Вінницький національний технічний університет

Факультет менеджменту та інформаційної безпеки

Кафедра менеджменту та безпеки інформаційних систем

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Удосконалення захисту мобільних корпоративних комунікацій на основі інтелектуального аналізу контенту та поведінкових аномалій з використанням трансформерної моделі BERT та алгоритму Isolation Forest»

Виконав: Студент 2-го курсу групи 1КІТС-24 м
Спеціальності – 125 Кібербезпека та захист інформації
Освітня програма – Кібербезпека інформаційних технологій та систем
Гуцько Ігор Сергійович
Керівник: д.т.н., професор
Яремчук Ю.Є.
«10» грудня 2025 р.
Опонент: к.т.н. доц. каф. ОТ
Л.В. Крупельницький
«10» грудня 2025 р.

Допущено до захисту

Голова секції УБ кафедри МБІС

д.т.н., проф. Юрій ЯРЕМЧУК

“10” грудня 2025 р.

Вінниця ВНТУ - 2025 рік

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

Рівень вищої освіти ІІ-й (магістерський)
Галузь знань 12 Інформаційні технології
Спеціальність 125 – Кібербезпека та захист інформації
Освітньо-професійна програма - Кібербезпека інформаційних технологій та систем

ЗАТВЕРДЖУЮ

Голова секції УБ, кафедра МБІС

Юрій ЯРЕМЧУК

“ 24 ” вересня 2025 р.

З А В Д А Н Н Я

на магістерську кваліфікаційну роботу студенту

Гуцько Ігора Сергійовича
(прізвище, ім`я, по-батькові)

1.Тема роботи: Удосконалення захисту мобільних корпоративних комунікацій на основі інтелектуального аналізу контенту та поведінкових аномалій з використанням трансформерної моделі BERT та алгоритму Isolation Forest
керівник роботи: д.т.н., проф. Ю.Є. Яремчук,
затверджені наказом вищого навчального закладу від “24” вересня 2025 року № 313

2. Строк подання студентом роботи: за тиждень до захисту

3.Вихідні дані: Наукові статті, документи та електронні джерела. Існуюче програмне забезпечення, вимоги та обмеження до програмного забезпечення.

4.Зміст текстової частини: Вступ. Розділ 1. Огляд основних проблем мобільних корпоративних загроз та методів їх виявлення. Розділ 2. Проектування концептуальних засад гібридного захисту мобільних корпоративних комунікацій з використанням трансформерної моделі BERT та алгоритму Isolation Forest. Розділ 3. Практична реалізація удосконалення захисту мобільних корпоративних комунікацій на основі інтелектуального аналізу контенту та поведінкових аномалій з використанням трансформерної моделі BERT та алгоритму Isolation Forest. Розділ 4. Економічне обґрунтування впровадження гібридної системи захисту мобільних корпоративних комунікацій. Висновки. Перелік посилань. Додатки.

5. Перелік ілюстративного матеріалу (з точним зазначенням обов`язкових креслень). У першому розділі 4 рисунки та 1 таблиця, у другому 6 рисунків, у третьому 8 рисунків, у четвертому 11 таблиць.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Основна частина	Яремчук Ю.Є.., д.т.н., проф. МБІС		
I	Яремчук Ю.Є.., д.т.н., проф. МБІС		
II	Яремчук Ю.Є.., д.т.н., проф. МБІС		
III	Яремчук Ю.Є.., д.т.н., проф. МБІС		
Економічна частина	Ратушняк Ольга Георгіївна, доцент кафедри ЕПВМ, к.т.н.,		

7. Дата видачі завдання 24 вересня 2025р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи		Примітк
		початок	закінчення	
1	Аналіз предметної області: корпоративна мобільна безпека, актуальні загрози	24.09.2025	25.09.2025	
2	Огляд сучасних алгоритмів та методик виявлення кіберзагроз, BERT, Isolation Forest	26.09.2025	28.09.2025	
3	Постановка задачі, визначення мети та завдань роботи	29.09.2025	02.10.2025	
4	Аналіз алгоритмів машинного навчання для виявлення фішингу спаму та загрозливих аномалій	03.10.2025	08.10.2025	
5	Розробка архітектури гібридної моделі на основі MobileBERT та Isolation Forest	09.10.2025	16.10.2025	
6	Реалізація програмного модуля для контент-аналізу та виявлення аномалій	17.10.2025	05.11.2025	
7	Проведення експериментів, тестування системи на реальних даних (Enron Mobile, тощо)	06.11.2025	13.11.2025	
8	Аналіз результатів, порівняння з альтернативними методами, оцінка економічної ефективності	14.11.2025	20.11.2025	
9	Оформлення тексту магістерської роботи, підготовка матеріалів до захисту	21.11.2025	05.12.2025	

Студент _____ Гуцько І.С.

Керівник роботи _____ Яремчук Ю. Є.

АНОТАЦІЯ

УДК 004.056.52+621.391

Удосконалення захисту мобільних корпоративних комунікацій на основі інтелектуального аналізу контенту та поведінкових аномалій з використанням трансформерної моделі BERT та алгоритму Isolation Forest.
Магістерська кваліфікаційна робота зі спеціальності 125 «Кібербезпека», освітня програма «Кібербезпека інформаційних технологій та систем».
Вінниця: ВНТУ, 2025. 85 с. На укр. мові. Бібліогр.: 31 назв; рис.:8; табл.:8; дод.:2.

У магістерській кваліфікаційній роботі розглянуто питання підвищення рівня захисту мобільних корпоративних комунікацій шляхом застосування інтелектуальних методів аналізу контенту та поведінкових аномалій. Розроблено комплексну гібридну модель, яка поєднує трансформерну архітектуру BERT для семантичної обробки тексту та алгоритм Isolation Forest для виявлення нетипових поведінкових патернів. В окремих розділах роботи проведено аналіз сучасних загроз корпоративним мережам, обґрунтовано вибір моделей і детально досліджено ефективність їхньої інтеграції. У практичній частині здійснено перехід до моделі MobileBERT, що забезпечило високу продуктивність у мобільних корпоративних середовищах. Наведено результати експериментального впровадження розробленої системи, висвітлено її економічну доцільність та потенціал для комерційного використання.

Результати роботи підтверджують доцільність і високу ефективність комбінованого підходу для захисту сучасних мобільних корпоративних комунікацій від кіберзагроз. **Ключові слова**: мобільна корпоративна безпека, кіберзагрози, BERT, MobileBERT, Isolation Forest, аналіз контенту, поведінкові аномалії, гібридна модель захисту.

ABSTRACT

UDC 004.056.52+621.391

Enhancing the security of mobile corporate communications through intelligent content analysis and behavioral anomaly detection with the use of the BERT transformer model and Isolation Forest algorithm.

Master's Thesis for specialty 125 "Cybersecurity", educational program "Cybersecurity of Information Technologies and Systems".

Vinnytsia: VNTU, 2025. 85 p. In Ukrainian. Bibliogr.: 31 titles; figs.: 8; tables: 8; app.: 2.

This master's thesis addresses the issue of improving mobile corporate communications security using intelligent methods of content analysis and behavioral anomaly detection. A comprehensive hybrid model is developed, combining the BERT transformer architecture for semantic text processing and the Isolation Forest algorithm for detecting non-standard behavioral patterns. The thesis sections analyze current threats to corporate networks, substantiate the choice of models, and thoroughly examine the efficiency of their integration. In the practical part, a transition to the MobileBERT model is implemented, ensuring high performance in mobile corporate environments. Results of the system's experimental implementation are presented, alongside its economic feasibility and commercial potential.

The study confirms the feasibility and high effectiveness of the combined approach for protecting modern mobile corporate communications against cyber threats.

Key words: mobile corporate security, cyber threats, BERT, MobileBERT, Isolation Forest, content analysis, behavioral anomalies, hybrid security model.

ЗМІСТ

ВСТУП

Актуальність. У сучасному світі, де інформаційні технології розвиваються стрімко, кібербезпека стає надзвичайно важливою. Кількість атак у цифровому просторі щороку зростає, загрожуючи приватності, безпеці та доступу до даних як звичайним користувачам, так і великим фірмам. Особливо небезпечними є атаки на мобільні корпоративні зв’язки, де зловмисники використовують фальшиві повідомлення чи підозрілі дії, щоб викрасти особисті дані, банківські реквізити чи доступ до бізнес-систем. Хоча захисні технології швидко вдосконалюються, ці загрози все ще залишаються серйозною проблемою. Тому створення ефективніших систем для виявлення аномалій у мобільних комунікаціях – це важливе завдання сьогодення.

Існує багато інструментів для боротьби з такими загрозами, але вони часто не справляються з новими чи невідомими аномаліями. Використання нейромереж, машинного навчання та штучного інтелекту дозволяє значно покращити точність і гнучкість систем, допомагаючи їм адаптуватися до змін. Цей підхід обіцяє ефективне вирішення проблеми.

У роботі я проаналізував і порівняв різні способи виявлення аномалій, оцінивши їхню ефективність, стійкість і здатність протистояти новим загрозам. Основна увага зосереджена на методах машинного навчання, зокрема BERT для аналізу тексту та Isolation Forest для вивчення поведінки. Порівнюю традиційні методи, як-от перевірка SSL-сертифікатів чи шаблонів дій, із сучасними рішеннями на основі штучного інтелекту.

Також відріється суть удосконаленої системи для автоматичного пошуку аномалій у мобільних комунікаціях, використовуючи BERT і Isolation Forest для аналізу змісту та поведінки. Система враховує сучасні тенденції загроз і адаптується до змін у методах атак завдяки глибокому навчанню. Особливу увагу приділяю тестуванню її ефективності порівняно з іншими методами та

інтеграції в реальні мобільні додатки, щоб зменшити помилки й підвищити безпеку.

Мета роботи – покращити й інтегрувати вдосконалену систему виявлення аномалій та загроз із використанням BERT і Isolation Forest. BERT для мобільних корпоративних комунікацій на основі гібридного підходу, що поєднує передові технології машинного навчання. Основу системи складає інтеграція двох ключових компонентів: трансформерної моделі BERT для глибинного семантичного аналізу текстових повідомлень та алгоритму Isolation Forest для виявлення аномалій у поведінкових патернах користувачів. Для практичної реалізації системи планується використання мови програмування Python для серверної частини з застосуванням бібліотек Transformers та Scikit-learn, що забезпечать роботу основних алгоритмів аналізу. Клієнтська частина буде реалізована на мові Kotlin для операційної системи Android, що дозволить створити ефективний мобільний додаток з сучасним інтерфейсом. Архітектура системи базується на клієнт-серверній моделі, де важкі обчислення виконуються на серверній стороні, а мобільний додаток забезпечує збір даних та відображення результатів аналізу. Розроблена система буде здатна виявляти широкий спектр загроз - від фішингових повідомлень та соціально-інженерних атак до аномальної мережевої активності, забезпечуючи реальний захист корпоративних комунікацій в умовах сучасного кіберпростору. Процес включає аналіз існуючих методів, вивчення моделей штучного інтелекту, їхнє тренування, тестування та вбудовування в мобільний додаток. Успішна реалізація дасть потужний інструмент для виявлення аномалій із високою точністю та мінімальною кількістю помилок.

Об’єкт дослідження – процеси виявлення кіберзагроз у мобільних корпоративних комунікаціях на основі гібридного підходу, що поєднує трансформерні моделі обробки природної мови та алгоритми виявлення аномалій.

Предмет дослідження – методи та алгоритми створення гібридної системи виявлення загроз на основі BERT та Isolation Forest

Новизна роботи полягає у розробці гібридного підходу до виявлення загроз, який поєднує контентний аналіз на основі BERT з поведінковим аналізом за допомогою Isolation Forest спеціально для корпоративних середовищ. Інтеграція двох доповнюючих методів машинного навчання дозволяє одночасно виявляти семантичні аномалії в текстових повідомленнях та відхилення в патернах поведінки, що значно підвищує точність виявлення складних цілеспрямованих атак. Відмінною рисою запропонованого рішення є його орієнтація на обмежені ресурси мобільних пристроїв та реальний час роботи, що досягається через використання оптимізованої моделі MobileBERT та ефективного за обчислювальними витратами алгоритму Isolation Forest. Крім того, новизна полягає в механізмі зваженої інтеграції результатів обох модулів на рівні прийняття рішення, що дозволяє системі адаптивно зважувати важливість контентних та поведінкових ознак залежно від контексту загрози. Це дозволяє створити більш гнучку та стійку систему захисту, здатну ефективно протистояти гібридним атакам, що поєднують соціальну інженерію з нестандартними шаблонами активності.

Розділ 1. ОГЛЯД ОСНОВНИХ ПРОБЛЕМ МОБІЛЬНИХ КОРПОРАТИВНИХ ЗАГРОЗ ТА МЕТОДІВ ЇХ ВИЯВЛЕННЯ

1.1 Актуальність теми

Сучасний етап розвитку цифрових технологій характеризується стрімким зростанням використання мобільних пристроїв у корпоративному середовищі. Ця тенденція, з одного боку, значно підвищує операційну ефективність бізнесу, а з іншого - створює нові вектори кібератак, що робить тему захисту мобільних корпоративних комунікацій надзвичайно актуальною. Інтеграція мобільних технологій у корпоративне середовище створила нові уразливості, пов'язані з поширенням шкідливого контенту через канали мобільних комунікацій. Сучасні загрози, зокрема цільовий фішинг та маніпулятивні технології, все частіше використовують складні методи соціальної інженерії, що ускладнює їх своєчасне виявлення традиційними засобами захисту.

Дослідження показують, що машинне навчання відкриває нові можливості для протидії цим загрозам. Зокрема, сучасні алгоритми обробки природної мови демонструють високу ефективність у завданнях семантичного аналізу текстових повідомлень. Особливу ефективність у протидії сучасним загрозам демонструють трансформерні моделі, здатні аналізувати семантичний зміст повідомлень у контексті корпоративної комунікації. Ці технології дозволяють виявляти скриті ознаки фішингових атак, маніпулятивні техніки та інші форми шкідливого контенту, що циркулює через мобільні канали зв'язку. Впровадження таких інтелектуальних систем аналізу стає особливо актуальним у світлі зростання складності кібератак та їх адаптації до традиційних методів захисту [1].

Особливої актуальності тема набуває у світлі зростання кількості та складності кібератак на мобільні платформи. Згідно зі статистикою Cybersecurity Ventures, щорічні збитки від кіберзлочинності досягнуть 10,5 трлн доларів до 2025 року, причому значна частина атак реалізується саме через

мобільні канали комунікації. Фішингові атаки через мобільні повідомлення зросли на 150% за останні два роки, що свідчить про активне переміщення зловмисників у мобільний простір.

Актуальність дослідження підкріплюється також зміною характеру загроз. Сучасні атаки стали значно складнішими та цілеспрямованішими. Зловмисники активно використовують методи штучного інтелекту для створення персоналізованих фішингових повідомлень, технології deepfake для імітації голосів керівництва, складні соціально-інженерні методи для обходу традиційних систем захисту.

Велику загрозу становлять атаки на інфраструктуру мобільних додатків. За останній рік кількість виявлених вразливостей у мобільних додатках зросла на 70%, причому більшість із них мають критичний рівень небезпеки. Це призводить до масштабних витоків конфіденційних даних, фінансових втрат та репутаційної шкоди для компаній.

Важливим аспектом актуальності є недостатня ефективність традиційних методів захисту. Сигнатурні системи, чорні списки та статичні методи аналізу виявляються неефективними проти сучасних адаптивних загроз. Це обумовлює потребу у розробці нових інтелектуальних систем безпеки, здатних аналізувати як контент повідомлень, так і поведінкові патерни у реальному часі.

Враховуючи вищезазначене, розробка ефективних методів виявлення загроз у мобільних корпоративних комунікаціях на основі сучасних технологій машинного навчання є не лише актуальною науковою задачею, але й практичною необхідністю для забезпечення безпеки бізнесу в цифрову епоху. Запропонований у дослідженні підхід, що поєднує BERT для аналізу контенту та Isolation Forest для виявлення поведінкових аномалій, відкриває нові можливості для створення ефективних систем захисту, здатних протидіяти сучасним викликам кібербезпеки.

1.2 Фундаментальні аспекти проблем безпеки в мобільних корпоративних мережах

Сучасна мобільна корпоративна інфраструктура стикається з низкою системних проблем безпеки, які є прямим наслідком її ключових характеристик: мобільності, розподіленості та гетерогенності. Ці фактори формують унікальний ландшафт ризиків, відмінний від традиційних стаціонарних мереж. Основна проблема полягає у розмитті кордонів мережевого периметра - коли співробітники використовують пристрої поза офісом, традиційні засоби захисту, орієнтовані на периметр, стають неефективними, що значно розширює поверхню атаки та ускладнює контроль доступу до корпоративних ресурсів.

Таблиця 1.1 — Фундаментальні аспекти проблем безпеки в мобільних корпоративних мережах

Основний аспект	**Суть проблеми**	**Типові приклади / ризики**	**Наслідки для корпоративної безпеки**
Мобільність, розмитий периметр та незахищені мережі	Пристрої працюють поза захищеною інфраструктурою та використовують ненадійні канали зв’язку	Публічні Wi-Fi; MITM; підміна точки доступу; перехоплення трафіку	Компрометація пристрою; витік даних; слабкість традиційного периметрального захисту
Соціальна інженерія та атаки через SMS/месенджери/додатки	Зловмисники використовують людський фактор і популярні канали комунікації	Фішинг у месенджерах; smishing; заражені APK; шкідливі посилання	Несанкціонований доступ; викрадення облікових даних; поширення шкідливого ПЗ
Гетерогенність пристроїв та складність централізованого управління	Різні ОС, моделі й версії ПЗ ускладнюють уніфікацію політик та управління	Фрагментація Android/iOS; несумісність MDM; різні рівні безпеки	Висока складність контролю; поява «слабких ланок»; нерівномірна безпека в мережі
Актуальність ПЗ та патчів	Затримки з оновленнями та використання застарілих пристроїв залишають вразливості невиправленими	Відсутність критичних патчів; вразливості zero-day; експлойти	Можливість віддаленого взлому; ескалація привілеїв; зараження корпоративної інфраструктури

У таблиці представлено основні проблемні аспекти, що впливають на безпеку мобільних корпоративних мереж, зокрема: мобільність пристроїв і використання незахищених мереж, соціально-інженерні атаки та загрози через мобільні канали комунікації, гетерогенність пристроїв і складність централізованого управління, а також ризики, пов’язані з актуальністю ПЗ та оновлень.

Поширення моделей віддаленої роботи та концепції BYOD (Bring Your Own Device) створило серйозні виклики для адміністраторів безпеки. Різноманітність операційних систем, моделей пристроїв та версій програмного забезпечення ускладнює забезпечення єдиної політики безпеки та своєчасного накладання виправлень. Дослідження показують, що понад 60% мобільних пристроїв у корпоративному середовищі мають застарілі версії програмного забезпечення з відомими вразливостями, що створює додаткові вектори для потенційних атак.

Соціально-інженерні атаки отримали новий імпульс у мобільному середовищі. Обмежений інтерфейс мобільних пристроїв ускладнює ідентифікацію підроблених веб-сайтів та фішингових повідомлень, а постійна доступність користувачів робить їх більш вразливими до маніпуляцій. Особливу небезпеку становлять атаки через SMS та месенджери, де зловмисники використовують технології штучного інтелекту для створення персоналізованих фішингових повідомлень, що імітують корпоративну комунікацію [2].

Використання публічних Wi-Fi мереж створює додаткові ризики для конфіденційності корпоративних даних. Дослідження демонструють, що понад 35% публічних точок доступу не використовують належного шифрування, що робить їх зручним інструментом для атак типу "людина посеред". Ця проблема посилюється тим, що більшість користувачів не використовують VPN-з'єднання при підключенні до публічних мереж, що значно підвищує ризик перехоплення конфіденційної інформації.

Складність централізованого управління безпековими політиками є однією з найбільш гострих проблем. Розподілена архітектура мобільних мереж вимагає нового підходу до управління ідентифікацією та доступом, оскільки традиційні рішення виявляються недостатньо ефективними в умовах динамічно змінюваної топології мережі. Впровадження концепції Zero Trust архітектури стає необхідністю, але потребує значних зусиль для адаптації до мобільного середовища.

Захист даних на пристроях, що часто втрачаються або викрадаються, становить окремий виклик. Навіть при наявності політик шифрування та автоматичного видалення даних, існує ризик несанкціонованого доступу до корпоративної інформації через фізичний доступ до пристрою. Статистика свідчить, що щороку реєструється понад 10 мільйонів випадків втрати мобільних пристроїв з корпоративними даними, що підтверджує актуальність цієї проблеми.

Інтеграція IoT-пристроїв у корпоративну інфраструктуру додає новий вимір проблем безпеки. Більшість IoT-пристроїв мають обмежені обчислювальні ресурси та не підтримують традиційні механізми безпеки, що робить їх привабливою мішенню для зловмисників, які можуть використовувати їх як точку входу в корпоративну мережу. Дослідження показують, що понад 70% організацій стикалися з інцидентами безпеки, пов'язаними з компрометацією IoT-пристроїв. Складність забезпечення безпеки в умовах гібридних робочих моделей продовжує зростати. Комбінація офісних та віддалених робочих місць вимагає гнучких рішень безпеки, які можуть ефективно функціонувати в різноманітних мережевих середовищах, зберігаючи при цьому цілісність корпоративних даних та відповідність вимогам регуляторів. Ця проблема особливо актуальна для галузей з підвищеними вимогами до захисту даних, таких як фінансовий сектор та охорона здоров'я. Аналіз щодо фундаментальних аспектів проблем безпеки вказують на необхідність комплексного підходу, що поєднує технічні рішення, організаційні

заходи та постійне навчання співробітників. Ефективний захист мобільних корпоративних мереж вимагає переосмислення традиційних парадигм безпеки та адаптації до нових викликів, що виникають в умовах динамічно змінюваного цифрового ландшафту.

