та взаємодію з базою даних. Такий підхід дозволяє формалізовано представити послідовність дій та потоки інформації між усіма складовими системи.

UML-діаграма активності процесу обробки запитів користувача (рисунок 2.2) відображає послідовність дій користувача та системи при взаємодії з застосунком. На діаграмі показано, як користувач вводить запит або обирає довідковий розділ, як подія обробляється логічним модулем, надсилається на обробку модулем мовлення, передається у модуль ШІ для генерації відповіді та повертається назад у чатове вікно для відображення користувачу. Діаграма активності демонструє деталі внутрішніх процесів і логіку переходів між різними станами системи.

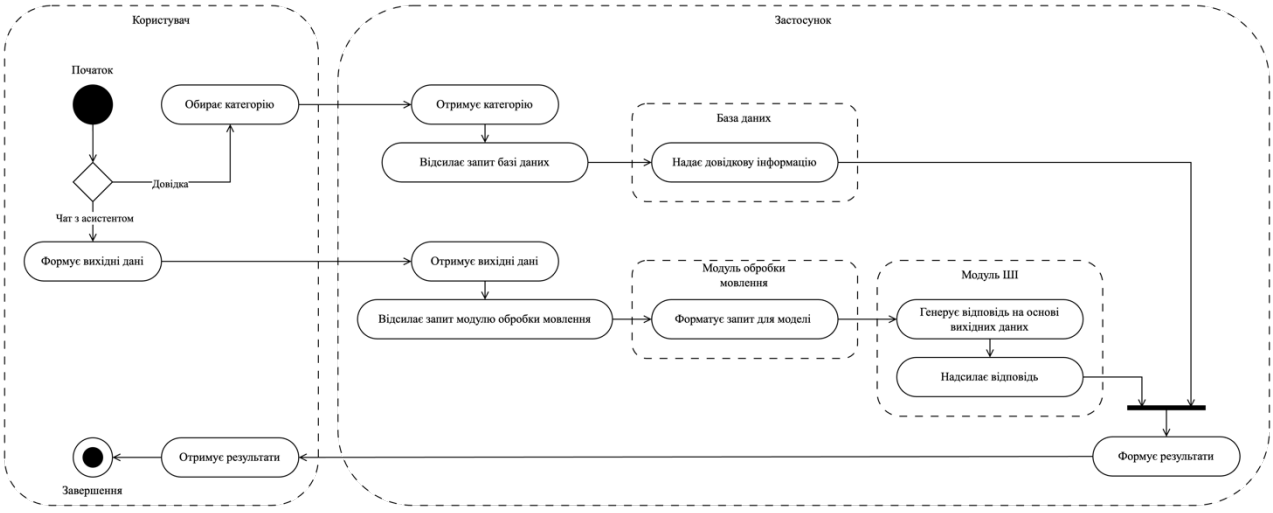


Рисунок 2.2 – UML-діаграма активності процесу обробки запитів користувача

UML-діаграма послідовності для запиту довідки і запиту в чат (рисунок 2.3-2.4) показує часову послідовність взаємодії між блоками системи. На діаграмі відображено, як логіка застосунку отримує події від інтерфейсу користувача, надсилає запити до модулю обробки мовлення та модулю ШІ, отримує результати і передає їх у інтерфейс. Діаграма послідовності дозволяє наочно побачити порядок викликів функцій, обмін повідомленнями між блоками та затримки у процесі обробки запиту.

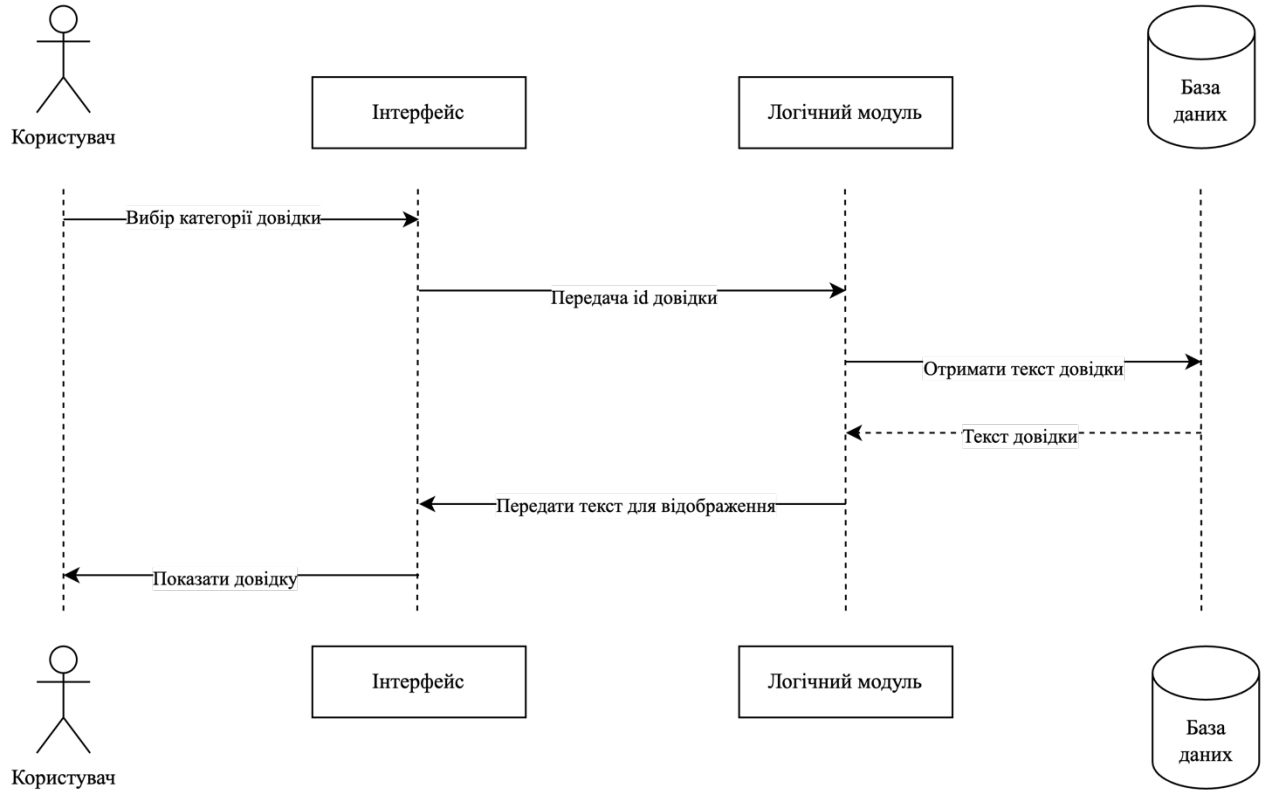


Рисунок 2.3 – UML-діаграма послідовності для запиту довідки

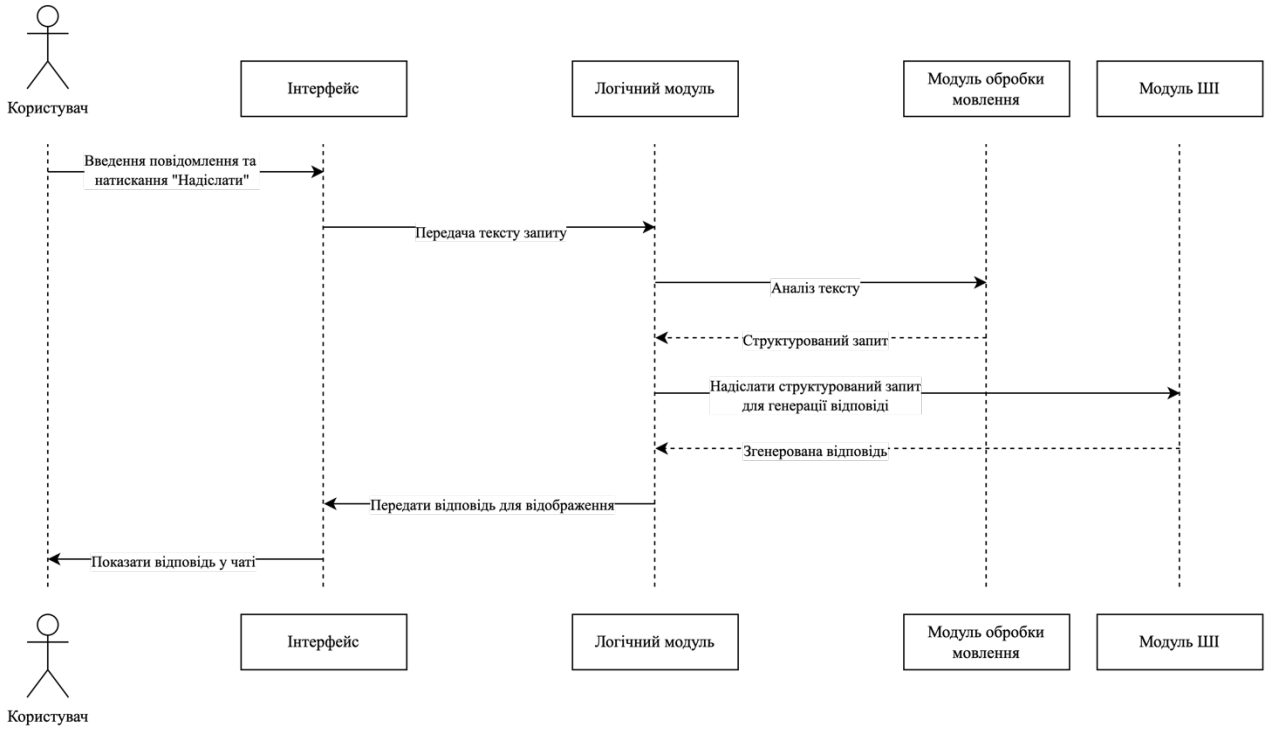


Рисунок 2.4 – UML-діаграма послідовності для запиту в чат

UML-діаграма потоків даних (рисунок 2.5) демонструє передачу інформації між блоками системи. Загальна діаграма потоків даних (рисунок 2.5 а).) відображає всі компоненти: користувача, інтерфейс, логічний модуль, модуль мовлення, модуль ШІ та базу даних, а також потоки інформації між ними. Діаграма потоків даних для чату (рисунок 2.5 б).) показує обробку текстових запитів користувача, передачу їх через модуль обробки мовлення до модуля ШІ та повернення відповідей у інтерфейс. Діаграма потоків даних для довідки (рисунок 2.5 в).) ілюструє, як запит на отримання довідкового матеріалу обробляється логічним модулем та отримується з бази даних для відображення користувачу.

Завдяки представленим моделям процесів можна детально описати логіку роботи системи, взаємозв’язки між її компонентами та послідовність обробки даних від ініціації користувачем до отримання результату.

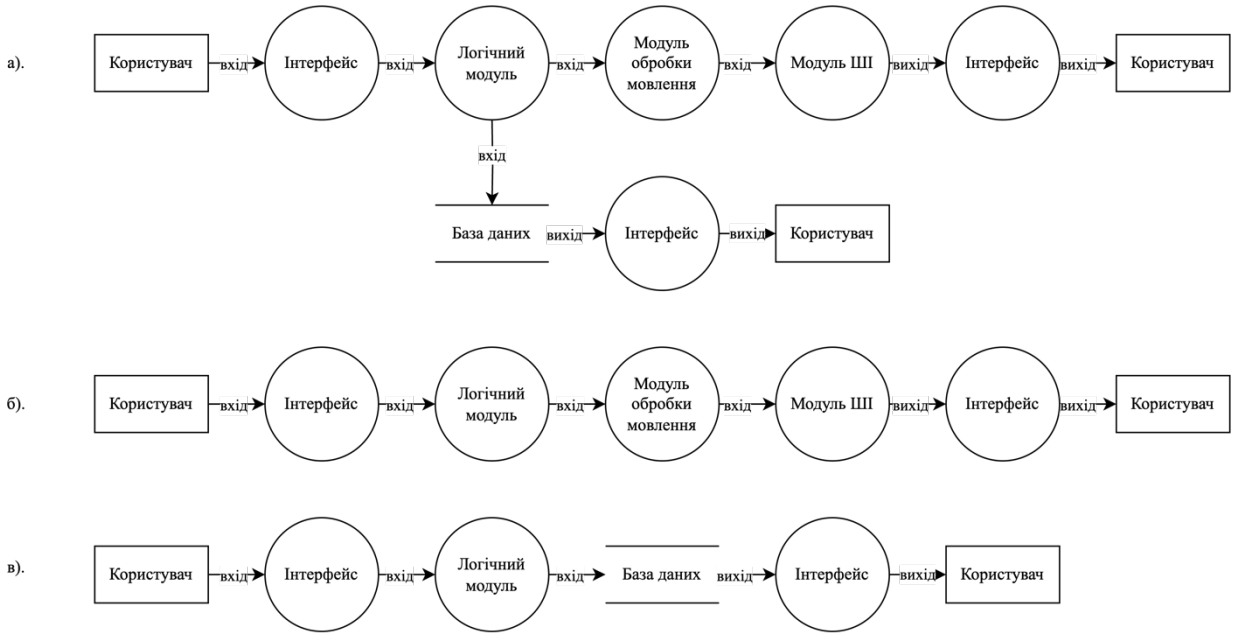


Рисунок 2.5 – UML-діаграма потоків даних а). загальна, б). для запиту в чат, в). для запиту довідки

На основі розроблених моделей процесів та визначених блоків системи, для забезпечення зручності та інтуїтивності роботи з застосунком були сформовані основні алгоритми, які описують ключові сценарії взаємодії користувача з системою. Кожен алгоритм демонструє послідовність дій і обмін інформацією між компонентами системи.

Алгоритм запуску застосунку описує послідовність дій від моменту запуску програми до готовності інтерфейсу до взаємодії з користувачем (рис. 2.6). Він включатиме такі кроки:

Крок 1. Запуск головного вікна програми

Крок 2. Ініціалізувати з’єднання з базою даних та моделлю

Крок 3. Вивести інтерфейс користувача

Схему алгоритму запуску застосунку зображено на рисунку 2.5.

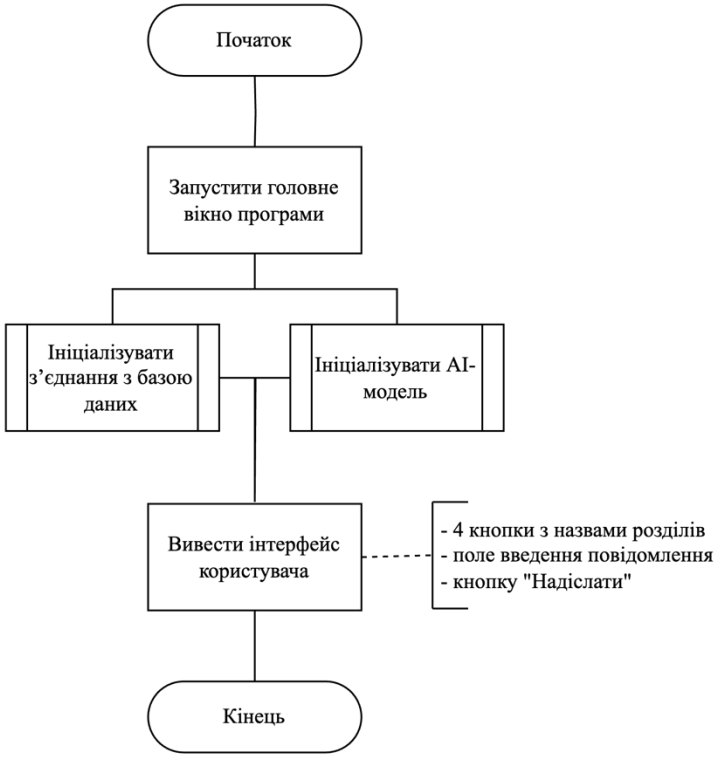


Рисунок 2.6 – Схема алгоритму запуску застосунку

Алгоритм запиту довідки демонструє процес обробки запиту на довідкову інформацію (рис. 2.7). Він включатиме такі кроки:

Крок 1. Отримання id розділу довідки

Крок 2. Якщо id = 0, перехід до кроку 3. Якщо id = 1, перехід до кроку 5. Якщо id = 2, перехід до кроку 7. Якщо id = 3, перехід до кроку 9.

Крок 3. Виконання запиту до БД по інформації за розділом 1

Крок 4. Отримання результатів і перехід до кроку 11.

Крок 5. Виконання запиту до БД по інформації за розділом 2

Крок 6. Отримання результатів і перехід до кроку 11.

Крок 7. Виконання запиту до БД по інформації за розділом 3

Крок 8. Отримання результатів і перехід до кроку 11.

Крок 9. Виконання запиту до БД по інформації за розділом 4

Крок 10. Отримання результатів і перехід до кроку 11.

Крок 11. Відображення результатів у вікні

Схема алгоритму обробки запиту довідки зображена на рисунку 2.6.

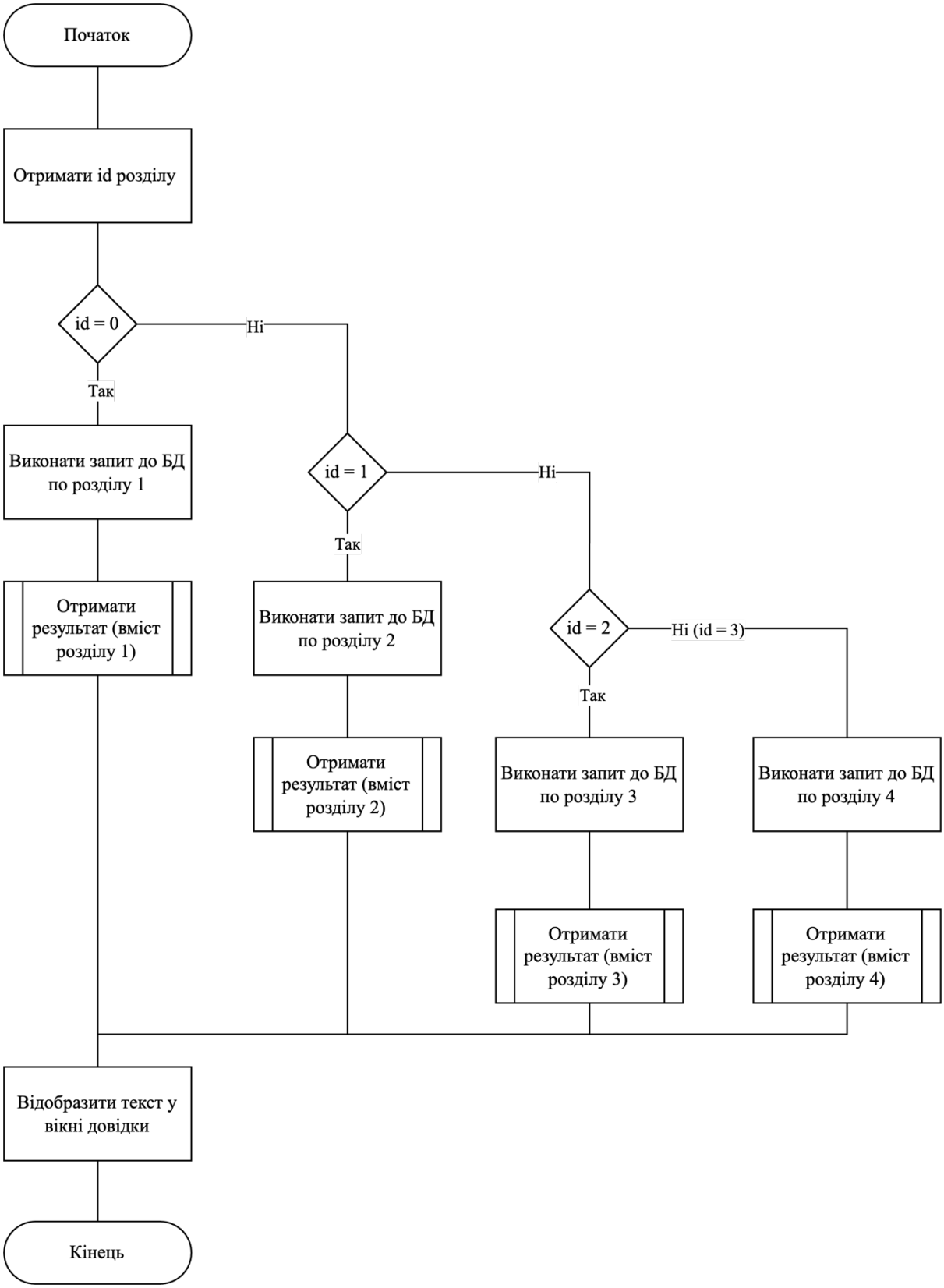


Рисунок 2.7 – Схема алгоритму запиту довідки

Алгоритм запиту в чаті відображає процес обробки текстових повідомлень користувача у чаті (рис. 2.8). Він включатиме такі кроки:

Крок 1. Отримання тексту повідомлення з поля

Крок 2. Якщо поле містить текст перехід до кроку 4, якщо ні – до кроку 3

Крок 3. Відображення повідомлення про необхідність введення повідомлення і перехід до кроку 1

Крок 4. Збереження повідомлення в БД

Крок 5. Відображення повідомлення в чаті і передача його до модуля обробки мовлення

Крок 6. Форматування повідомлення

Крок 7. Формування запиту до моделі ШІ

Крок 8. Отримання відповіді від моделі ШІ

Крок 9. Відображення повідомлення в вікні чату

Крок 10. Якщо користувач ввів нове повідомлення перехід до кроку 1, якщо ні – завершення.

Схема алгоритму обробки запиту в чаті зображена на рисунку 2.7.