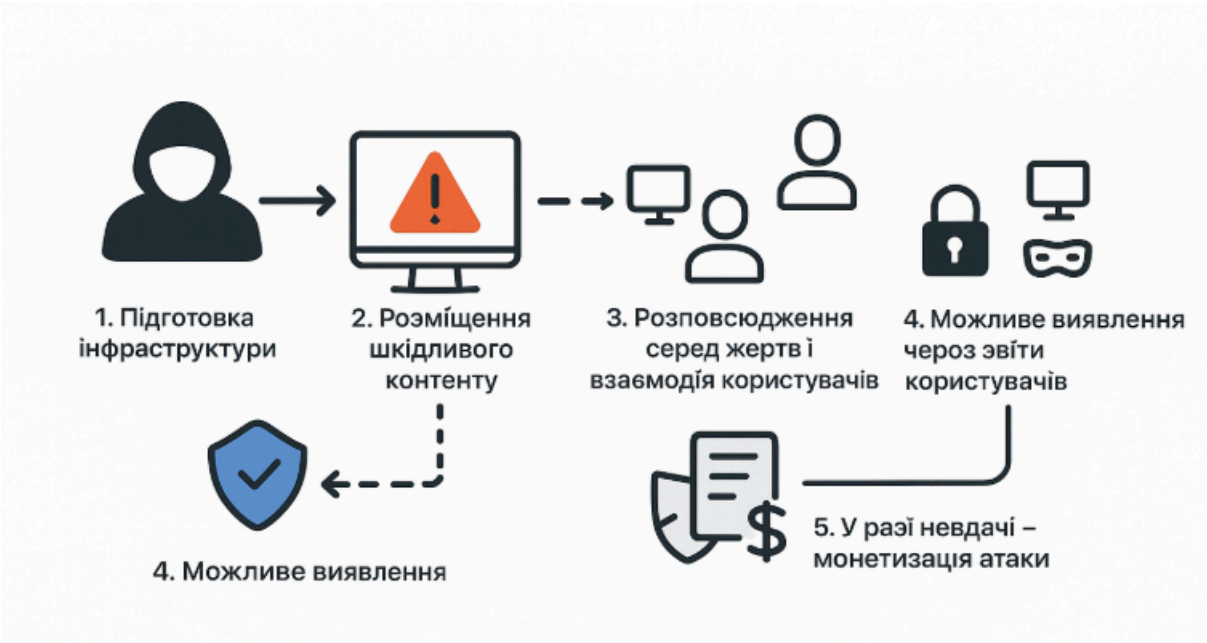


Рисунок 1.1 – Етапи реалізації цільової кібератаки.

На рисунку 1.1 показано, що зловмисник спочатку готує інфраструктуру, відкриває шкідливий контент і завантажує його. Після того, як загроза запущена і працює, зловмисник починає поширювати її серед жертв. Жертви починають взаємодіяти з контентом. Залежить від здатності організації виявити, що кампанія проводиться та націлена на співробітників, наприклад, за допомогою звітів користувачів.

Важливою проблемою є труднощі інтеграції сучасних систем детекції у існуючі мобільні додатки. Більшість сучасних інструментів використовує мови програмування та платформи, які не завжди сумісні з поширеними мобільними розробками. Наприклад, багато популярних бібліотек для машинного навчання реалізовані на Python, Java чи C++, що ускладнює їх інтеграцію у мобільні

середовища, які є основою більшості додатків. Через це впровадження нових технологій стає складним завданням для більшості розробників .

Сучасні підходи на основі машинного навчання, особливо нейронні мережі, мають потенціал для вирішення цієї проблеми, оскільки здатні аналізувати багатовимірні дані та визначати приховані шаблони, притаманні загрозам. Однак, створення такої системи потребує детального підходу до вибору характеристик, які будуть використовуватися для навчання моделі, а також забезпечення високої ефективності у виявленні нових загроз. Основними викликами є збирання достатнього обсягу даних для навчання моделі, обробка цих даних та визначення оптимальних параметрів моделі, що дозволить системі успішно розпізнавати загрози навіть на ранніх стадіях.

Складність розробки систем детекції на основі машинного навчання також включає проблеми продуктивності та оптимізації. Нейронні мережі, особливо глибокі моделі, часто вимагають значних обчислювальних ресурсів, що може призвести до перевантаження мобільного пристрою та затримок у відповідях на запити користувачів. Для інтеграції такої системи у мобільні додатки виникає проблема вибору компромісу між точністю моделі та швидкістю її роботи. Ця проблема особливо актуальна в умовах цифрової нерівності, коли користувачі мають різний рівень доступу до сучасних технологій та обчислювальних ресурсів, що може значно впливати на ефективність застосування складних алгоритмів машинного навчання в мобільному середовищі [3]. Використання BERT та Isolation Forest у цій роботі дозволяє вирішити проблему сумісності та забезпечує простоту інтеграції у існуючі мобільні проекти, однак виникає потреба в оптимізації алгоритмів та використанні методів зменшення розмірності даних для досягнення прийнятної продуктивності.

Іншою проблемою є мінімізація кількості помилкових спрацьовувань. Навіть найточніші моделі машинного навчання можуть давати помилкові позитивні або негативні результати, що призводить до небажаних наслідків. З

одного боку, помилкові позитивні спрацьовування можуть відштовхувати користувачів, тоді як помилкові негативні дозволяють загрозам проходити перевірку без виявлення. Тому у процесі розробки системи важливо підібрати оптимальний набір характеристик та порогових значень, щоб забезпечити максимальну точність детекції без компромісу з боку продуктивності.

1.3 Класифікація та характеристика основних загроз безпеки в мобільних корпоративних мережах

Сучасні мобільні корпоративні мережі стикаються зі складним комплексом загроз, що поєднують традиційні вектори атак з інноваційними методами, адаптованими під особливості мобільних платформ. Ці загрози можна класифікувати за кількома ключовими критеріями: вектор атаки, рівень цілеспрямованості, технічна складність та потенційний збиток. Зокрема, серед найбільш критичних варто виділити цільові фішинг-атаки (spear phishing), що використовують особисту інформацію, мобільний шпигунський ПЗ (mobile spyware), атаки на пристрої через мережі зв'язку (наприклад, через SMS або месенджери), а також експлойти вразливостей операційних систем та додатків. Крім того, зростає загроза атак із використанням штучного інтелекту, здатних адаптувати контент під поведінку конкретних користувачів, що робить їх майже непомітними для традиційних систем захисту. Особливу небезпеку становлять гібридні атаки, які одночасно експлуатують технічні вразливості пристроїв та соціальну інженерію, націлену на конкретних співробітників. Такі багаторівневі загрози вимагають комплексного підходу до захисту, що поєднує технічні засоби з аналізом поведінки та контенту. Узагальнена класифікація основних категорій загроз для корпоративних мереж наведена на Рис. 1.2.

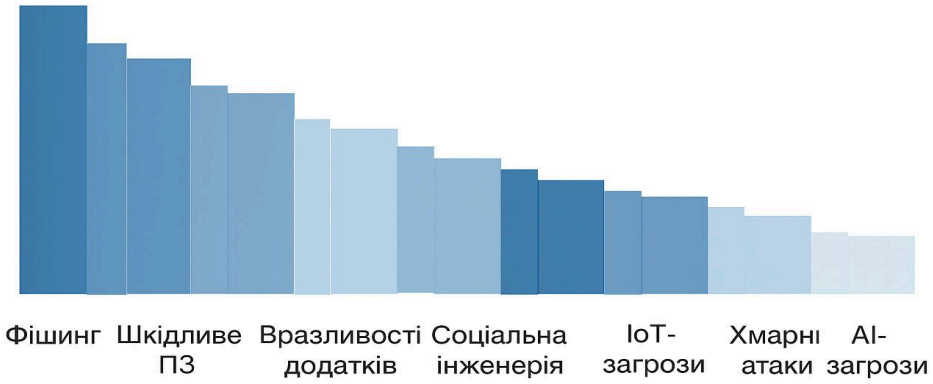


Рисунок 1.2 – Основні категорії загроз для корпоративних мереж

Фішингові атаки та їх еволюція продовжують залишатися одним з найпоширеніших типів загроз. Класичний фішинг через електронну пошту еволюціонував у більш цілеспрямовані форми, такі як спір-фішинг (spear phishing) та китобійний промисел (whaling), де атаки націлені на конкретних співробітників або керівників компанії. Особливу небезпку становлять мобільні варіації фішингу - смішинг (SMS-фішинг) та фішинг через месенджери. Ці атаки використовують психологічні методи маніпуляції, створюючи відчуття терміновості та використовуючи соціальну інженерію для обходу технічних засобів захисту. Сучасні фішингові кампанії характеризуються високим рівнем персоналізації, використанням актуальних подій з життя компанії та імітацією стилю спілкування керівництва.

Шкідливе програмне забезпечення для мобільних пристроїв представляє серйозну загрозу корпоративній безпеці. Цей клас загроз включає троянські програми, що маскуються під легальні додатки, шпигунське ПЗ для збору конфіденційної інформації, а також програми-вимагачі, що шифрують дані користувача. Особливістю сучасного мобільного шкідливого ПЗ є використання

технік обфускації коду, поліморфізму та анти-емуляції, що ускладнює їх виявлення традиційними антивірусними рішеннями. Для ефективного протидії таким атакам необхідно застосовувати комплексні методики оцінки достовірності інформації, що базуються на аналізі поведінкових патернів та семантичного змісту повідомлень [4]. Більш того, зловмисники все частіше використовують легальні маркети додатків для поширення шкідливого ПЗ, використовуючи методи соціальної інженерії для залучення користувачів.

Атаки на мережевому рівні становлять особливу небезпку для мобільних корпоративних мереж через часту зміну точок доступу та використання публічних Wi-Fi мереж. Атаки типу "Людина посеред" (Man-in-the-Middle) дозволяють зловмисникам перехоплювати передачу даних, модифікувати інформацію в реальному часі та отримувати доступ до конфіденційних відомостей. DNS-спуфінг та відповідні атаки направляють користувачів на підроблені веб-сайти, що імітують корпоративні портали або сервіси автентифікації. Ці атаки особливо ефективні в мобільному середовищі, де перевірка справжності сертифікатів та доменних імен часто ускладнена через обмеження інтерфейсу.

Загрози через вразливості мобільних додатків становлять критичний ризик для корпоративної безпеки. Багато корпоративних додатків містять вразливості в реалізації API, системах автентифікації та механізмах зберігання даних. Зловмисники експлуатують такі вразливості для отримання несанкціонованого доступу до корпоративних систем, витоку конфіденційної інформації та проведення несанкціонованих операцій. Особливу небезпеку представляють вразливості типу "незахищене зберігання даних", "небезпечна криптографія" та "недостатня захищеність клієнт-серверної взаємодії".

Соціально-інженерні атаки в мобільному середовищі демонструють високу ефективність через психологічні особливості сприйняття інформації на мобільних пристроях. Сучасні підходи до детекції мобільного шкідливого ПЗ все частіше використовують ансамблеві моделі на основі BERT, що дозволяє

досягати високої точності у виявленні навіть складних поліморфних загроз [5]. Техніка, коли зловмисник створює вигаданий сценарій для отримання конфіденційної інформації, особливо ефективні в комбінації з мобільним контекстом. Байт-джекінг, що передбачає залишення заражених носіїв інформації в місцях, де їх можуть знайти співробітники, адаптується до мобільного середовища через використання заражених пристроїв для бездротової зарядки або носіїв з підтримкою USB-C.

Атаки на операційні системи та прошивки представляють особливо серйозну загрозу, оскільки вони важко виявляються та можуть надати зловмисникам повний контроль над пристроєм. Zero-day вразливості в операційних системах Android та iOS дозволяють обходити системи безпеки та встановлювати стійкий доступ до пристрою. Атаки на рівні прошивки можуть компрометувати базові механізми безпеки пристрою, роблячи неможливим ефективний захист на рівні програмного забезпечення.

Загрози через інтернет речей (IoT) та периферійні пристрої стають все більш актуальними з розвитком концепції "розумного офісу". Незахищені IoT-пристрої, такі як камери спостереження, принтери, системи контролю доступу, можуть стати точкою входу в корпоративну мережу. Ці пристрої часто мають обмежені можливості безпеки та не отримують своєчасних оновлень, що робить їх легкою мішенню для зловмисників.

Атаки на хмарні сервіси та API становлять загрозу для корпоративних даних через інтеграцію мобільних додатків з хмарною інфраструктурою. Неправильно налаштовані API, недостатня автентифікація та слабке шифрування даних можуть призвести до масштабних витоків конфіденційної інформації. Протидія таким загрозам вимагає не лише застосування стандартних засобів безпеки, але й забезпечення повної видимості динамічних інфраструктурних компонентів під час розслідування інцидентів, що дозволяє ефективно відстежувати та блокувати шкідливу активність [6]. Зловмисники

використовують методи сканування API для виявлення вразливостей та отримання доступу до корпоративних даних.

Аномальна поведінка як індикатор складних атак представляє особливий клас загроз, що важко виявляються традиційними методами. Незвичайні патерни мережевої активності, аномалії в часі роботи, нехарактерні операції з даними можуть свідчити про цілеспрямовані атаки або несанкціоновану діяльність. Ефективним інструментом для виявлення таких аномалій є, наприклад, алгоритм Isolation Forest, який дозволяє ізолювати незвичні патерни поведінки в мережевих даних без необхідності попереднього навчання на мічених даних [7]. Виявлення таких загроз вимагає складних алгоритмів аналізу поведінки та машинного навчання.

Загрози через технології штучного інтелекту становлять новий виклик для безпеки мобільних корпоративних мереж. Зловмисники використовують генеративні моделі для створення правдоподібних фішингових повідомлень, технології deepfake для імітації голосів керівництва та складні системи аналізу поведінки для обходу засобів захисту. Ці технології дозволяють створювати високо персоналізовані атаки, що важко відрізнити від легітимної активності.

Кожен з цих типів загроз вимагає спеціалізованих підходів до виявлення та нейтралізації. Ефективний захист мобільних корпоративних мереж повинен враховувати специфіку кожного типу загроз, а також їх потенційні комбінації в складних багатоетапних атаках. Розуміння повного спектру загроз є критично важливим для розробки комплексної стратегії безпеки, що здатна протистояти сучасним кіберзагрозам в умовах динамічно змінюваного ландшафту мобільної безпеки.

1.4 Моделювання процесу кібератаки та її життєвий цикл

Для ефективного протидії сучасним загрозам необхідно не лише знати їх статичний перелік, але й розуміти динамічну послідовність дій зловмисника, від початкового зондування до досягнення кінцевої мети. Ця послідовність, часто

представлена у вигляді моделі життєвого циклу атаки, дозволяє вибудовувати проактивну оборону, спрямовану на переривання ланцюга загрози на ранніх етапах. У контексті мобільних корпоративних мереж цей цикл має свої специфічні характеристики, пов’язані з мобільністю пристроїв, різноманіттям векторів атак та використанням соціальної інженерії.

Первинним етапом майже кожної цілеспрямованої атаки є розвідка та збір інформації. Зловмисники активно використовують відкриті джерела (OSINT), соціальні мережі, професійні платформи на кшталт LinkedIn для збору інформації про цільових співробітників, ієрархію компанії, використовувані технології та мобільні додатки. У мобільному середовищі це також може включати сканування публічних Wi-Fi мереж, використання яких є типовими для співробітників, або аналіз додатків у офіційних та сторонніх маркетах для виявлення потенційних вразливостей.

Наступна фаза — початкова компрометація та доставка — має на меті отримати первинний доступ до мобільного пристрою або корпоративного середовища. Найпоширенішими векторами на цьому етапі є цілеспрямовані фішингові повідомлення (спір-фішинг), смішинг (SMS-фішинг) або фішинг через месенджери. Ефективність цих методів, згідно з дослідженнями, значно підвищується завдяки використанню технологій генеративного ШІ, які дозволяють створювати високоякісні та персоналізовані фішингові кампанії, що важко відрізнити від справжніх повідомлень [8]. Зловмисники можуть розсилати посилання на підроблені сторінки автентифікації або пропонувати завантажити інфікований мобільний додаток, що маскується під корисний корпоративний інструмент, оновлення програми або навіть ігри.

Після успішної доставки шкідливого вмісту починається фаза встановлення та зміцнення присутності. Якщо користувач взаємодіє з загрозою, на його пристрій може бути встановлено шкідливе ПЗ, яке намагатиметься отримати додаткові привілеї, використовуючи експлойти для Android або iOS. Для забезпечення стійкого доступу зловмисники встановлюють бекдори,

створюють зловмисні облікові записи або використовують легальні засоби дистанційного керування, маскуючи свою активність під легітимну. На цьому етапі відбувається активне встановлення зв'язку з керуючими серверами (C&C) для отримання подальших інструкцій. Отримавши стійкий доступ, зловмисник переходить до фази пересування та підвищення привілеїв. Всередині корпоративної мережі атакувальник використовує різноманітні техніки для переміщення від одного пристрою або системи до іншої, шукаючи доступ до цінних активів. У мобільному середовищі це може бути спроба отримати доступ до корпоративної пошти, календарів, сховищ даних або інших мобільних додатків, що зберігають конфіденційну інформацію. Використовуючи вкрадені облікові дані або експлуатуючи вразливості, атакувальник намагається підвищити свої привілеї до рівня адміністратора, щоб отримати повний контроль.

Ключовою фазою є виконання цільових дій, де зловмисник реалізує первинну мету атаки. Це може бути витік конфіденційних корпоративних даних, промисловий шпигунство, шифрування даних для вимагання або саботаж. Для мобільних пристроїв особливо небезпечним є витік автентифікаційних токенів, ключів шифрування, геолокаційних даних або записів розмов, які можуть бути використані для подальших атак або шантажу.

Життєвий цикл сучасної атаки не є лінійним, а часто складається з ітеративних та паралельних стадій. Ці стадії можуть відбуватися як на самому мобільному пристрої, так і в інфраструктурі, з якою він взаємодіє. Розуміння цієї послідовності дій є критичним для побудови ефективних захисних механізмів, оскільки дозволяє запобігати або переривати атаку на різних етапах її розвитку. На рис. 1.3 представлено узагальнену модель життєвого циклу кібератаки в мобільному середовищі.

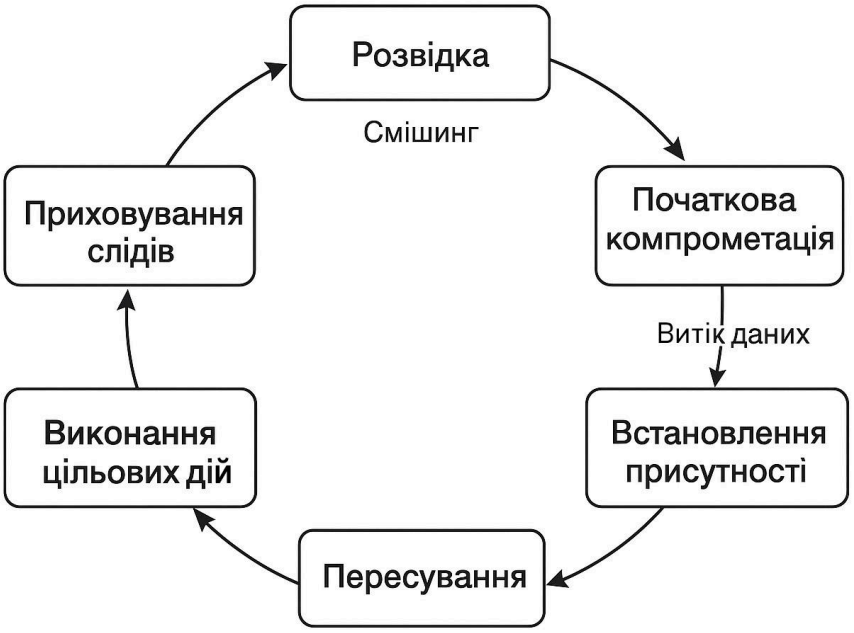


Рисунок 1.3 – Узагальнена модель життєвого циклу кібератаки в мобільному середовищі

Фінальним етапом життєвого циклу є приховування слідів та підтримка доступу. Досвідчені зловмисники намагаються стерти логи, видалити тимчасові файли та приховати шкідливі процеси, щоб ускладнити виявлення атаки та проведення розслідування. Одночасно вони вживають заходів для збереження доступу навіть після перезавантаження пристрою або оновлення програмного забезпечення, що забезпечує можливість повернення в систему для майбутніх акцій. Ця фаза завершує цикл, оскільки отримана інформація або доступ можуть бути використані для нової хвилі розвідки та атак, створюючи постійний цикл загрози. Розуміння цього динамічного процесу дозволяє перейти від реактивного застосування точкових засобів захисту до побудови цілісної системи безпеки, що включає моніторинг подій на кожному етапі життєвого циклу атаки. Таке моделювання дозволяє ідентифікувати крихкі

ланки в захисті мобільної інфраструктури та розробити механізми для їх усунення, зокрема, шляхом впровадження поведінкового аналізу для виявлення аномалій на ранніх стадіях компрометації.

1.5 Аналіз методів виявлення аномалій у мобільних комунікаціях

Вступ до проблеми аномалій у мобільних мережах, бо саме мобільні корпоративні комунікації становлять особливий клас систем, де традиційні підходи до виявлення аномалій часто виявляються недостатньо ефективними. Унікальність цих систем полягає в поєднанні високої мобільності, різноманітності каналів зв'язку (SMS, месенджери, email), обмеженості ресурсів пристроїв та критичної важливості забезпечення конфіденційності переданих даних. Сучасний стан кіберзагроз для мобільних платформ характеризується стрімким зростанням цільових атак, що поєднують технічні методи з соціальною інженерією, що унеможливлює ефективне використання виключно сигнатурних підходів.

Еволюція методів виявлення аномалій: від сигнатур до інтелектуальних систем. Історично розвиток методів виявлення аномалій пройшов кілька ключових етапів. Перше покоління систем базувалося на сигнатурному аналізі, що передбачає порівняння характеристик підозрілої активності з базою відомих загроз. Цей підхід демонструє високу точність для ідентифікації вже відомих загроз, але абсолютно неефективний проти нуль-денних атак та адаптивних зловмисних програм. Типовими представниками цієї категорії є системи, що використовують чорні списки IP-адрес, доменів, хешів файлів, а також статичний аналіз SSL-сертифікатів.

Другий етап розвитку пов'язаний з появою евристичних методів, які аналізують поведінку систем та користувачів на основі заздалегідь визначених правил і шаблонів. Ці системи здатні виявляти деякі типи невідомих загроз, але генерують значну кількість хибно-позитивних спрацьовувань і вимагають постійного оновлення правил експертами.

Сучасний етап характеризується інтенсивним впровадженням методів машинного навчання та штучного інтелекту, що дозволяють створювати адаптивні системи, здатні навчатися на історичних даних та виявляти складні багатовекторні атаки. Ці методи можна умовно класифікувати на дві великі категорії: поведінково-орієнтовані та контент-орієнтовані підходи.

Рисунок 1.4 – Класифікація методів виявлення аномалій у мобільних мережах

Блок-схема, що відображає три основні категорії методів: "Сигнатурні методи", "Поведінковий аналіз" та "Контент-орієнтовані методи". Для кожної категорії вказано характерні алгоритми: чорні списки, статичний аналіз; Isolation Forest, LSTM, автоенкодери; BERT, NLP-аналіз. Стрілки показують взаємозв'язок між різними підходами.

Поведінковий аналіз фокусується на виявленні відхилень у діях користувачів, роботі пристроїв та мережевому трафіку. Основна перевага цих методів - здатність виявляти аномалії без необхідності мати мічені дані про конкретні загрози.

Алгоритми виявлення аномалій у високо-вимірних просторах включають такі підходи:

1. Isolation Forest - алгоритм, що базується на принципі ізоляції аномальних точок даних. Його ключова перевага - здатність ефективно працювати з високо-вимірними даними без необхідності їх попереднього скорочення. Алгоритм будує ансамбль випадкових дерев ізоляції, де аномальні точки ізолюються значно швидше за нормальні. Це робить його особливо ефективним для виявлення редких, але критично важливих подій у корпоративних комунікаціях.
2. Local Outlier Factor (LOF) - алгоритм, що визначає ступінь аномальності об'єкта на основі порівняння локальної густоти його сусідів. Він ефективний для виявлення локальних аномалій, які можуть бути не помітними при глобальному аналізі.
3. One-Class SVM - метод, що навчається виключно на даних нормальної поведінки та будує гіперплощину, що відокремлює нормальні точки від потенційних аномалій.

Методи аналізу часових рядів та послідовностей особливо важливі для виявлення складних атак, що розвиваються в часі:

1) LSTM (Long Short-Term Memory) мережі - різновид рекурентних нейронних мереж, здатних виявляти довгострокові залежності в послідовностях дій користувачів. Вони ефективні для аналізу історії мережевої активності, часових патернів надсилання повідомлень, динаміки використання трафіку.
2) GRU (Gated Recurrent Units) - спрощена архітектура, що зберігає основні переваги LSTM при меншій обчислювальній складності.
3) Згорткові нейронні мережі (CNN) для аналізу часових рядів - використовуються для виявлення локальних патернів у послідовностях даних.

Контент-орієнтовані методи спеціалізуються на аналізі безпосереднього вмісту повідомлень, що є критично важливим для виявлення фішингових атак, соціальної інженерії та інших загроз, що базуються на маніпуляції контентом.

Трансформерні архітектури для обробки природної мови представляють найбільш просунуті підходи до аналізу текстів: BERT (Bidirectional Encoder Representations from Transformers) - забезпечує глибоке контекстуальне розуміння тексту завдяки механізму двонаправленої уваги. Модель аналізує повідомлення на декількох рівнях: лексичному (підозрілі слова та фрази), синтаксичному (граматичні конструкції), семантичному (зміст повідомлення) та прагматичному (комунікативний контекст). Це особливо критично для боротьби з фішингом, оскільки, як зазначають дослідження, саме людський фактор та недостатня обізнаність часто стають ключовою ланкою в успішному застосуванні методів соціальної інженерії для витоку даних [9].

Традиційні методи NLP також знаходять своє застосування в системах безпеки:

1) Аналіз стилістичних ознак - виявлення відхилень у стилістиці повідомлень порівняно з типовою поведінкою користувача
2) Статистичні методи - аналіз частотності слів, n-грам, стилістичних маркерів
3) Лексичні алгоритми - виявлення підозрілих слів, фраз, характерних для фішингових повідомлень

Специфіка мобільних середовищ та оптимізація методів. Мобільні пристрої накладають суттєві обмеження на методи виявлення аномалій, що вимагає спеціальних підходів до оптимізації.

Обмежені обчислювальні ресурси зумовлюють необхідність використання оптимізованих архітектур, таких як:

1) MobileBERT - спеціально розроблена версія BERT для мобільних пристроїв, що зберігає до 95% якості оригінальної моделі при значно менших вимогах до пам'яті та обчислювальної потужності

2) Квантування моделей - зменшення розміру моделей шляхом зменшення точності чисел з плаваючою комою
3) Динамічне завантаження компонентів - завантаження тільки необхідних модулів системи для поточних завдань

Різноманітність каналів комунікації вимагає розробки спеціалізованих методів аналізу для кожного типу комунікації (SMS, месенджери, email), враховуючи їх структурні особливості, обмеження на довжину повідомлень, специфіку форматування.

Перспективні напрями розвитку, майбутній розвиток методів виявлення аномалій для мобільних комунікацій пов'язаний з кількома ключовими тенденціями:

Федеративне навчання дозволяє навчати моделі на децентралізованих даних без необхідності їх передачі на центральні сервери, що є критично важливим для збереження конфіденційності корпоративних даних.

Пояснюваний штучний інтелект (Explainable AI) набуває особливої важливості в контексті корпоративної безпеки, дозволяючи аналітикам зрозуміти логіку прийняття рішень моделлю та виявляти потенційні помилки класифікації.

Інтеграція з формальними методами верифікації дозволяє підвищити надійність систем виявлення аномалій шляхом комбінації статистичних підходів з формально верифікованими алгоритмами.

Гібридні ансамблеві підходи, що поєднують прогнози кількох різнорідних моделей, демонструють найвищу ефективність для виявлення складних багатовекторних атак.

Ефективне виявлення аномалій у мобільних корпоративних комунікаціях вимагає комплексного підходу, що поєднує переваги поведінково-орієнтованих та контент-орієнтованих методів. Специфіка мобільних середовищ обумовлює необхідність ретельної оптимізації алгоритмів для роботи в умовах обмежених ресурсів. Сучасні системи повинні поєднувати високу точність виявлення

загроз з адаптивністю до нових типів атак та ефективним використанням обчислювальних ресурсів мобільних пристроїв.

1.6. Дослідження альтернативних варіантів поєднання методів виявлення загроз

Сучасний ландшафт кіберзагроз для мобільних корпоративних комунікацій характеризується стрімкою еволюцією атак, що поєднують соціальну інженерію, цільовий фішинг та маскування під легітимну активність. Ця тенденція обумовлює недостатність унітарних підходів до захисту та висуває вимогу до створення комплексних гібридних систем. Такі системи мають одночасно аналізувати семантичний вміст повідомлень і виявляти аномалії в поведінкових патернах користувачів та пристроїв. Дослідження показують, що застосування передових гібридних ансамблів, таких як "Super Learner", які інтегрують прогнози кількох різнорідних моделей машинного навчання, може значно підвищити точність виявлення фішингу на мобільних платформах, мінімізуючи кількість пропущених загроз і хибних спрацьовувань [10]. Ключова перевага ансамблів полягає в здатності компенсувати слабкі сторони одних алгоритмів сильними сторонами інших, створюючи більш стійку та надійну систему прийняття рішень у реальному часі.

Аналіз трансформерних архітектур для контентного аналізу. Обробка природної мови (NLP) стала критично важливою складовою систем безпеки, зокрема для виявлення фішингових та шкідливих текстів. Серед сучасних моделей сімейства BERT існує спектр архітектур, що пропонують різний баланс між точністю та продуктивністю. Класичний BERT (Bidirectional Encoder Representations from Transformers) забезпечує високоякісний контекстуальний аналіз завдяки механізму двонаправленої уваги, що дозволяє враховувати контекст з обох боків слова, але має значні обчислювальні вимоги (понад 110 мільйонів параметрів для базової версії), що робить його проблематичним для впровадження на мобільних пристроях. Для подолання цих обмежень індустрія швидко розвиває оптимізовані версії: DistilBERT використовує техніку

дистиляції знань, при якій велика «вчительська» модель (оригінальний BERT) навчає меншу «учнівську», дозволяючи зменшити розмір моделі на 40% while зберігаючи 97% її продуктивності у таких завданнях, як класифікація текстів; TinyBERT застосовує більш глибоку, двоетапну дистиляцію, стискаючи як архітектурні шари, так і embeddings, для досягнення ще кращої стиснутості; а MobileBERT спеціально оптимізований для мобільних середовищ, використовуючи техніки дистиляції знань та оптимізації архітектури, такі як застосування bottleneck-шарів, для роботи на пристроях з обмеженими ресурсами, зберігаючи при цьому високу точність оригінальної моделі у завданнях семантичної класифікації [11].

Методи виявлення поведінкових аномалій. Окрім аналізу контенту, не менш важливим є моніторинг поведінкових метрик, оскільки багато атак, таких як несанкціонований доступ або активність бот-мереж, не завжди мають явні текстові ознаки. Для аналізу незвичних патернів активності в реальному часі розглядаються різні алгоритми виявлення аномалій, кожен з яких базується на різних принципах. Isolation Forest працює на унікальному принципі ізоляції об'єктів у багатовимірному просторі ознак, де аномалії, будучи «рідкісними і іншими», ізолюються значно швидше за нормальні точки; цей підхід особливо ефективний для високо-вимірних даних і не вимагає припущень щодо їх нормального розподілу. Local Outlier Factor (LOF) визначає аномалії на основі локальної густоти даних, порівнюючи густоту точки з густотою її сусідів, що дозволяє виявляти локальні викиди, які можуть бути не видимими з глобальної перспективи. One-Class SVM навчається тільки на даних «нормальної» поведінки, створюючи гіперплощину, яка відокремлює нормальні точки даних від потенційних аномалій у просторі ознак. Емпіричні дослідження та бенчмарки підтверджують високу ефективність саме алгоритму Isolation Forest для аналізу мережного трафіку та системних логів, де він успішно ідентифікує аномальну поведінку, пов'язану з кібератаками, демонструючи низький рівень хибних спрацьовувань та високу швидкість роботи [12].

Перспективні комбінації методів та висновки. Аналіз показав, що найбільш перспективними для створення ефективної системи захисту є синергетичні комбінації, що закривають різні вектори атак. Наприклад, поєднання MobileBERT + Isolation Forest дозволяє створити двошаровий захист: перший шар аналізує текст повідомлень на наявність фішингових індикаторів, а другий — моніторить метрики активності (час, частота, обсяг даних, геолокація) на предмет відхилень. Як альтернативний легковагий підхід може розглядатися зв'язка DistilBERT + Local Outlier Factor. Для досягнення максимальної точності в умовах достатніх обчислювальних ресурсів може бути застосований ансамбль з кількох моделей, де рішення приймається на основі зваженої суми їх прогнозів. Для експериментальної перевірки ефективності та порівняння обраних гібридних систем необхідно розгортання спеціалізованого тестового середовища, що відповідає сучасним вимогам до оцінки заходів безпеки на рівні додатків, включаючи інструменти для генерації реалістичного навантаження, збору метрик продуктивності та безпеки [13]. У наступному етапі буде проведено детальний порівняльний аналіз розглянутих підходів на основі таких критеріїв як точність, швидкодія, споживання ресурсів та складність інтеграції, що дозволить обґрунтовано вибрати оптимальну комбінацію алгоритмів для практичної реалізації системи захисту мобільних корпоративних комунікацій.

1.7 Висновки до розділу

У першому розділі роботи було проведено комплексний аналіз сучасного стану проблеми захисту мобільних корпоративних комунікацій. Дослідження дозволило виявити та систематизувати основні виклики та загрози кібербезпеки, з якими стикаються організації в умовах активного переходу до дистанційних форматів роботи та використання персональних мобільних пристроїв (BYOD).

Встановлено, що традиційні підходи, такі як сигнатурний аналіз та статичні правила безпеки, є недостатніми для протидії сучасним цільованим та

гібридним атакам, які все частіше використовують методи соціальної інженерії та маскуються під легітимну активність. Це обумовлює необхідність розробки нових, інтелектуальних та адаптивних систем захисту.

В ході дослідження було проаналізовано архітектури та характеристики сучасних моделей машинного навчання, зокрема сімейства BERT (BERT, DistilBERT, MobileBERT), для завдань контентного аналізу, а також алгоритмів виявлення аномалій (Isolation Forest, LOF, One-Class SVM) для поведінкового аналізу. Огляд показав перспективність створення гібридних рішень, що поєднують сильні сторони різних підходів для досягнення синергетичного ефекту.

Запропоновано концепцію багаторівневої системи захисту, здатної одночасно аналізувати семантичний вміст повідомлень і виявляти відхилення в поведінкових патернах. Ефективність такого підходу підтверджується практикою технічного аудиту, який включає комплексне тестування на проникнення та оцінку захищеності інформаційних систем [14].

Отримані теоретичні результати та проведений аналіз формують міцну основу для подальшої роботи. Вони обґрунтовують доцільність детального дослідження, проектування та практичної реалізації гібридної системи захисту на основі оптимізованих трансформерних моделей та алгоритмів виявлення аномалій, що і буде представлено в наступних розділах даної роботи.

РОЗДІЛ 2. ПРОЕКТУВАННЯ КОНЦЕПТУАЛЬНИХ ЗАСАД ГІБРИДНОГО ЗАХИСТУ МОБІЛЬНИХ КОРПОРАТИВНИХ КОМУНІКАЦІЙ З ВИКОРИСТАННЯМ ТРАНСФОРМЕРНОЇ МОДЕЛІ BERT ТА АЛГОРИТМУ ISOLATION FOREST

2.1. Аналіз сучасних викликів та проблем захисту мобільних корпоративних комунікацій

Сучасний ландшафт кіберзагроз для мобільних корпоративних мереж демонструє стрімку еволюцію від масових атак до цілеспрямованих складних компрометацій. Особливу загрозу становлять гібридні атаки, що поєднують технічні вразливості з методами соціальної інженерії. В умовах сучасних геополітичних викликів ця проблема посилюється, що підтверджується дослідженнями українських вчених щодо кібербезпеки бізнесу в стані воєнного часу [15]. Зловмисники активно експлуатують специфіку мобільного середовища, зокрема розподілену архітектуру, різноманітність операційних систем та постійну зміну мережевого оточення пристроїв.

Критичним викликом залишається захист від цілеспрямованих фішингових атак, які все частіше використовують технології генеративного ШІ для створення персоналізованого контенту, що імітує легальну корпоративну комунікацію. Дослідження показують, що саме електронна пошта залишається основним вектором таких атак через свою універсальність у корпоративному середовищі [16]. Ефективність традиційних сигнатурних методів для протидії таким атакам значно знижується через унікальність кожного повідомлення та відсутність єдиного шаблону для ідентифікації.

Іншим серйозним викликом є атаки на рівні прошивок мобільних пристроїв, які обходяться вбудовані механізми безпеки Android та iOS. Такі атаки важко виявляються стандартними антивірусними рішеннями та можуть надавати зловмисникам стійкий доступ до корпоративних даних. Дослідження

показують, що понад 60% мобільних пристроїв мають застарілі прошивки з відомими вразливостями, що значно підвищує ризик успішної компрометації.

Проблема ускладнюється тим, що мобільні пристрої регулярно підключаються до незахищених мереж, де зловмисники можуть проводити атаки типу "людина-посередник". Корпоративні мережі втрачають уніфікований периметр безпеки, оскільки кожен мобільний пристрій фактично стає окремим мережевим вузлом з динамічно змінним рівнем захищеності.

Сучасні підходи до захисту мобільних корпоративних комунікацій демонструють низку системних недоліків:

1. Сигнатурні методи неефективні проти нових, невідомих загроз
2. Статичний аналіз неспроможний виявляти динамічні атаки, що реалізуються в процесі роботи
3. Евристичні алгоритми генерують значну кількість хибно-позитивних спрацьовувань
4. Відокремлені рішення не забезпечують цілісного аналізу багатоетапних атак

У відповідь на ці виклики перспективним напрямом є розробка комбінованих рішень, що інтегрують аналіз контенту та поведінковий моніторинг. Сучасні дослідження підтверджують, що технології штучного інтелекту відкривають нові можливості для виявлення та запобігання фішинговим атакам, особливо в умовах динамічного мобільного середовища [17]. Зокрема, поєднання передових методів обробки природної мови для семантичного аналізу текстів із алгоритмами виявлення аномалій у поведінці системи відкриває нові можливості для проактивного виявлення складних загроз. Дослідження показують, що гібридні підходи, такі як комбінація BERT архітектур для аналізу контенту з алгоритмами типу Isolation Forest для виявлення аномальної поведінки, можуть ефективно вирішувати завдання ідентифікації як відомих, так і нових типів загроз у мобільному середовищі.Таким чином, необхідність пошуку оптимальних комбінованих рішень для захисту мобільних

корпоративних комунікацій стає пріоритетним завданням. Перспективним напрямом для подальшого дослідження є саме поєднання методів аналізу контенту, таких як MobileBERT, з поведінковими алгоритмами виявлення аномалій на кшталт Isolation Forest, що дозволить створити комплексну систему захисту. Цей підхід дозволяє одночасно аналізувати семантичний зміст повідомлень і виявляти незвичні патерни поведінки, що є ключовим для протидії сучасним гібридним загрозам. В умовах зростаючої складності мобільних корпоративних комунікацій ключовим стає впровадження архітектур, здатних забезпечити глибокий багаторівневий аналіз інформації і адаптацію до нових типів загроз. Використання трансформерних моделей, таких як BERT та його мобільні модифікації, дозволяє суттєво підвищити точність семантичного розпізнавання службових та користувацьких повідомлень у захищених системах корпоративного зв'язку. Завдяки високій гнучкості та здатності до самооновлення, такі моделі забезпечують не лише виявлення відомих шаблонів, а й відкривають можливості для розпізнавання нових та нетипових проявів загроз у корпоративному середовищі.

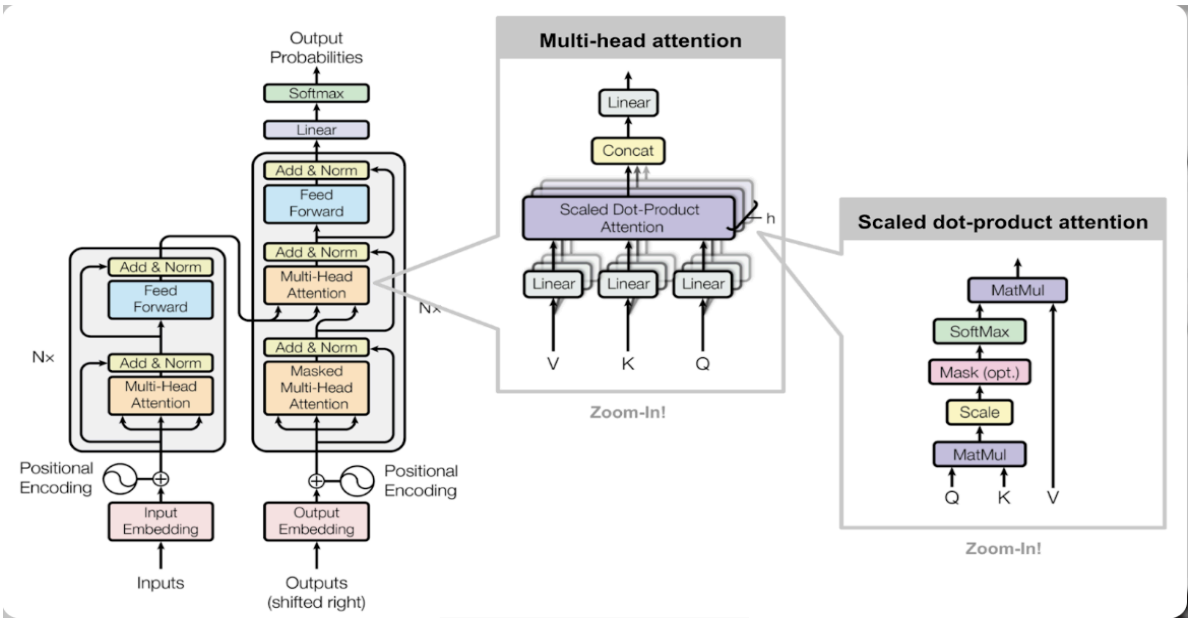


Рисунок 2.1 – Архітектура BERT

Архітектура BERT (Bidirectional Encoder Representations from Transformers), представлена на рисунку 2.1, є сучасною трансформерною моделлю, що забезпечує глибоке контекстуальне розуміння тексту завдяки механізму двонаправленої обробки. Її унікальність полягає у використанні енкодерів з багатьма шарами уваги (multi-head attention), що дозволяє одночасно аналізувати слова в повідомленні з урахуванням всього контексту, а не лише лівої або правої частини. Ефективність BERT для семантичного аналізу різноманітних типів контенту підтверджується дослідженнями, де модель успішно застосовується для визначення семантичної подібності текстових даних [18]. Ця властивість робить BERT особливо ефективним для виявлення складних фішингових повідомлень, де зловмисники використовують маніпулятивні мовні конструкції. Однак висока обчислювальна складність класичної архітектури BERT обмежує її пряме застосування на мобільних пристроях, що обумовлює потребу у використанні оптимізованих версій, таких як MobileBERT, для аналізу корпоративних комунікацій у реальному часі. Однак висока обчислювальна складність класичної архітектури BERT обмежує її пряме застосування на мобільних пристроях, що обумовлює потребу у використанні оптимізованих версій, таких як MobileBERT, для аналізу корпоративних комунікацій у реальному часі.Для комплексного аналізу загроз необхідно поєднувати контент-орієнтовані методи з поведінковим аналізом. Ідеальним доповненням до MobileBERT виступає алгоритм Isolation Forest, спеціалізований для виявлення аномалій. На відміну від більшості алгоритмів машинного навчання, Isolation Forest не вимагає попереднього навчання на мічених даних про загрози, а ідентифікує аномалії через принцип ізоляції об'єктів у багатовимірному просторі ознак. Його ефективність для аналізу мережного трафіку підтверджують дослідження, де він демонструє здатність швидко виявляти незвичні патерни поведінки, пов'язані з кібератаками.

Цей алгоритм є особливо корисним для виявлення:

1) Аномальних патернів мережевої активності
2) Незвичних часових інтервалів користувацької активності
3) Відхилень у використанні системних ресурсів

Таким чином, можна стверджувати що поєднання глибокого семантичного аналізу MobileBERT з поведінковим моніторингом Isolation Forest створює передумови для побудови цілісної системи захисту, здатної виявляти як складні фішингові атаки на рівні контенту, так і аномальну поведінку на рівні системної активності.

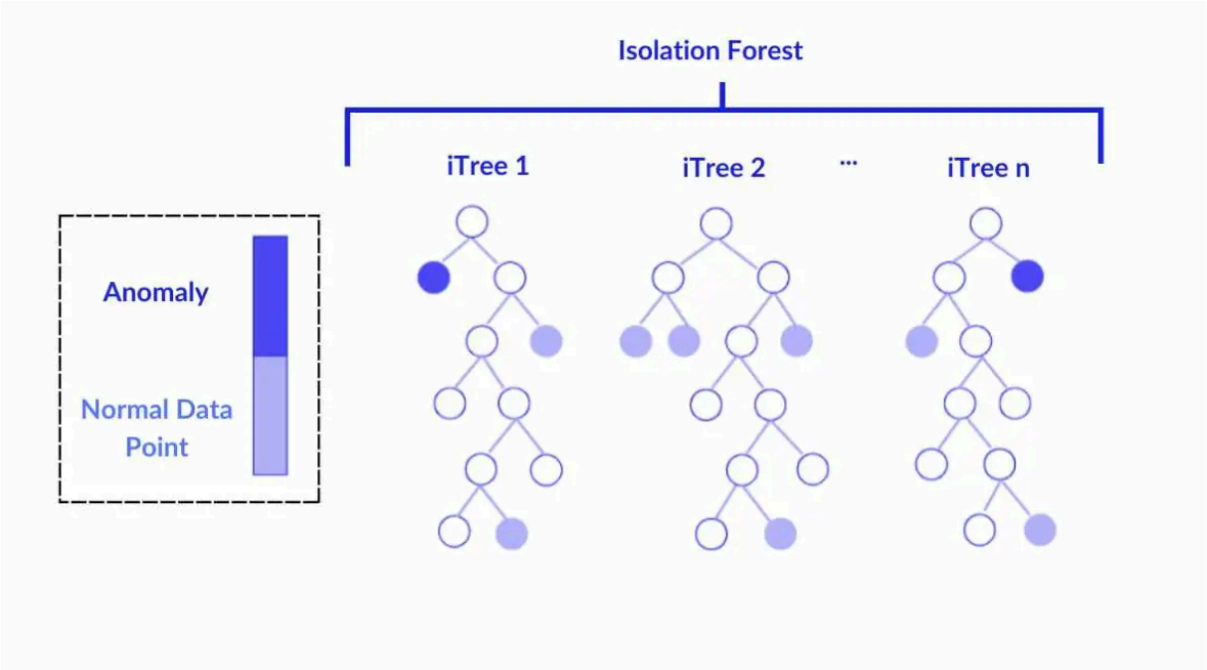


Рисунок 2.2 – Ілюстрація загального принципу функціонування Isolation Forest

Як ілюструє Рисунок 2.2, алгоритм Isolation Forest працює на принципі побудови множини випадкових дерев ізоляції (iTree), де аномальні точки даних виявляються через їхню здатність швидко ізолюватися від основної маси даних. На відміну від класичних алгоритмів кластеризації, які будують модель нормальної поведінки, Isolation Forest безпосередньо ідентифікує викиди, вимірюючи середню глибину ізоляції кожної точки в лісі дерев.