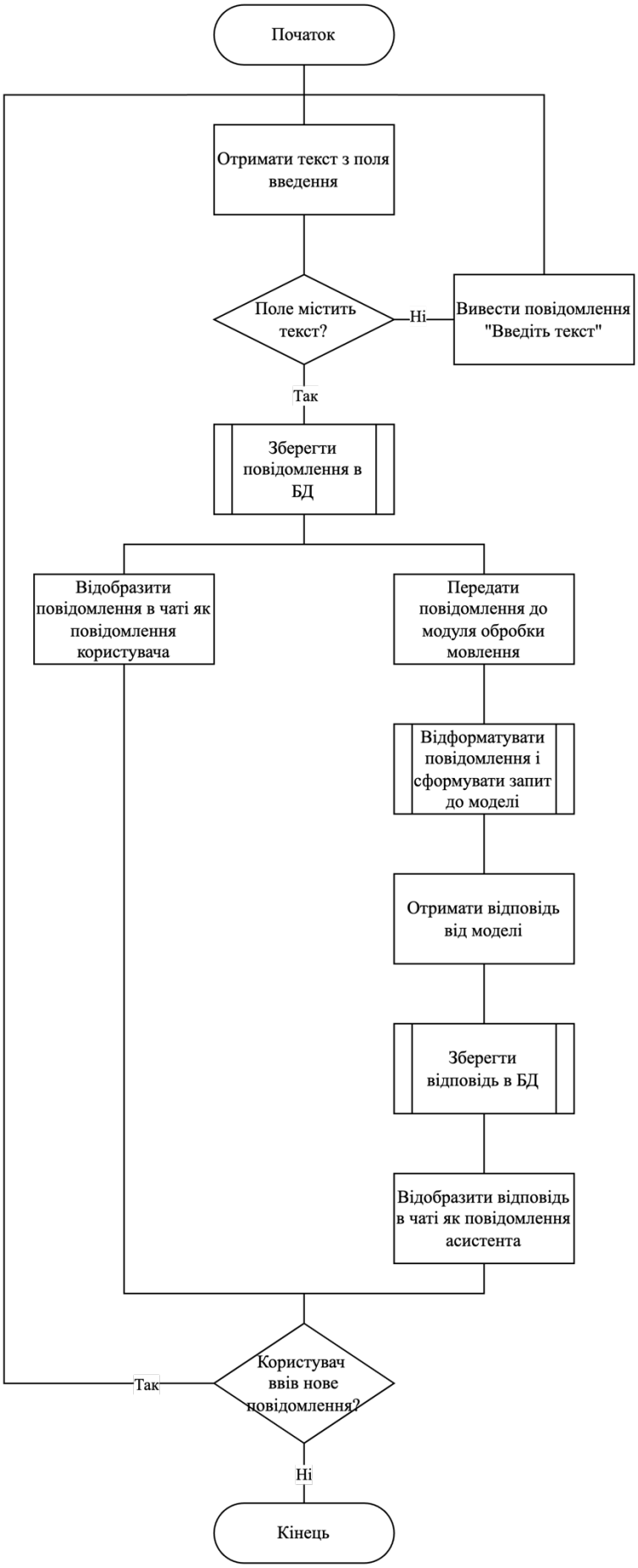


Рисунок 2.8 – Схема алгоритму запиту в чат

Детальний алгоритм генерування відповіді показує внутрішній процес формування відповіді на запит користувача (рис. 2.9). Він включатиме наступні кроки:

Крок 1. Отримання вхідного повідомлення користувача

Крок 2. Передавання повідомлення в модуль обробки мовлення

Крок 3. Проведення попередньої обробки повідомлення

Крок 4. Визначення ключових характеристик

Крок 5. Передача характеристик до моделі

Крок 6. Якщо характеристика «intent» визначена – перехід до кроку 7. Якщо характеристика «intent» невизначена – перехід до кроку 9. В інакших випадках перехід до кроку 11

Крок 7. Пошук відповідних даних в базі знань за ключовими словами

Крок 8. Формування відповіді і перехід до кроку 12

Крок 9. Виведення помилки яка зазначає що запит користувача недостатньо зрозумілий

Крок 10. Пропозиція уточнити або перефразувати запит

Крок 11. Виведення помилки яка зазначає що запит не підтримується системою

Крок 12. Передача результатів в логіку застосунку

Схема детального алгоритму генерування відповіді зображена на рисунку 2.8.

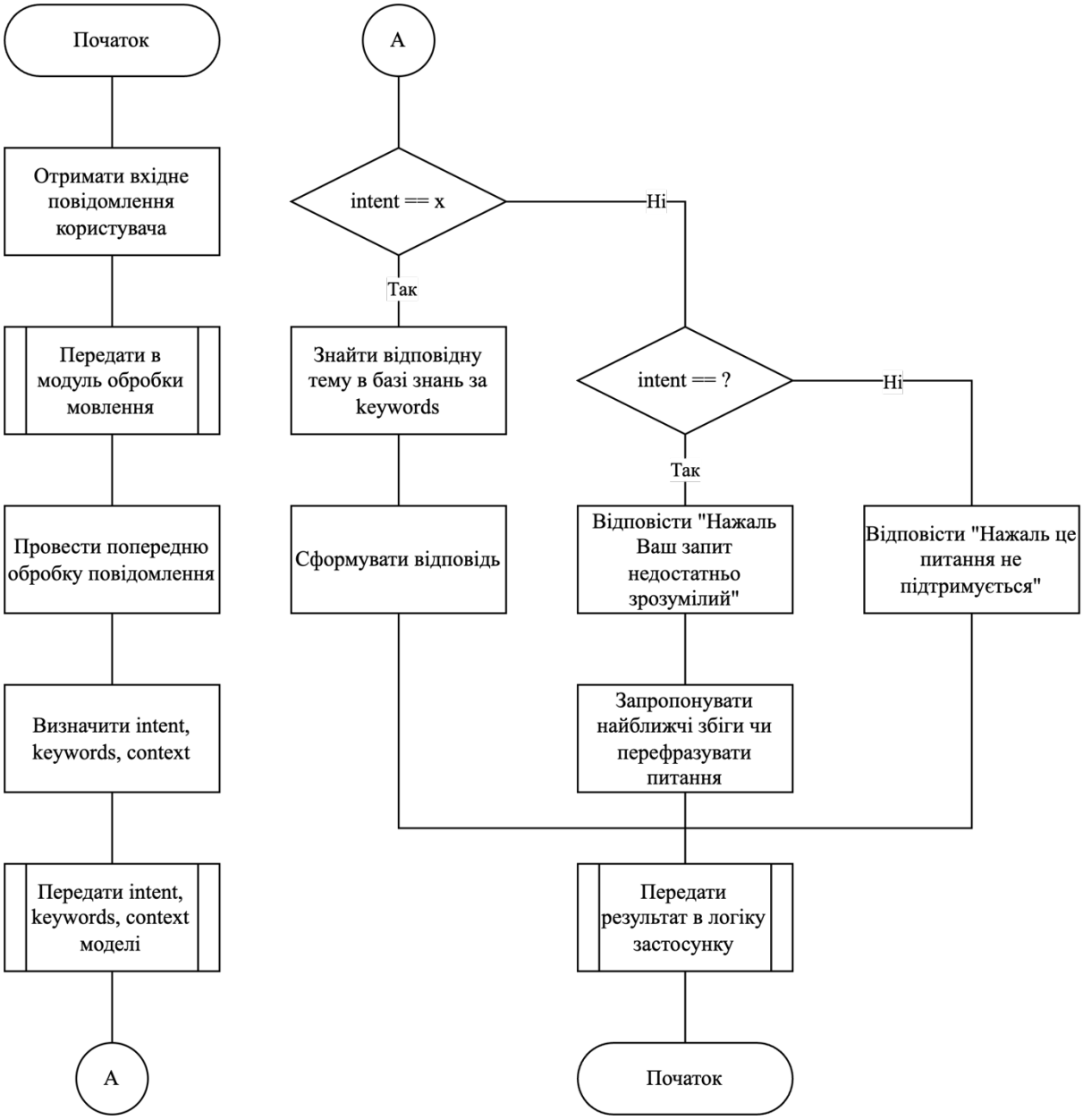


Рисунок 2.9 – Схема детального алгоритму генерування відповіді

Алгоритм завершення роботи описує процедуру коректного завершення роботи застосунку. Він включатиме такі кроки:

Крок 1. Закриття всіх активних з’єднань з БД та звільнення ресурсів моделі

Крок 2. Закриття вікна застосунку

Схема алгоритму завершення роботи зображена на рисунку 2.10.

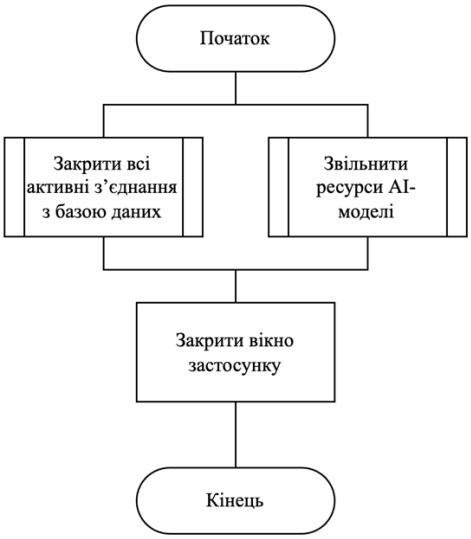


Рисунок 2.10 – Схема алгоритму завершення роботи

Висновки до розділу 2

У даному розділі було проведено комплексне теоретичне та практичне обґрунтування підходів до розробки програмного асистента фахівця з криміналістичного аналізу кіберзлочинів.

Було розроблено теоретико-множинну модель застосунку, що формалізує взаємозв'язки між користувачем, модулями системи та базами даних. Це дозволило визначити логічну структуру функціональних елементів і межі їхньої взаємодії.

Створено структуру програмного комплексу, яка включає інтерфейс користувача, логічний модуль, базу даних, модуль обробки мовлення та модуль штучного інтелекту. Таке структурування забезпечує модульність, розширюваність і гнучкість системи.

Також було розроблено моделі та алгоритми основних процесів, що описують послідовність дій системи під час взаємодії з користувачем, обробки запитів та надання рекомендацій.

Отже, результати даного розділу створюють науково та технічно обґрунтований фундамент для реалізації програмного асистента на наступних етапах розробки.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ПРОГРАМНОГО АСИСТЕНТА ФАХІВЦЯ З КРИМІНАЛІСТИЧНОГО АНАЛІЗУ КІБЕРЗЛОЧИНІВ

3.1 Обґрунтування засобів розробки програмного асистента фахівця з криміналістичного аналізу кіберзлочинів

Для розробки програмного асистента фахівця з криміналістичного аналізу кіберзлочинів було розглянуто три мови програмування: Python, C++ та C#. Кожна з них має свої переваги та сфери оптимального застосування.

Python – це високорівнева інтерпретована мова програмування з простою та зрозумілою синтаксичною структурою [43]. Вона підтримує об’єктно-орієнтоване, процедурне та функціональне програмування. Python має велику кількість бібліотек для роботи з даними, штучним інтелектом, кібербезпекою та криміналістикою (наприклад, scikit-learn, pandas, numpy, matplotlib, pytsk3, Volatility). Завдяки цьому Python широко використовується у цифровій криміналістиці, аналізі мережевих даних і створенні інтелектуальних систем підтримки прийняття рішень.

C++ – це компільована мова програмування, відома своєю швидкодією, ефективним керуванням пам’яттю та можливістю розробки системного програмного забезпечення [44]. Вона підходить для створення високопродуктивних рішень, проте вимагає значно більших витрат часу на розробку, налагодження та тестування. Для завдань, пов’язаних із аналітикою даних або розробкою інтерфейсів, використання C++ може бути надмірно складним.

C# – це мова програмування, створена компанією *Microsoft*, орієнтована на розробку застосунків у середовищі .NET [45]. Вона має сучасний синтаксис, підтримує об’єктно-орієнтований підхід, добре інтегрується з Windows і базами даних. Проте C# менш зручний для роботи з аналітичними бібліотеками, машинним навчанням або криміналістичними інструментами, ніж Python.

Порівняння характеристик мов програмування наведено в таблиці 3.1.

Таблиця 3.1 – Порівняння характеристик мов програмування

Характеристика	Python	C++	C#
Тип	Інтерпретована, високорівнева	Компільована, високопродуктивна	Компільована, високорівнева
Простота синтаксису	Висока	Низька	Середня
Швидкодія	Середня	Висока	Висока
Портативність	Висока	Висока	Середня (переважно Windows)
Підтримка бібліотек для аналізу даних	Дуже висока	Обмежена	Обмежена
Робота з базами даних	Добра	Складна	Добра
Підтримка штучного інтелекту	Широка	Обмежена	Помірна
Застосування у криміналістиці	Дуже поширене	Рідкісне	Обмежене

Для реалізації програмного асистента було обрано Python, оскільки ця мова:

1. Має велику кількість готових бібліотек для криміналістичного аналізу, обробки даних, машинного навчання та автоматизації процесів.

2. Забезпечує швидку розробку прототипів і скорочує час налагодження коду завдяки простому синтаксису.

3. Підтримується в більшості середовищ розробки, зокрема Visual Studio Code, що полегшує інтеграцію з інструментами аналізу.

4. Є кросплатформенною, що дозволяє запускати програму на різних операційних системах без модифікацій.

5. Активно використовується у сфері цифрової криміналістики та кібербезпеки, що підтверджується наявністю професійних бібліотек і спільнот.

Отже, Python є оптимальним вибором для розробки інтелектуального програмного асистента фахівця з криміналістичного аналізу кіберзлочинів, оскільки поєднує простоту, гнучкість, широкий інструментарій і орієнтованість на науково-аналітичні завдання.

Для створення графічного інтерфейсу програмного асистента фахівця з криміналістичного аналізу кіберзлочинів було розглянуто три інструменти для Python: Flet, PyQt5 та PySide6. Кожен із них має власні особливості, архітектуру та переваги.

Flet – це сучасний фреймворк для створення кросплатформених інтерфейсів користувача на Python із використанням вебтехнологій [46]. Він дозволяє створювати застосунки, які працюють як у вигляді настільних програм, так і як вебдодатки. Flet базується на компонентній архітектурі, подібній до Flutter, що забезпечує простоту розробки, адаптивність інтерфейсу та мінімальні вимоги до встановлення. Його перевагою є підтримка інтерактивних елементів, швидке оновлення UI без перезапуску застосунку та можливість інтеграції з моделями штучного інтелекту.

PyQt5 – це бібліотека для створення графічних інтерфейсів на Python на основі Qt Framework [47]. Вона підтримує складні інтерфейси з вікнами, меню, таблицями, графікою тощо. PyQt5 надає великий набір віджетів і є стабільним рішенням для корпоративних застосунків. Проте вона має складну систему ліцензування (GPL або комерційна) і потребує значного обсягу коду для реалізації навіть простих елементів.

PySide6 – це офіційна бібліотека Qt for Python, яка забезпечує можливості, аналогічні PyQt5, але з відкритою ліцензією LGPL [48]. Вона більш зручна для комерційного використання, але її структура і складність розробки інтерфейсу залишаються схожими з PyQt5, що робить її менш придатною для швидкого створення прототипів або сучасних адаптивних UI.

Порівняння засобів розробки інтерфейсу наведено в таблиці 3.2.

Для реалізації інтерфейсу програмного асистента обрано Flet, оскільки він:

1. Забезпечує просту та швидку розробку адаптивного інтерфейсу, що підходить для інтерактивних асистентів і систем аналітики.

2. Підтримує кросплатформеність і дозволяє запускати застосунок як локально, так і через веббраузер.

3. Має інтеграцію з Python-бібліотеками, що дозволяє легко підключати модулі для аналізу даних, машинного навчання та кіберкриміналістики.

4. Є повністю безкоштовним і відкритим, що спрощує використання у навчальних і дослідницьких проєктах.

Отже, Flet є оптимальним вибором для створення графічного інтерфейсу програмного асистента фахівця з криміналістичного аналізу кіберзлочинів, поєднуючи сучасність, простоту та інтерактивність.

Таблиця 3.2 – Порівняння засобів розробки інтерфейсу

Характеристика	Flet	PyQt5	PySide6
Тип фреймворку	Компонентний (на основі Flutter)	Класичний GUI на Qt	Класичний GUI на Qt
Ліцензія	Повністю безкоштовна (open source)	GPL або комерційна	LGPL
Простота розробки	Висока	Середня	Середня
Кросплатформеність	Так (Web, Desktop)	Так	Так
Адаптивний дизайн	Так	Обмежений	Обмежений
Підтримка інтеграції з AI та вебсервісами	Висока	Обмежена	Обмежена
Продуктивність	Висока	Висока	Висока
Підходить для	Легких і середніх застосунків, інтерактивних асистентів	Складних корпоративних систем	Десктопних застосунків з GUI

Для розробки програмного асистента фахівця з криміналістичного аналізу кіберзлочинів було розглянуто три популярні середовища програмування для мови Python: Visual Studio Community, Visual Studio Code та Jupyter Notebook.

Visual Studio Community – це потужна інтегрована середа розробки (IDE), створена компанією *Microsoft* [49]. Вона підтримує багато мов програмування, має розширені засоби налагодження, тестування та управління великими проєктами. Однак для Python вона потребує додаткових розширень або встановлення середовища *Anaconda* і може бути надмірно важкою для невеликих або спеціалізованих застосунків.

Visual Studio Code (VS Code) – це легка, але функціональна IDE, також розроблена *Microsoft* [50]. Вона підтримує Python через розширення *Python Extension*, має широкий вибір плагінів, інтеграцію з системами контролю версій, засоби для налагодження та тестування, а також кросплатформеність. Завдяки гнучкості та швидкодії VS Code є зручним інструментом як для створення прототипів, так і для розробки повноцінних застосунків.

Jupyter Notebook – це інтерактивне середовище, орієнтоване на аналітику даних, машинне навчання та наукові обчислення [51]. Воно дозволяє поєднувати код, текстові пояснення, графіки та таблиці в одному документі. Проте Jupyter не призначений для створення великих застосунків із графічним інтерфейсом або складною архітектурою.

Порівняння середовищ програмування наведено в таблиці 3.3.

Таблиця 3.3 – Порівняння характеристик середовищ програмування

Особливість	Visual Studio Community	Visual Studio Code	Jupyter Notebook
Тип	Повноцінна інтегрована середа розробки (IDE)	Легка інтегрована середа розробки	Інтерактивне середовище
Підтримка Python	Через розширення або Anaconda	Повна підтримка через Python Extension	Основна мова – Python
Розширюваність	Помірна	Дуже велика (через плагіни)	Обмежена
Кросплатформеність	Так	Так	Так
Інтерактивність	Середня	Середня	Висока
Веб-додаток	Ні	Ні	Так
Призначення	Великі та комплексні проєкти	Гнучка розробка різних застосунків	Наукові обчислення та аналітика

Для реалізації програмного асистента фахівця з криміналістичного аналізу кіберзлочинів обрано Visual Studio Code.

Це рішення обґрунтоване такими перевагами:

1. Підтримка Python – через офіційне розширення Python Extension забезпечується зручне написання, налагодження та тестування коду.

2. Гнучке налаштування – великий набір плагінів дозволяє адаптувати середовище до потреб криміналістичного аналізу, інтегрувати бібліотеки штучного інтелекту, бази даних та системи логування.

3. Кросплатформеність – робота на Windows, Linux і macOS забезпечує зручність у середовищах з різними системами.

4. Інтеграція з Git – дає можливість ефективно керувати версіями коду та документувати зміни під час розслідувань.

5. Безкоштовність – VS Code є відкритим і безоплатним продуктом, що робить його доступним для академічного та наукового використання.

Таким чином, Visual Studio Code є оптимальним вибором для розробки інтелектуального програмного асистента, оскільки поєднує в собі легкість, функціональність, гнучкість і підтримку сучасних інструментів аналізу кіберзлочинів.

Для зберігання даних у розроблюваному застосунку необхідно обрати засіб роботи з базою даних, який забезпечуватиме стабільну роботу, простоту використання, легкість інтеграції з мовою програмування та зручність у розгортанні. Розглянемо три популярні варіанти: SQLite, MySQL та PostgreSQL.

SQLite – це вбудована реляційна база даних, яка зберігає всі дані в одному локальному файлі [52]. Вона не потребує встановлення сервера, має невеликий розмір, підтримується практично всіма мовами програмування (зокрема Python), ідеально підходить для настільних застосунків, прототипів або невеликих проєктів. Серед її переваг: простота налаштування, висока швидкість при роботі з локальними даними, автономність і відсутність залежності від зовнішніх служб.

MySQL – потужна серверна система керування базами даних (СКБД), яка часто використовується для вебзастосунків [53]. Вона забезпечує багатокористувацький доступ, високу надійність і масштабованість. Проте її встановлення та налаштування вимагають більше ресурсів і часу, що робить її менш зручною для невеликих локальних програм.

PostgreSQL – ще одна потужна СКБД, орієнтована на надійність і відповідність стандартам SQL [54]. Вона підтримує складні запити, транзакції, розширення та реплікацію. Проте, як і MySQL, потребує встановлення сервера, адміністрування та складнішої конфігурації.

Порівняння засобів роботи з БД наведено в таблиці 3.4.

Таблиця 3.4 – Порівняння засобів роботи з БД

Характеристика	SQLite	MySQL	PostgreSQL
Тип розгортання	Вбудована (файл)	Сервер-клієнт	Сервер-клієнт
Встановлення/налаштування	Мінімальне	Потребує сервера	Потребує сервера
Потреба в адмініструванні	Немає	Середня	Висока
Багатокористувацька робота	Обмежена (локальні сценарії)	Так	Так
Масштабованість	Низька – локальні дані	Висока	Дуже висока
Підтримка складних запитів / типів даних	Базова	Добра	Відмінна
Продуктивність для локальних завдань	Висока	Висока (сервер)	Висока (сервер)
Розгортання для користувача	Дуже просте	Складніше	Складніше
Ідеальне застосування	Настільні та прототипи	Веб та середні системи	Аналітика, великі БД, enterprise

Для даного проєкту оптимальним вибором є SQLite, оскільки головним критерієм є простота інтеграції, мінімальні вимоги до налаштування та автономність роботи застосунку. SQLite дозволяє швидко організувати збереження та обробку даних без необхідності запуску серверних процесів чи створення додаткової інфраструктури, що значно спрощує розробку і тестування.

3.2 Реалізація програмного застосунку

Відповідно до визначеної архітектури програмного застосунку було розроблено низку функціональних модулів, що забезпечують його комплексну роботу: Інтерфейс застосунку, Логічний модуль, Модуль обробки мовлення, Модуль штучного інтелекту та База даних. Кожен із зазначених модулів виконує специфічні функції та взаємодіє з іншими компонентами для забезпечення безперебійного та ефективного функціонування застосунку.

Інтерфейс застосунку реалізується через набір взаємодійних елементів, що дозволяють користувачу здійснювати керування функціональністю системи. Для переходу до довідкового розділу користувач може натиснути кнопку з назвою

відповідного розділу. Для взаємодії з чат-асистентом передбачено введення повідомлення у текстове поле та натискання кнопки «Надіслати».

Головна сторінка застосунку, що демонструє основні елементи інтерфейсу та їх розташування, наведена на рисунку 3.1.