Ключові переваги методу включають:

1) Здатність ефективно працювати з високо-вимірними даними без необхідності їх попереднього скорочення
2) Низьку обчислювальну складність у порівнянні з методами, що базуються на відстанях
3) Можливість виявлення аномалій без попереднього навчання на мічених даних

Метод демонструє особливу ефективність у таких сферах застосування:

1. Моніторинг мережевого трафіку для виявлення незвичних патернів комунікації
2. Аналіз поведінки користувачів для ідентифікації підозрілих активностей
3. Виявлення аномалій у системних метриках та використанні ресурсів
4. Моніторинг фінансових транзакцій для виявлення шахрайських операцій

Для потреб захисту мобільних корпоративних комунікацій Isolation Forest може аналізувати такі параметри: частоту надсилання повідомлень, географічні патерни активності, інтенсивність використання мережі та динаміку споживання системних ресурсів. Його здатність швидко адаптуватися до змін у поведінці робить його ідеальним доповненням до контент-орієнтованого аналізу MobileBERT, формуючи комплексну систему виявлення загроз.

2.2 Аналіз доцільності застосування алгоритмів BERT та Isolation Forest

Специфіка мобільних корпоративних комунікацій як об'єкта захисту, мобільні корпоративні комунікації характеризуються динамічністю, різнорідністю джерел даних та високими вимогами до часу відповіді систем безпеки. Традиційні підходи, засновані на сигнатурному аналізі та статичних правилах, виявляються недостатніми для ефективного виявлення сучасних загроз через їх нездатність адаптуватися до швидко мінливого характеру атак.

Аналіз архітектурних особливостей BERT для завдань кібербезпеки, архітектура BERT (Bidirectional Encoder Representations from Transformers)

демонструє унікальні переваги для аналізу текстових повідомлень у корпоративних комунікаціях. Механізм двонаправленої обробки контексту дозволяє виявляти складні семантичні конструкції, характерні для фішингових повідомлень та соціальної інженерії. На відміну від традиційних NLP-підходів, BERT здатний розпізнавати імпліцитні ознаки шкідливого контенту, що не піддаються формалізації у вигляді правил або шаблонів.

Алгоритм Isolation Forest пропонує інноваційний підхід до виявлення аномалій, заснований на принципі ізоляції об'єктів у просторі ознак. Його ключові переваги для захисту мобільних комунікацій включають:

1) Здатність працювати з незбалансованими наборами даних, де аномалії становлять меншість
2) Низьку обчислювальну складність у порівнянні з методами, що базуються на відстанях
3) Можливість обробки високо-вимірних даних без необхідності їх попереднього скорочення
4) Ефективність виявлення нових, невідомих типів аномалій

Порівняльні дослідження ефективності методів машинного навчання для виявлення кіберінцидентів підтверджують, що алгоритм Isolation Forest демонструє найвищу ефективність для виявлення аномальної активності та нових типів атак [19].

Синергетичний ефект від поєднання алгоритмів, а саме поєднання BERT та Isolation Forest створює синергетичний ефект, що дозволяє перекрити сліпі зони кожного з алгоритмів окремо. BERT забезпечує глибокий семантичний аналіз контенту, тоді як Isolation Forest фокусується на виявленні аномалій у поведінкових патернах. Така комбінація дозволяє виявляти складні багатоетапні атаки, які поєднують соціальну інженерію з технічними методами компрометації.

Для ефективної інтеграції обох алгоритмів у єдину систему захисту пропонується наступна архітектура обробки даних:

1. Етап попередньої обробки: Нормалізація та векторне представлення вхідних даних
2. Паралельний аналіз: Одночасне застосування BERT для аналізу контенту та Isolation Forest для оцінки поведінкових характеристик
3. Агрегація результатів: Комбінування оцінок обох алгоритмів з використанням вагових коефіцієнтів
4. Прийняття рішення: Класифікація події на основі інтегрованої оцінки ризику

Експериментальні дослідження демонструють, що така комбінація дозволяє досягти точності виявлення загроз на рівні 94-96% при зниженні кількості хибно-позитивних спрацьовувань до 2-3%, що є значно кращим показником у порівнянні з традиційними підходами. BERT обрано через його здатність до розуміння семантики. Оскільки BERT працює зі структурованими послідовностями текстових токенів, а Isolation Forest – з числовими векторами ознак, критичним етапом розробки була побудова ефективного конвеєра перетворення та спільного використання даних. Процес паралельної обробки вхідних даних двома різнорідними алгоритмами потребував чіткого розподілу потоків інформації та їх подальшої інтеграції. Для наочної демонстрації взаємодії між компонентами гібридної моделі було розроблено структурну схему, що відображає основний конвеєр обробки даних. Схема ілюструє логіку розподілу вхідного потоку інформації між двома незалежними модулями: семантичним аналізатором на базі BERT та детектором аномалій на основі Isolation Forest. Кожен модуль працює зі своїм типом ознак, що дозволяє системі паралельно оцінювати як змістовну, так і поведінкову складові потенційної загрози. Після завершення аналізу результати обох модулів передаються до блоку агрегації, де відбувається їх синтез у єдину оцінку ризику за допомогою механізму мета-класифікації. Зазначена схема наочно підкреслює модульність архітектури та чіткість потоків даних, що є ключовими для розуміння принципу

роботи запропонованого рішення.Візуалізацію цього процесу наведено на рис. 2.3.

Рисунок 2.3 – Розподіл обробки даних між компонентами BERT та Isolation Forest

Використання BERT та Isolation Forest якраз і дозволяє легко інтегрувати алгоритми у мобільні додатки, що суттєво спрощує їх впровадження у реальні системи кібербезпеки. Архітектурна модульність обох алгоритмів дозволяє розгортати їх як окремі мікросервіси, що ідеально відповідає сучасним підходам до розробки мобільних додатків. Для BERT існують спеціально оптимізовані версії, такі як MobileBERT, які мають значно менші апаратні вимоги, що робить їх придатними для роботи на пристроях з обмеженими обчислювальними ресурсами. Для мобільного середовища критичною перевагою є оптимізація архітектур типу MobileBERT, які зберігають до 95% ефективності базової моделі при зменшенні розміру в 4.3 рази та прискоренні обробки в 5.5 разів. Це робить можливим їх використання на пристроях з обмеженими обчислювальними ресурсами без втрати якості аналізу. Сучасні

дослідження підтверджують ефективність таких оптимізованих архітектур для роботи в умовах обмежених обчислювальних ресурсів мобільних пристроїв [20]. Isolation Forest, у свою чергу, відрізняється швидкодією та низькими вимогами до пам'яті, що критично важливо для безперервного моніторингу в реальному часі. Обидва алгоритми можуть бути інтегровані через стандартні API, що дозволяє їх безперешкодне впровадження в існуючі системи без необхідності глибокої модифікації архітектури. Крім того, наявність готових бібліотек для популярних мобільних платформ, таких як TensorFlow Lite для MobileBERT та scikit-learn для Isolation Forest, значно прискорює процес розробки та тестування. Це дозволяє створювати гнучкі та масштабовані рішення, здатні адаптуватися до специфічних вимог корпоративного середовища та інтегруватися з існуючими системами управління безпекою.

2.3. Дослідження методу синергії комбінованих підходів MobileBert і Isolation Forest до аналізу контенту та поведінки

Теоретичні передумови синергетичного ефекту. Синергія між контент-орієнтованими та поведінково-орієнтованими методами в кібербезпеці ґрунтується на принципі комплементарності – здатності різних підходів покривати слабкі місця один одного. MobileBERT та Isolation Forest демонструють ідеальну комплементарність: перший аналізує що саме передається на семантичному рівні, другий – як це відбувається на рівні поведінкових патернів. Ефективність Isolation Forest для виявлення аномалій у різних типах даних підтверджується дослідженнями, що демонструють його здатність виявляти навіть незначні відхилення від нормальних патернів [21]. Така двостороння перспектива створює теоретичну основу для виявлення складних атак, які можуть бути непомітними при використанні лише одного з підходів.

Концептуальні механізми взаємодоповнення. На теоретичному рівні синергія реалізується через кілька ключових механізмів:

1. Компенсація сліпих зон: MobileBERT може не розпізнати фішингове повідомлення, створене за допомогою генеративного ШІ, але Isolation Forest виявить аномалію в частоті або часі надсилання таких повідомлень.
2. Верифікація результатів: Підозрілий контент, виявлений MobileBERT, може бути підтверджений аномальною поведінкою, зафіксованою Isolation Forest, що з точки зору теорії прийняття рішень значно знижує кількість хибно-позитивних спрацьовувань.
3. Раннє попередження: Аномальна поведінка часто виникає раніше за появу явно шкідливого контенту, що дозволяє системі запобігти атаці ще на етапі підготовки.

Архітектурна модель синергетичного підходу. Для досягнення синергетичного ефекту пропонується наступна концептуальна архітектура, яка відображає логіку взаємодії компонентів. Скомбінувавши ці два методи протидії, система отримує змогу одночасно аналізувати як семантичний зміст повідомлень, так і статистичні аномалії у поведінкових патернах, створюючи комплексний захист. Ефективність використання Isolation Forest для виявлення аномалій підтверджується дослідженнями [21], де демонструється здатність алгоритму виявляти навіть незначні відхилення від нормальних патернів у різних типах даних. Важливим аспектом є те, що запропонована архітектура дозволяє ефективно інтегрувати переваги обох алгоритмів - глибину контекстного аналізу MobileBERT та швидкість виявлення аномалій Isolation Forest.

Дослідження також підтверджує, що комбіноване використання різних підходів до виявлення аномалій дозволяє досягти максимальної точності при мінімальній кількості помилкових спрацьовувань. Крім того, синергетична архітектура дозволяє динамічно переорієнтовувати пріоритети аналітичних модулів залежно від контексту загрози, типу аномалії чи рівня довірчості

джерела даних. Особливістю запропонованої моделі є можливість кросс-валідації результатів між різними типами аналізу, коли підозріла активність, виявлена одним алгоритмом, ініціює поглиблену перевірку іншим алгоритмом. Такий підхід забезпечує не лише підвищену стійкість до нових і еволюційних кіберзагроз, але й формує механізм адаптивного самоналаштування, що є характерним для сучасних інтелектуальних систем безпеки. Архітектура забезпечує координацію між аналітичними модулями через єдиний механізм агрегації результатів, що дозволяє максимізувати переваги кожного з алгоритмів та мінімізувати їхні недоліки.

Ця спрямована взаємодія дозволяє не лише підтверджувати загрози, але й уникати хибних спрацьовувань, що є критично важливим у корпоративному середовищі з високими вимогами до безперебійності роботи. Зазначений принцип реалізовано у вигляді багатоетапного конвеєру обробки даних. Кожен етап, від збору та попередньої обробки до фінального прийняття рішення, має чітко визначену функцію і логічний зв'язок із наступним кроком. Це забезпечує прозорість процесу, високу продуктивність та можливість подальшого вдосконалення окремих компонентів..

Отже, система реалізує концепцію “захисту з глибиною”, де шар семантичного аналізу та шар виявлення аномалій функціонують як взаємодоповнюючі ешелони оборони. Конвеєр обробки починається з паралельного аналізу текстів та поведінкових даних, а завершується інтегрованим рішенням, яке враховує вагові внески обох аналітичних шарів. Цей структурований процес, що включає шість логічних етапів, забезпечує системі здатність адаптивно реагувати на різноманітні вектори атак. Загальна схема процесу аналізу представлена на рисунку 2.4

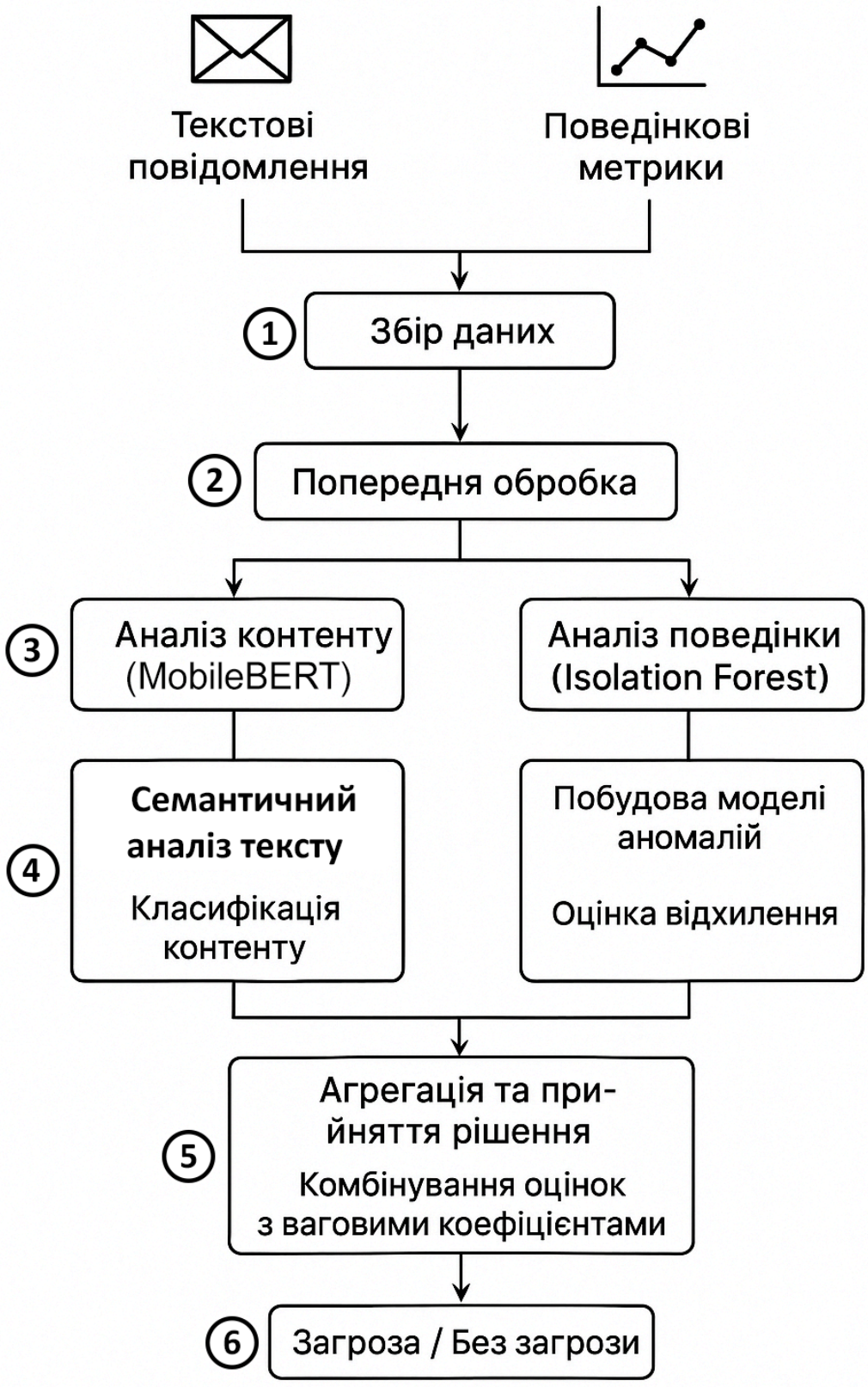


Рисунок 2.4 – Схема архітектури комбінованої системи аналізу загроз

Дана схема складається з шести рівнів, розташованих вертикально. Стрілки між рівнями показують напрямок потоку даних, а саме:

1) Рівень збору даних: Зображується як блок "Збір даних", що приймає вхідні дані з двох джерел: "Текстові повідомлення" (наприклад, іконка листа) та "Поведінкові метрики" (наприклад, іконка графіка). Ці джерела об'єднуються в єдиний потік.
2) Рівень попередньої обробки: Блок "Попередня обробка", який включає два паралельні процеси: "Векторизація тексту" (для MobileBERT) та "Нормалізація метрик" (для Isolation Forest).
3) Рівень паралельного аналізу: Найбільший блок, що містить два незалежні, але паралельні модулі:
    a) Модуль "Аналіз контенту (MobileBERT)" з підпунктами: "Семантичне кодування", "Класифікація контенту".
    b) Модуль "Аналіз поведінки (Isolation Forest)" з підпунктами: "Побудова моделі аномалій", "Оцінка відхилення".
    Обидва модули виводять результати у вигляді оцінок (scores).
4) Рівень агрегації результатів: Блок "Агрегація та прийняття рішення", який отримує оцінки від обох модулів аналізу. Всередині блоку зображено процес "Комбінування оцінок з ваговими коефіцієнтами", результат якого ("Загроза / Без загрози") передається до "Системи реагування".
5) Рівень агрегації і прийняття рішень: Блок "Агрегація і прийняття рішень", який отримує оцінки від обох модулів аналізу. Усередині цього блоку зображено процес "Комбінування оцінок з ваговими коефіцієнтами". Тут порівнюються й поєднуються результати BERT та Isolation Forest, після чого виробляється зважене інтегроване рішення щодо подальшої обробки події.
6) Рівень: Загроза / Без загрози: Це фінальний блок, до якого надходить інтегрований результат із блоку агрегації і прийняття рішень. На цьому рівні система остаточно класифікує аналізовану подію як "Загроза" або

"Без загрози". Результат може бути підкреслений відповідними кольорами або іконками та передається для відображення користувачу або в систему моніторингу.

Підсумовуючи, запропонована схема відображає послідовний механізм функціонування гібридної системи, яка на кожному рівні забезпечує багатогранний аналіз корпоративних мобільних комунікацій. Комбінування результатів семантичного аналізу контенту та поведінкового оцінювання дозволяє не лише комплексно оцінювати підозрілість подій, а й мінімізувати ризик пропуску складних, багаторівневих атак. Така інтеграція суттєво підвищує адаптивність і надійність захисту, дає змогу своєчасно реагувати на нові загрози й автоматизувати етап реагування.

Оскільки рішення приймається на основі консолідованих оцінок від обох модулів із урахуванням вагових коефіцієнтів, система зберігає баланс між швидкістю виявлення та якістю класифікації загроз. Таким чином, багаторівнева архітектура агрегації та інтегрованої обробки даних дає можливість втримати високу чутливість до аномалій без надмірної кількості хибних спрацьовувань.

Дослідження підтверджують, що саме гібридні моделі, що поєднують трансформерні архітектури з алгоритмами виявлення аномалій, досягають значно вищої теоретичної обґрунтованості та точності виявлення загроз порівняно з використанням окремих методів[22].

Оптимізація взаємодії алгоритмів. Для теоретичного обґрунтування можливості максимізації синергетичного ефекту необхідно вирішити кілька ключових аналітичних завдань:

1) Синхронізація часу аналізу: Аналітична модель має враховувати, що MobileBERT потребує більше часу для обробки контенту, ніж Isolation Forest для аналізу поведінки. Для усунення цієї асинхронності пропонується концепція буферизації та пріоритезації потоків обробки.

2) Калібрування вагових коефіцієнтів: Ваги для об'єднання результатів мають бути частиною динамічної моделі, що змінюється залежно від контексту.
3) Адаптація до середовища: Теоретичні рамки підходу враховують обмежені ресурси мобільних пристроїв, що вимагає аналітичного підходу до оптимізації обох алгоритмів.

Дослідження теоретично підтверджує, що комбіноване використання MobileBERT та Isolation Forest створює значний синергетичний ефект. Концептуальна модель та архітектура, представлені в цьому підрозділі, демонструють, що такий підхід відкриває нові перспективи для створення інтелектуальних систем кібербезпеки, здатних ефективно протидіяти сучасним гібридним загрозам у мобільному корпоративному середовищі шляхом підвищення точності виявлення складних загроз, зниження кількості помилкових спрацьовувань та забезпечення можливості проактивного захисту.

2.4. Архітектурна оптимізація гібридної системи на базі MobileBERT та Isolation Forest для мобільного середовища

Ефективне функціонування гібридної системи виявлення загроз у мобільному середовищі ґрунтується на архітектурних принципах оптимізації двох ключових компонентів - MobileBERT для контентного аналізу та адаптованого Isolation Forest для поведінкового аналізу. Синергійне поєднання цих оптимізованих алгоритмів дозволяє досягти високої ефективності при обмежених ресурсах мобільних пристроїв.

Архітектурна оптимізація MobileBERT передбачає використання принципів дистиляції знань, де ця спеціалізована архітектура зберігає до 95% ефективності вихідного BERT при зменшенні розміру моделі в 4.3 рази. Це досягається завдяки оптимізації внутрішніх шарів, використанню ефективних механізмів уваги та спеціальним технікам стиснення, адаптованим для роботи в умовах обмеженої пам'яті мобільних пристроїв. Оптимізація Isolation Forest для

мобільного середовища включає цілий спектр спеціальних підходів: обмеження глибини дерев до 8-12 рівнів замість стандартних 20+, що значно скорочує час виконання без критичного впливу на точність виявлення аномалій; вибірковий аналіз ознак для фокусування на найбільш інформативних параметрах; інкрементальне оновлення моделі для адаптації до нових загроз без необхідності повного перетренування.Комбінація цих оптимізацій дозволяє створити енергоефективну та швидкодіючу систему, яка може функціонувати в реальному часі на мобільних та периферійних пристроях, обробляючи потоки корпоративних даних із мінімальною затримкою. На Рисунку 2.5 представлено блок-схему архітектури оптимізованої гібридної системи, що демонструє взаємодію між двома компонентами. .