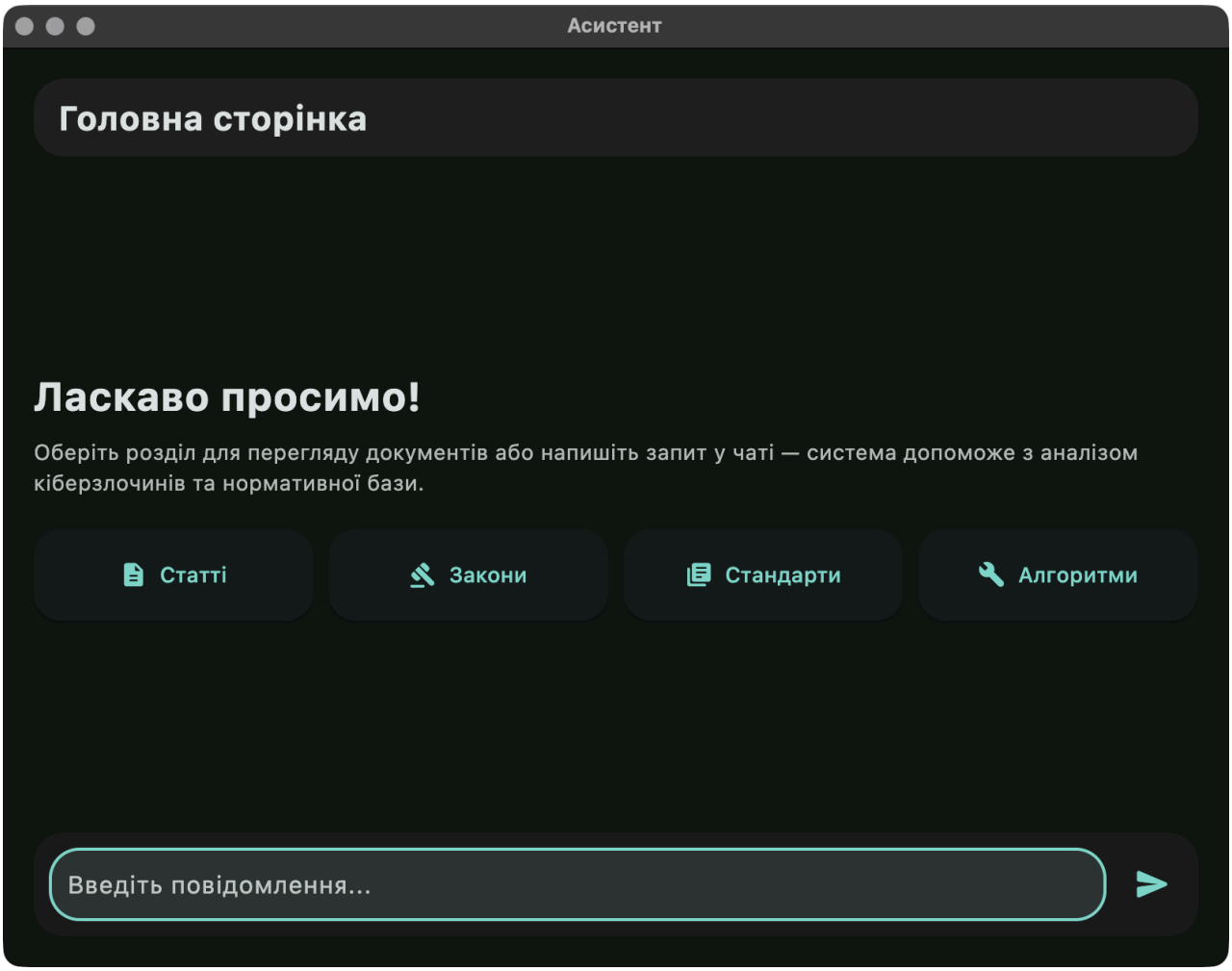


Рисунок 3.1 – Головна сторінка програмного застосунку

Сторінки відповідних розділів із передбаченими матеріалами представлені на рисунку 3.2. Застосунок забезпечує можливість перегляду документів шляхом відкриття випадаючого блока з назвою обраного документа. Така реалізація дозволяє ефективно організувати доступ до інформаційних ресурсів, забезпечуючи швидкий та зручний перегляд необхідних матеріалів без перевантаження інтерфейсу.

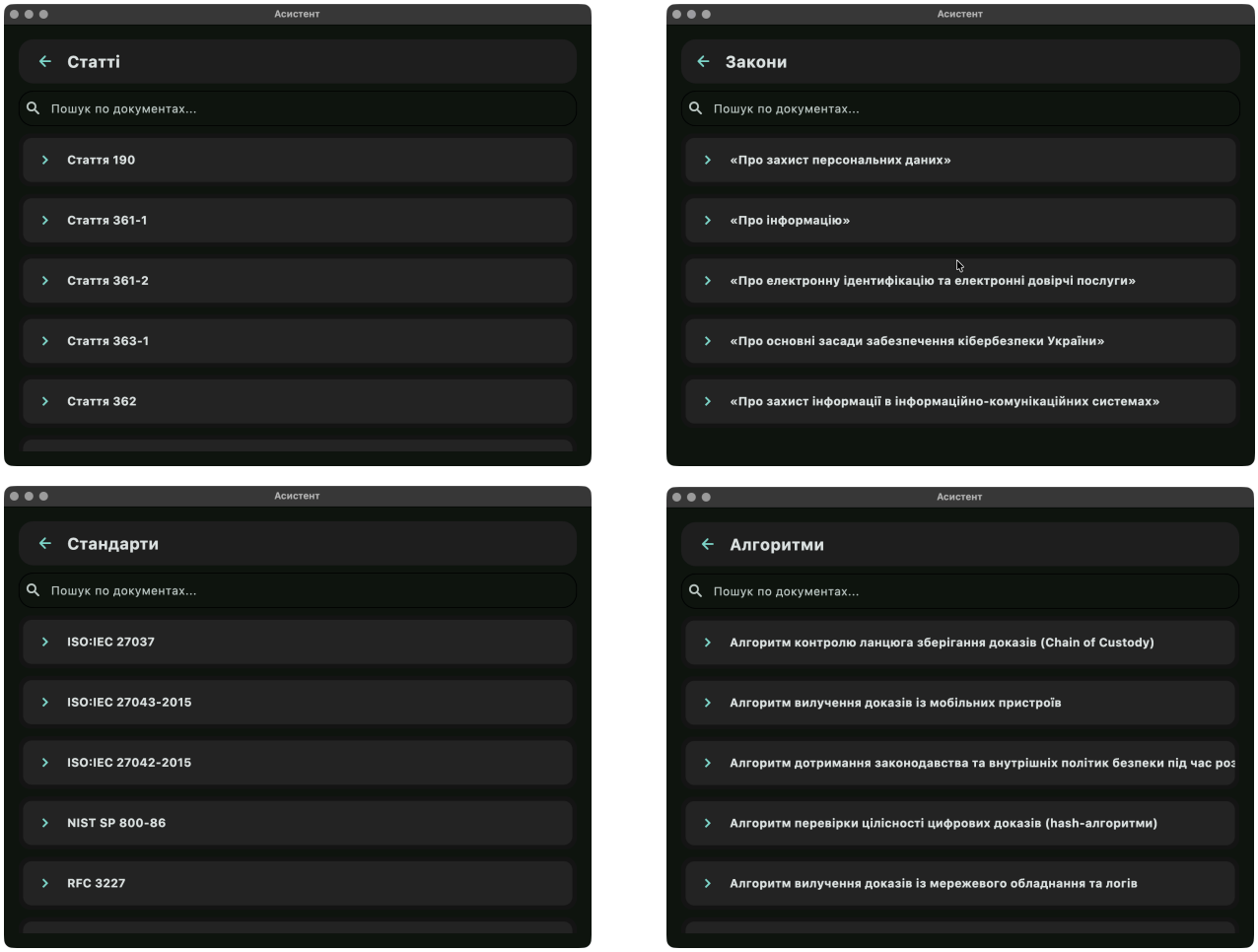


Рисунок 3.2 – Довідкові сторінки програмного застосунку

Сторінка чату з асистентом реалізована у вигляді класичного інтерфейсу чат-бота, що забезпечує інтерактивну взаємодію користувача із системою. Користувач має можливість вводити текстові повідомлення у спеціально відведене поле та надсилати їх для обробки модулем штучного інтелекту, який забезпечує формування відповідей на основі наявних даних і логіки застосунку. Крім того, передбачено механізм повернення на головну сторінку, що забезпечує швидку навігацію між основними функціональними розділами застосунку. Така реалізація інтерфейсу сприяє підвищенню зручності користування та ефективності взаємодії користувача з інформаційними ресурсами системи, а також забезпечує безперервність та інтуїтивність робочого процесу. Вигляд сторінки чату зображено на рисунку 3.3.

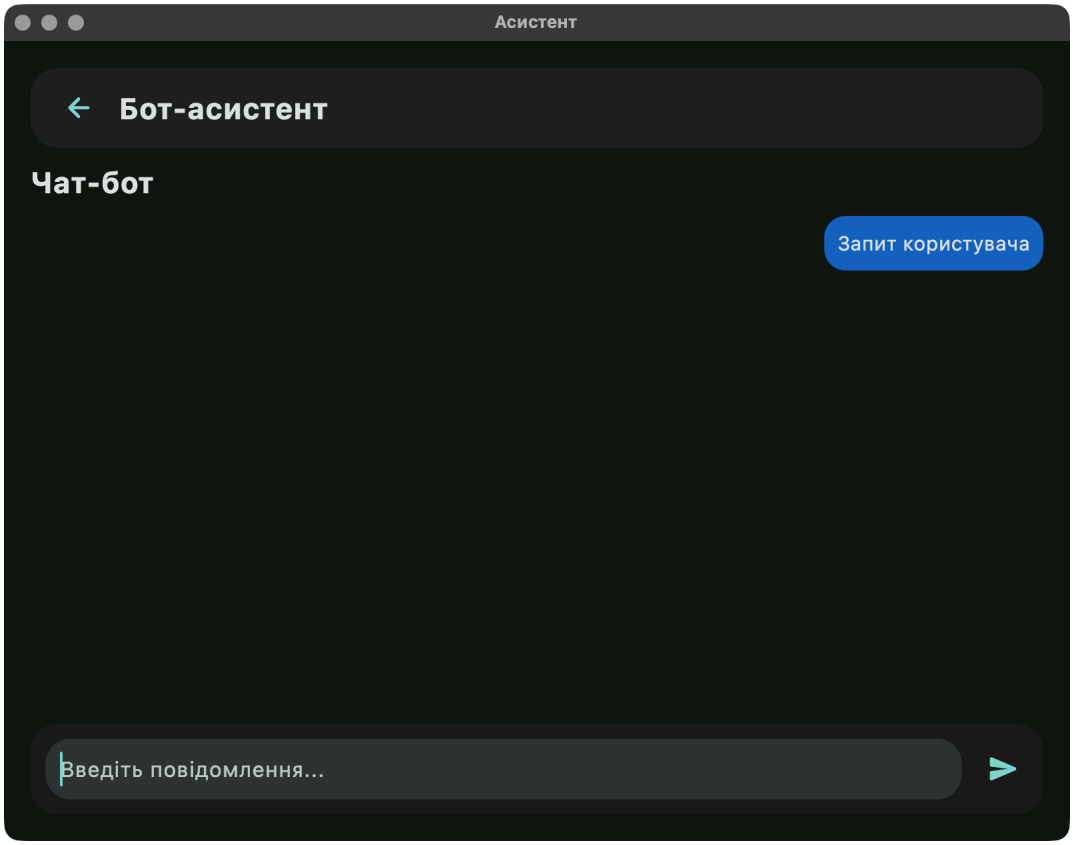


Рисунок 3.3 – Сторінка запитів до асистента програмного застосунку

База даних програмного асистента фахівця з криміналістичного аналізу кіберзлочинів виконує роль центрального сховища формалізованих знань, необхідних для коректної роботи інтелектуальних модулів системи. Її структура побудована за принципами модульності та розширюваності, що забезпечує можливість поступового нарощування змісту відповідно до потреб користувачів та вимог практики цифрової криміналістики.

На початковому етапі реалізації база даних зосереджена на зберіганні систематизованих характеристик кримінально-правових норм, а також довідкової інформації щодо нормативних документів і стандартів, що забезпечують навігацію та підтримку аналітичних процесів. Такий підхід дозволяє оптимізувати початкову функціональність системи, мінімізувати залежність від великих масивів даних та гарантувати високу керованість оновлень на ранніх стадіях розробки.

Закладена архітектура БД орієнтована на подальше масштабування. Застосування реляційної структури, чітке розмежування сутностей і логічних

залежностей забезпечують можливість безперешкодної інтеграції додаткових типів інформації без зміни основного функціоналу системи. У перспективі база даних може бути доповнена розширеними наборами даних – зокрема, матеріалами правозастосовної практики, прецедентними рішеннями або спеціалізованими відомостями, що дозволить підвищити глибину аналітичних висновків асистента. Запропонована структура бази даних наведена на рисунку 3.4.

При цьому модульний характер сховища є ключовою перевагою, адже забезпечує простоту заміни або модернізації окремих компонентів без втручання у роботу інших підсистем. База даних може бути адаптована до зовнішніх джерел або альтернативних форматів зберігання, що сприяє гнучкості системи та її здатності до функціонального зростання.

Таким чином, реалізована база даних не лише повністю задовольняє потреби поточного етапу розробки, але й формує надійну основу для подальшого розширення моделі знань програмного асистента, забезпечуючи стабільність, масштабованість і довгострокову життєздатність системи.

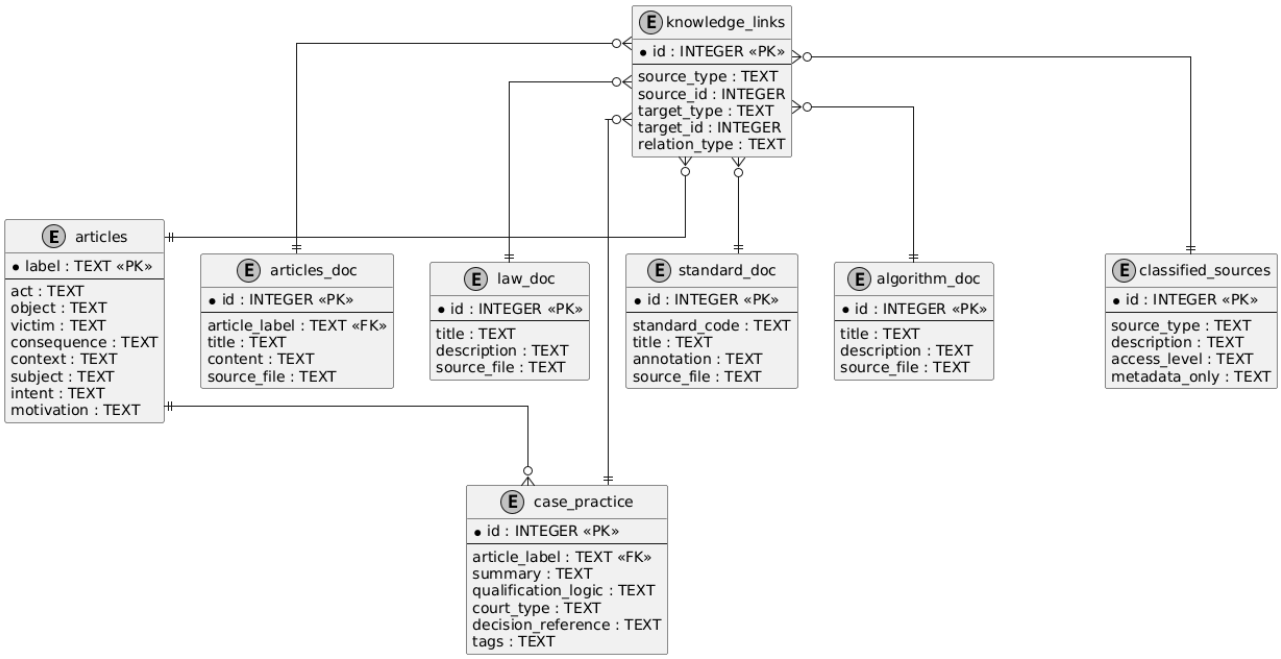


Рисунок 3.4 – ER-діаграма бази даних програмного асистента фахівця з криміналістичного аналізу кіберзлочинів.

На рисунку 3.5 представлено фрагмент бази даних, що містить характеристики кіберзлочинів із прив’язкою до відповідних статей Кримінального кодексу України. Застосування структурованої бази даних дозволяє ефективно здійснювати пошук, сортування та аналіз інформації, що необхідна для функціонування модулів логіки та штучного інтелекту. Кожен запис у базі даних містить сукупність атрибутів, що описують конкретний злочин, його ознаки, відповідну статтю законодавства та додаткові метадані, що забезпечують можливість подальшої обробки та інтеграції даних у функціональні процеси застосунку.

362-1	Зміна, знищення або блокування інформації	Електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі або носії інформації	Особа	Зміна, знищення або блокування інформації	Спосіб — несанкціонований; суб'єкт має право доступу	Особа з правом доступу	Прямий умисел до діяння, умисел або необережність до наслідків	Мета — зміна, знищення або блокування інформації
362-2	Перехоплення або копіювання інформації, яка оброблюється	Електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі або носії інформації		Витік інформації	Спосіб — несанкціонований; суб'єкт має право доступу	Особа з правом доступу	Прямий умисел до діяння, умисел або необережність до наслідків	Мета — перехоплення або копіювання інформації
362-3	Зміна, знищення або блокування інформації; перехоплення або копіювання інформації, яка оброблюється	Електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі або носії інформації		Заподіяли значну шкоду	Спосіб — вчинені повторно або за попередньою змовою групою осіб	Особа з правом доступу	Прямий умисел до діяння, умисел або необережність до наслідків	Мета — зміна, знищення або блокування; перехоплення або копіювання інформації

Рисунок 3.5 – Фрагмент таблиці БД з характеристиками кіберзлочинів

Модуль обробки мовлення забезпечує приймання й попередню нормалізацію текстових даних, що вводяться користувачем у довільній формі. Під час обробки виконуються операції лінгвістичної нормалізації: приведення тексту до нижнього регістру, видалення сторонніх символів, уніфікація пробілів та заміна варіативних символів (рисунок 3.6). Такий підхід сприяє зменшенню впливу мовних варіацій і орфографічних відхилень на подальший аналіз. Результатом роботи модуля є уніфіковане текстове подання, яке відображає зміст

складових ймовірного правопорушення та є придатним для подальшої семантичної та класифікаційної обробки.

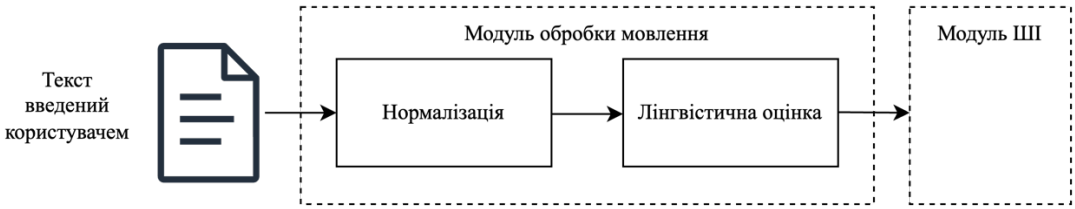


Рисунок 3.6 – Схема модуля обробки мовлення

У модулі інтелектуального аналізу текстових описів застосовано метод Term Frequency–Inverse Document Frequency (TF-IDF), який є одним з найпоширеніших статистичних підходів до подання документів у числовій формі. Сутність TF-IDF полягає у визначенні ваги кожного слова в документі з урахуванням його частотності в межах окремого тексту та рідкісності у всій колекції документів.

Частота терміна (TF) відображає, наскільки часто слово використано в конкретному описі злочину, тоді як зворотна частота документа (IDF) зменшує вагу слів, які зустрічаються надто часто в усій базі статей та, відповідно, мають низьку дискримінативну цінність.

Таким чином, TF-IDF забезпечує формування розрідженого високовимірного векторного представлення, яке дозволяє кількісно порівнювати текстові описи різних кримінальних правопорушень. Дане представлення є вхідними даними для алгоритму класифікації.

На основі TF-IDF-векторів побудовано модель *Logistic Regression*, яка виконує багатокласову класифікацію шляхом оптимізації логістичної функції втрат. Логістична регресія визначає ймовірність належності вхідного опису до певного класу – тобто до конкретної статті та частини статті Кримінального кодексу України.

Переваги цього методу полягають у його інтерпретованості, стійкості до лінійного розділення даних, можливості роботи з великою кількістю ознак та ефективності при навчанні на текстових корпусах обмеженого обсягу.

У запропонованій системі логістична регресія виконує роль базового класифікатора, який пропонує найбільш вірогідну правову кваліфікацію на основі статистичного аналізу ключових термінів.

Оскільки юридичні описи можуть бути сформульовані різними словами, логістичної регресії недостатньо для коректного відображення семантичної близькості між запитами користувача та моделями складу злочину.

Для підвищення точності використано модель SentenceTransformer (архітектура MiniLM-L12-v2), яка формує щільні контекстні векторні представлення (ембеддинги) для всіх статей та для вхідного повідомлення.

Схожість між векторами обчислюється за косинусною мірою, що дозволяє:

- визначати найбільш близькі за змістом статті навіть при значних лексичних відмінностях,
- інтерпретувати запити, сформульовані неповною, розмовною або нефаховою мовою,
- будувати рейтинг правових норм, які найбільше відповідають описаним у запиті ознакам.

Семантичний модуль працює паралельно з класичним класифікатором і фактично відіграє роль другого незалежного механізму перевірки, що підвищує стійкість системи до помилкових формулювань.

Окрім статистичних та семантичних моделей, інтелектуальна система використовує набір *евристичних правил уточнення*, побудованих на доменних знаннях у сфері кіберзлочинів.

У сукупності ці правила формують гібридну модель прийняття рішення, що поєднує формальні статистичні методи, контекстну семантику та експертні юридичні евристики. Структуру модуля наведено на рисунку 3.7.

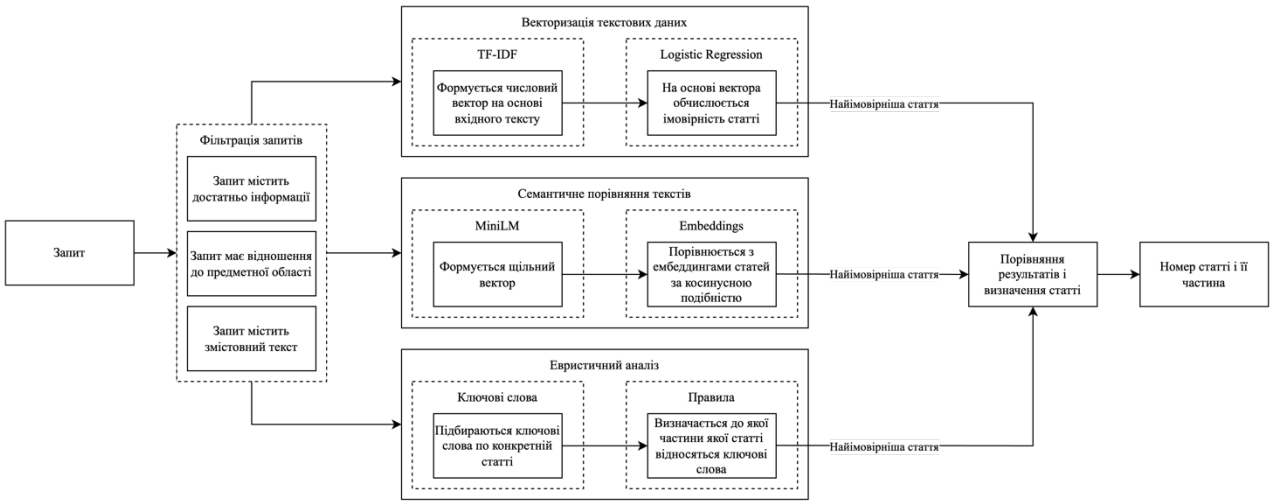


Рисунок 3.7 – Схема модуля штучного інтелекту

Логічний модуль відіграє ключову роль у функціонуванні програмного застосунку, забезпечуючи узгоджену взаємодію між усіма його компонентами. Він реалізує механізми маршрутизації даних, обробки подій та координації роботи модулів обробки мовлення, штучного інтелекту, бази даних і користувацького інтерфейсу (рисунок 3.8). Завдяки цьому забезпечується своєчасне отримання, передавання та відображення інформації.