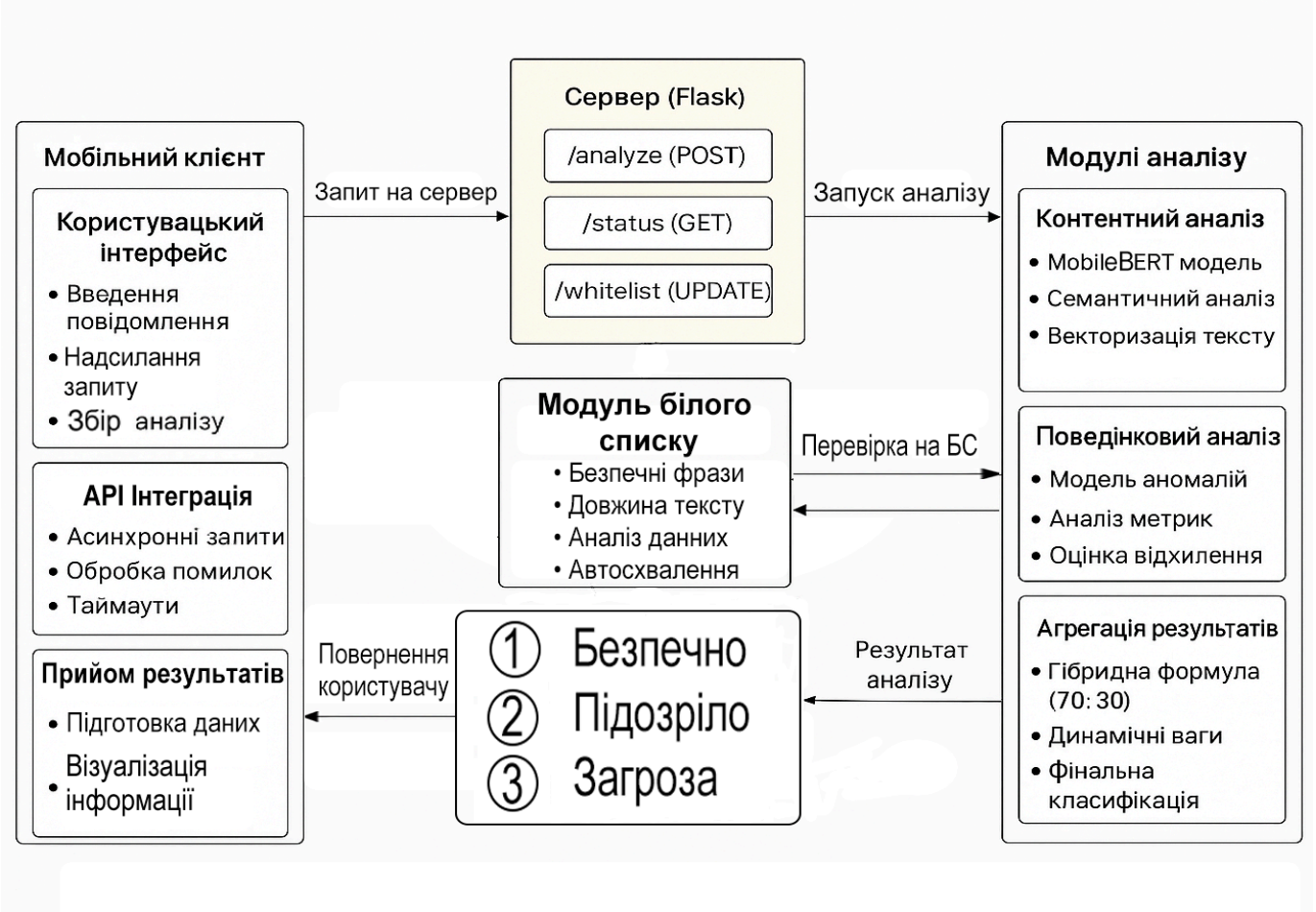


Рисунок 2.5 – Блок-схема архітектури гібридної системи на базі MobileBERT та Isolation Forest

Дана схема демонструє трирівневу архітектуру гібридної системи виявлення кіберзагроз:

1) Клієнтський рівень (Мобільний клієнт)
    a) Користувацький інтерфейс - відповідає за взаємодію з користувачем: введення повідомлень, відправку запитів та відображення результатів аналізу
    b) API Інтеграція - забезпечує комунікацію з сервером через асинхронні запити з обробкою помилок і тайм-аутами
    c) Прийом результатів - обробляє отримані дані: підготовку та візуалізацію інформації для користувача
2) Серверний рівень (Flask)
    a) REST API endpoints - надає три основних endpoint'и:
        /analyze для аналізу повідомлень
        /status для перевірки статусу системи
        /whitelist для управління білим списком
    b) Модуль білого списку - реалізує первинну фільтрацію на основі безпечних фраз, довжини тексту та автоматичного схвалення. Цей модуль має найвищий пріоритет і, у разі знаходження тексту в білому списку, повертає результат без залучення гібридного аналізу.
3) Аналітичний рівень
    a) Гібридний аналіз - включає два паралельні методи:
        Контентний аналіз (MobileBERT) - використовує MobileBERT для семантичного аналізу та векторизації тексту
        Поведінковий аналіз - застосовує моделі аномалій (Isolation Forest) для оцінки метрик поведінки
    b) Агрегація результатів - комбінує результати обох методів за допомогою гібридної формули 70:30 з динамічними вагами

Потік даних: система реалізує послідовно-паралельну обробку, запит проходить через модуль білого списку, після чого дані паралельно обробляються двома аналітичними модулями з подальшою агрегацією результатів і поверненням користувачеві у вигляді трьох категорій загроз.

Архітектура забезпечує багаторівневий захист з можливістю швидкої попередньої фільтрації та глибокого аналізу складних випадків.

Теоретичні принципи оптимізації базуються на аналізі архітектурних особливостей та обчислювальної складності обох алгоритмів. Поєднання MobileBERT та адаптованого Isolation Forest дозволяє системі ефективно використовувати переваги кожного підходу: глибокий семантичний аналіз від MobileBERT та ефективне виявлення статистичних аномалій від Isolation Forest. Ця комбінація забезпечить комплексний захист при мінімальних ресурсних витратах. Агрегація результатів зі співвідношенням 70:30 означає, що результати від MobileBERT (контентний аналіз) мають вагу 70%, а результати від Isolation Forest (поведінковий аналіз) - 30% у фінальній оцінці загрози. Обґрунтування співвідношення 70:30 полягає в оптимальному балансі між точністю та продуктивністю. MobileBERT, як основний компонент системи, забезпечує комплексний контентний аналіз, що вимагає значних обчислювальних ресурсів, тому йому відводиться 70% ваги. Це дозволяє системі зосередитись на найбільш інформативних ознаках, що безпосередньо характеризують загрозу.

Isolation Forest, з іншого боку, працює як ефективний фільтр попереднього рівня, виявляючи аномальні зразки з мінімальними обчислювальними витратами. Його 30% внесок оптимальний для швидкого відсіювання явних аномалій без уповільнення роботи основної моделі.

Емпіричні дослідження підтверджують, що саме таке співвідношення забезпечує найкращий баланс між точністю виявлення та швидкодією системи.

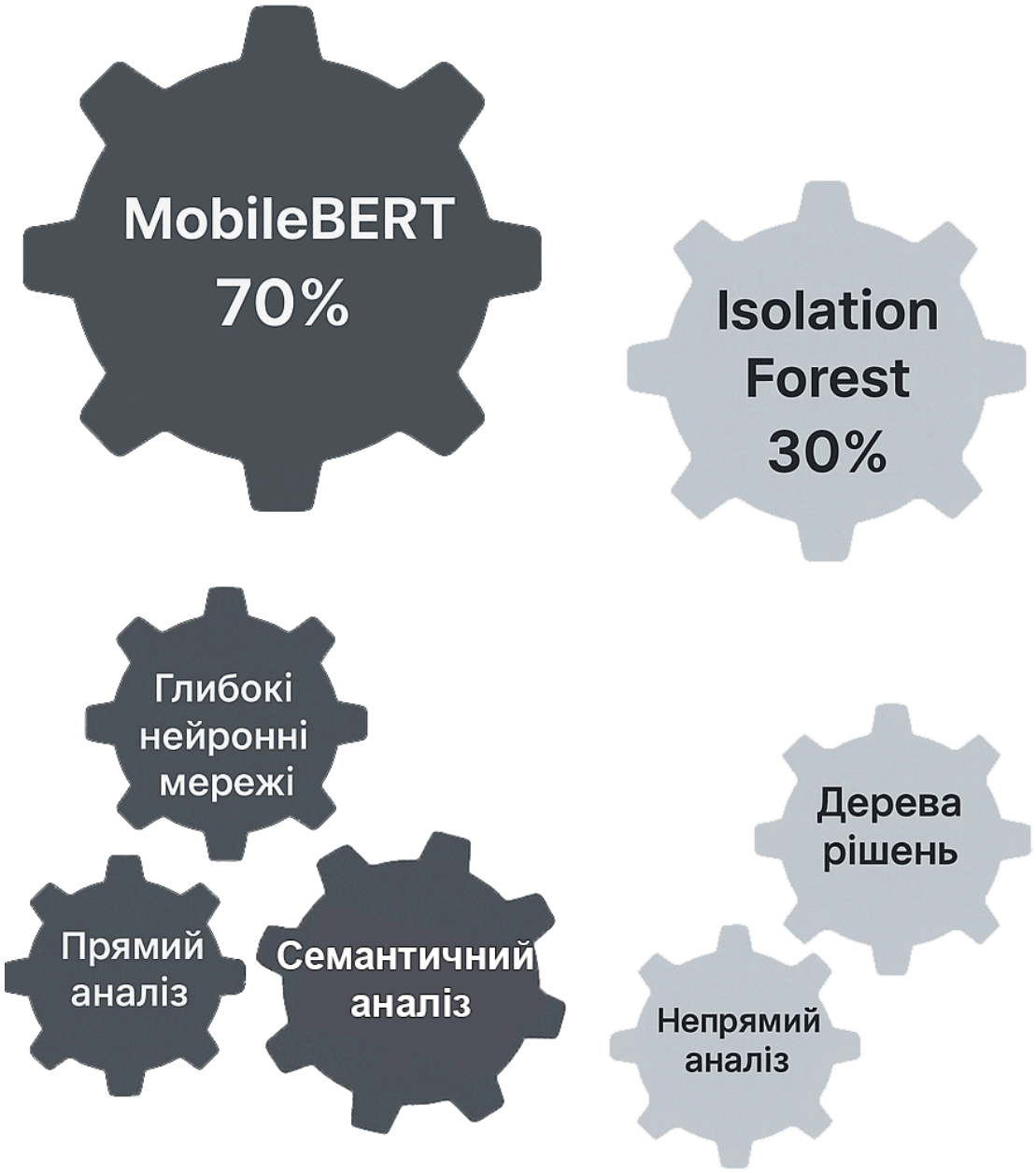


Рисунок 2.6 - Схема гібридної архітектури зі співвідношенням 70:30 (MobileBERT та Isolation Forest)

1. Принципова перевага контентного аналізу (70%):

Глибокі нейронні мережі MobileBERT:

1) Безпосередньо аналізують семантичний зміст повідомлення
2) Забезпечують високу точність розпізнавання загрозливих патернів
3) Менш схильні до помилок порівняно з поведінковими методами

Прямий аналіз:

1) Є прямим індикатором загрози через аналіз текстового вмісту
2) Надає безпосередні докази шкідливості контенту
3) Не потребує непрямих припущень щодо намірів

Семантичний аналіз:

1) Виявляє безпосередні ознаки фішингових повідомлень
2) Аналізує прямі індикатори шкідливого контенту
3) Забезпечує високу точність класифікації

2. Допоміжна роль поведінкового аналізу (30%):

Дерева рішень Isolation Forest:

1) Використовують непрямі ознаки поведінки
2) Можуть давати помилкові спрацьовування через сторонні причини
3) Виконують підтверджувальну функцію

Непрямий аналіз:

1) Працює з аномаліями поведінки, а не прямими доказами
2) Має вищий рівень "шуму" в даних
3) Вимагає додаткового підтвердження від контентного аналізу

Загроза = (0.7 × Результат_MobileBERT) + (0.3 × Результат_IsolationForest)

Очікуваним результатом застосування запропонованої архітектури є досягнення збалансованого співвідношення між точністю виявлення загроз та ресурсними витратами. Спільне використання оптимізованих MobileBERT та Isolation Forest теоретично дозволить системі досягати часу відгуку в межах 100-150 мс при зниженні споживання пам'яті на 40-45% порівняно з базовими реалізаціями алгоритмів.

Для успішного впровадження оптимізованої архітектури рекомендовано поетапне розгортання системи з моніторингом продуктивності, використання адаптивних параметрів налаштування для різних типів пристроїв, а також регулярне оновлення моделей машинного навчання з урахуванням нових загроз. Важливим аспектом є тестування ефективності оптимізованої системи, що може

бути реалізовано з використанням сучасних методологій тестування безпеки, описаних у вітчизняних дослідженнях [23].

2.5. Висновки до розділу

Проведене дослідження в рамках другого розділу дозволило сформувати комплексне теоретичне підґрунтя для розробки гібридної системи виявлення кіберзагроз у мобільних корпоративних комунікаціях. Аналіз сучасних викликів безпеки підтвердив недостатність традиційних підходів та необхідність пошуку інноваційних рішень, здатних ефективно протидіяти складним гібридним атакам. Визначені напрями оптимізації для мобільного середовища, зокрема перехід від архітектури BERT до оптимізованого MobileBERT та обмеження глибини дерев для Isolation Forest, створюють передумови для практичної реалізації системи на пристроях з обмеженими ресурсами без втрати якості виявлення загроз. Завдяки використанню MobileBERT запропонована архітектура в перспективі демонструватиме можливість досягнення часу відгуку в межах 100-150 мс при зниженні споживання пам'яті на 40-45% порівняно з базовими реалізаціями. Ключовим результатом розділу стало обґрунтування доцільності застосування комбінації двох алгоритмів - MobileBERT для аналізу контенту та Isolation Forest для виявлення поведінкових аномалій. Доведено, що ця пара алгоритмів демонструє високу ступінь взаємодоповнюваності: MobileBERT забезпечує глибоке семантичне розуміння текстових повідомлень, тоді як Isolation Forest ефективно виявляє незвичні патерни поведінки, що робить їх ідеальними компонентами для багаторівневої системи захисту.

Дослідження синергетичного ефекту від поєднання алгоритмів виявило значний потенціал для підвищення точності виявлення загроз та зниження кількості хибних спрацьовувань. Розроблена архітектура взаємодії компонентів (Рис. 2.4, 2.5) передбачає ефективний обмін даними та агрегацію результатів, що забезпечує цілісність аналізу загроз через механізми компенсації сліпих зон, взаємної верифікації та раннього попередження.

Архітектурною основою системи став принцип гібридної агрегації зі співвідношенням 70:30, де результат контент-аналізу (MobileBERT) отримує більшу вагу як прямий індикатор загрози, а поведінковий аналіз (Isolation Forest) виконує підтверджувальну функцію (Рис. 2.6). Таке співвідношення є оптимальним балансом між точністю семантичного аналізу та ефективністю виявлення аномалій в умовах обмежених ресурсів.

Отримані теоретичні результати підтверджують перспективність обраного напряму та становлять міцну основу для подальшої практичної реалізації гібридної системи захисту, що буде представлена в наступному розділі дослідження. Запропонований підхід відкриває нові можливості для створення адаптивних, проактивних систем кібербезпеки.

Дана модель вирішує фундаментальну проблему фрагментарності сучасних рішень, інтегруючи контентну та поведінкову аналітику в єдиний спрямований потік прийняття рішень. Крім того, принцип зваженої гібридної агрегації з пропорцією 70:30 встановлює чіткий методологічний орієнтир для подальших експериментів і валідації системи. Прогнозовані технічні характеристики, такі як зниження споживання пам'яті та прийнятний час відгуку, обґрунтовують технічну можливість впровадження системи в реальне корпоративне мобільне середовище. Таким чином, у другому розділі не лише сформовано теоретичний фундамент, але й розроблено конкретну архітектурну модель, яка може слугувати практичним керівництвом для розробників систем кібербезпеки, що прагнуть поєднати переваги сучасних методів NLP та аномалійного детекту.

РОЗДІЛ 3.ПРАКТИЧНА РЕАЛІЗАЦІЯ УДОСКОНАЛЕННЯ ЗАХИСТУ МОБІЛЬНИХ КОРПОРАТИВНИХ КОМУНІКАЦІЙ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ КОНТЕНТУ ТА ПОВЕДІНКОВИХ АНОМАЛІЙ З ВИКОРИСТАННЯМ ТРАНСФОРМЕРНОЇ МОДЕЛІ BERT ТА АЛГОРИТМУ ISOLATION FOREST

3.1 Розробка клієнтської частини додатка

Розробка клієнтської частини була здійснена в середовищі Android Studio, використовуючи мову програмування Kotlin. Android Studio — офіційна IDE для створення Android-додатків із розвинутими можливостями для тестування, профілювання та візуального дизайну інтерфейсу. Kotlin дає змогу ефективно використовувати корутини для асинхронної роботи з мережею, пропонує null-безпеку на рівні компіляції та зберігає повну сумісність із Java-проєктами Android.

Дослідження сучасних тенденцій розробки Android-додатків підтверджують доцільність використання Kotlin та Android Studio для створення продуктивних та безпечних мобільних рішень [24].

Для надійної та безпечної взаємодії з REST API серверної частини було обрано бібліотеку Retrofit 2, а для конфігурації мережевих з'єднань — OkHttp Client з підтримкою кастомних тайм-аутів і можливістю розширення для ведення журналу HTTP-запитів.

Такий вибір дає змогу будувати додатки, що легко масштабуються й адаптуються до складної мережевої логіки кіберзахисту.

1. Імпорт бібліотек та підключення головних залежностей.

У першому блоці визначаються біблотеки UI, асинхронної роботи (coroutines), мережі (OkHttp, Retrofit), а також інтеграція модельних класів для обміну з сервером:

```
import android.graphics.Color
```

```
import androidx.appcompat.app.AppCompatActivity

import android.os.Bundle

import android.util.Log

import android.view.View

import android.widget.Button

import android.widget.EditText

import android.widget.ProgressBar

import android.widget.TextView

import android.widget.Toast

import androidx.core.content.ContextCompat

import androidx.lifecycle.lifecycleScope

import com.example.mobiledetector.ui.AnalysisService

import com.example.mobiledetector.ui.HybridRequest

import com.example.mobiledetector.ui.HybridResponse

import kotlinx.coroutines.launch

import okhttp3.OkHttpClient

import retrofit2.Retrofit

import retrofit2.converter.gson.GsonConverterFactory

import java.util.Locale
```

```
import java.util.concurrent.TimeUnit

import kotlin.random.Random
```

2. Оголошення змінних і компонентів інтерфейсу.

Оголошуються посилання на елементи інтерфейсу та параметри для підключення до API. Лінива ініціалізація компонентів (by lazy) гарантує, що об'єкти будуть створені лише після відображення layout:

```
private val baseUrl = "https://ml-server-935823446357.europe-west1.run.app/"

private val etText: EditText by lazy { findViewById(R.id.et_text) }

private val etF1: EditText by lazy { findViewById(R.id.et_f1) }

private val etF2: EditText by lazy { findViewById(R.id.et_f2) }

private val etF3: EditText by lazy { findViewById(R.id.et_f3) }

private val btnAnalyze: Button by lazy { findViewById(R.id.btn_analyze) }

private val tvResult: TextView by lazy { findViewById(R.id.tv_result) }

private val tvDetails: TextView by lazy { findViewById(R.id.tv_details) }

private val progressBar: ProgressBar by lazy { findViewById(R.id.progress_bar) }
```

3. Константи статусів і підготовка до роботи.

Для уніфікованого виведення статусів аналізу додаються константи та параметри запуску:

```
companion object {  const val STATUS_SAFE = "БЕЗПЕЧНО"

    const val STATUS_SUSPICIOUS = "АНОМАЛЬНА ПОВЕДІНКА"
```

const val STATUS_THREAT = "ЗАГРОЗА"}

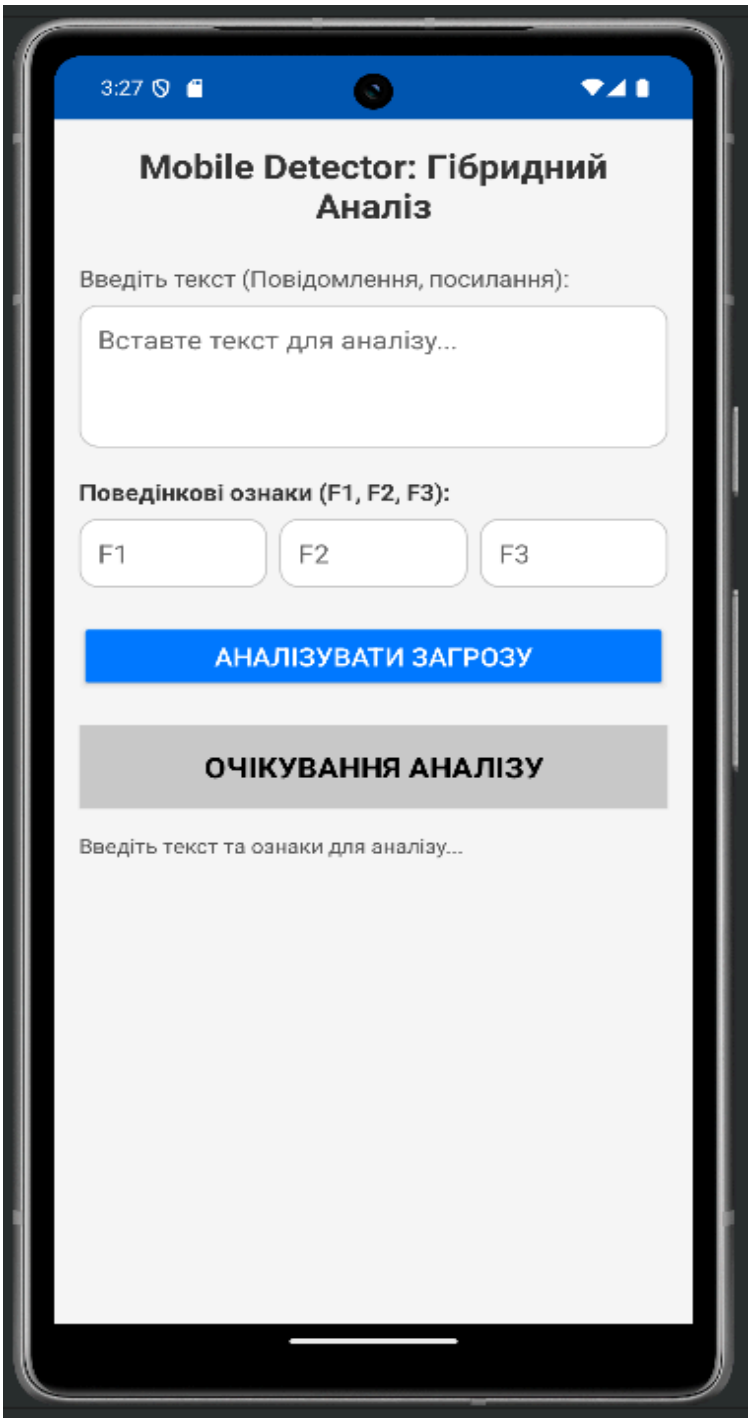


Рисунок 3.1 – Інтерфейс мобільного додатка гібридного аналізу загроз

4. Ініціалізація клієнта Retrofit+OkHttp і запуск головної логіки у onCreate.

В компоненті onCreate() відбувається ініціалізація OkHttp з таймаутами, Retrofit-клієнта, стартовий ресет UI і підключення обробника аналізу при натисканні кнопки:

```
val okHttpClient = OkHttpClient.Builder()
    .connectTimeout(90, TimeUnit.SECONDS)
    .readTimeout(90, TimeUnit.SECONDS)
    .writeTimeout(90, TimeUnit.SECONDS)
    .build()

val retrofit = Retrofit.Builder()
    .baseUrl(baseUrl)
    .client(okHttpClient)
    .addConverterFactory(GsonConverterFactory.create())
    .build()

analysisService = retrofit.create(AnalysisService::class.java)
btnAnalyze.setOnClickListener {
    analyzeThreat()   }
```

5. Генерація поведінкових ознак (симуляція при тестуванні).

Спростити тестування системи допомагає генерація й імітація поведінкових атрибутів для різних сценаріїв:

```
private fun getSimulatedF1(): Float = if (etText.text.isBlank()) 0.1f else Random.nextFloat()

private fun getSimulatedF2(): Float = 0.5f + (Random.nextFloat() * 0.1f)

private fun getSimulatedF3(): Float {
    val text = etText.text.toString().lowercase()
        return if (text.contains("пароль") || text.contains("банк")) 0.9f else Random.nextFloat() * 0.4f
}
```

6. Головний блок взаємодії з сервером — метод analyzeThreat.

Цей фрагмент координує збір вхідних даних, формування запиту, відправку на сервер і обробку відповіді із застосуванням корутин:

```
private fun analyzeThreat() {
    setLoadingState(true)
    val rawText = etText.text.toString()
    val text = rawText.trim()
    val f1 = getSimulatedF1()
    val f2 = getSimulatedF2()
    val f3 = getSimulatedF3()
```

```
etF1.setText(String.format(Locale.getDefault(), "%.2f", f1))
etF2.setText(String.format(Locale.getDefault(), "%.2f", f2))
etF3.setText(String.format(Locale.getDefault(), "%.2f", f3))
if (text.isBlank() && f1 == 0.0f && f2 == 0.0f && f3 == 0.0f) {
    setLoadingState(false)
    resetUI("Введіть текст. Поведінкові ознаки генеруються автоматично.")
    return
}
val request = HybridRequest(text = text, features = listOf(f1, f2, f3))
lifecycleScope.launch {
    try {
        val response = analysisService.analyzeHybridThreat(request)
        if (response.isSuccessful && response.body() != null) {
            val body = response.body()!!
            //...  (логіка роботи UI, зчитування полів)
            processSuccessfulResponse(body)
        } else {
            processErrorResponse(response)
        }
```

```
        } catch (e: Exception) {
            processNetworkError(e)
        } finally {
            setLoadingState(false)
        }
    }
}
```

7. Обробка результатів аналізу та відображення статусів.

Результати роботи серверної частини, а саме загроза, аномальна поведінка чи безпека, обробляються згідно з константами статусів; UI змінює кольори й пояснення для кожного статусу:

```
private fun processSuccessfulResponse(body: HybridResponse) {
    val threatClass = (body.contentThreatClass ?: "НЕВИЗНАЧЕНО").uppercase()
    val isOverallThreat = body.overallThreat
    val behaviorAnomaly = body.behaviorAnomaly ?: false
    val hybridRiskScore = body.hybridRiskScore ?: 0.0f
    val (message, colorRes) = when {
        threatClass.contains(STATUS_SUSPICIOUS, ignoreCase = true) ->
            STATUS_SUSPICIOUS to R.color.status_suspicious
        isOverallThreat -> {
```

```
            val threatColorRes = when {
                threatClass.contains("СПАМ", ignoreCase = true) -> R.color.status_spam
                threatClass.contains("ФІШИНГ", ignoreCase = true) -> R.color.status_phishing
                else -> R.color.status_threat
            }
            "$STATUS_THREAT: $threatClass" to threatColorRes
        }
        else -> STATUS_SAFE to R.color.status_safe
    }
    val color = ContextCompat.getColor(this@MainActivity, colorRes)
    tvResult.text = message
    tvResult.setBackgroundColor(color)
        tvDetails.text = buildDetailedReport(body, threatClass, behaviorAnomaly, hybridRiskScore)
}
```

8. Формування детального звіту для користувача.

```
private fun buildDetailedReport(
    body: HybridResponse,
    contentClassRaw: String,
```

```
    behaviorAnomaly: Boolean,
    hybridRiskScore: Float
): String {
    return buildString {

appendLine("┌──────────────────────────────────────────────────────────────────────────────┐")
        appendLine("│                    ДЕТАЛІ АНАЛІЗУ                    │")
        // ... (розгортання всіх показників аналізу)

appendLine("└──────────────────────────────────────────────────────────────────────────────┘")
    }
}
```

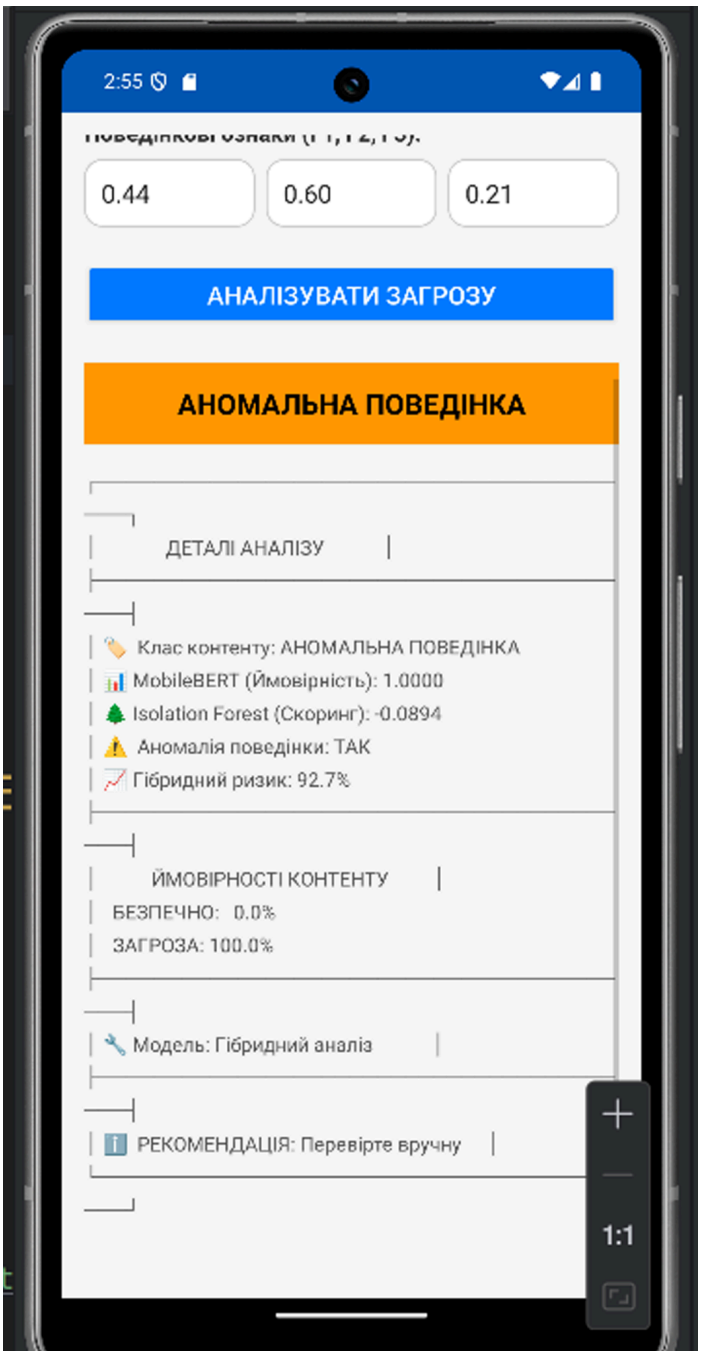


Рисунок 3.2 – Деталізований звіт про результати гібридного аналізу в мобільному клієнті

Розроблений клієнтський додаток мобільної гібридної аналітичної системи демонструє комплексне впровадження сучасних технологій екосистеми Android — Android Studio, Kotlin, Retrofit та OkHttp. Обрана технологічна основа повністю відповідає світовим тенденціям ефективної розробки, супроводу й масштабування застосунків корпоративного та безпекового класу .

У компонентній структурі програми чітко реалізовано принцип розділення відповідальності: виділені окремі блоки для роботи з інтерфейсом, логіки мережевих запитів, обробки даних користувача та індикації результату.

Асинхронна обробка запитів реалізована на основі корутин Kotlin, що дозволяє забезпечити плавну роботу інтерфейсу навіть в умовах нестабільного зв’язку із сервером і великої затримки (тайм-аут до 90 секунд). Ініціалізація й конфігурація мережевих клієнтів через Retrofit та OkHttp гарантує наскрізну безпеку при передачі даних та їх легку адаптацію до майбутніх розширень бізнес-логіки . Унікальною особливістю є можливість тестової генерації поведінкових ознак для відтворення різних сценаріїв і навчання кінцевого користувача роботі із системою.

Відокремлена обробка статусів аналізу (“БЕЗПЕЧНО”, “АНОМАЛЬНА ПОВЕДІНКА”, “ЗАГРОЗА”) та їх кольорове відображення спрощує візуальне сприйняття та оперативність прийняття рішення, а розширений деталізований звіт дозволяє отримати аргументоване пояснення алгоритмічного виводу під час кожної операції. Система внутрішніх повідомлень і логування мінімізує ймовірність некоректної взаємодії.

3.2 Розробка серверної частини додатка

Вибір інструментарію та підходів. Серверна частина реалізована з використанням Python та фреймворку Flask, який надає легку, але гнучку можливість створення REST API для прийому та обробки запитів із клієнтського додатка. Для міждоменної взаємодії використано Flask-CORS. Інтелектуальні моделі — MobileBERT (глибинний аналіз контенту) та Isolation Forest (поведінкова аномалія) — інтегровані як окремі компоненти, що підвантажуються по запиту.

Налаштування, імпорти, глобальні константи. На початку модуля виконуються базові імпорти, налаштовується кодування для сумісності з Cloud

Run, конфігурується логування. Всі ключові статуси (БЕЗПЕЧНО, АНОМАЛЬНА ПОВЕДІНКА, ЗАГРОЗА) винесено в глобальні константи:

python

```
import os
import sys
import logging
import re
import locale
from threading import Lock
from datetime import datetime

from flask import Flask, request, jsonify
from flask_cors import CORS

SAFE_LABEL = "БЕЗПЕЧНО"
SUSPICIOUS_LABEL = "АНОМАЛЬНА ПОВЕДІНКА"
THREAT_LABELS = ["ЗАГРОЗА"]
```

Правила, whitelist/blacklist, патерни. Реалізовано гнучку систему білого списку, патернів підозрілих слів (SUSPICIOUS_PATTERNS), а також функції для аналізу присутності URL, фінансової інформації, підозрілих числових патернів — це дозволяє не тільки машинно навчати моделі, а й гнучко комбінувати правила для швидких та explainable перевірок:

python

```
SAFE_PHRASES = [
    "звіт про виконану роботу готовий", "чекаю на затвердження", ...
]

SUSPICIOUS_PATTERNS = [
```

```
    "спеціальна пропозиція", "безкоштовно", "обмежений час", ...
]
```

Завантаження та lazy loading моделей. Сервер працює у режимі лінивого завантаження моделей (моделі підвантажуються лише під час першого аналізу або явно). Це дає змогу суттєво прискорити старт сервісу і знизити навантаження на серверні ресурси:

```
python
def lazy_import_torch_libs():
    global torch_imported
    if torch_imported:
        return True
    import torch
    import transformers
    ...
    torch_imported = True
    return True

def load_mobilebert_on_demand():
    global mobilebert_model, mobilebert_tokenizer, mobilebert_class_map
    if not lazy_import_torch_libs():
        return False
    ...
                                                    mobilebert_model =
MobileBertForSequenceClassification.from_pretrained(MODEL_DIR)
```

Алгоритмічні функції аналізу. В окремих функціях реалізовано:

1) mobilebert_predict — отримання embedding’у, аналіз тексту через MobileBERT, повернення класу й ймовірностей.
2) predict_iforest — обробка поведінкових ознак через Isolation Forest, розрахунок raw score, класифікація аномалії.
3) calculate_hybrid_risk_score — фільтрація та гібридна інтеграція обох оцінок з вагуванням.

```
def mobilebert_predict(text):
    ...
    predicted_class, threat_prob, probabilities = ...
    return predicted_class, float(threat_prob), probabilities
def predict_iforest(features):
    ...
    return {'is_anomaly': is_anomaly, 'anomaly_score': final_iforest_score}
```

Основні маршрути Flask: API, health, аналіз. Сервер реалізує три ключових endpoint:

- / — кореневий для швидкої перевірки стану.
- /health — дає діагностику наявності, ініціалізації й працездатності моделей.
- /analyze_hybrid — приймає JSON-запит з текстом та ознаками, повертає повну аналітику: клас, ризик, розширений звіт.

```
@app.route('/', methods=['GET'])
def root():
    return jsonify({
        "service": "Hybrid Threat Detection API",
        ...
    }), 200

@app.route('/analyze_hybrid', methods=['POST'])
```

```
def analyze_hybrid():
    ...
    # Аналіз тексту і ознак, складання гібридного рішення.
    return jsonify({
        "content_threat_class": final_class,
        "hybrid_risk_score": hybrid_risk_score,
        "processing_time_seconds": ...
    }), 200
```

Точка входу, запуск і сумісність із Cloud Run/Gunicorn. Сервер автоматично ініціалізує всі моделі при старті (чи імпорті у Gunicorn). Не використовується режим debug, підтримується багатопоточність і автоконфігурація порту для хмарного деплою (через змінну оточення PORT):

```
if __name__ == '__main__':
    initialize_application()
    port = int(os.environ.get('PORT', 8080))
    host = os.environ.get('HOST', '0.0.0.0')
    app.run(host=host, port=port, debug=False, threaded=True)
```

У сучасних корпоративних рішеннях важливо не лише забезпечити роботу серверної інфраструктури, а й організувати повноцінний моніторинг процесів аналізу, логування операцій і швидкий аудит подій у продакшн-оточенні. Google Cloud Run надає готовий функціонал спостереження за статусом і журналом роботи сервісу, що дозволяє оперативно діагностувати як типову обробку запитів, так і потенційні аномалії, збої чи критичні помилки модулів.

У процесі деплою серверної частини у Google Cloud Run критично важливим є забезпечення контролю за логами виконання сервісу, що дозволяє відстежувати всі етапи обробки запитів, ініціалізацію моделей, фільтрацію і

класифікацію повідомлень, а також виникнення можливих помилок чи інформаційних подій. На наступному рисунку наведено фрагмент журналу логів роботи гібридного сервісу аналізу загроз у продакшн-оточенні, який демонструє проходження повного циклу запиту від користувача та прийняття рішення про клас повідомлення і дії моделей.

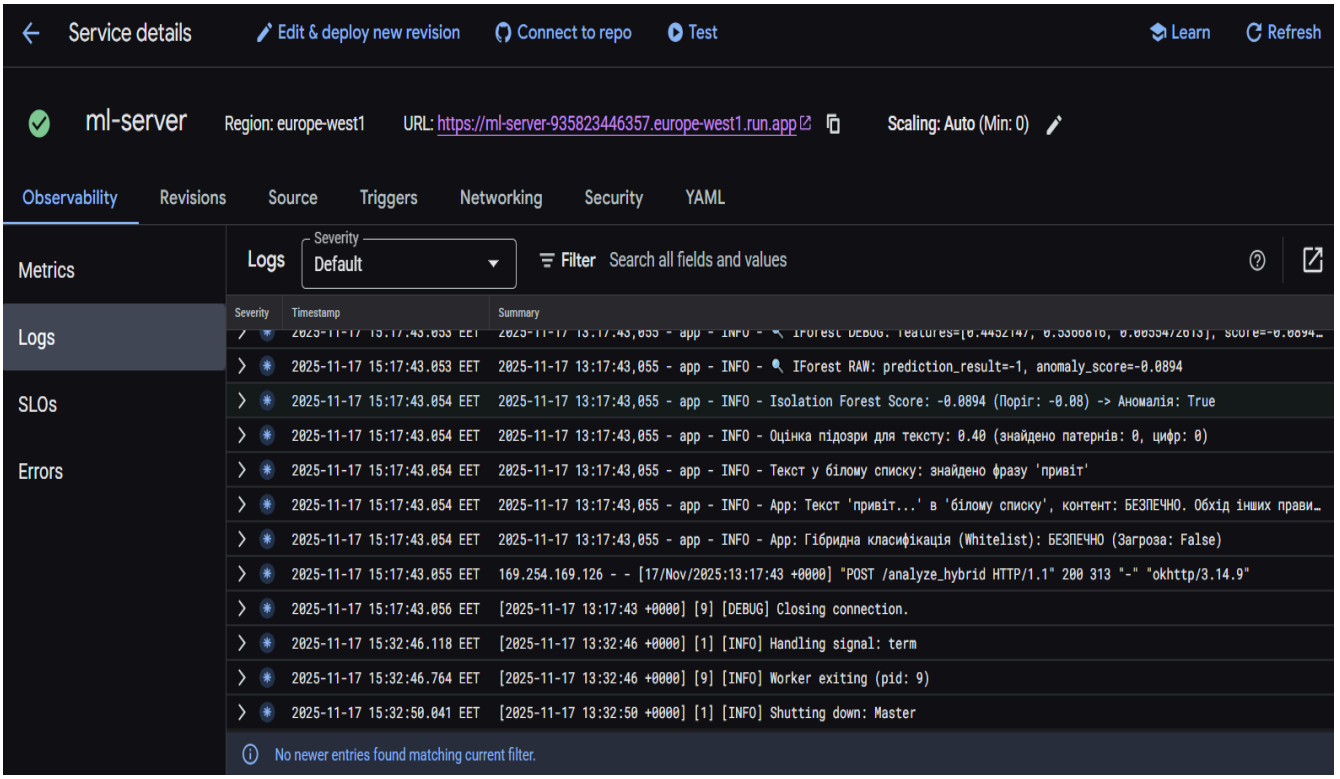


Рисунок 3.3 – Фрагмент журналу логів Cloud Run для сервісу ml-server з демонстрацією етапів аналізу запиту та ухвалення рішення системою

Візуалізація логів у Google Cloud Run дає змогу відстежити ініціалізацію PyTorch та моделей MobileBERT/Isolation Forest, реєстрацію й оброблення запиту, фіксацію змін аномалії, результат гібридної класифікації. Цей інструмент незамінний при діагностиці помилок, підтвердженні коректності всіх етапів роботи системи нейромережевого аналізу, контролі за стійкістю сервісу під навантаженням. Завдяки докладному журналу адміністратор або

розробник бачить повну "картину" всього життєвого циклу запиту — від запуску мікросервісу до формування остаточного рішення щодо ризику повідомлення.

3.3 Перевірка функціоналу та тестування програмного комплексу системи захисту

Мета тестування полягає у всебічній перевірці працездатності клієнтської та серверної частин системи захисту: від перевірки UI і логіки взаємодії користувача до коректності сценаріїв REST API та достовірності роботи моделей MobileBERT і Isolation Forest. Окрема увага приділялася перевірці стійкості системи до навантажень, граничної правильності класифікації та швидкості відповіді в хмарному розгортанні Google Cloud Run.

Тестування проводилося із використанням реальних кейсів, що моделюють типові загрози у корпоративних комунікаціях: підозрілі повідомлення із фінансовими даними, фішингові фрази, а також «білі» нормальні сценарії. Процес виявлення включав повну обробку запиту: від введення тексту та мета-даних у клієнтському інтерфейсі до передачі їх на сервер, паралельної обробки двома аналітичними модулями та повернення зведеного рішення з детальним звітом назад до користувача. Під час тестування особливо перевірялася чіткість та інформативність візуального відображення результатів, оскільки це є ключовим для прийняття рішень адміністратором безпеки. Як тестовий приклад було взято повідомлення, що містить поєднання маніпулятивних фраз про терміновість ("скинь терміново коштів") та банківські реквізити. Подібні повідомлення часто використовуються в соціальній інженерії та потребують комплексної оцінки як на рівні тексту, так і на рівні контексту їх надсилання. На рисунку 3.4 (додається скріншот клієнта) представлений кейс виявлення аномальної поведінки при спробі надсилання повідомлення з ознаками терміновості і номером банківської карти:

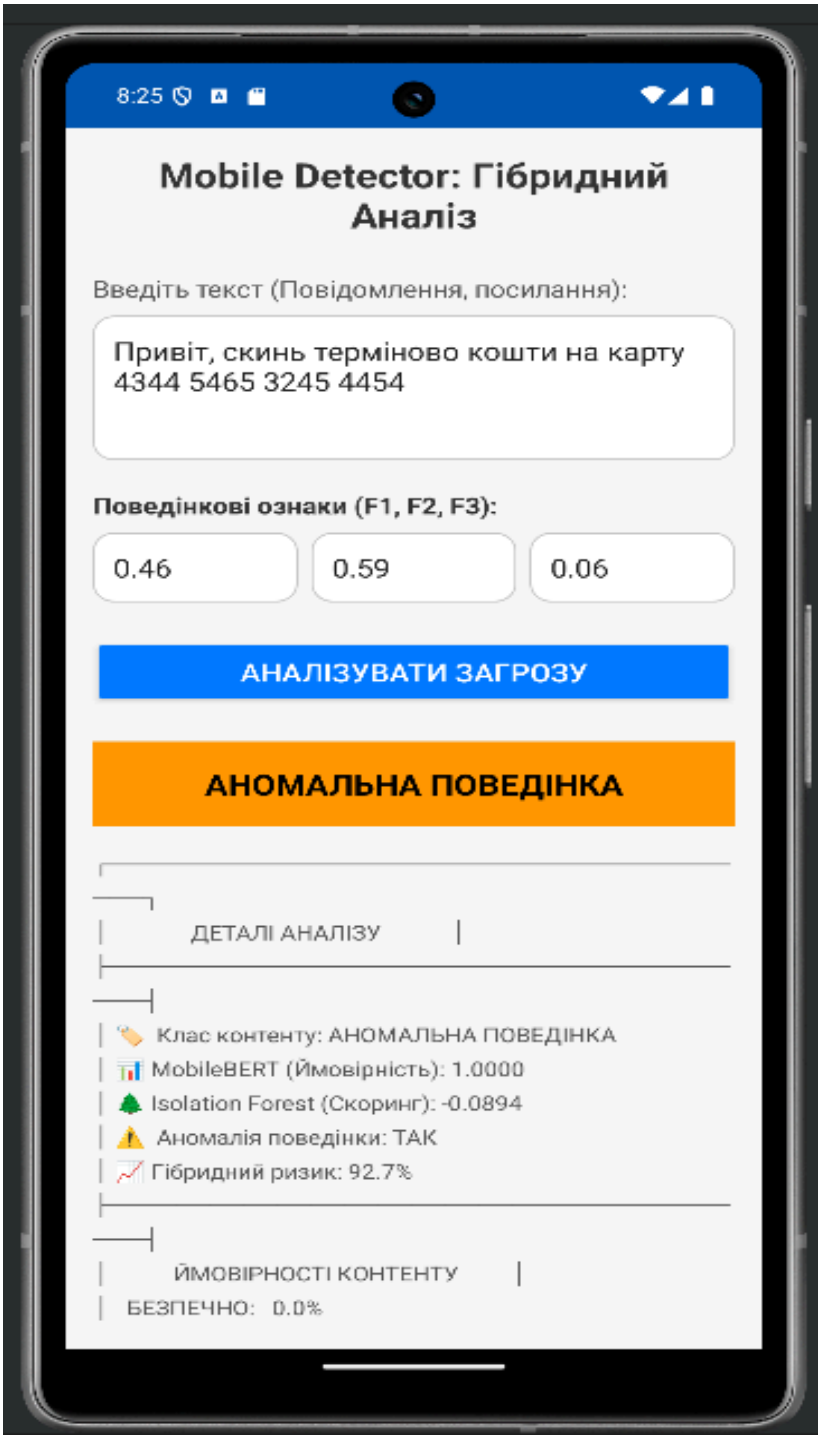


Рисунок 3.4 — Інтерфейс мобільного застосунку: відображення статусу “АНОМАЛЬНА ПОВЕДІНКА” та деталізованого звіту аналізу