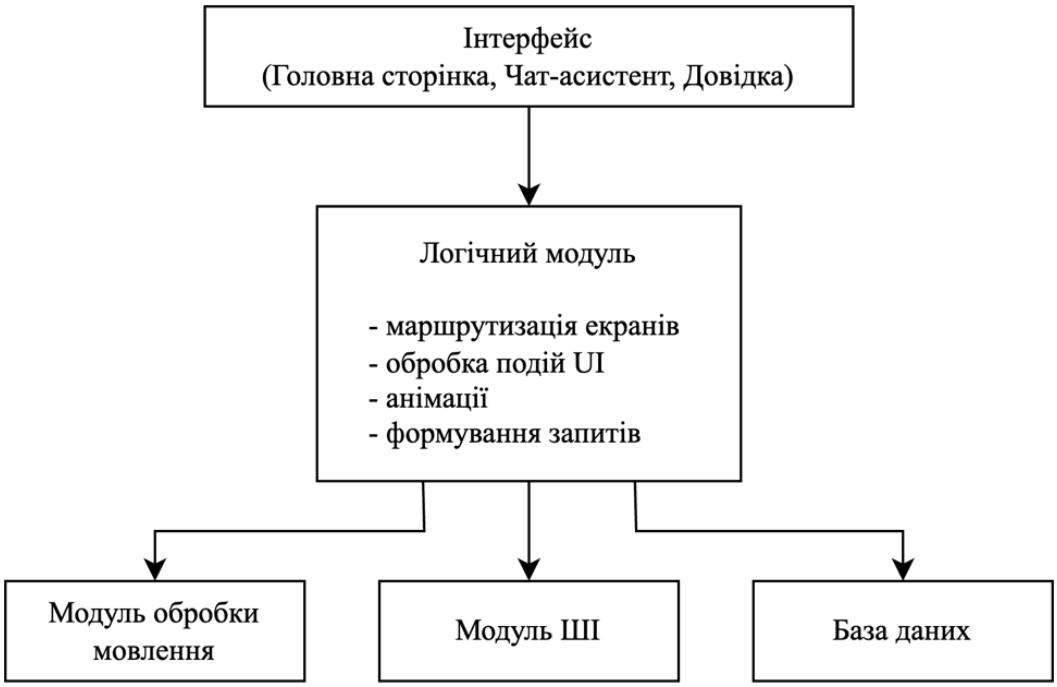


Рисунок 3.8 – Схема логічного модуля

3.3 Тестування та оцінювання розробленого програмного застосунку

Тестування програмного застосунку проводилося з метою перевірки стабільності роботи інтерфейсу, коректності логічних переходів між основними модулями та оцінки функціональних можливостей системи в цілому. На першому етапі було досліджено працездатність головної сторінки, яка виконує роль навігаційного центру та забезпечує можливість переходу до довідкових розділів або в режим інтерактивної взаємодії з чат-ботом. Перевірка виконувалася шляхом послідовного відкриття всіх доступних розділів, відстеження поведінки системи у випадку багаторазових повернень на початковий екран та оцінювання стійкості інтерфейсу до повторних викликів. Результати тестування зображено на рисунках 3.9 – 3.10.

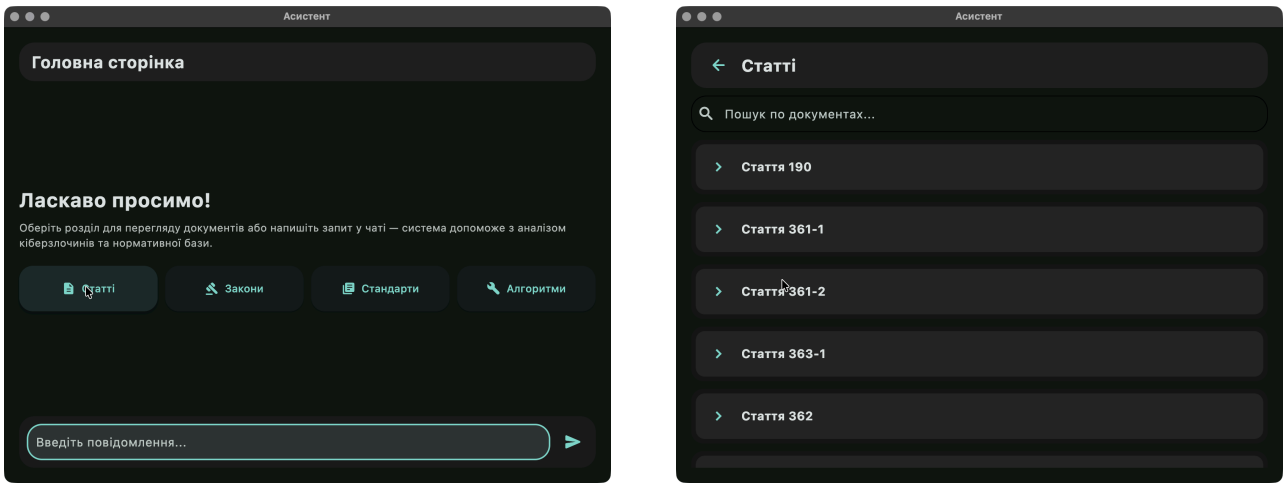


Рисунок 3.9 – Перехід з головної сторінки до довідкового розділу «Статті»

За аналогічною методикою було проведено тестування всіх інших розділів застосунку. У процесі перевірки встановлено, що всі елементи інтерфейсу функціонують відповідно до визначеного функціонального призначення та не демонструють відхилень у роботі.

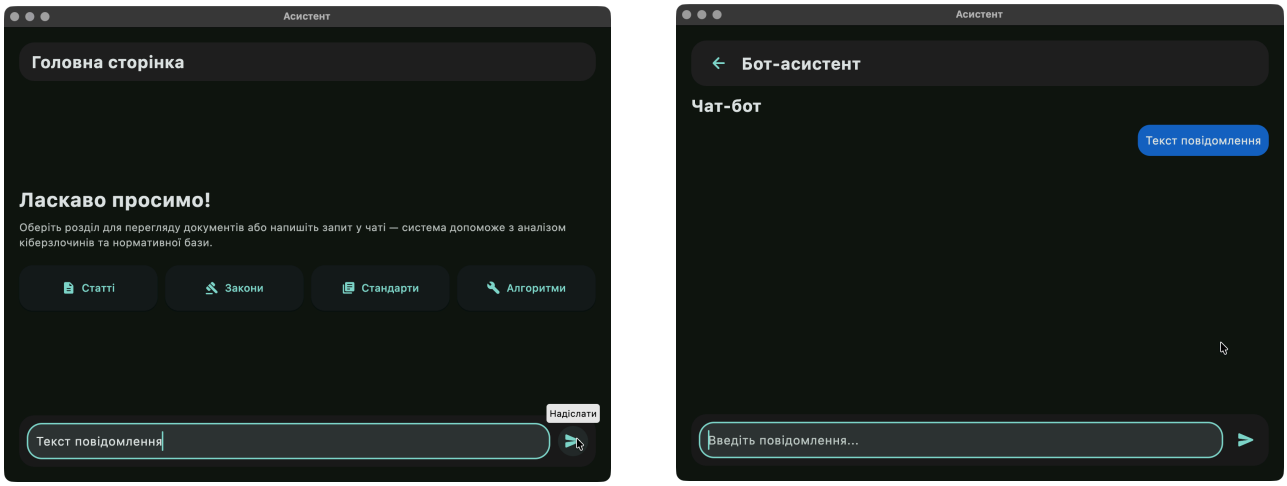


Рисунок 3.10 – Перехід з головної сторінки в чат з асистентом

Під час надсилання повідомлення система коректно здійснює перехід у режим взаємодії з чат-асистентом. Функція відправлення реалізована належним чином і активується як шляхом натискання відповідної кнопки, так і за допомогою клавіші Enter.

Окрема серія тестів була зосереджена на довідкових розділах, у межах яких користувач може переглядати надані документи, розгортати їх зміст у вигляді випадаючих блоків та здійснювати пошук матеріалів за назвами. Під час тестування вивчалися коректність завантаження документів, швидкість візуального відтворення вмісту, стабільність роботи пошукового механізму та відповідність результатів введеним користувачем ключовим словам. Особливу увагу приділено перевірці інваріантності пошуку до варіацій регістру, часткових співпадінь та специфічних символів у назві файлу. Результати наведено на рисунку 3.11.

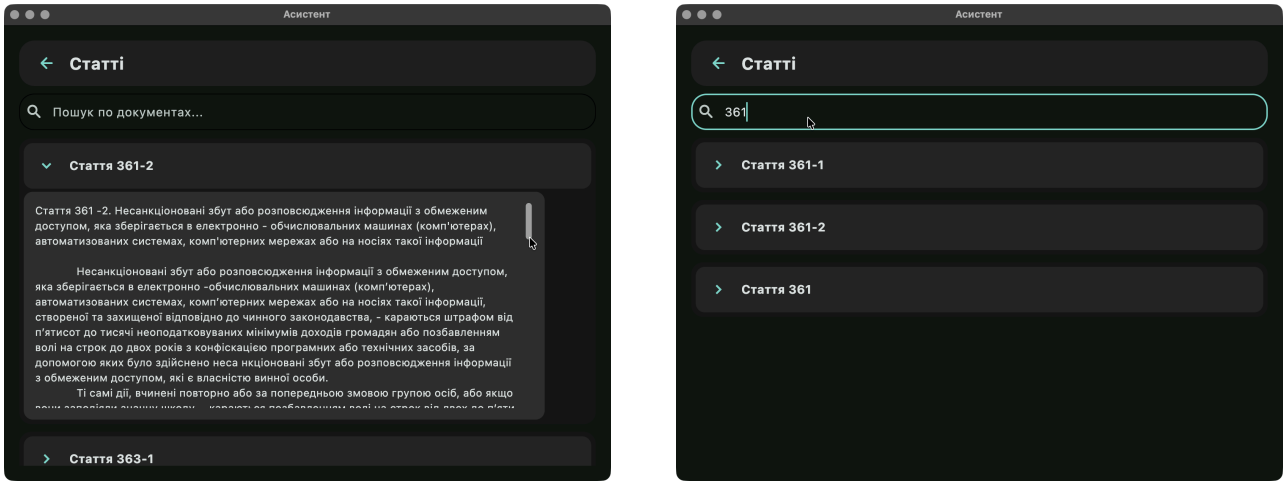


Рисунок 3.11 – Тестування функціоналу довідкових розділів

Тестування режиму чат-бота проводилося в умовах імітації типових сценаріїв, характерних для введення описів кіберзлочинів. Користувач вводив текстові характеристики інциденту, після чого бот генерував попередню юридичну кваліфікацію відповідно до бази статей Кримінального кодексу України. Перевірялася стійкість чат-бота до неповних, неструктурованих або розмовних формулювань, а також узгодженість відповідей на різні формулювання одного й того самого сценарію. Додатково оцінювалися реакція системи на випадковий або беззмістовний введений текст та відсутність хибних відповідей у таких випадках (рис. 3.12 – 3.14).

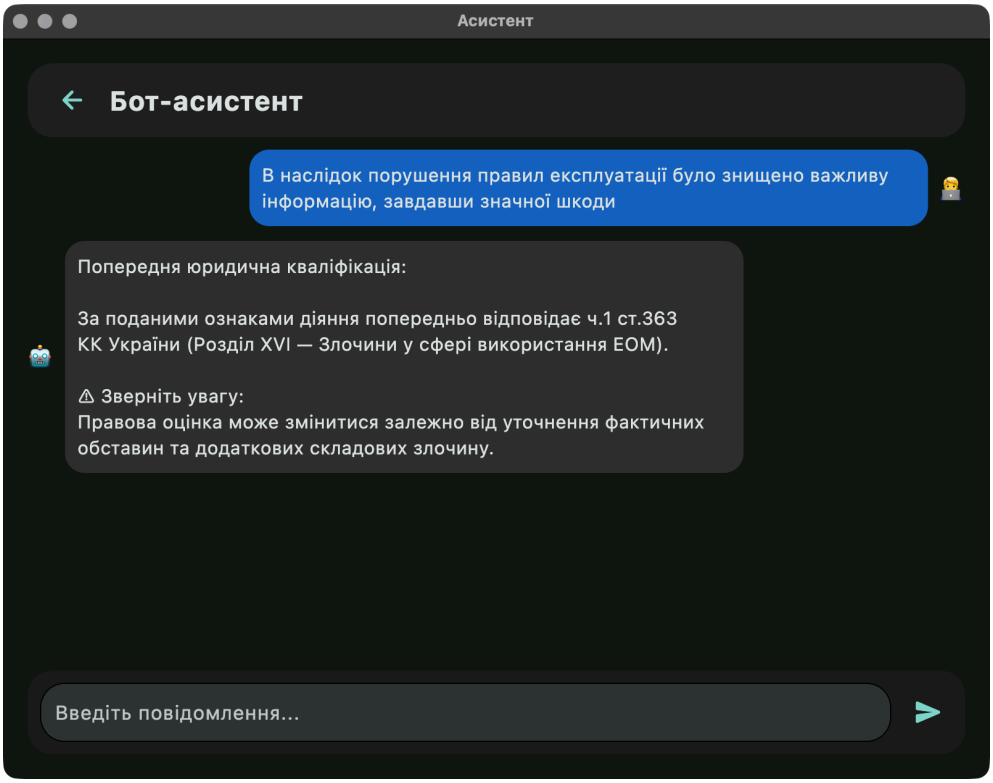


Рисунок 3.12 – Реакція системи на валідний запит

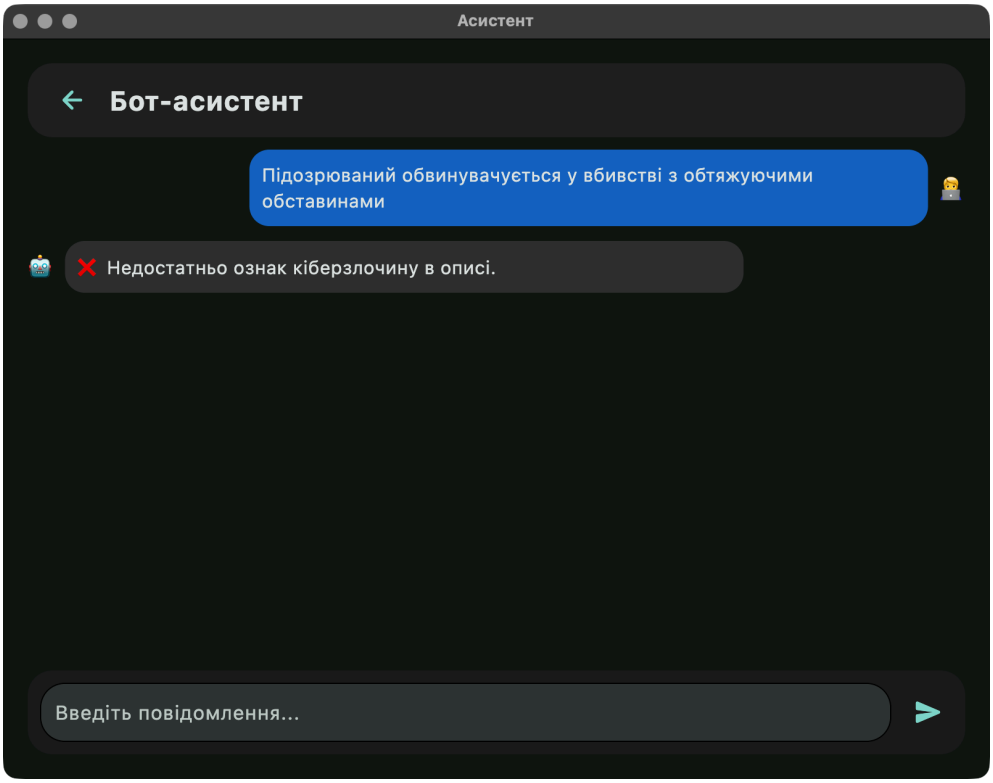


Рисунок 3.13 – Реакція системи на запит, який не відноситься до сфери кіберзлочинів

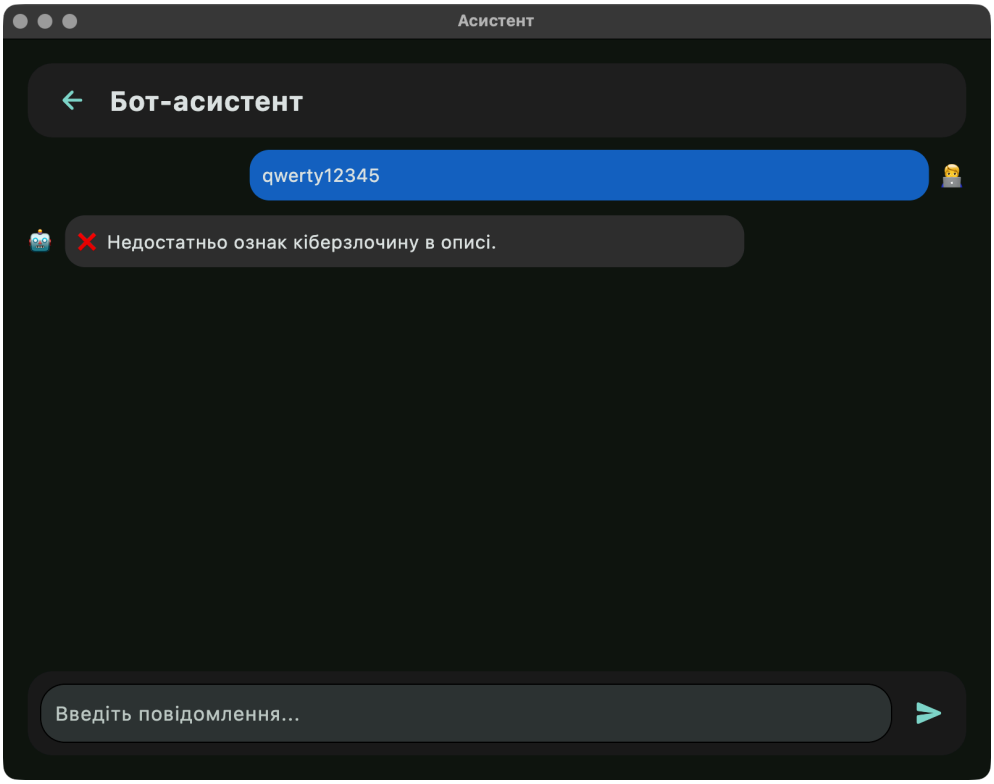


Рисунок 3.14 – Реакція системи на запит який містить випадкові символи

Оскільки точність класифікаційної моделі не може бути визначена через брак репрезентативного набору валідаційних прикладів, для оцінювання роботи чат-бота було застосовано альтернативний кількісний підхід. Замість метрик машинного навчання використовувався показник узгодженості відповідей, який характеризує частку випадків, у яких система повертає однакову або функціонально еквівалентну відповідь на декілька варіантів опису одного й того самого кіберзлочину. Для цього формувалися контрольні набори сценаріїв, що відрізнялися формулюванням, рівнем деталізації та стилістикою подання, але описували однакову юридичну ситуацію. Узгодженість обчислювалася як відношення кількості коректно узгоджених відповідей до загальної кількості тестових варіацій.

Такий підхід дає змогу кількісно оцінити стабільність роботи чат-бота. Чим вищий показник узгодженості, тим більш надійною вважається система з точки зору практичного застосування у процесах попереднього аналізу кіберзлочинів. У поєднанні з якісним аналізом сценаріїв та відтворюваності поведінки системи така метрика дозволяє сформувати всебічну оцінку функціональних

характеристик застосунку та визначити напрями його подальшого вдосконалення.

$$C = \frac{N_{\text{узгоджених}}}{N_{\text{усіх}}} \times 100\%, \qquad (3.1)$$

де, Nусіх – кількість варіантів опису одного й того ж сценарію,
Nузгоджених – кількість випадків, у яких чат-бот повернув ідентичну або доречно еквівалентну статтю.

На прикладі статті 363 КК України (таблиця 3.5) було здійснено експериментальне тестування, у межах якого системі подавалися різні за формулюванням користувацькі запити, що описували ідентичний склад правопорушення. Це дозволило оцінити здатність програмного забезпечення коректно ідентифікувати одну й ту саму норму кримінального законодавства незалежно від варіативності мовного подання ознак діяння. Результати тестування наведено в таблиці 3.6.

Таблиця 3.5 – Характеристика кіберзлочину, передбаченого ст. 363 КК України [6]

Стаття КК України	Діяння	Предмет	Потерпілий	Наслідки	Місце, час, спосіб, засоби, знаряддя, обстави ни, ситуація	Суб'єкт	Форма вини	Мета, мотивація, емоційний стан
ч.1 ст.363	Порушення правил експлуатації	Правила експлуатації, порядок або правила захисту інформації	–	Заподіяли значну шкоду	–	Особа, яка відповідає за експлуатацію	Умисел або необережність до діяння; необережність до наслідків	Мета – зміна, знищення або блокування інформації

Таблиця 3.6 – Результати тестування програмного застосунку в сценарії тесту (різні запити/одна відповідь)

№	Текст запиту	Передбачена стаття	Правильна стаття	Результат відповіді
1	«В наслідок порушення правил експлуатації було знищено важливу інформацію, завдавши значної шкоди»	ч.1 ст.363	ч.1 ст.363	Правильно
2	«Підозрюваний порушив правила експлуатації завдавши значної шкоди підприємству»	ч.1 ст.363	ч.1 ст.363	Правильно
3	«Через порушення правил експлуатації відповідальною особою було втрачено доступ до важливої інформації»	ч.1 ст.363	ч.1 ст.363	Правильно
4	«Особа проігнорувала правила захисту інформації з прямим умислом, з метою обмежити доступ до інформації»	ч.1 ст.363	ч.1 ст.363	Правильно
5	«Особа відповідальна за експлуатацію спричинила втрату інформації»	ч.1 ст.363	ч.1 ст.363	Правильно

Аналогічним чином було проведено тестування із використанням набору запитів, що відрізнялися за змістовними характеристиками складових злочину, але належали до однієї групи кіберправопорушень. Такий підхід дав змогу перевірити стійкість алгоритму до змін окремих елементів опису діяння, включно з варіаціями об’єкта посягання, наслідків чи суб’єктного складу. Результати експерименту дозволили оцінити гнучкість системи в умовах різноманітності фактичних обставин та підтвердили її здатність коректно визначати релевантну правову норму навіть при зміні структури введених даних. Результати тестів наведено на рисунку 3.15.