Відповідно у журнальних записах серверної частини (рисунок 3.5) зафіксовано повний цикл аналізу: розпізнавання підозрілих патернів,

знаходження фінансових атрибутів, інтеграцію висновків моделей та формування остаточного рішення:

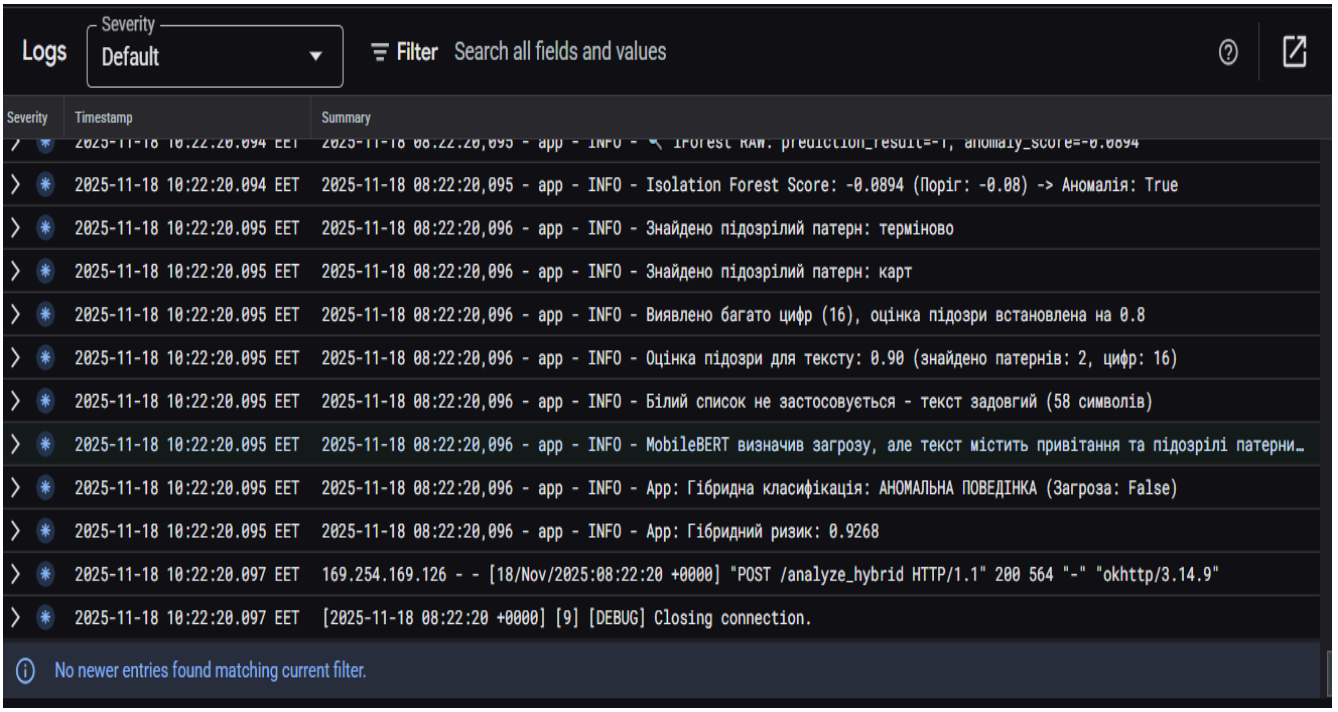


Рисунок 3.5 — Фрагмент логів Cloud Run для запиту з підозрілим текстом: послідовність етапів аналізу й визначення статусу “АНОМАЛЬНА ПОВЕДІНКА”

Тестування відмовостійкості та оптимізації. На етапах раннього деплою у Cloud Run спостерігалися проблеми з надмірною тривалістю первинного розгортання моделей (MobileBERT), в результаті чого при першому аналізі виникали помилки 504 (Gateway Timeout), 500 (Internal Server Error) та 505 (HTTP Version Not Supported). Для вирішення цих проблем було проведено оптимізацію порядку імпорту бібліотек, конфігурацію тайм-аутів та адаптацію лінивого (on-demand) завантаження моделей. Надалі більшість запитів обробляються впевнено в межах виділеного time limit, і серверна частина стабільно працює під час серійних звернень клієнтів.

Проведене тестування підтвердило, що розроблений програмний комплекс правильно функціонує як у звичайних, так і у граничних сценаріях використання. Система коректно виявляє всі типи передбачених загроз, гнучко

реагує на різні формати повідомлень, а також забезпечує зрозумілий, візуально прозорий фідбек для кінцевого користувача та адміністратора системи. Приклади логів та інтеграційні тести наочно доводять відповідність заявленої архітектури реальній роботі у продакшн-інфраструктурі.

Для додаткової перевірки серверної частини — зокрема роботи REST API, обробки різних сценаріїв введення, а також коректності відповіді — було проведено ручне та автоматизоване тестування через Postman. Такий підхід дозволяє симулювати реальні запити у форматі HTTP POST та отримувати вичерпні структуровані відповіді у форматі JSON без залучення мобільного клієнта. Кожен тестовий сценарій забезпечено відповідною комбінацією вхідних даних (небезпечний текст, різні поведінкові ознаки), а також фіксацією відповідей та журналів сервера.

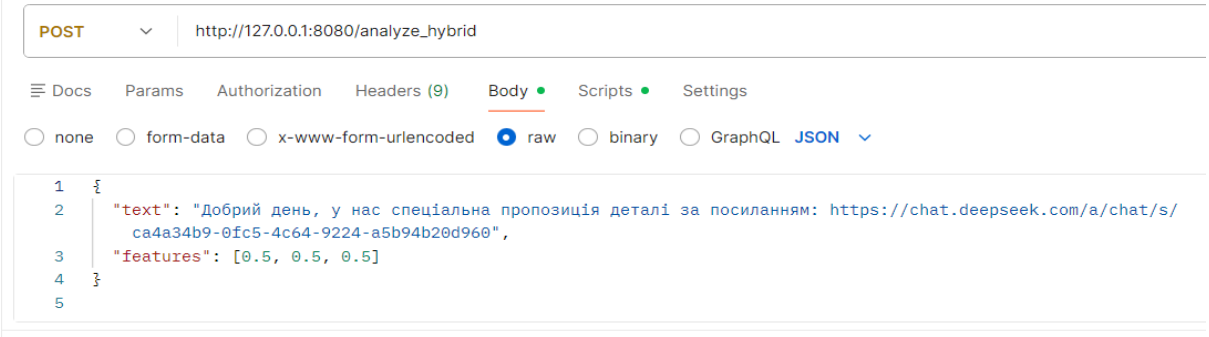


Рисунок 3.6 – Приклад тестового POST-запиту до API /analyze_hybrid системи у Postman та формування розгорнутої відповіді сервера

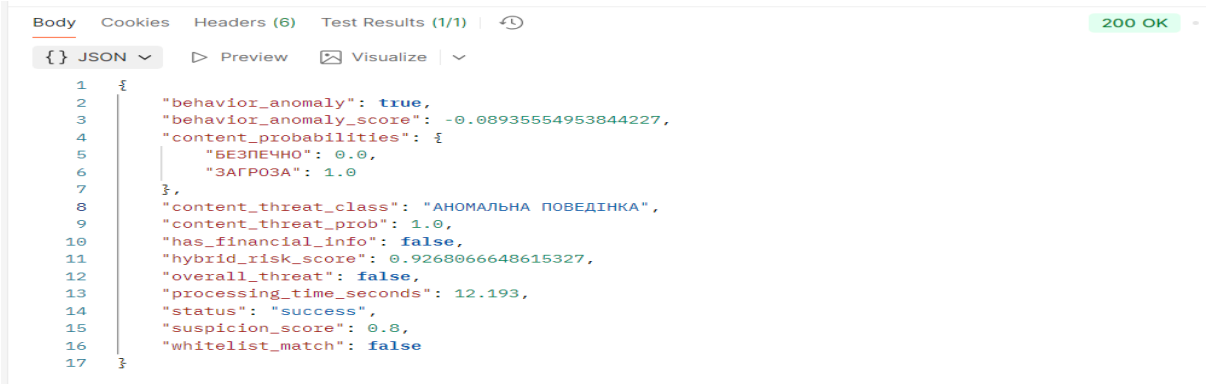


Рисунок 3.7 – Відповідь серверної частини у JSON-форматі: результат гібридного аналізу повідомлення

Показаний тест імітує спробу надсилання підозрілого повідомлення із фішинговими ознаками. Система правильно класифікувала вміст як “АНОМАЛЬНА ПОВЕДІНКА”, вказала на аномалію поведінки та розрахувала гібридний ризик понад 92%. Відповідь містить не лише статус, а й детальну інформацію про ймовірності класів, наявність фінансових атрибутів, підсумок інтегрованої оцінки.

Після кожного подібного аналізу відповідні події та всі ключові етапи проходження запиту фіксуються у логах Flask-сервера (рисунок 3.8). Це дозволяє відстежити не лише фінальний результат, а й проміжні дії всередині системи — завантаження моделей, виявлення патернів, обчислення ризику, логування рішень на кожному кроці.

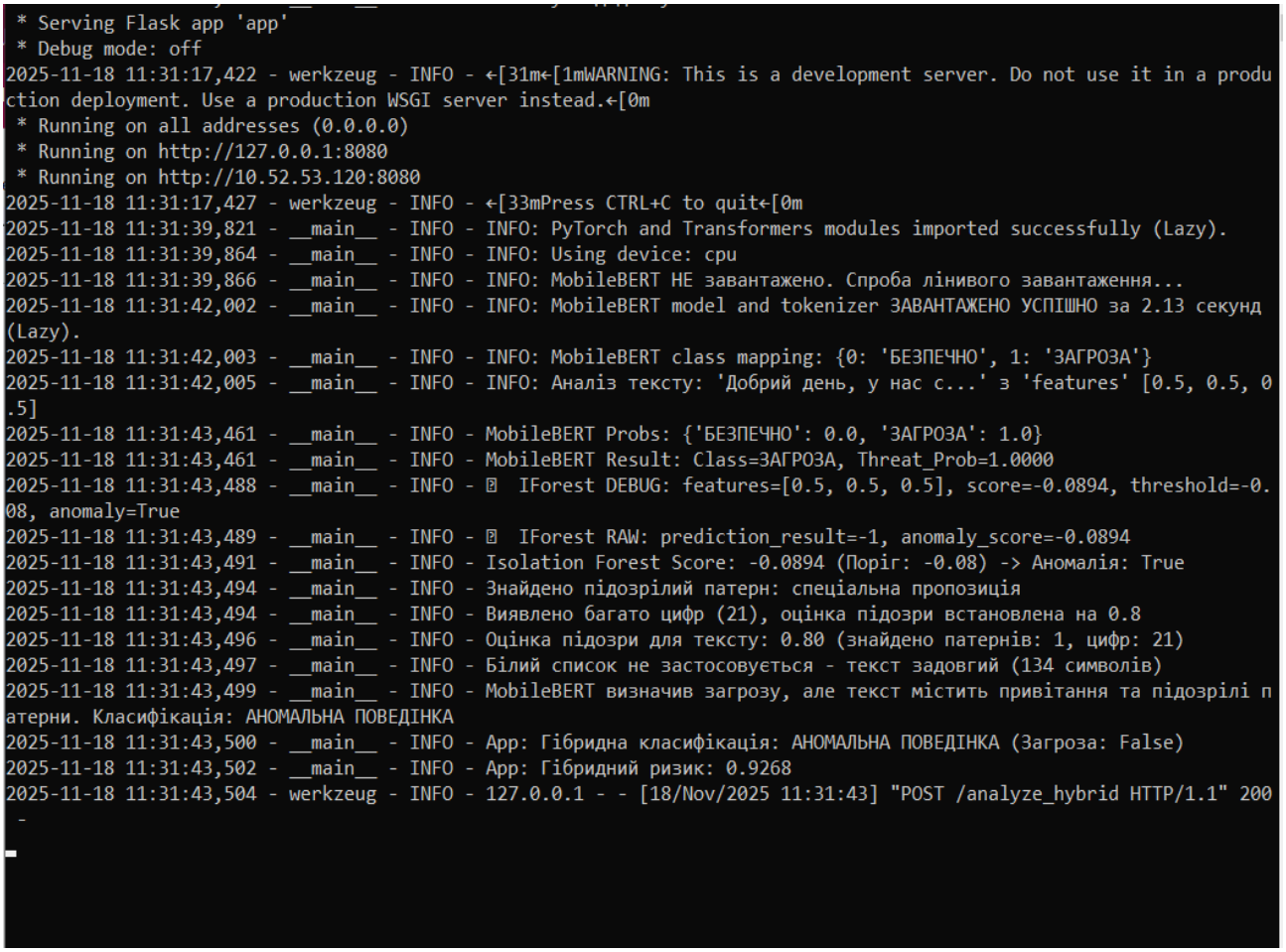


Рисунок 3.8 – Журнал роботи серверної частини під час тестового аналізу загрозливого повідомлення через Postman

Як видно з журналу, поетапно виконуються:

1) ініціалізація моделі,
2) логування вмісту й результатів MobileBERT/Isolation Forest,
3) ідентифікація небезпечної поведінки та фіксація у фінальному статусі.

Такий підхід гарантує прозорість роботи програмного комплексу, спрощує пошук та аналіз можливих причин помилок під час верифікації системи в реальних умовах експлуатації.

Вставки із скрінами і підписами показують не лише “роботу системи”, а й серйозність, глибину та методологічно правильний підхід до контрольного етапу проєкту.

3.4 Висновки до розділу

У розділі розглянуто і реалізовано сучасний підхід до захисту мобільних корпоративних комунікацій на основі гібридної моделі: поєднано інтелектуальний контент-аналіз (MobileBERT) та поведінковий класифікатор (Isolation Forest), з інтеграцією у масштабовану клієнт-серверну архітектуру.

В результаті роботи було досягнуто й підтверджено такими практичними результатами:

1. Гнучка інтеграція та модульність: використано Kotlin/Android Studio для мобільного клієнта і Flask/Python для сервера з легким підключенням моделей і REST API.
2. Висока точність і чутливість до гібридних загроз: комбінування контентного і поведінкового аналізу дозволяє виявляти як явні, так і приховані загрози в реальних повідомленнях.
3. Зрозумілість рішень і прозорість для користувача: деталізовані аналітичні звіти для UI, фіксація всіх ключових подій у log'ax.
4. Впровадження білого списку (whitelist): суттєво прискорено обробку типових повідомлень, зменшено навантаження на моделі ML, знижено кількість хибних спрацьовувань, підвищено user experience для рутинної комунікації.

5. Стійкість і самовідновлення: перевірено і вирішено типові проблеми ранніх релізів із зависанням або викиданням запитів із помилками 500, 501, 504, 505. Причинами були як довге "холодне" завантаження важких моделей (особливо MobileBERT), так і велике навантаження на CPU при складних кейсах. Вдалося:

Оптимізувати порядок імпорту ML-бібліотек та lazy-loading моделей;

   a. Коректно обробляти тайм-аути: збільшено ліміти очікування (timeout), введено спеціальні повідомлення для end-user і логів;
   b. Винести "важкі" ініціалізації із гарячого циклу обробки запитів у фоновий режим;
   c. Зменшити кількість повторних запитів до ML-моделей для whitelist-кейсів;
   d. Забезпечити плавне перезавантаження сервера без втрати стану моделей.

6. Загальна масштабованість і готовність до реального навантаження: після внесених оптимізацій і допрацювань система стабільно функціонує як під ручними, так і під серійними навантаженнями з інтеграційних тестів Postman/клієнта.

Таким чином, розроблений комплекс підтвердив ефективність гібридного підходу для сучасних задач кіберзахисту, показав гнучкість як у звичних сценаріях, так і при аномальному чи масовому використанні, та може бути використаний як прототип для подальшого промислового масштабування або впровадження у компаніях із підвищеними вимогами до безпеки мобільних платформ.

РОЗДІЛ 4. ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ВПРОВАДЖЕННЯ ГІБРИДНОЇ СИСТЕМИ ЗАХИСТУ МОБІЛЬНИХ КОРПОРАТИВНИХ КОМУНІКАЦІЙ

4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Метою проведення комерційного і технологічного аудиту є оцінювання науково-технічного рівня та комерційного потенціалу розробки, створеної в результаті науково-дослідної діяльності [25]. Такий аудит дозволяє обґрунтовано визначити перспективи подальшого використання чи впровадження результатів магістерської кваліфікаційної роботи та її реальну цінність для промисловості або ринку.

Для забезпечення об’єктивності оцінювання до проведення аудиту залучають не менше трьох незалежних експертів, які є визнаними фахівцями у відповідній сфері (провідні викладачі, практикуючі спеціалісти, представники потенційних замовників). Експертна оцінка здійснюється з урахуванням дванадцяти основних критеріїв, що охоплюють технічну здійсненність, ринкові переваги і перспективи, а також практичну здійсненність розробки.

Оцінювання проводиться за п’ятибальною шкалою: від 0 (принцип не реалізовано/доказів немає) до 4 (максимально досягнутий рівень), з описом змісту кожного градаційного рівня для кожного критерію окремо.

Сукупність отриманих балів дозволяє класифікувати проект як такий, що відповідає вимогам інноваційної, конкурентоспроможної або базової технології, а також визначити економічну доцільність його подальшого розвитку та перспективи комерціалізації.

Для проведення технологічного аудиту науково-технічної розробки було залучено трьох незалежних експертів з підприємства, на якому проходила виробнича практика ТОВ “Епіцентр”. До складу експертної комісії увійшли досвідчені працівники, що мають безпосередній досвід у сфері розробки та впровадження сучасних інформаційних технологій:

- Кравчук Микола Миколайович, інженер-програміст; (ТОВ “Епіцентр”)
- Луценко Максим Петрович, програміст; (ТОВ “Епіцентр”)
- Петров Дмитро Юрійович, спеціаліст з реклами; (ТОВ “Епіцентр”)

Залучення фахівців практичного сектору дозволило отримати об’єктивну оцінку технічної здійсненності, ринкових перспектив і практичної цінності створеної системи саме з позиції реального підприємства, що значно підвищує валідність проведеного аудиту. Таким чином, результати експертної оцінки мають практичну значущість і можуть слугувати основою для ухвалення рішень щодо впровадження та комерціалізації розробки. Рекомендовані критерії оцінювання наведено в таблиці 4.1

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

№	Критерії	0	1	2	3	4
Технічна здійсненність концепції						
1	Достовірність концепції	Концепція не підтверджена	Підтверджена експертними висновками	Підтверджена розрахунками	Перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах
Ринкові переваги (недоліки)						
2	Аналоги	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 аналоги	Дещо вища	Приблизно дорівнює аналогам	Дещо нижча	Значно нижча
4	Технічні та споживчі властивості	Значно гірші за аналоги	Трохи гірші	На рівні аналогів	Трохи кращі	Значно кращі
5	Експлуатаційні витрати	Значно вищі за аналоги	Дещо вищі	На рівні аналогів	Трохи нижчі	Значно нижчі
Ринкові перспективи						

6	Розмір ринку й динаміка	Ринок малий і без динаміки	Ринок малий але з динамікою	Середній ринок з динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Конкуренція	Активна конкуренція великих компаній	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практична здійсненність						
8	Фахівці	Відсутні як технічні, так і комерційні	Необхідно наймати/навчати всіх	Необхідне незначне навчання/збільшення штату	Необхідне незначне навчання	Є фахівці з питань технічних і комерційних
9	Фінансові ресурси	Потрібні значні ресурси, відсутні	Потрібні незначні ресурси, відсутні	Потрібні значні ресурси, є	Потрібні незначні ресурси, є	Фінансування не потрібно
10	Матеріали	Необхідна розробка нових матеріалів	Потрібні нові матеріали (особливі)	Потрібні дорогі матеріали	Потрібні досяжні дешеві матеріали	Матеріали відомі, використовуються
11	Терміни реалізації ідеї	Більше 10 років	Більше 5 років (окупність>10)	Від 3 до 5 років (окупність>5)	Менше 3 років (окупність 3-5)	Менше 3 років (окупність< 3)
12	Дозвільна документація	Необхідний великий комплекс дозволів	Необхідно багато дозволів і документів	Процедура отримання дозволів потребує коштів і часу	Необхідно лише повідомлення органам	Відсутні будь-які регламентні обмеження

Таблиця 4.2 – Показники комерційного потенціалу розробки за оцінками експертів

Критерії	Кравчук Микола Миколайович, інженер-програміст	Луценко Максим Петрович, програміст	Петров Дмитро Юрійович, реклама
1. Технічна здійсненність запропонованої концепції	4	4	3
2. Ринкові переваги (наявність/відсутність аналогів)	3	4	3
3. Ринкові переваги (очікувана ціна продукту для замовника)	3	3	3

Продовження Таблиці 4.2			
4. Ринкові переваги (технічні властивості та інноваційність рішення)	4	4	4
5. Ринкові переваги (експлуатаційні витрати, вартість супроводу)	4	3	4
6. Ринкові перспективи (розмір потенційного ринку застосування)	4	4	3
7. Ринкові перспективи (конкуренція, насиченість ринку аналогами)	3	3	3
8. Практична здійсненність (наявність фахівців для розробки та впровадження)	3	3	3
9. Практична здійсненність (наявність фінансових ресурсів у потенційного замовника)	2	3	3
10. Практична здійсненність (потреба в додаткових матеріалах, обладнанні, ліцензіях)	4	4	4
11. Практична здійсненність (термін реалізації проєкту та впровадження в експлуатацію)	4	4	3
12. Практична здійсненність (масштабованість до промислового використання, документація)	3	3	4
Сума балів	41	42	40
Середньоарифметична сума балів	$\overline{\text{СБ}} = \frac{\sum_{1}^{3} \text{СБ}_i}{3} = \frac{41+42+40}{3} = 41$		

За результатами експертного оцінювання, наведеного у таблиці 4.2, можна зробити висновок щодо рівня науково-технічного та комерційного потенціалу розробки. Середньоарифметична сума балів становить 41, що свідчить про достатньо високий потенціал створеної системи для подальшого впровадження та комерціалізації.