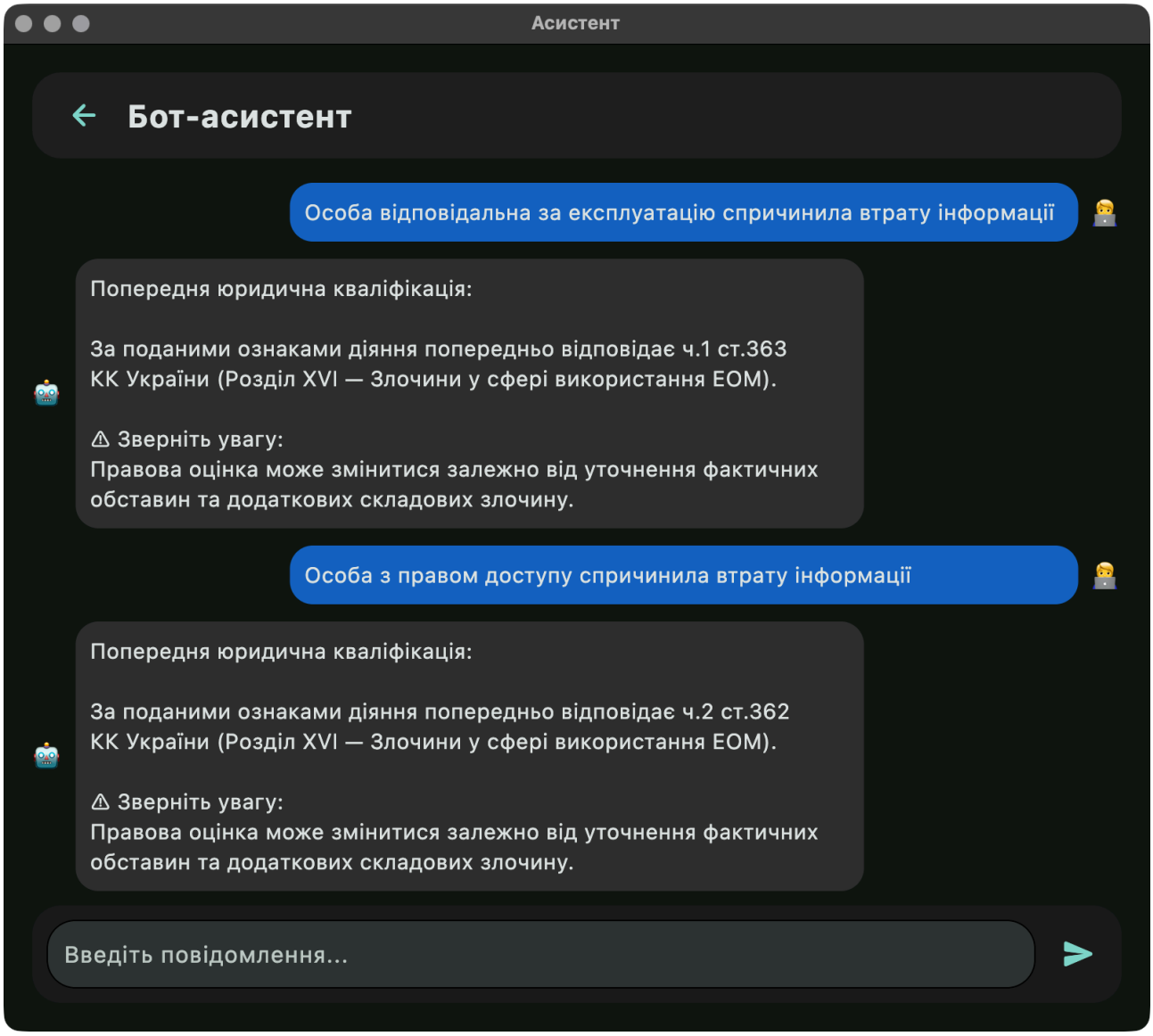


Рисунок 3.15 – Результати тестування програмного застосунку в сценарії тесту (схожі запити/різна відповідь)

Було виконано 200 тестових запусків системи, з яких 100 стосувалися ситуацій із різними формулюваннями одного й того ж запиту, а ще 100 – зі схожими запитами, що описували різні склади злочину. Результати показали високу ефективність: у першому випадку правильний вибір правової норми було отримано у 98 зі 100 тестів, а в другому – у 97 зі 100. На основі формули 3.1 обчислено відсоток коректних відповідей, який наближається до 100%.

$$C = \frac{(98 + 97)}{(100 + 100)} \times 100\% = 97{,}5\%$$

Водночас проаналізовано характер допущених похибок: у випадках з умовно «неправильною» відповіддю система коректно визначала саму статтю КК України, проте помилково ідентифікувала її частину. Причиною цього стало недостатнє уточнення фактичних обставин у вхідному описі злочину, оскільки різні частини статті можуть містити однакові ключові ознаки з мінімальними відмінностями, про що асистент додатково попереджає користувача. Враховуючи зазначене, такі відхилення можна віднести до допустимої похибки, що дозволяє стверджувати про фактичну майже стовідсоткову точність розробленої системи.

Сценарій застосування програмного асистента фахівця з криміналістичного аналізу кіберзлочинів. Під час підготовки до розслідування кіберінциденту фахівець з криміналістичного аналізу кіберзлочинів запускає програмний асистент, який на головній сторінці надає йому зручну точку входу до всієї релевантної інформації. Інтерфейс головного вікна містить структуровані розділи «Статті», «Закони», «Стандарти» та «Алгоритми», що дозволяє користувачу швидко переходити до перегляду відповідних документів. Наприклад, у розділі «Статті» він може ознайомитися текстом статей Кримінального кодексу України, у «Законах» – з повним текстом законів, у «Стандартах» – з міжнародними рекомендаціями з цифрової криміналістики, а в «Алгоритмах» – з послідовностями дій щодо вилучення, аналізу та документування електронних доказів. Завдяки реалізації перегляду документів безпосередньо в інтерфейсі застосунку, фахівець може працювати з великим обсягом нормативної та методичної інформації, не виходячи за межі єдиного програмного середовища (рис. 3.16).

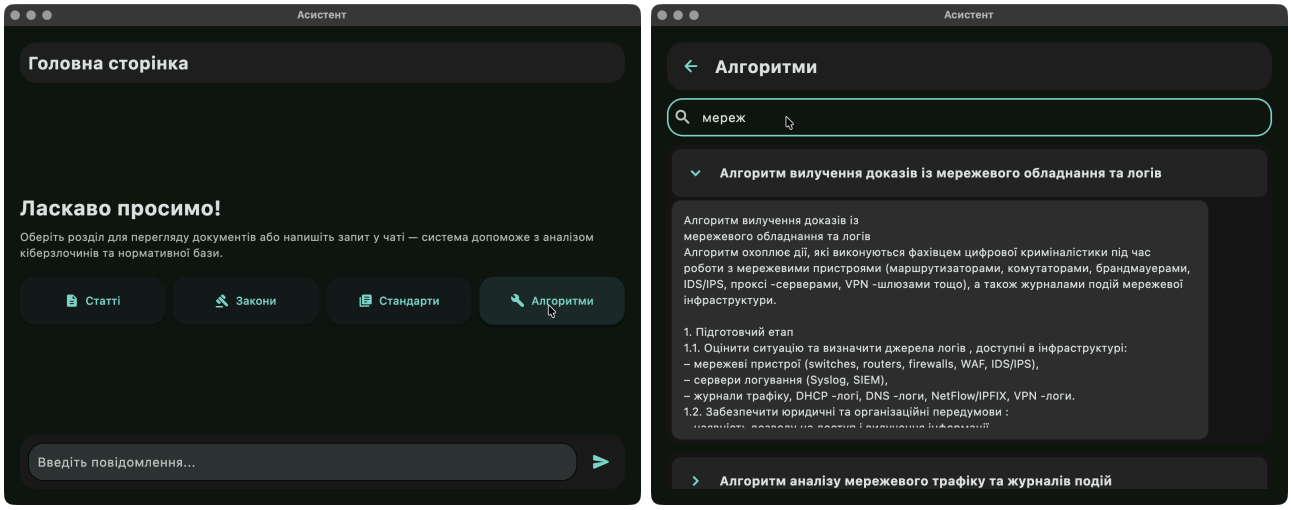


Рисунок 3.16 – Перегляд нормативної та методичної інформації

У процесі аналізу конкретної події, наприклад несанкціонованого втручання до інформаційної системи із зловживанням правами доступу, фахівцю необхідно здійснити попередню юридичну кваліфікацію діяння. Для цього він може скористатися інтегрованим чат-ботом, доступ до якого реалізовано безпосередньо з головної сторінки. Користувач формулює опис складу правопорушення у довільній формі, указуючи фактичні обставини (роль суб’єкта, характер доступу, наслідки для інформації, спосіб вчинення дій) та надсилає запит у чат. Після надсилання повідомлення інтерфейс автоматично переключається в режим діалогу з асистентом, де в окремих «бульбашках» відображаються як вихідне формулювання користувача, так і відповідь системи. На основі поєднання статистичних методів (TF-IDF і логістична регресія), семантичного аналізу (SentenceTransformer) та вбудованих експертних правил програмний асистент генерує попередню юридичну кваліфікацію, вказуючи статтю та, за можливості, частину КК України, а також відповідний розділ кодексу. Такий механізм дозволяє фахівцю оперативно звірити інтуїтивну оцінку зі «штучним» аналізом і, за потреби, відразу перейти до перегляду повного тексту норми або відповідних методичних матеріалів у довідкових розділах (рис. 3.17)/

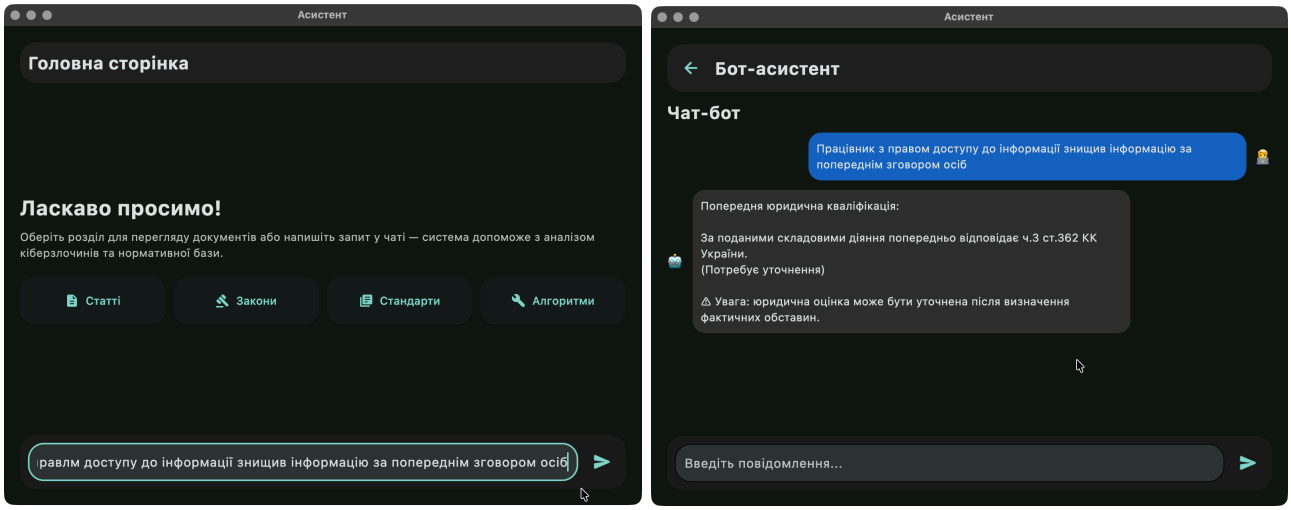


Рисунок 3.17 – Попередня юридична кваліфікація за допомогою чат-бота

Застосування програмного асистента в такому сценарії сприяє підвищенню як швидкості, так і обґрунтованості прийняття рішень під час криміналістичного аналізу. Фахівець отримує єдине робоче середовище, де поєднано доступ до структурованої нормативної бази, довідкових документів і інтелектуального інструменту попередньої кваліфікації. Перспективним напрямом подальшого розвитку подібних систем є розширення функціональності чат-бота в бік глибшого врахування контексту: зокрема, додатковий аналіз релевантних документів (статей, стандартів, алгоритмів) з автоматичним формуванням коротких рекомендацій щодо доцільних дій слідчого або експерта. Також доцільним видається інтеграція знань про типові інструменти цифрової криміналістики та методики їх застосування, що дозволило б у рамках діалогу не лише здійснювати кваліфікацію діяння, а й орієнтовно пропонувати підходи до пошуку, фіксації та дослідження цифрових доказів. Такі розширення органічно доповнили б наявну концепцію програмного асистента, поглиблюючи його роль як інтелектуального помічника фахівця з криміналістичного аналізу кіберзлочинів.

Висновки до розділу 3

У цьому розділі було проведено комплексне обґрунтування вибору технологічних засобів та програмних інструментів, необхідних для створення програмного застосунку. Використання мови програмування Python забезпечило гнучкість та швидкість розробки, а фреймворк Flet дозволив реалізувати сучасний кросплатформний інтерфейс із мінімальними витратами на підтримку. Середовище Visual Studio Code було застосовано як основний інструмент розробника, що надало можливість ефективної організації коду та керування проєктом. Для зберігання структурованих даних було обґрунтовано використання SQLite, яке забезпечує необхідну продуктивність та автономність для настільного застосунку.

У межах розділу розроблено програмний застосунок, що включає інтерфейс користувача, логічний модуль, модуль обробки мовлення, модуль штучного інтелекту та базу даних. Архітектура застосунку забезпечує узгоджену взаємодію між модулями та стійкість до різних сценаріїв користувацької активності.

Проведене тестування дозволило оцінити працездатність як інтерфейсу, так і функціональних модулів, зокрема чат-бота. Для оцінювання його ефективності було застосовано метрику узгодженості відповідей, що визначає здатність системи відтворювати стабільну юридичну оцінку при варіативному формулюванні ідентичних сценаріїв. Отриманий результат, що наближається до 100%, свідчить про високу стійкість алгоритмічної обробки та узгодженість роботи моделі в межах наявного набору сценаріїв.

Таким чином, у розділі продемонстровано коректність вибору технологічного стеку, ефективність розробленої архітектури та високу функціональну надійність створеного програмного забезпечення, що підтверджується результатами тестування та показником узгодженості відповідей чат-бота.

4 ЕКОНОМІЧНА ЧАСТИНА

Науково-технічна розробка може бути впроваджена у практичну діяльність лише за умови відповідності сучасним вимогам науково-технічного прогресу та економічної доцільності. Саме тому при виконанні науково-дослідних робіт важливим є проведення оцінювання економічної ефективності отриманих результатів.

Магістерська кваліфікаційна робота на тему «Програмний асистент фахівця з криміналістичного аналізу кіберзлочинів» належить до науково-технічних розробок, потенційно орієнтованих на вихід на ринок програмних продуктів. Рішення про комерціалізацію такої розробки може бути прийнято як заздалегідь, так і в процесі її виконання. Такий напрям є актуальним і практично значущим, оскільки результати розробки можуть бути використані широким колом споживачів, забезпечуючи при цьому реальний економічний ефект. Водночас реалізація подібного проєкту потребує залучення потенційного інвестора, якому необхідно продемонструвати економічну обґрунтованість та доцільність впровадження програмного асистента у практику криміналістичного аналізу кіберзлочинів.

Для наведеного випадку нами мають бути виконані такі етапи робіт:

1) проведено комерційний аудит науково-технічної розробки, тобто встановлення її науково-технічного рівня та комерційного потенціалу;

2) розраховано витрати на здійснення науково-технічної розробки;

3) розрахована економічна ефективність науково-технічної розробки у випадку її впровадження і комерціалізації потенційним інвестором і проведено обґрунтування економічної доцільності комерціалізації потенційним інвестором.

4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Метою проведення комерційного та технологічного аудиту дослідження за темою «Програмний асистент фахівця з криміналістичного аналізу кіберзлочинів» є визначення рівня науково-технічної досконалості створеної розробки, а також установлення її комерційного потенціалу як результату виконаної науково-технічної діяльності.

Оцінювання науково-технічного рівня розробки та перспектив її комерційного впровадження доцільно здійснювати із використанням п’ятибальної системи за 12-ма критеріями, що наведені у таблиці 4.1 [55].

Таблиця 4.1 – Рекомендовані критерії оцінювання науково-технічного рівня і комерційного потенціалу розробки та бальна оцінка

Бали (за 5-ти бальною шкалою)					
	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено працездатність продукту в реальних умовах
Ринкові переваги (недоліки)					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів

Продовження таблиці 4.1

Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуютьс я у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь- які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання науково-технічного рівня та комерційного потенціалу науково-технічної розробки потрібно звести до таблиці.

Таблиця 4.2 – Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки експертами

Критерії	Експерт (ПІБ, посада)		
	1	2	3
	Бали:		
1. Технічна здійсненність концепції	4	4	4
2. Ринкові переваги (наявність аналогів)	4	4	3
3. Ринкові переваги (ціна продукту)	3	4	4
4. Ринкові переваги (технічні властивості)	4	3	4
5. Ринкові переваги (експлуатаційні витрати)	4	3	4
6. Ринкові перспективи (розмір ринку)	4	4	4
7. Ринкові перспективи (конкуренція)	3	4	3
8. Практична здійсненність (наявність фахівців)	4	4	3
9. Практична здійсненність (наявність фінансів)	1	1	1
10. Практична здійсненність (необхідність нових матеріалів)	3	4	4
11. Практична здійсненність (термін реалізації)	4	4	4
12. Практична здійсненність (розробка документів)	3	3	3
Сума балів	40	43	40
Середньоарифметична сума балів $СБ_с$	41		

На основі результатів розрахунків, поданих у таблиці 4.2, може бути сформульовано висновок щодо науково-технічного рівня та комерційного потенціалу розробки із застосуванням критеріїв, наведених у таблиці 4.3 [55].

Таблиця 4.3 – Науково-технічні рівні та комерційні потенціали розробки

Середньоарифметична сума балів СБ, розрахована на основі висновків експертів	Науково-технічний рівень та комерційний потенціал розробки
41…48	Високий
31…40	Вище середнього
21…30	Середній
11…20	Нижче середнього
0…10	Низький

Згідно з отриманими даними, інтегральний показник комерційного потенціалу науково-технічної розробки за темою «Програмний асистент фахівця з криміналістичного аналізу кіберзлочинів» становить 41 бал, що відповідно до класифікації таблиці 4.3 характеризує її як таку, що має високий ступінь комерційної перспективності та підтверджує доцільність проведення досліджень у цьому напрямі.

4.2 Розрахунок витрат на проведення науково-дослідної роботи

Витрати, пов’язані з виконанням науково-дослідної роботи за темою «Програмний асистент фахівця з криміналістичного аналізу кіберзлочинів», у процесі планування, бухгалтерського обліку та визначення собівартості доцільно систематизувати за встановленими статтями витрат.

4.2.1 Витрати на оплату праці

До статті «Витрати на оплату праці» належать витрати на виплату основної та додаткової заробітної плати керівникам відділів, лабораторій, секторів і груп, науковим, інженерно-технічним працівникам, конструкторам, технологам, креслярам, копіювальникам, лаборантам, робітникам, студентам, аспірантам та іншим працівникам, безпосередньо зайнятим виконанням конкретної теми, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці.

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників ($З_о$) розраховуються у відповідності до посадових окладів працівників, за формулою [55]:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \qquad (4.1)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дн.;

T_p – середнє число робочих днів в місяці, T_p=22 дні.

Результати розрахунків наведено в таблиці 4.4.

Таблиця 4.4 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник науково-дослідної роботи	20000,00	909,1	22	20000,00
Всього				20000,00

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) розраховуються за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i, \quad (4.2)$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}}, \quad (4.3)$$

де $М_М$ – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), $Мм$ = 8000,00 грн (станом на 2025 рік);

$К_і$ – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. Б.2, додаток Б) [55];

$К_с$ – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об’єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати, $К_с$ = 1,15.

$Т_р$ – середнє число робочих днів в місяці, в середньому $Т_р$ = 22 дн;

$t_{зм}$ – тривалість зміни, год.

Результати розрахунків наведено в таблиці 4.5.

Таблиця 4.5 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Підготовка робочого місця та встановлення обчислювального обладнання	5,0	2	1,1	57,5	287,5
Інсталяція та конфігурація системного і прикладного ПЗ для розробки	6,0	3	1,35	70,57	423,42
Налаштування середовища розробки та тестування	5,5	3	1,35	70,57	388,135
Розроблення модулів логіки та обробки даних	20,0	4	1,5	78,41	1568,2
Розроблення модулів обробки мовлення та штучного інтелекту	24,0	5	1,7	88,86	2132,64
Створення інтерфейсу програмного асистента	16,0	4	1,5	78,41	1254,56

Продовження таблиці 4.5.

Побудова бази знань та довідкових матеріалів для аналітика	12,0	3	1,35	70,57	846,84
Інтеграція модулів у єдиний програмний комплекс	10,0	5	1,7	88,86	888,6
Проведення тестування та налагодження програмних модулів	14,0	4	1,5	78,41	1097,74
Проведення контрольного цифрового експерименту	7,0	4	1,5	78,41	548,87
Підготовка технічної документації та методичних матеріалів	9,0	3	1,35	70,57	635,13
Всього	128,5				10071,635

Додаткова заробітна плата дослідників та робітників

Додаткова заробітня плата розраховується як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (4.4)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати, в середньому 11%.

$З_{дод} = (20000,00 + 10071,63) \cdot (11\% / 100\%) = 3307,88$ *грн.*

4.2.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховується як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (4.5)$$

де $Н_{зп}$ – норма нарахування на заробітну плату.

Зн = (20000,00 + 10071,63 + 3307,88) · (22% / 100%) = 7343,5 грн.

4.2.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за темою «Програмний асистент фахівця з криміналістичного аналізу кіберзлочинів».

Витрати на матеріали (*М*), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$M = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j - \sum_{j=1}^{n} В_j \cdot Ц_{в\,j}, \qquad (4.6)$$

де $Н_j$ – норма витрат матеріалу *j*-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу *j*-го найменування, грн/кг;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = *1,1 … 1,15*);

$В_j$ – маса відходів *j*-го найменування, кг;

$Ц_{вj}$ – вартість відходів *j*-го найменування, грн/кг.

Результати розрахунків наведено в таблиці 4.6.

Таблиця 4.6 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 шт, грн	Норма витрат, од.	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Папір 80г/м, А4, Crystal Pro 80, 500арк (клас С+)	169,00	1,000	0	0	185,90
Ручка BIC Round Stick M	14,00	2,000	0	0	30,80
Картридж Canon 728 (3500B002) для принтера MF4410	2648,00	1,000	0	0	2912,8
Всього					3129,50

4.2.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему «Програмний асистент фахівця з криміналістичного аналізу кіберзлочинів», розраховуються, згідно з їхньою номенклатурою, за формулою:

$$К_в = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j \qquad (4.7)$$

де $Н_j$ – кількість комплектуючих j-го виду, шт.;

$Ц_j$ – покупна ціна комплектуючих j-го виду, грн;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = *1,1 … 1,15*).

Результати розрахунків наведено в таблиці 4.7.

Таблиця 4.7 – Витрати на комплектуючі

Найменування комплектуючих	Кількість, шт.	Ціна за штуку, грн	Сума, грн
USB флеш накопичувач ADATA 16GB S102PRO Black USB 3.1	1	158,00	173,80
Всього			173,80

4.2.5 Спецустаткування для наукових (експериментальних) робіт

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування необхідного для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування, монтаж та встановлення. Витрати на «Спецустаткування» відсутні.

4.2.6 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та придбання спеціальних програмних засобів і програмного забезпечення, (програм, алгоритмів, баз даних) необхідних для проведення досліджень, також витрати на їх проектування, формування та встановлення. Витрати на «Програмне забезпечення для наукових (експериментальних) робіт» відсутні, оскільки було вибрано безкоштовне ПЗ для розробки.

4.2.7 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуються з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \qquad (4.8)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

Результати розрахунків наведено в таблиці 4.8.

Таблиця 4.8 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Персональний комп'ютер аналітичного дослідження ПК AMD Ryzen 7 5700G / NVIDIA RTX 3060 / 32 GB DDR4 / 1 TB SSD M2 NVME / ASUS ROG STRIX B550	59699,00	5	1	994,98
Багатофункціональний пристрій i-SENSYS MF4410 Canon	10561,00	5	1	176,01
Маршрутизатор Xiaomi Mesh System AX3000 NE 1pack EU	2499,00	5	1	41,65
Apple MacBook Pro 13, 512GB, Silver with Apple M1, 2020	79993,00	7	1	952,30
Ноутбук Lenovo ThinkPad L14 Gen 2 Black	47051,00	4	1	980,23
ОС Windows 10	8460,00	3	1	235,00
Прикладний пакет Microsoft Office 2019	7840,00	3	1	217,78
Всього				3597,95

4.2.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \quad (4.9)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_е$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), станом на 2025 рік $Ц_е$ = 12,56 грн;

$К_{вні}$ – коефіцієнт, що враховує використання потужності, $К_{вні} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

Результати розрахунків наведено в таблиці 4.9.

Таблиця 4.9 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Персональний комп'ютер аналітичного дослідження ПК AMD Ryzen 7 5700G / NVIDIA RTX 3060 / 32 GB DDR4 / 1 TB SSD M2 NVME / ASUS ROG STRIX B550	0,65	172,0	1375,25
Багатофункціональний пристрій i-SENSYS MF4410 Canon	0,15	5,0	9,22
Маршрутизатор Xiaomi Mesh System AX3000 NE 1pack EU	0,02	172,0	42,31
Apple MacBook Pro 13, 512GB, Silver with Apple M1, 2020	0,06	172,0	126,95
Ноутбук Lenovo ThinkPad L14 Gen 2 Black	0,06	172,0	126,95
Всього			1680,68

4.2.9 Службові відрядження

До статті «Службові відрядження» дослідної роботи на тему «Програмний асистент фахівця з криміналістичного аналізу кіберзлочинів» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов'язані з проведенням випробувань машин та приладів, а також витрати на відрядження на наукові з'їзди, конференції, наради, пов'язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» розраховуємо як 20…25% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{св} = (З_о + З_р) \cdot \frac{H_{св}}{100\%}, \quad (4.10)$$

де $H_{св}$ – норма нарахування за статтею «Службові відрядження», $Н_{св}$ = 20%.

$B_{св}$ = (20000,00 + 10071,63) · 20% / 100% = 6014,20 грн.

4.2.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» розраховуються як 30…45% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{сп} = (З_о + З_р) \cdot \frac{H_{сп}}{100\%}, \quad (4.11)$$

де $Н_{сп}$ – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації», $Н_{сп}$= 30%.

$B_{сп}$ = (20000,00 + 10071,63) · 30 / 100% = 9021,30 грн.

4.2.11 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.12)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», $Н_{ів} = 50\%$.

$I_в = (20000,00 + 10071,63) \cdot 50 / 100\% = 15035,50$ грн.

4.2.12 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов'язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов'язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов'язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$В_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.13)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», $Н_{нзв} = 100\%$.

$В_{нзв} = (20000,00 + 10071,63) \cdot 100 / 100\% = 30071$ грн.

Витрати на проведення науково-дослідної роботи на тему «Програмний асистент фахівця з криміналістичного аналізу кіберзлочинів» розраховуються як сума всіх попередніх статей витрат за формулою:

$$B_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{св} + В_{сп} + І_в + В_{нзв}, \quad (4.14)$$

$B_{заг}$= 20000,00 + 10071,00 + 3307,88 + 7343,50 + 3129,50 + 173,80 + 0,00 + 0,00 + 3597,95 + 1680,68 + 6014,20 + 9021,30 + 15025,50 + 30071,00 = 109446,31 грн.

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (4.15)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,9.

ЗВ = 230978,24 / 0,9 = 121607,01 грн.

4.3 Розрахунок економічної ефективності науково-технічної розробки від її впровадження безпосередньо розробником (замовником)

Результати дослідження, виконаного за темою «Програмний асистент фахівця з криміналістичного аналізу кіберзлочинів», передбачають подальше впровадження на спеціалізованому підприємстві, діяльність якого пов’язана з криміналістичним аналізом кіберзлочинів. З урахуванням функціональної специфіки розробки прогнозується життєвий цикл програмного продукту тривалістю шість років.

Розробка та впровадження автоматизованої системи управління (електронного документообігу, управління логістикою, управління складською

системою, управління перевезеннями тощо) для конкретного підприємства (організації)

В цьому випадку майбутній економічний ефект та ефективність буде формуватися на основі використання таких показників: Δ*Пя* – зростання прибутку підприємства внаслідок зниження витрат на оплату праці працівників, які виконують окремі виробничі чи інформаційно-технічні управлінські функції, грн. Причому Δ*Пя* може бути визначено як [55]:

$$\Delta П_я = \frac{ЧП \cdot ЗП \cdot 12}{N} - \frac{(0,2...0,6) \cdot ЗВ}{\Delta N_i}, \tag{4.16}$$

де *ЧП* – чисельність працівників, які виконують певні функції вручну, осіб (*ЧП* = 10);

ЗП – середня заробітна плата працівника, який виконує відповідну функцію вручну, грн (*ЗП = 30000)*;

ЗВ – приблизні витрати на розробку автоматизованої системи управління, грн (*ЗВ = 121607)*;

Пя – прибуток, який отримує підприємство від автоматизації виконання окремої виробничої чи інформаційно-технічної управлінської функції у кожному із років після впровадження науково-технічної розробки, грн.

Цей прибуток можна приблизно оцінити, виходячи з формули:

$$П_я = \frac{\Delta ЧП \cdot ЗП \cdot 12}{N}, \tag{4.17}$$

де Δ*ЧП* – економія чисельності працівників, виконання виробничої чи управлінської функції яких було автоматизовано в аналізованому році, осіб (Δ*ЧП = 5)*;

N – кількість функцій, які виконуються вручну у році до впровадження результатів нової науково-технічної розробки, шт ($N = 500$);

ΔNi – прогнозоване зростання кількості виробничих чи інформаційно-технічних управлінських функцій, виконання яких автоматизується, в аналізованому році (відносно року до впровадження цієї розробки), шт ($\Delta Ni = 1000$).

Оскільки засіб пришвидшує роботу над функціями приблизно на 50%, Кількість виконуваних функцій збільшиться з 500 до 1000, а кількість працівників, необхідних для виконання такої кількості функцій як до впровадження засобу зменшиться з 10 до 5. Тоді:

$$\Delta Пя = (10 \cdot 30000 \cdot 12) / 500 – (0,2 \cdot 121607) / 1000 = 7175,68$$

$$Пя = (5 \cdot 30000 \cdot 12) / 500 = 3600$$

Для даного випадку можливе збільшення чистого прибутку підприємства $\Delta Пi$ для кожного із років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комерціалізації науково-технічної розробки, розраховується за формулою:

$$\Delta П_i = (\Delta П_я \cdot N + П_я \cdot \Delta N)_i, \tag{4.18}$$

де $\Delta Пя$ – покращення основного якісного показника від впровадження на підприємстві результатів науково-технічної розробки в аналізованому році;

N – основний кількісний показник, який визначає обсяг діяльності підприємства у році до впровадження результатів нової науково-технічної розробки;

Пя – основний якісний показник, який визначає результати діяльності підприємства у кожному із років після впровадження науково-технічної розробки;

ΔNi – зміна основного кількісного показника діяльності підприємства в результаті впровадження науково-технічної розробки в аналізованому році.

$$\Delta Пі = (7175{,}68 \cdot 500 + 3600 \cdot 1000) = 7187840$$

Далі розраховується приведена вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати розробник (замовник) від можливого впровадження науково-технічної розробки на власному підприємстві:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \tag{4.19}$$

де $\Delta Пі$ – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн;

T – період часу, протягом якого очікується отримання позитивних результатів від впровадження науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, $\tau = 0{,}05 \ldots 0{,}15$;

t – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання підприємством збільшеної величини чистого прибутку в аналізованому році.

$$ПП = \sum_{i=1}^{5} \frac{7187840}{(1+\tau)} = 34199238$$

Далі розраховується величина початкових інвестицій *PV* , які розробник (замовник) має вкласти для здійснення науково-технічної розробки. Для цього можна використати формулу:

$$PV = k_{розр} \cdot ЗВ, \tag{4.20}$$

де *кроzр* – коефіцієнт, що враховує витрати розробника (замовника) на впровадження науково-технічної розробки. Це можуть бути витрати на підготовку приміщень, розробку технологій, навчання персоналу, маркетингові заходи тощо; зазвичай *кроzр =2...5*, але може бути і більшим;

ЗВ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, грн.

PV = 3 · 121607 = 364821

Тоді абсолютний економічний ефект *Еабс* або чистий приведений дохід *(NPV, Net Present Value)* для розробника (замовника) від можливого впровадження науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV, \tag{4.21}$$

де *ПП* – приведена вартість збільшення всіх чистих прибутків від можливого впровадження науково-технічної розробки, грн;

PV – теперішня вартість початкових інвестицій, грн.

Еабс = ПП – PV = 34199238 – 364821 = 33834417

Для остаточного прийняття рішення в такому випадку необхідно розрахувати внутрішню економічну дохідність *Ев* або показник внутрішньої норми дохідності *(IRR, Internal Rate of Return)* вкладених розробником (замовником) коштів.

Внутрішня економічна дохідність інвестицій *Ев*, які можуть бути вкладені розробником (замовником) у впровадження науково-технічної розробки, розраховується за формулою:

$$E_в = \sqrt[Тж]{1 + \frac{E_{абс}}{PV}} - 1, \tag{4.22}$$

де *Еабс* – абсолютний економічний ефект вкладених інвестицій, грн;

PV – теперішня вартість початкових інвестицій, грн;

Тж – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження, роки.

$$\text{Ев} = \sqrt[6]{1 + \frac{33834417}{364821}} - 1 = 1{,}13$$

Далі розраховується період окупності інвестицій *Ток* (*DPP, Discounted Payback Period*), які можуть бути вкладені розробником (замовником) у впровадження та комерціалізацію науково-технічної розробки:

$$T_{ок} = \frac{1}{E_в}, \tag{4.23}$$

де *Ев* – внутрішня економічна дохідність вкладених інвестицій.

Якщо *Ток* < 3-х років, то це свідчить про економічну ефективність впровадження науково-технічної розробки її розробником (замовником).

Ток = 1 / 1,13 = 0,88

Результат свідчить про комерційну привабливість науково-технічної розробки і може спонукати підприємство профінансувати впровадження даної розробки.

Висновки до розділу 4

За результатами проведених досліджень встановлено, що рівень комерційного потенціалу науково-технічної розробки за темою «Програмний асистент фахівця з криміналістичного аналізу кіберзлочинів» становить 41 бал, що свідчить про високий ступінь її ринкової перспективності та актуальність виконання дослідження.

Розрахований термін окупності становить 0,88 року, що є істотно меншим за нормативний трирічний період. Це підкреслює інвестиційну привабливість проєкту та свідчить про потенційну зацікавленість підприємств у фінансуванні його впровадження.

Таким чином, встановлено доцільність подальшого проведення науково-дослідної роботи за зазначеною тематикою.

ВИСНОВКИ

У висновках магістерської роботи представлено підсумки, що узагальнено відображають мету, завдання й наукову новизну дослідження.

1. У результаті виконання магістерської кваліфікаційної роботи сформовано та реалізовано концепцію програмного асистента для підтримки криміналістичного аналізу кіберзлочинів, що забезпечує інтелектуальне зіставлення опису ознак правопорушення з відповідними нормами кримінального законодавства України. Розроблена система вирішує поставлене у роботі завдання, демонструючи наукову і практичну новизну у сфері цифрової криміналістики.

2. Проведений аналіз нормативно-правової бази, сучасних тенденцій та технологій у галузі розслідування кіберзлочинів дозволив визначити ключові вимоги до функціонування цифрових інструментів криміналістичного призначення. Це забезпечило відповідність розробленої системи актуальним підходам міжнародної практики та підвищило її цінність для використання у правоохоронній діяльності.

3. Запропонована архітектура асистента, що включає модулі обробки мовлення, штучного інтелекту, бази знань та користувацького інтерфейсу, продемонструвала здатність комплексно реалізовувати процес криміналістичного аналізу. Узгодженість моделей даних, алгоритмів та інтерфейсних рішень забезпечує зручність застосування і можливість подальшої інтеграції у інформаційні системи відповідних органів.

4. У ході модельних експериментів підтверджено правильність реалізованих алгоритмів логічного мапінгу ознак кіберзлочину на статті Кримінального кодексу України. Система коректно визначає належність діяння до домінуючих груп кіберправопорушень навіть у випадках неповного або побутового формулювання вхідного опису.

5. Практичне тестування програмного забезпечення проведено на основі 200 контрольних запитів двох типів: 1). 100 тестів з різними формулюваннями одного

складу злочину – правильність становить 96%; 2). 100 тестів зі схожими описами різних складів злочину – правильність становить 97%. Узагальнений показник точності, обчислений за формулою становить 97,5%, що підтверджує високу достовірність результатів.

6. Виявлені відхилення не стосувалися неправильного визначення статті: асистент вірно ідентифікував норму кримінального закону, однак у поодиноких випадках помилявся щодо її частини. Причиною цього було недостатнє уточнення обставин у користувацькому тексті, оскільки окремі частини статті можуть мати однакові основні складові із відмінністю лише у кваліфікуючому критерії. З урахуванням того, що система попереджає про потребу додаткових уточнень, такі похибки є допустимими у статистичному сенсі та не впливають на загальну оцінку ефективності.

7. Економічний аналіз показав, що рівень комерційного потенціалу науково-технічної розробки за темою «Програмний асистент фахівця з криміналістичного аналізу кіберзлочинів» становить 41 бал, що свідчить про її високу ринкову перспективність. Розрахований термін окупності – 0,88 року, що є суттєво меншим за нормативний трирічний період, підкреслює інвестиційну привабливість проєкту та перспективність фінансування його впровадження. Таким чином, підтверджено економічну доцільність розвитку і комерціалізації даної розробки.

8. Отримані результати мають значущість для правоохоронних органів, експертних установ та освітніх інституцій, оскільки сприяють підвищенню якості та оперативності криміналістичного аналізу кіберзлочинів, а також зниженню ризику суб’єктивних помилок на початкових етапах розслідування.

9. Робота має вагомий потенціал для подальшого наукового розвитку. Перспективами є розширення бази знань, удосконалення моделей розпізнавання контексту із застосуванням методів глибинного навчання, підтримка мультимодальних даних, інтеграція з системами автоматичного збору та аналізу цифрових артефактів, а також адаптація до міжнародних правових класифікацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Майданевич, Л. О., Тарасюк, М. Б., Комп'ютерно-технічна експертиза: основні аспекти підготовки до проведення, ВНТУ, 2025.
2. Майданевич Л. О., Кирбят'єв О. О., Тарасюк М. Б., Алгоритм отримання електронних доказів в умовах потенційного самознищення електронних (цифрових) слідів. *Кримінальний аналіз і кібербезпека: об'єднання зусиль для нових викликів*, Одеський державний університет внутрішніх справ, 23 травня 2025 року.
3. Майданевич Л. О., Войтович О. П, Шелепало Г. В. Техніко-криміналістичне забезпечення кіберзлочинів : навч. посіб. Вінниця : 2025. 5 с.
4. Kent, K., Chevalier, S., Grance, T., Dang, H. Guide to Integrating Forensic Techniques into Incident Response (NIST Special Publication 800-86). Gaithersburg, MD : National Institute of Standards and Technology, 2006. 97 p. ES-1.
5. Бараненко Р. В. Кіберзлочин, комп'ютерний злочин чи кіберправопорушення? Аналіз особливостей застосування термінології. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право.* Випуск 1 (49) 2021. С. 85-90.
6. Азаров Д.С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : дис. … канд. юрид. наук : 12.00.08. НАНУ. Інститут держави і права ім. В.М. Корецького. Київ, 2002. 228 с.
7. Карчевский Н.В. Кіберправопорушення чи правопорушення в сфері використання інформаційних технологій? *Кібербезпека в Україні: правові та організаційні питання* : матеріали всеукр. наук.-практ. конф., м. Одеса, 21 жовтня 2016 р. Одеса : ОДУВС, 2016. С. 10–15.
8. Скулиш Є.Д. Теоретико-методологічні засади визначення об'єкта та предмета кіберзлочинів. *Правова інформатика.* 2014. *№ 2.* С. 47–53.
9. Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права*. 2022. Вип. 1. С. 176-180.
10. Степанюк Р. Л., Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник ЛДУВС ім. Е. О. Дідоренка*. 2022. Вип. 3 (99). С. 283-294.
11. Когутич І. І. Застосування цифрових технологій –новий напрям криміналістики. *Наукові читання пам'яті Ганса Гросса: збірник тез*

міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2021 р.). Чернівецький національний університет імені Юрія Федьковича. Чернівці : Технодрук, 2021. С. 79-84.

12. Думчиков М. О. Процеси діджиталізації і криміналістика: ректроспективний аналіз. *Криміналістика і судова експертиза*. 2020. Вип. 65. С. 100-108.
13. Guarino A. Digital Forensics as a Big Data Challenge. In: Reimer, H., Pohlmann, N., Schneider, W. (eds) *ISSE 2013 Securing Electronic Business Processes*. Springer Vieweg, Wiesba den. DOI : 10.1007/978-3-658-03371-2_17.
14. Delp E., Memo N., Wu M. Digital forensics. *IEEE Signal Processing Magazine*. 2009. Iss. 26(2). P. 14–15.
15. Vincze Eva A. Challenges in digital forensics. *Police Practice and Research*. 2016. Iss. 17:2. P. 183–194. DOI: 10.1080/15614263.2015.1128163.
16. Ricci S.C. Ieong. FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*. 2006. Vol. 3. Supplement. P. 29–36. URL: https://doi.org/10.1016/ j.diin.2006.06.004. (дата звернення: 22.09.2025)
17. Convention on Cybercrime (European Treaty Series No 185: Budapest, 23 November 2001). Strasbourg: , 2001. URL : https://eur-lex.europa.eu/EN/legal-content/summary/convention-on-cybercrime.html (дата звернення: 22.09.2025)
18. Enhanced co-operation and disclosure of electronic evidence: 22 countries sign new protocol to Cybercrime Convention. Council of Europe. URL : https://www.coe.int/en/web/portal/-/enhanced-co-operation-and-disclosure-of-electronic-evidence-22-countries-sign-new-protocol-to-cybercrime-convention (дата звернення: 22.09.2025)
19. United Nations General Assembly, Resolution 57/239: «The fight against the criminal misuse of information technologies.» New York: , 2002. URL : https://docs.un.org/en/A/RES/57/239 (дата звернення: 22.09.2025)
20. United Nations General Assembly, Resolution 64/211: «Creation of a comprehensive international convention on combating the use of information and communications technologies for criminal purposes.» New York: United Nations, 2009. URL : https://docs.un.org/en/a/res/64/211 (дата звернення: 08.10.2023)
21. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. Official Journal of the European Union (OJ L 333, 27.12.2022, p. 80).

URL : https://eur-lex.europa.eu/eli/dir/2022/2555/oj (дата звернення: 22.09.2025)

22. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act). Official Journal of the European Union (OJ L 151, 07.06.2019, p. 15). URL : https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng (дата звернення: 22.09.2025)
23. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union (OJ L 119, 04.05.2016, p. 1). URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (дата звернення: 22.09.2025)
24. Конвенція про кіберзлочинність : від 23.11.2001р. Верховна Рада України. *Офіційний вісник України від 10.09.2007.* №65, стор.107. URL : https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 12.09.2025)
25. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. ст. 32.
26. Кримінальний кодекс України : Закон України від 5 квітня 2001 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131. Розд. XVI, ст. 361–363.
27. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.
28. Урядова команда реагування на комп’ютерні надзвичайні події України .URL : https://cert.gov.ua/ (дата звернення: 22.09.2025)
29. Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.
30. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 5 лип. 1994 р. № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.
31. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.

32. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 5 жовт. 2017 р. № 2155-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 400.

33. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серп. 2021 р. № 447/2021. *Офіційний вісник Президента України*. 2021. № 22. Ст. 1172.

34. ISO/IEC 27037:2012. Information technology, Security techniques, Guidelines for identification, collection, acquisition and preservation of digital evidence. *Geneva: International Organization for Standardization*, 2012. 36 p.

35. Kent, K., Chevalier, S., Grance, T., Dang, H. Guide to Integrating Forensic Techniques into Incident Response (NIST Special Publication 800-86). Gaithersburg, MD: National Institute of Standards and Technology, 2006. 97 p.

36. ISO/IEC 27041:2015. Information technology, Security techniques, Guidance on assuring suitability and adequacy of incident investigative method. *Geneva: International Organization for Standardization*, 2015. 24 p.

37. ISO/IEC 27042:2015. Information technology, Security techniques, Guidelines for the analysis and interpretation of digital evidence. *Geneva: International Organization for Standardization*, 2015. 44 p.

38. ISO/IEC 27043:2015. Information technology, Security techniques, Incident investigation principles and processes. *Geneva: International Organization for Standardization*, 2015. 38 p.

39. Brezinski, D., Killalea, T. Guidelines for Evidence Collection and Archiving (RFC 3227). Fremont, CA: Internet Engineering Task Force (IETF), 2002. 20 p. URL : https://www.rfc-editor.org/rfc/rfc3227 (дата звернення: 25.09.2025)

40. Cybersecurity and Infrastructure Security Agency. URL : https://www.cisa.gov/ (дата звернення: 25.09.2025)

41. Global Information Assurance Certification. URL : https://www.giac.org/ (дата звернення: 25.09.2025)

42. SysAdmin, Audit, Network and Security Institute. URL : https://www.sans.org/ (дата звернення: 25.09.2025)

43. Мова програмування Python. URL : https://docs.python.org/3/ (дата звернення: 20.10.2025)

44. Мова програмування C++. URL : https://learn.microsoft.com/en-us/cpp/?view=msvc-170 (дата звернення: 20.10.2025)

45. Мова програмування C#. URL : https://learn.microsoft.com/en-us/dotnet/csharp/ (дата звернення: 20.10.2025)
46. Середовище програмування Visual Studio. URL : https://learn.microsoft.com/en-us/visualstudio/windows/?view=vs-2022 (дата звернення: 21.10.2025)
47. Середовище програмування Visual Studio Code. URL : https://code.visualstudio.com/docs (дата звернення: 21.10.2025)
48. Середовище програмування Jupyter Notebook. URL : https://docs.jupyter.org/en/latest/ (дата звернення: 21.10.2025)
49. Фреймворк Flet. URL : https://flet.dev/docs/ (дата звернення: 22.10.2025)
50. Фреймворк PyQT5. URL : https://doc.qt.io/qtforpython-6/ (дата звернення: 22.10.2025)
51. Фреймворк PySide6. URL : https://doc.qt.io/qtforpython-6/PySide6/QtWidgets/index.html (дата звернення: 22.10.2025)
52. Бібліотека SQLite .URL : https://sqlite.org/docs.html (дата звернення: 23.10.2025)
53. Система керування базами даних MySQL. URL : https://dev.mysql.com/doc/ (дата звернення: 23.10.2025)
54. Система керування базами даних PostgreSQL. URL : https://www.postgresql.org/docs/ (дата звернення: 23.10.2025)
55. Козловський В. О. , Лесько О. Й., Кавецький В. В. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт. Вінниця. ВНТУ. 2021. 42 с.

ДОДАТКИ

Додаток А

ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Назва роботи: Програмний асистент фахівця з криміналістичного аналізу кіберзлочинів.

Автор роботи: Тарасюк Микола Борисович

Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ , група 1 БС-24м

Коефіцієнт подібності текстових запозичень, виявлених у роботі системою StrikePlagiarism **4, 14%**

Висновок щодо перевірки кваліфікаційної роботи (відмітити потрібне)

√ Запозичення, виявлені у роботі, є законними і не містять ознак плагіату, фабрикації, фальсифікації. Роботу прийняти до захисту

☐ У роботі не виявлено ознак плагіату, фабрикації, фальсифікації, але надмірна кількість текстових запозичень та/або наявність типових розрахунків не дозволяють прийняти рішення про оригінальність та самостійність її виконання. Роботу направити на доопрацювання.

☐ У роботі виявлено ознаки плагіату та/або текстових маніпуляцій як спроб укриття плагіату, фабрикації, фальсифікації, що суперечить вимогам законодавства та нормам академічної доброчесності. Робота до захисту не приймається.

Експертна комісія:

В. о. зав. кафедри ЗІ д. т. н., проф. _____ Володимир ЛУЖЕЦЬКИЙ

Гарант освітньої програми «Безпека інформаційних і комунікаційних систем» к.т.н., доцент _____ Олеся ВОЙТОВИЧ

Особа, відповідальна за перевірку _____ Валентина КАПЛУН

З висновком експертної комісії ознайомлений(-на)

Керівник _____ Леонід МАЙДАНЕВИЧ

Здобувач _____ Микола ТАРАСЮК

Додаток Б
Лістинг програми

```
import os
import re
import sqlite3
import pandas as pd
import flet as ft

from PyPDF2 import PdfReader
from sklearn.pipeline import Pipeline
from sklearn.linear_model import LogisticRegression
from sklearn.feature_extraction.text import TfidfVectorizer
from sentence_transformers import SentenceTransformer, util

BASE_PATH = os.path.dirname(__file__)
DB_PATH = os.path.join(BASE_PATH, "law.db")

def load_articles_from_db():
    if not os.path.exists(DB_PATH):
        raise FileNotFoundError(f"База даних не знайдена: {DB_PATH}")

    conn = sqlite3.connect(DB_PATH)
    cursor = conn.cursor()
    cursor.execute("""
        SELECT label, dianyia, predmet, poterpyliy,
               naslidky, obstavyny, subiekt, forma_vyny, meta
        FROM articles
    """)
    rows = cursor.fetchall()
    conn.close()

    data = []
    for r in rows:
        data.append({
            "label": r[0],
            "діяння": r[1],
            "предмет": r[2],
            "потерпілий": r[3],
            "наслідки": r[4],
            "обставини": r[5],
            "субєкт": r[6],
            "форма_вини": r[7],
            "мета": r[8]
        })
    return data

articles = load_articles_from_db()
df = pd.DataFrame(articles).fillna("")

def combine(row):
```

```
    parts = [
        row["діяння"], row["предмет"], row["потерпілий"],
        row["наслідки"], row["обставини"], row["суб'єкт"],
        row["форма_вини"], row["мета"]
    ]
    return " ".join(str(p) for p in parts if p)

df["text"] = df.apply(combine, axis=1)

X = df["text"]
y = df["label"]

model = Pipeline([
    ("tfidf", TfidfVectorizer()),
    ("clf", LogisticRegression(max_iter=3000))
])
model.fit(X, y)

embedder = SentenceTransformer("sentence-transformers/paraphrase-
multilingual-MiniLM-L12-v2")
embeddings = embedder.encode(df["text"].tolist(), convert_to_tensor=True)

def normalize_text(txt):
    txt = txt.lower().replace("’", "'")
    txt = re.sub(r"[^\w\si']+", " ", txt)
    return re.sub(r"\s+", " ", txt).strip()

def semantic_match(text, top_k=3):
    q_emb = embedder.encode([text], convert_to_tensor=True)
    sim = util.cos_sim(q_emb, embeddings)[0]
    idx = sim.argsort(descending=True)[:top_k]
    return [{"label": df.iloc[int(i)]["label"], "score":
float(sim[int(i)])} for i in idx]

def determine_section(label):
    m = re.search(r"(\d+)", label)
    if not m:
        return "Невідомий розділ"
    n = int(m.group(1))
    if 361 <= n <= 363:
        return "Розділ XVI — Злочини у сфері ЕОМ"
    if 190 == n:
        return "Розділ VI — Проти власності"
    if 200 == n:
        return "Розділ VII — Господарські злочини"
    return "Потребує уточнення"

def AI_response(text: str) -> str:
    t = normalize_text(text)

    if not any(w in t for w in CRIME_KEYWORDS):
```

```
        return "Недостатньо ознак кіберзлочину в описі."

    matches = semantic_match(t)
    top = matches[0]
    if top["score"] < 0.15:
        return f"Семантична відповідність слабка
(score={top['score']:.2f})"

    pred = model.predict([t])[0]

    if any(w in t for w in ACCESS_KEYWORDS):
        for m in matches:
            if "362" in m["label"]:
                pred = m["label"]
                break

    section = determine_section(pred)

    return f"""Попередня юридична кваліфікація:

За поданими складовими діяння попередньо відповідає {pred} КК України.
({section})

Увага: юридична оцінка може бути уточнена після визначення фактичних
обставин."""

def create_pdf_accordion(filename, text, page):
    display_name = os.path.splitext(filename)[0]

    content_box = ft.Container(
        content=ft.Column([ft.Text(text, selectable=True)],
scroll="auto", spacing=8),
        bgcolor="#2E2E2E",
        padding=15,
        border_radius=12,
        visible=False,
        height=300,
    )

    arrow_btn = ft.IconButton(icon=ft.Icons.KEYBOARD_ARROW_RIGHT)

    def toggle(e):
        content_box.visible = not content_box.visible
        arrow_btn.icon = ft.Icons.KEYBOARD_ARROW_DOWN if
content_box.visible else ft.Icons.KEYBOARD_ARROW_RIGHT
        page.update()

    arrow_btn.on_click = toggle

    header_row = ft.Row(
```

```
        [arrow_btn, ft.Text(display_name, weight=ft.FontWeight.BOLD,
size=16)],
        alignment="start",
    )

    header = ft.Container(
        content=header_row,
        padding=10,
        border_radius=12,
        bgcolor="#252525",
        on_click=toggle,
    )

    card = ft.Container(
        content=ft.Column([header, content_box], spacing=4),
        border_radius=16,
        padding=6,
        bgcolor="#181818",
    )

    wrapper = ft.Column([card], spacing=0)
    wrapper.data = display_name
    return wrapper

def load_pdf_list(page, folder_name):
    pdf_controls = []

    if not os.path.exists(folder_name):
        return [ft.Text(f"Папка '{folder_name}' не знайдена!")]

    for filename in os.listdir(folder_name):
        if filename.lower().endswith(".pdf"):
            path = os.path.join(folder_name, filename)
            try:
                reader = PdfReader(path)
                text = ""
                for page_obj in reader.pages:
                    t = page_obj.extract_text()
                    if t:
                        text += t + "\n"
                if not text.strip():
                    text = "[Не вдалося витягнути текст]"
            except:
                text = "[Помилка читання PDF]"

            pdf_controls.append(create_pdf_accordion(filename, text,
page))

    return pdf_controls or [ft.Text("У цій папці немає PDF-файлів.")]

def main(page: ft.Page):
```

```
    page.title = "Асистент"
    page.theme_mode = ft.ThemeMode.DARK
    page.theme = ft.Theme(color_scheme_seed="teal")

    page.window_min_width = 900
    page.window_min_height = 600
    page.padding = 20

    current_title = ft.Text("Головна сторінка", size=22,
weight=ft.FontWeight.BOLD)
    back_icon = ft.IconButton(
        icon=ft.Icons.ARROW_BACK_ROUNDED,
        tooltip="На головну",
        visible=False,
    )

    top_bar = ft.Container(
        content=ft.Row([back_icon, current_title], alignment="start"),
        bgcolor="#1E1E1E",
        padding=10,
        border_radius=20,
    )

    chat_messages = ft.Column(expand=True, scroll="auto", spacing=12,
auto_scroll=True)
    bubble_width = 550

    def add_user_bubble(text):
        chat_messages.controls.append(
            ft.Row(
                [
                    ft.Container(content=ft.Text(text),
bgcolor="#1565C0",
                                 padding=10, border_radius=16,
width=bubble_width),
                    ft.Text("", size=20),
                ],
                alignment="end",
            )
        )
        chat_messages.update()
        chat_messages.scroll_to("end")

    def add_bot_bubble(text):
        chat_messages.controls.append(
            ft.Row(
                [
                    ft.Text("", size=20),
                    ft.Container(content=ft.Text(text),
bgcolor="#303030",
```

```
                                    padding=10, border_radius=16,
width=bubble_width),
                ],
                alignment="start",
            )
        )
        chat_messages.update()
        chat_messages.scroll_to("end")

    user_input = ft.TextField(
        hint_text="Введіть повідомлення...",
        expand=True,
        filled=True,
        border_radius=20,
    )

    def process_message(text):
        add_user_bubble(text)
        try:
            reply = AI_response(text)
        except Exception as err:
            reply = f"Помилка аналізу: {err}"
        add_bot_bubble(reply)

    def send_message(e):
        text = user_input.value.strip()
        if not text:
            return

        user_input.value = ""

        if switcher.content == home_view:
            go_chat()

        process_message(text)
        page.update()

    send_btn = ft.IconButton(icon=ft.Icons.SEND_ROUNDED,
on_click=send_message)
    user_input.on_submit = send_message

    chat_view = ft.Column(
        [
            ft.Text("Чат-бот", size=22, weight=ft.FontWeight.BOLD),
            ft.Container(chat_messages, expand=True),
            ft.Container(ft.Row([user_input, send_btn]),
bgcolor="#1A1A1A", padding=10, border_radius=20),
        ],
        expand=True,
    )
```

```
    home_intro = ft.Column(
        [
            ft.Text("Ласкаво просимо!", size=26,
weight=ft.FontWeight.BOLD),
            ft.Text(
                "Оберіть розділ для перегляду документів або напишіть
запит у чаті — "
                "система допоможе з аналізом кіберзлочинів та нормативної
бази.",
                size=14,
                opacity=0.8,
            ),
        ],
        spacing=8,
    )

    FUNCTION_FOLDERS = {
        "Статті": "articles",
        "Закони": "laws",
        "Стандарти": "standards",
        "Алгоритми": "algorithms",
    }

    def menu_btn(label, icon):
        return ft.ElevatedButton(
            text=label,
            icon=icon,
            width=200,
            height=60,
            style=ft.ButtonStyle(
                shape=ft.RoundedRectangleBorder(radius=18),
                padding=ft.padding.symmetric(horizontal=10, vertical=10),
            ),
            on_click=lambda e, x=label: go_function(x),
        )

    home_buttons = ft.ResponsiveRow(
        controls=[
            ft.Container(
                content=menu_btn("Статті", ft.Icons.DESCRIPTION_ROUNDED),
                col={"xs": 12, "sm": 6, "md": 3},
            ),
            ft.Container(
                content=menu_btn("Закони", ft.Icons.GAVEL_ROUNDED),
                col={"xs": 12, "sm": 6, "md": 3},
            ),
            ft.Container(
                content=menu_btn("Стандарти",
ft.Icons.LIBRARY_BOOKS_ROUNDED),
                col={"xs": 12, "sm": 6, "md": 3},
            ),
```

```
            ft.Container(
                content=menu_btn("Алгоритми", ft.Icons.BUILD_ROUNDED),
                col={"xs": 12, "sm": 6, "md": 3},
            ),
        ],
        spacing=10,
        run_spacing=10,
    )

    home_bottom = ft.Container(
        content=ft.Row([user_input, send_btn], alignment="center"),
        border_radius=20,
        bgcolor="#1A1A1A",
        padding=10,
    )

    home_view = ft.Column(
        [
            ft.Column([home_intro, home_buttons], alignment="center",
spacing=20, expand=True),
            home_bottom,
        ],
        expand=True,
        alignment="spaceBetween",
    )

    pdf_column = ft.Column(expand=True, scroll="auto")
    pdf_all_controls = []

    def on_pdf_search_change(e):
        query = e.control.value.lower().strip()
        if not query:
            pdf_column.controls = pdf_all_controls
        else:
            filtered = [c for c in pdf_all_controls if isinstance(c.data,
str) and query in c.data.lower()]
            pdf_column.controls = filtered or [ft.Text("Нічого не
знайдено")]
        page.update()

    pdf_search = ft.TextField(
        hint_text="Пошук по документах...",
        prefix_icon=ft.Icons.SEARCH_ROUNDED,
        border_radius=20,
        on_change=on_pdf_search_change,
    )

    function_view = ft.Column(
        [
            pdf_search,
            ft.Container(pdf_column, expand=True),
```

```
        ],
        expand=True,
    )

    switcher = ft.AnimatedSwitcher(
        home_view,
        duration=300,
        transition=ft.AnimatedSwitcherTransition.FADE,
        expand=True,
    )

    page.add(ft.Column([top_bar, switcher], expand=True))

    def fade_to(view):
        switcher.content = view
        page.update()

    def go_home():
        back_icon.visible = False
        current_title.value = "Головна сторінка"
        fade_to(home_view)

    def go_chat():
        back_icon.visible = True
        current_title.value = "Бот-асистент"
        fade_to(chat_view)

    def go_function(name):
        nonlocal pdf_all_controls
        back_icon.visible = True
        current_title.value = name

        folder = FUNCTION_FOLDERS[name]
        pdf_all_controls = load_pdf_list(page, folder)
        pdf_column.controls = pdf_all_controls
        pdf_search.value = ""

        fade_to(function_view)

    back_icon.on_click = lambda e: go_home()

    go_home()

ft.app(target=main)
```

ІЛЮСТРАТИВНА ЧАСТИНА

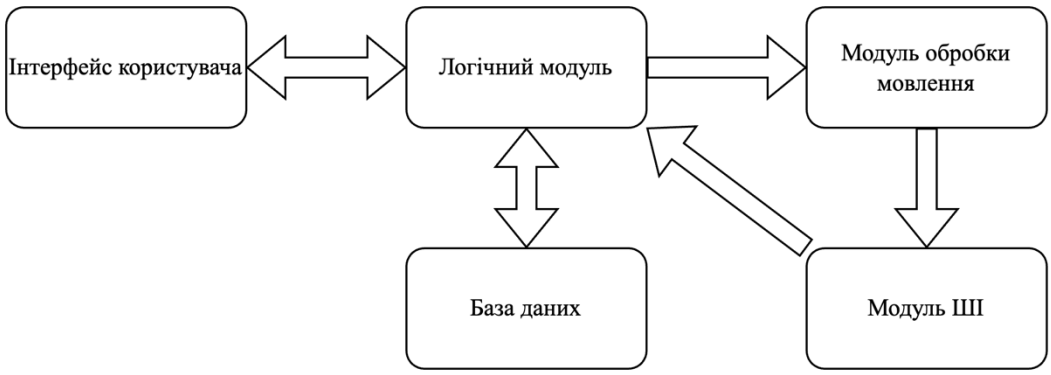
ПРОГРАМНИЙ АСИСТЕНТ ФАХІВЦЯ З КРИМІНАЛІСТИЧНОГО АНАЛІЗУ КІБЕРЗЛОЧИНІВ

(Назва магістерської кваліфікаційної роботи)

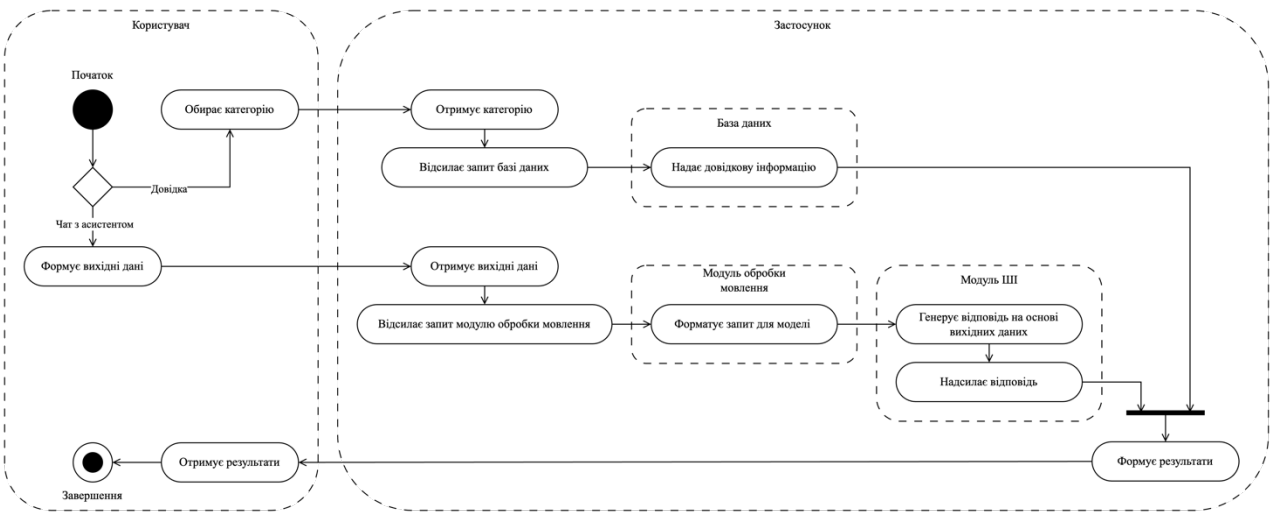
Виконав: студент групи 1БС-24 м
спеціальності 125 Кібербезпека та захист інформації
_____ Микола ТАРАСЮК
16 грудня 2025 р.

Керівник: к. т. н., доцент каф. ЗІ
_____ Леонід МАЙДАНЕВИЧ
16 грудня 2025 р.

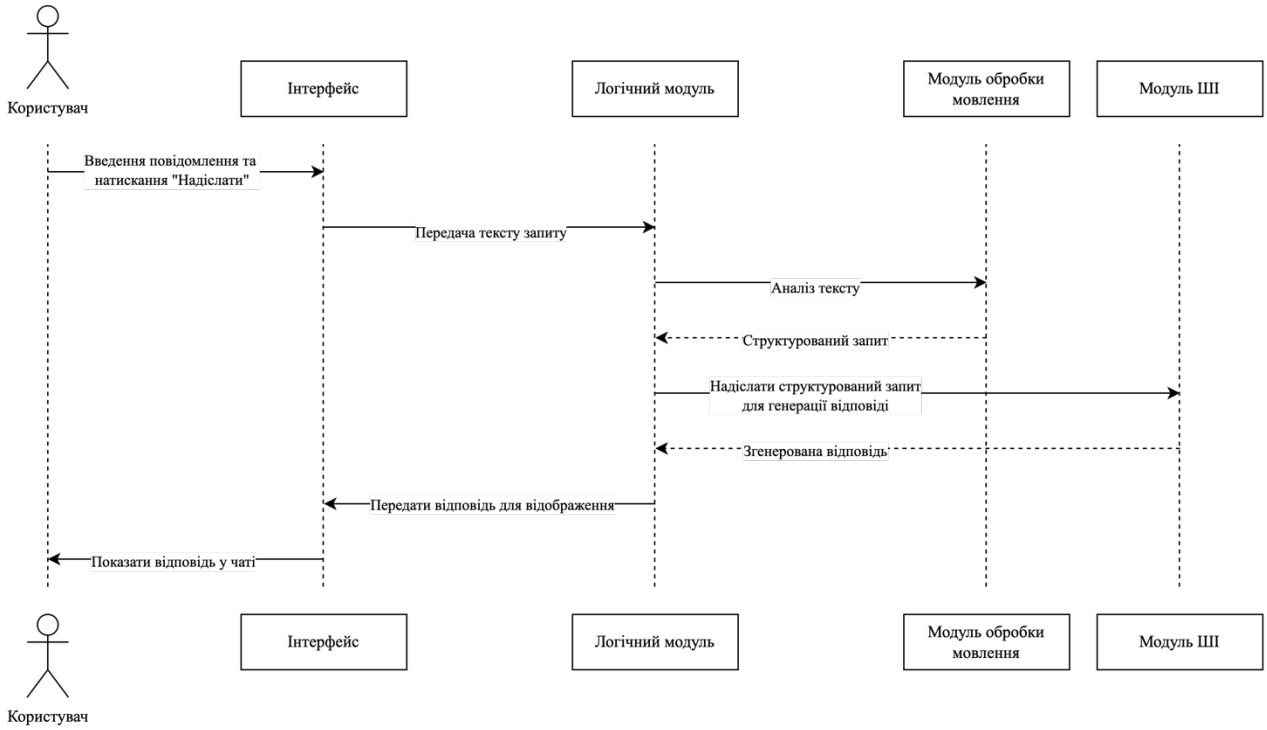
UML-ДІАГРАМА ВЗАЄМОДІЇ СКЛАДОВИХ ПРОГРАМНОГО АСИСТЕНТА ФАХІВЦЯ З КРИМІНАЛІСТИЧНОГО АНАЛІЗУ КІБЕРЗЛОЧИНІВ



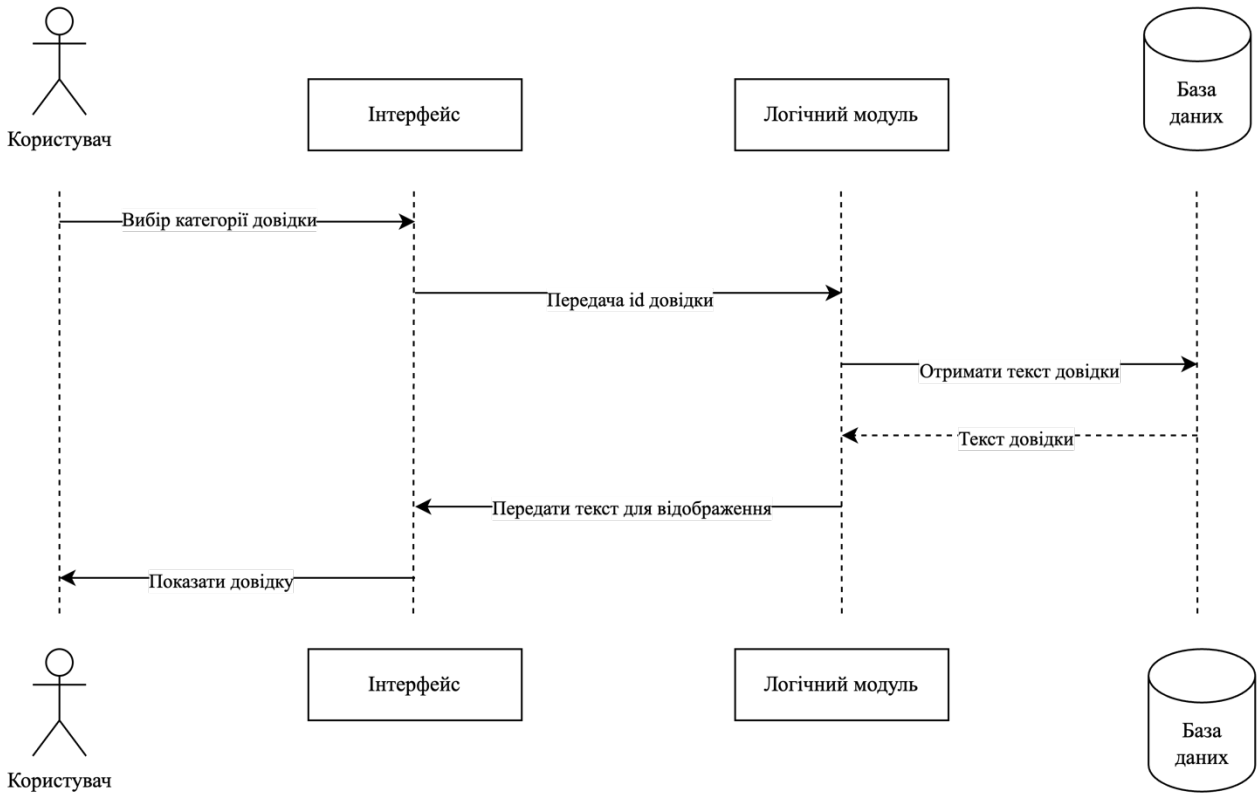
UML-ДІАГРАМА АКТИВНОСТІ ПРОЦЕСУ ОБРОБКИ ЗАПИТІВ КОРИСТУВАЧА



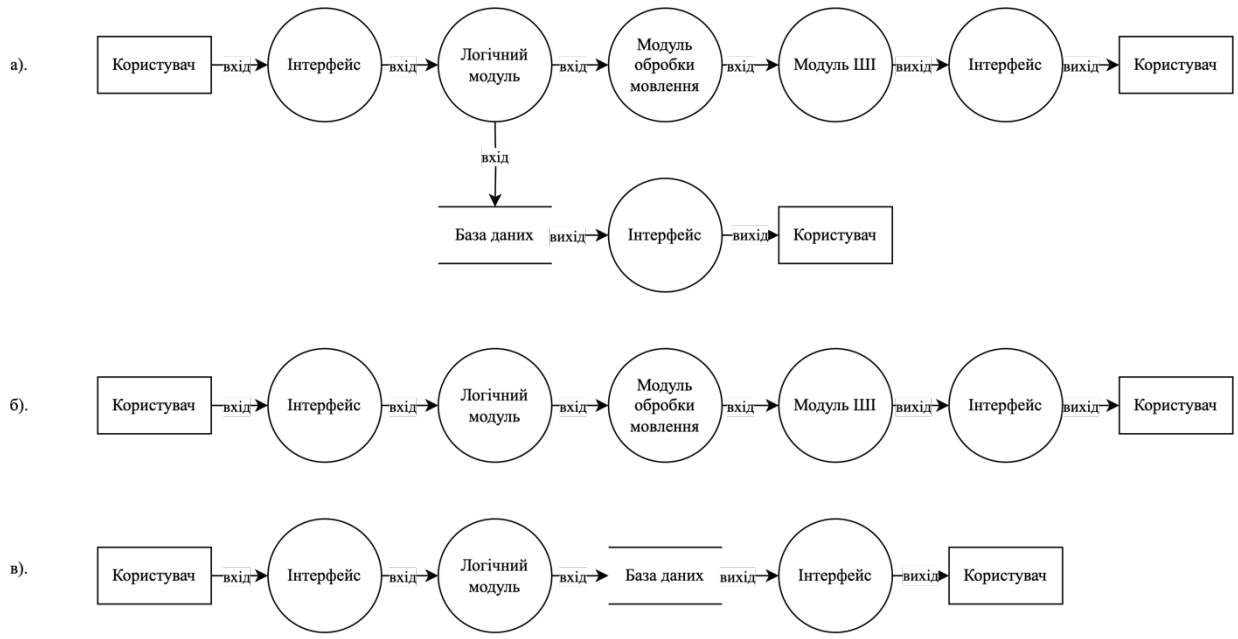
UML-ДІАГРАМА ПОСЛІДОВНОСТІ ДЛЯ ЗАПИТУ ДОВІДКИ



UML-ДІАГРАМА ПОСЛІДОВНОСТІ ДЛЯ ЗАПИТУ В ЧАТ



UML-ДІАГРАМА ПОТОКІВ ДАНИХ



а). загальна, б). для запиту в чат, в). для запиту довідки

СХЕМА АЛГОРИТМУ ЗАПУСКУ ЗАСТОСУНКУ

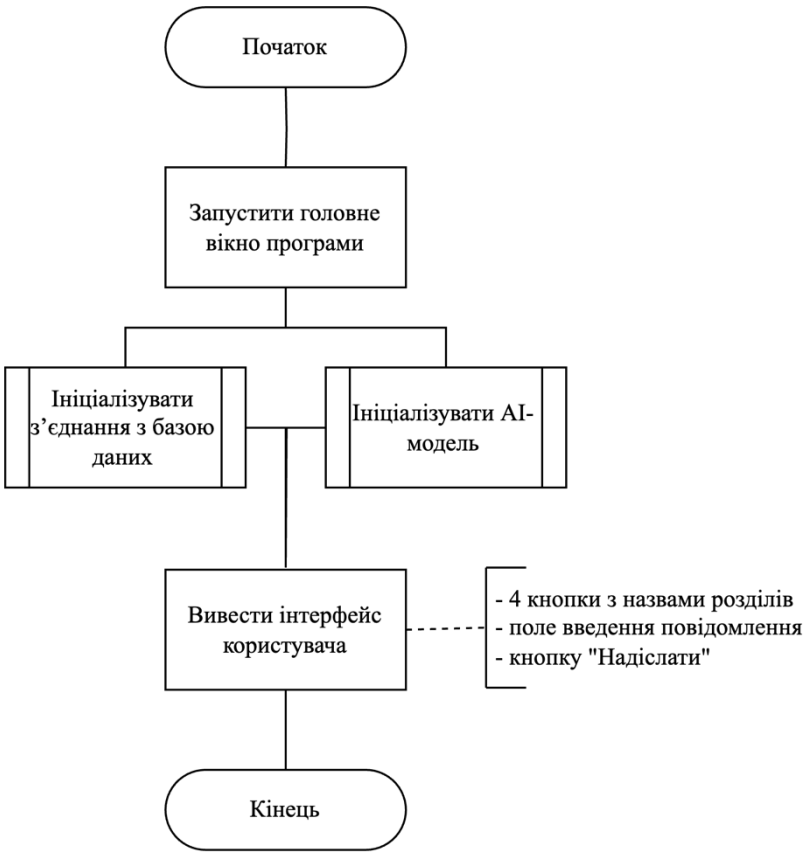


СХЕМА АЛГОРИТМУ ЗАПИТ ДОВІДКИ

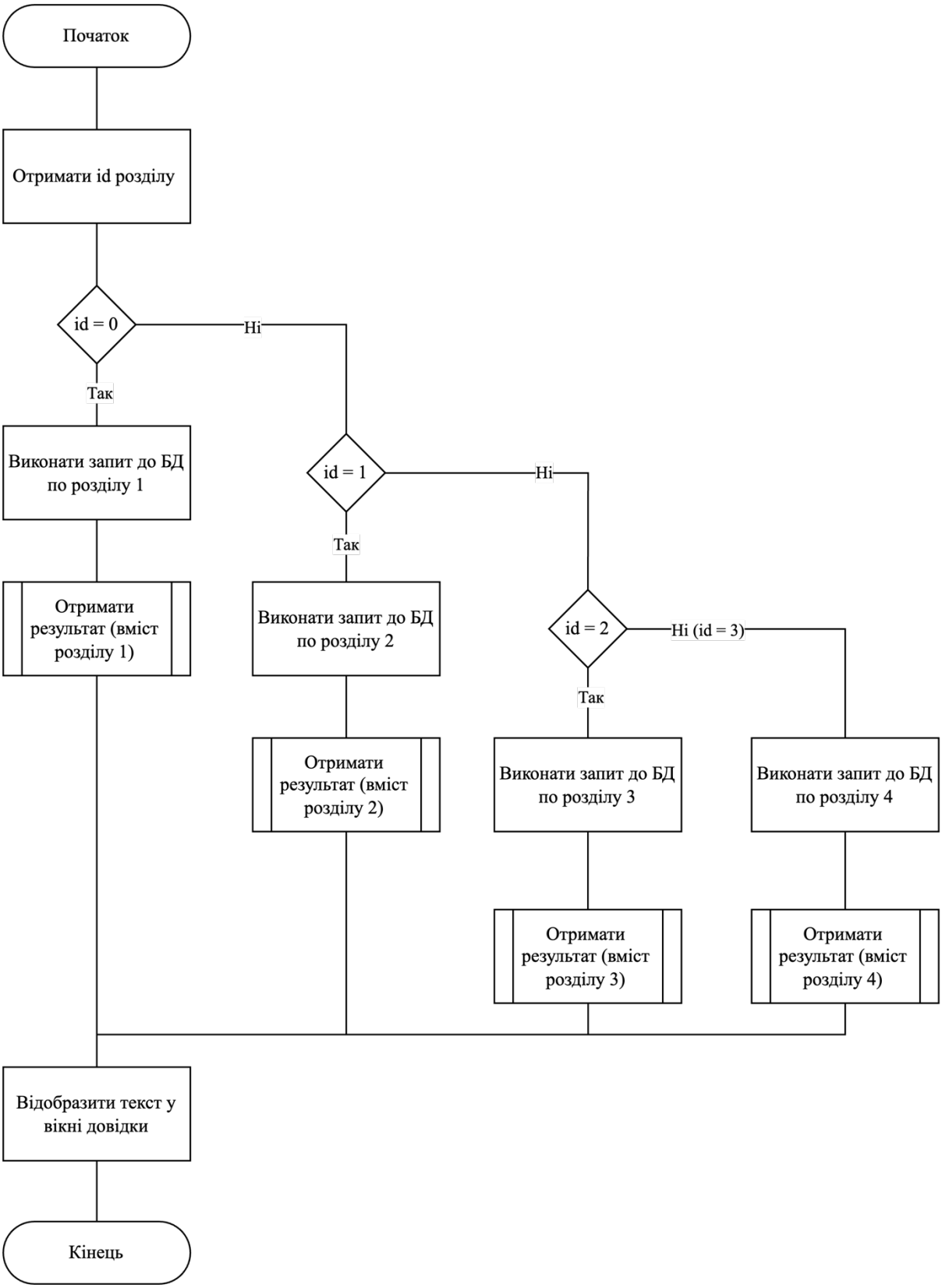


СХЕМА АЛГОРИТМУ ЗАПИТУ В ЧАТ

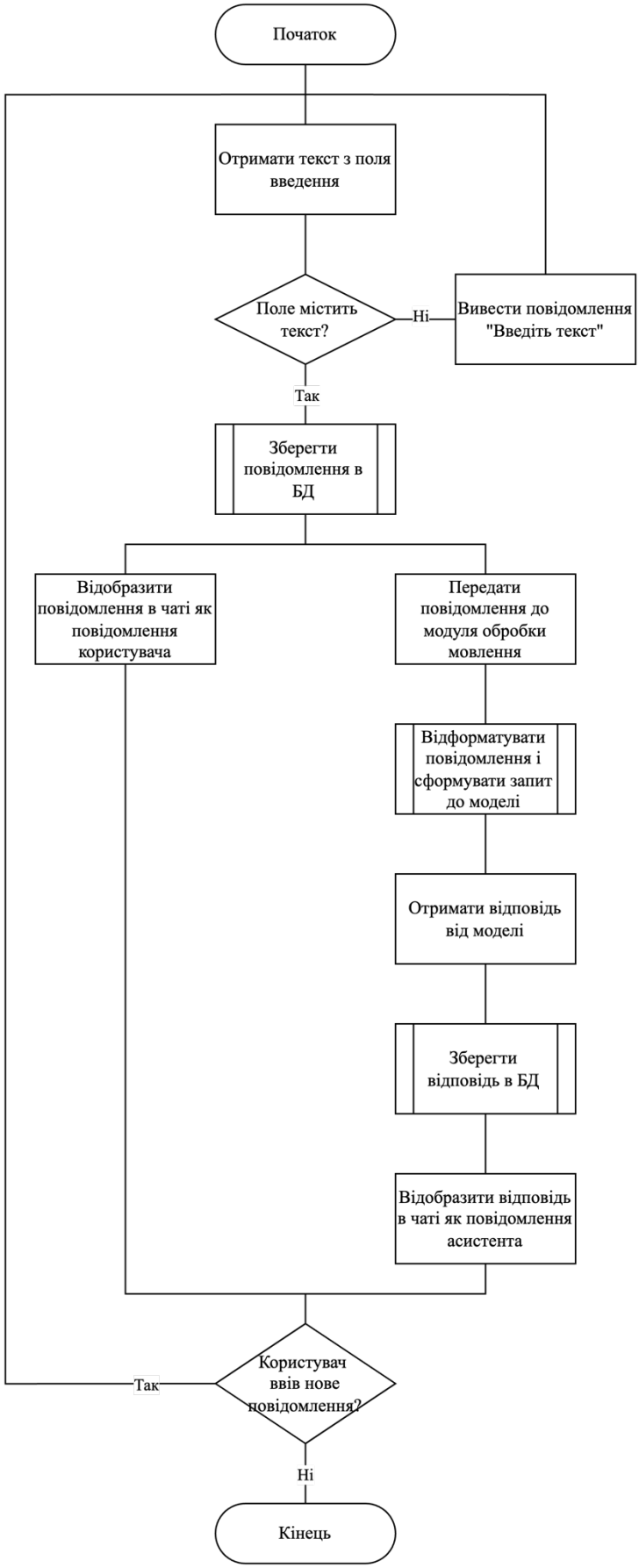


СХЕМА ДЕТАЛЬНОГО АЛГОРИТМУ ГЕНЕРУВАННЯ ВІДПОВІДІ

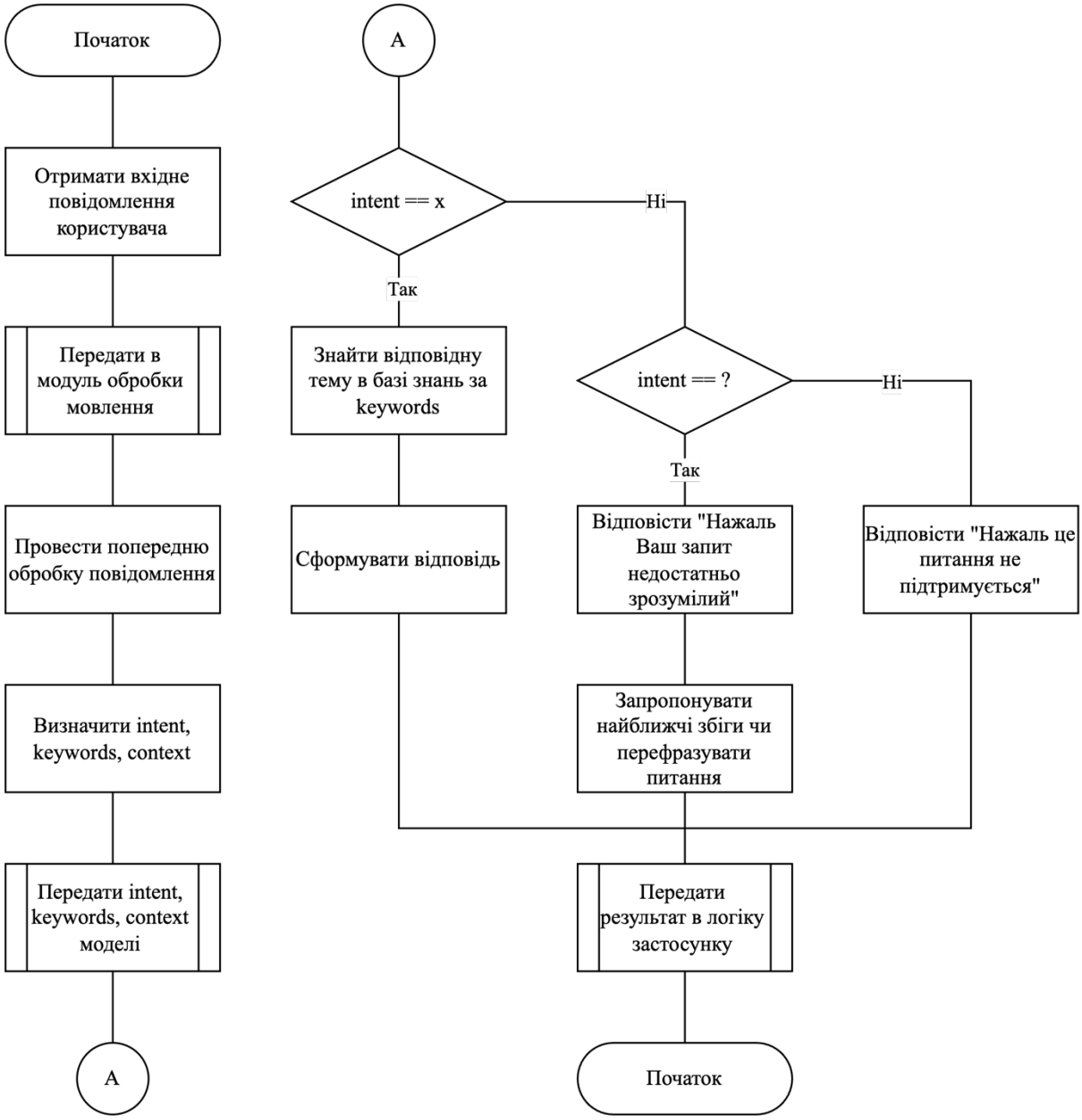


СХЕМА АЛГОРИТМУ ЗАВЕРШЕННЯ РОБОТИ

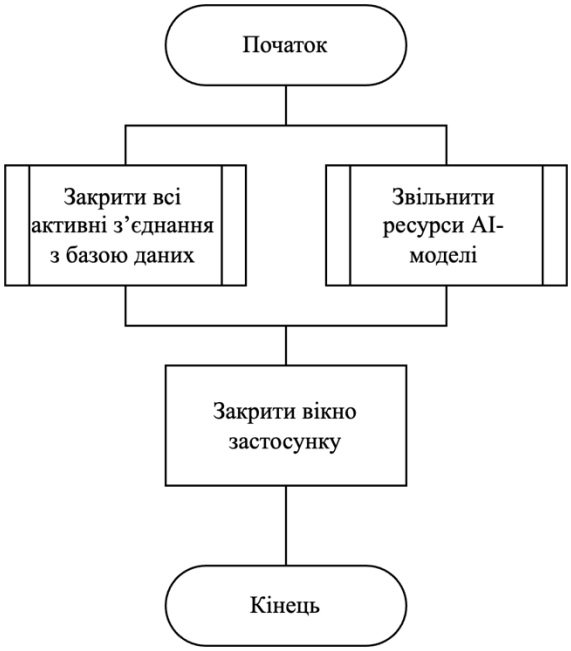


СХЕМА МОДУЛЯ ОБРОБКИ МОВЛЕННЯ

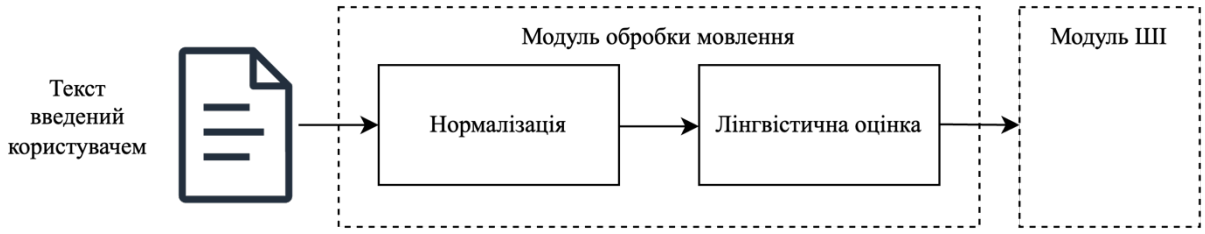


СХЕМА МОДУЛЯ ШТУЧНОГО ІНТЕЛЕКТУ

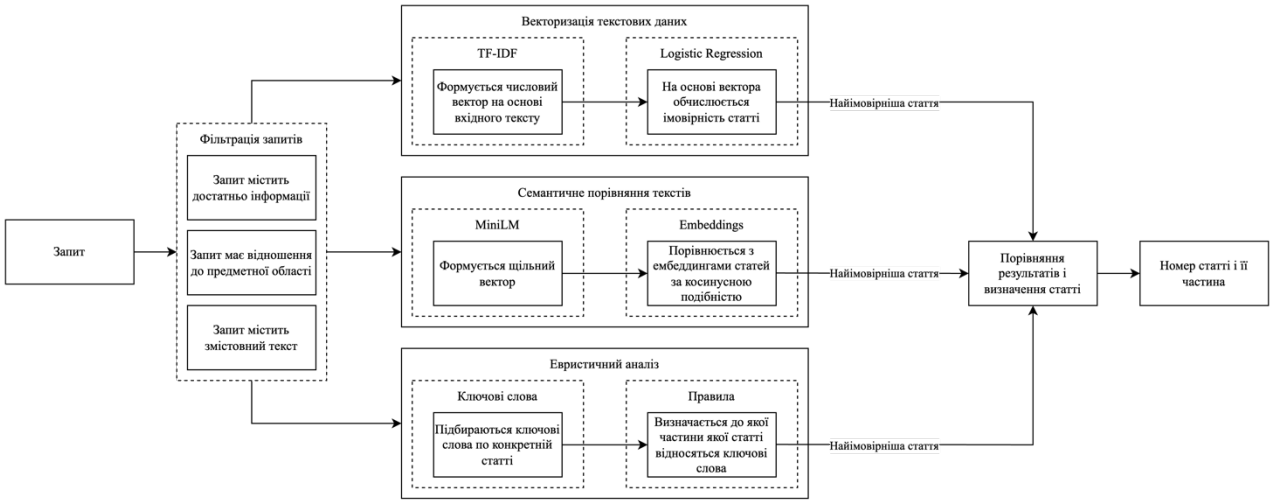


СХЕМА ЛОГІЧНОГО МОДУЛЯ ЗАСТОСУНКУ