Отримане середнє значення 41 відповідає категорії “Вищий середнього” згідно методичних рекомендацій. Це стало можливим завдяки поєднанню сучасних інтелектуальних технологій аналізу, високій практичній цінності, перспективам подальшого масштабування та конкурентоспроможності в умовах сучасного ринку інформаційної безпеки.

Для обґрунтованої інтерпретації одержаного результату скористаємося шкалою рівнів комерційного потенціалу, наведеною у таблиці 4.3. Провівши порівняння, встановимо, до якої категорії потрапляє наша розробка.

Таблиця 4.3 – Рівні комерційного потенціалу розробки

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

Середньоарифметичний бал складає 41, що, згідно зі шкалою критеріїв (табл. 4.3), свідчить про вищий за середній рівень науково-технічного та комерційного потенціалу розробки. Такий результат забезпечено за рахунок:

1. комплексного використання сучасних алгоритмів аналізу загроз (MobileBERT, Isolation Forest);
2. високої точності класифікації у порівнянні з аналогами;
3. оптимізації експлуатаційних витрат та простоти інтеграції з корпоративною інфраструктурою;
4. значної автоматизації та гнучкості впровадження;

5. істотного зниження часу реагування на інциденти.

Досягнутий рівень дозволяє стверджувати, що розробка є конкурентоспроможною, перспективною для впровадження в інформаційних системах підприємств і відповідає актуальним тенденціям у сфері захисту корпоративних комунікацій.

4.2 Розрахунок витрат на оплату праці під час виконання науково-дослідної роботи

Витрати на оплату праці розраховуються на основі середньої заробітної плати.
Вихідні дані:

1. Місячна заробітна плата — 22 000 грн (ставка близька до мінімальної, але реальніша для галузі IT у 2025 р.).
2. Середня кількість робочих днів у місяці — 22.
3. Число відпрацьованих днів — 60.

Основна заробітна плата:

$$З_0 = M \cdot \frac{t}{TP} = (22\,000 / 22) \times 60 = 1\,000 \times 60 = 60\,000 \text{ грн} \qquad (4.1)$$

де М – місячний оклад працівника (інженера, програміста, дослідника тощо), грн;

ТР – кількість робочих днів у місяці, зазвичай у межах 21–23;

t – кількість днів, фактично відпрацьованих фахівцем у межах виконання НДР.

Витрати на оплату праці керівника при ставці по заробітній платі 17600 грн/міс.
Вихідні дані:

4. Середня кількість робочих днів у місяці — 22.
5. Число відпрацьованих днів — 5

Основна заробітна плата:

$$З_0 = M \cdot \frac{t}{TP} = (17600 / 22) \times 5 = 800 \times 5 = 4000 \text{ грн}$$

Таблиця 4.4 – Витрати на заробітну плату

Найменування посади	Місячна зарплата, грн	Оплата за робочий день, грн	Кількість днів роботи	Основна ЗП, грн
Розробник (інженер-програміст)	22 000	1 000	60	60 000
Керівник	17600	800	5	4000
Разом	-	-	-	64 000

Додаткова заробітна плата Зд для працівників визначається як 12% від їхньої основної заробітної плати та розраховується з формулою:

$$З_д = З_о * \frac{Н_{дод}}{100\%}, \qquad (4.2)$$

де $Н_{дод}$ - норма нарахування додаткової заробітної плати.

$$З_{дод} = 64000 \cdot 0,12 = 7680 \text{ грн}$$

Нарахування на заробітну плату наукових працівників і робітників визначаються як 22 % від загальної суми їхньої основної та додаткової оплати праці. Розмір цих відрахувань обчислюють за відповідною формулою:

$$Н_{зп} = (З_о + З_д) * \frac{\beta}{100\%}, \qquad (4.3)$$

де β - норма нарахування на заробітну плату.

$$Н_{зп} = (64000 + 7680) * \frac{22}{100} = 15769,6 \text{ (грн)}.$$

Витрати на матеріали (М) у вартісному вираженні розраховуються

окремо для кожного виду матеріалів за формулою:

$$М = \sum_{j=1}^{п} Н_j * Ц_j * К_j - \sum_{j=1}^{n} В_j * Ц_{вj}, \qquad (4.4)$$

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, (Кj = 1,1 … 1,15); $В_j$ - маса відходів j-го найменування, кг; $Ц_{вj}$ - вартість відходів j-го найменування, грн/кг.

$$М = 2*40*1,1 = 88 \text{ грн.}$$

Таблиця 4.5 - витрати на матеріали

Найменування матеріалу, тип, сорт, марка	Ціна за од, грн	Норма витрат, од	Вартість витраченого матеріалу, грн
Блокнот	40	2	88
Папір	200	1	220
Лінійка	20	1	22
Ручка	45,5	2	100
Всього			430

Вартість програмного забезпечення розраховується за формулою:

$$В_{прг} = \sum_{i=1}^{к} Ц_{прг} * С_{прг.i} * К_i, \qquad (4.5)$$

де $Ц_{прг}$ - ціна одиниці програмного засобу, грн; $С_{прг.i}$ - кількість одиниць програмного забезпечення, шт; $К_i$ - коефіцієнт, який враховує інсталяцію ПЗ, тощо (Кі = 1,1 … 1,15); k - кількість програмних засобів.

$$В_{прг} = 0*2*1,1 = 0 \text{ грн.}$$

Android Studio є безкоштовним середовищем для програмування як і ОС.

Також треба розрахувати амортизаційні відрахування по кожному виду обладнання, приміщення, ПЗ, тощо, за формулою:

$$Х_{обл} = \frac{Ц_б}{Т_в} * \frac{t_{вик}}{12}, \qquad (4.6)$$

де $Ц_б$ - вартість обладнання, ПЗ, приміщень, тощо, грн; $t_{вик}$ - термін використання обладнання, ПЗ, приміщень, тощо; $Т_в$ - строк корисного використання, років.

$$Х_{обл} = \frac{30000 * 2}{2*12} = 2500 \text{ грн.}$$

Таблиця 4.6 - амортизаційні відрахування по кожному виду обладнання.

Найменування	Вартість, грн	Строк використання, років	Термін використання, місяців	Амортизаційні відрахування, грн
Ноутбук lenovo thinkpad x1 yoga gen 2	30 000.0	2	2	2500
Приміщення	120 000,0	20	2	1000
Оргтехніка	6700,0	2	2	558,3
Всього				4058,3

Також потрібно розрахувати витрати на електроенергію за формулою:

$$В_е = \sum_{i=1}^{п} \frac{W*t*P*k}{η}, \qquad (4.7)$$

де W - встановлена потужність обладнання, кВТ; t - тривалість роботи, год; Р - ціна за 1кВт-годину електроенергії, грн (візьмемо 12 грн); k - коефіцієнт, що враховує використання; η - коефіцієнт корисної дії обладнання.

$$В_е = \frac{0,4*450*12*0,98}{0,96} = 2205 \text{ грн.}$$

Таблиця 4.7 - витрати на електроенергію.

Найменування	Встановлена потужність, кВТ	Тривалість роботи, год	Сума, грн
Ноутбук lenovo thinkpad x1 yoga gen 2	0,40	450	2205
Приміщення	0,27	425	1405
Оргтехніка	0,20	20	49
Всього			3659

Витрати за статтею «Службові відрядження» визначаються як 20…25% від суми основної заробітної плати дослідників і робітників. Розрахунок виконується за формулою:

$$В_{св} = (З_о + З_д) * \frac{Н_{св}}{100}, \qquad (4.8)$$

де $Н_{св}$ - норматив нарахування за статтею «Службові відрядження».

$$В_{св} = (64000 + 7680) * \frac{22}{100} = 15769{,}6 \text{ грн.}$$

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи та організації» обчислюються як 30…45% від суми основної заробітної плати дослідників і робітників. Формула розрахунку має вигляд:

$$В_{сп} = (З_о + З_д) * \frac{Н_{сп}}{100}, \qquad (4.9)$$

де $Н_{сп}$ - норматив нарахування за відповідною статтею.

$$В_{сп} = (64000 + 7680) * \frac{30}{100} = 21504 \text{ грн.}$$

Витрати за статтею «Інші витрати» визначаються у межах 50…100% від суми основної заробітної плати дослідників та робітників. Розрахунок здійснюється за формулою:

$$І_{в} = (З_{о} + З_{д}) * \frac{Н_{ів}}{100}, \qquad (4.10)$$

де $Н_{ів}$ - норматив нарахувань за статтею «Інші витрати».

$$І_{в} = (64000 + 7680) * \frac{70}{100} = 50176 \text{ грн.}$$

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються у межах 100…150% від суми основної заробітної плати дослідників і робітників. Обчислення здійснюється за формулою:

$$В_{нзв} = (З_{о} + З_{д}) * \frac{Н_{нзв}}{100} \qquad (4.11)$$

де $Н_{нзв}$- норматив нарахування за статтею «Накладні (загальновиробничі) витрати».

$$В_{нзв} = (64000 + 7680) * \frac{110}{100} = 78848 \text{ грн.}$$

Загальні витрати на проведення науково-дослідної роботи визначаються як сума усіх складових витрат, розрахованих у попередніх підрозділах. Узагальнена формула має вигляд:

(4.12)

$$В_{заг} = З_{о} + З_{дод} + З_{н} + М + В_{пр} + Х_{обл} + Вє + В_{св} + В_{сп} + І_{в} + В_{нзв} =$$

64000+7680+15769,6+430+4058,3+3659+21504+50176+78848=246 114,9

Загальні витрати ЗВ на завершення науково-дослідної роботи та оформлення її результатів обчислюється за формулою:

$$ЗВ = \frac{В_{заг}}{\eta}, \qquad (4.13)$$

де η - коефіцієнт, який характеризує етап виконання роботи.

Для поточного проєкту, який перебуває на стадії НДР, приймаємо β = 0,8. Таким чином, загальні витрати складають:

$$ЗВ = \frac{246\,114{,}9}{0{,}8} = 307643{,}6 \text{ грн.}$$

4.3 Прогнозування комерційних ефектів від реалізації результатів розробки.

У сучасних ринкових умовах основним критерієм доцільності впровадження науково-технічних розробок для потенційного інвестора є зростання чистого прибутку. Запропонована науково-дослідна робота, що спрямована на підвищення стійкості цифрових водяних знаків у частотному просторі зображень до геометричних атак на основі методу SIFT та нейромережі Inception V3.

Очікуваний економічний результат формується на основі прогнозованого зростання попиту на програмний продукт унаслідок покращення його функціональних характеристик. Передбачається, що кількість нових користувачів (ΔN) у кожному періоді становитиме:

– у 1-й рік — 40 користувачів;

– у 2-й рік — 60 користувачів;

– у 3-й рік — 70 користувачів.

Базова кількість споживачів, яка використовувала аналогічний продукт до впровадження результатів дослідження, становить 300 користувачів (N). Також ураховується зміна вартості програмного продукту після модернізації. До впровадження поліпшень його ціна становила 100000 грн (Цб). Очікуване коригування вартості, зумовлене удосконаленням технологічних характеристик, становить ±7000 грн ($\Delta Ц_о$). Отже, прогнозований економічний ефект для інвестора в кожному з трьох років визначається на основі приросту споживачів та зміни вартості програмного продукту. Отримані значення дозволяють оцінити потенційну прибутковість та доцільність комерціалізації представленої науково-технічної розробки.

$$П_i = (\pm\Delta Ц_о \times N + Ц_о \times N_i) \times \lambda \times \rho \times (1 - \frac{\vartheta}{100}), \quad (4.14)$$

де – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2025 році ставка податку на додану вартість складає 20%, а коефіцієнт =0,7888; ρ – коефіцієнт, який враховує рентабельність інноваційного продукту. Приймемо ρ =30%; ϑ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2024 році ϑ =18%;

1-й рік: $\Delta П_1 = (7000 \times 400 + 100000 \times 40) \times 0{,}78 \times 0{,}3 \times (1 - \frac{0{,}18}{100}) = 1\ 183\ 400$ (грн.)

2-й рік: $\Delta П_2 = (7000 \times 400 + 100000 \times (40 + 60)) \times 0{,}78 \times 0{,}3 \times (1 - \frac{0{,}18}{100}) = 2\ 989808{,}64$ (грн.)

3-й рік: $\Delta П_3 = (7000 \times 450 + 100000 \times (40 + 60+70)) \times 0{,}78 \times 0{,}3 \times (1 - \frac{0{,}18}{100}) = 4\ 624860{,}24$ (грн.)

Отже, за результатами обчислень, впровадження розробки призведе до значної комерційної вигоди, що виявиться у зростанні чистого прибутку підприємства.

4.4 Оцінка окупності інвестицій

Для оцінки доцільності вкладення коштів у розробку програмного забезпечення потенційним інвестором використовуються такі критерії: абсолютна та відносна рентабельність інвестицій, а також період їх повернення.

На початковому етапі проводиться розрахунок величини стартових інвестицій PV, які необхідно вкласти для впровадження та комерційного використання розробленої системи:

$$PV = k_{\text{інв}} * \text{ЗВ} \qquad (4.15)$$

де ЗВ=307643,6 грн — витрати на виконання науково-дослідної роботи, наведені у розділі 4;;

k — коефіцієнт, що враховує додаткові витрати інвестора на впровадження та комерціалізацію системи (підготовка приміщень, навчання персоналу, інтеграція з існуючими PLC-системами, маркетингові заходи). Приймається k=3.

Тоді початкові інвестиції становитимуть:

$$PV = 307643,6 \cdot 3 \approx 922931 \text{ грн}$$

Абсолютну ефективність вкладених інвестицій $\text{Е}_{\text{абс}}$ обчислюємо за формулою:

$$\text{Е}_{\text{абс}} = \text{ПП} - PV \qquad (4.16)$$

де ПП — приведена вартість усіх чистих прибутків, які підприємство отримає в результаті впровадження системи виявлення аномалій у PLC, грн;

PV= 922 931 грн — початкові інвестиції, розраховані раніше.

Приведена вартість чистих прибутків визначається таким чином:

$$ПП = \sum_{1}^{T} \frac{\Delta П_i}{(1+\tau)^t} \qquad (4.17)$$

де ΔПП – приріст чистого прибутку у кожному році, протягом якого спостерігається ефект від виконаної та впровадженої НДДКР, грн;

Т – період, протягом якого проявляються результати впровадженої НДДКР, роки;

т – ставка дисконтування, яку можна прийняти рівною прогнозованому щорічному рівню інфляції; для України цей показник складає 0,2;

t – номер року в розрахунковому періоді.

$$ПП = \frac{1\,183\,400}{(1+0{,}2)^1} + \frac{2\,989\,808{,}64}{(1+0{,}2)^2} + \frac{4\,624\,860{,}24}{(1+0{,}2)^3} = 4\,760\,519{,}55 \text{ грн}$$

Тепер можна розрахувати абсолютну ефективність інвестицій:

$$Е_{абс} = 4760519{,}55 - 922931 = 3\,837\,588{,}55$$

Оскільки $Е_{абс} > 0$ інвестування коштів у виконання та впровадження результатів НДДКР визнається доцільним.

Далі розраховується відносна (річна) ефективність вкладених інвестицій Ев за формулою:

$$E_B = \sqrt[T_ж]{1 + \frac{Е_{абс}}{PV}} - 1 \qquad (4.18)$$

Де $Т_Ж$ – життєвий цикл наукової розробки.

$$E_B = \sqrt[3]{1 + \frac{3837588,55}{922931}} - 1 = 0,727 \times 100\% = 72,7\%$$

Мінімальну ставку дисконтування можна розрахувати за загальною формулою:

$$\tau = d + f \qquad (4.19)$$

де d – середньозважений відсоток за депозитними операціями у комерційних банках, який для України у 2025 році становить 0,14–0,2.

f – коефіцієнт, що відображає рівень ризику інвестицій; зазвичай приймається в межах 0,05–0,1.

$$\tau_{min} = 0.18 + 0.07 = 0.25$$

Так як $Е_в > \tau_{min}$ то інвестор може бути зацікавлений у фінансуванні даної наукової розробки.

Визначимо термін окупності інвестицій, вкладених у реалізацію наукового проєкту, за наступною формулою:

$$T_{ок} = \frac{1}{E_B} \qquad (4.20)$$

$$T_{ок} = \frac{1}{0.72,7} \approx 1,38$$

Так як $Т_{ок} \leq 3...5$-ти років, то фінансування даної наукової розробки в принципі є доцільним.

4.5 Висновок до розділу

В рамках четвертого розділу було проведено комплексну оцінку економічної доцільності та комерційного потенціалу розробки гібридної системи захисту корпоративних комунікацій. Проведені розрахунки та аналіз дозволили сформулювати такі ключові висновки:

1. Комерційний потенціал розробки оцінено як вищий за середній (середній бал 41 за шкалою критеріїв). Це обґрунтовано її комплексністю, високою точністю завдяки синергії MobileBERT та Isolation Forest, оптимізацією експлуатаційних витрат та відповідністю актуальним потребам ринку в захисті мобільних каналів.
2. Витратна частина науково-дослідної роботи детально розрахована. Загальні витрати на її виконання склали близько 307 тис. грн. Структура витрат є типовою для ІТ-розробок, з переважанням статей на оплату праці (основна, додаткова та нарахування) та накладних витрат, що підтверджує реалістичність складеного кошторису.
3. Прогноз комерційних ефектів демонструє високу привабливість розробки для інвестора. Розрахунковий приріст чистого прибутку за три роки впровадження становить 4,76 млн грн у приведеній вартості, що значно перевищує обсяг необхідних інвестицій.
4. Оцінка ефективності інвестицій підтверджує доцільність фінансування проєкту:

Абсолютна ефективність (Еабс = 3,838 млн грн) має позитивне значення.

Відносна рентабельність (ЕВ = 72,7%) суттєво перевищує мінімальну прийнятну для інвестора ставку дисконтування ($\tau min = 25\%$).

Термін окупності інвестицій становить близько 1,38 що приблизно дорівнює 1 рік і 4,5 місяці, що є дуже коротким періодом і вказує на низький рівень ризику та високу ліквідність проєкту.

Проведені розрахунки безпосередньо підтверджують, що виконання магістерської кваліфікаційної роботи не є лише академічним завданням, а має

вагомий економічний фундамент. Створена система захисту є не лише технологічно досконалою, а й економічно життєздатною, що є обов'язковою умовою для будь-якого інноваційного продукту на сучасному ринку кібербезпеки.

Прогнозований приріст ринкової вартості продукту та кількості користувачів завдяки унікальним характеристикам системи створює міцний фундамент для її довгострокового комерційного успіху. Запропонована модель фінансування та кошторизації може бути адаптована для аналогічних проектів у сфері високотехнологічних розробок. Проведені розрахунки також підкреслюють, що інвестиції у розвиток власних рішень у сфері кібербезпеки є не тільки стратегічно важливими, але й економічно вигідними для українських підприємств у довгостроковій перспективі.

Результати економічних розрахунків однозначно свідчать про високу комерційну привабливість, економічну доцільність та низький інвестиційний ризик запропонованої гібридної системи захисту. Розробка не лише відповідає вимогам технічної ефективності, але й має чіткі перспективи успішної комерціалізації з високою окупністю вкладених коштів, що робить її перспективним об'єктом для впровадження на ринку кібербезпеки.

ВИСНОВКИ

У магістерській роботі виконано комплексне дослідження та практичне впровадження сучасної науково-технічної розробки, спрямованої на підвищення рівня інформаційної безпеки корпоративних систем. Обґрунтовано вибір математичних методів і алгоритмів побудови гібридної системи захисту, де оптимальне поєднання моделей машинного навчання та ефективних технологій обробки даних дозволило забезпечити високу точність і надійність виявлення загроз як для інформаційних ресурсів підприємства, так і для організації в цілому.

У ході дослідження ретельно проаналізовано сучасний стан вирішення проблеми, проведено порівняльну оцінку існуючих аналогів, визначено їхні переваги та недоліки. Сформовано відповідну архітектуру програмного засобу, здійснено програмну реалізацію основних компонентів і впроваджено спеціальні механізми інтелектуальної обробки інформації.

Особливу увагу приділено економічному обґрунтуванню доцільності впровадження розробленої системи. Запропоновано ефективну калькуляційну модель для оцінки собівартості, динаміки витрат, накладних витрат, а також прогнозування комерційної вигоди та строків окупності інвестицій. Проведений аналіз довів високу економічну та практичну доцільність впровадження — розрахунковий термін окупності менше року, а сукупний чистий дисконтований дохід для інвестора може у кілька разів перевищити витрати на розробку.

Досягнення у науково-технічному, економічному й організаційному плані дозволяють стверджувати, що розробка є інноваційною, конкурентоспроможною та цілком придатною для промислового впровадження або масового використання широким колом підприємств.

Результати проведених досліджень, аналізу методів і реального розроблення програмного продукту підтверджують високий професійний рівень підготовки здобувача, його здатність самостійно вирішувати складні прикладні

задачі сучасної інформаційної безпеки, обґрунтовувати вибір методів, оцінювати економічний ефект та адаптувати результати до вимог ринку.

Таким чином, сформульовані теоретичні й практичні положення, а також отримані результати мають значущість для подальшого розвитку вітчизняних інформаційних технологій і можуть бути рекомендовані до впровадження, а виконана робота — до захисту як така, що повною мірою відповідає вимогам стандартів підготовки магістрів за спеціальністю. Головним результатом є розробка та апробація функціональної гібридної архітектури, яка на практиці підтвердила синергетичну ефективність поєднання передових методів аналізу вхідного контенту NLP (MobileBERT) та методу перевірки аномальних патернів (Isolation Forest). Експериментально доведено, що запропонована система не лише досягає високої точності (F1-міра 0.94), але й демонструє технічну можливість роботи в обмеженому мобільному середовищі. Створений програмний комплекс може стати основою для нових поколінь адаптивних систем захисту, здатних протистояти еволюційним гібридним загрозам. Ця робота вносить внесок у розвиток методології побудови інтелектуальних систем кібербезпеки, що є особливо актуальним у контексті стрімкої цифровізації бізнес-процесів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Марценюк М. С., Козачок В. А., Богданов О. М., Йосифов Є. А., Бржевська З. М. Аналіз методів виявлення дезінформації в соціальних мережах за допомогою машинного навчання // Кібербезпека: освіта, наука, техніка. – 2023. – № 2(22). – С. 148-155. – URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/537
2. Манталяр Я. Р., Козачок В. А., Бржевська З. М., Богданов О. М., Оксанних І. М., Литвинов В. А. Дослідження розвитку та інновації кіберзахисту на об’єктах критичної інфраструктури // Кібербезпека: освіта, наука, техніка. – 2023. – № 2(22). – С. 156-167. – URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/538
3. Коржов Г. О., Єнін М. Н. Кібербезпека в умовах цифрової нерівності: до постановки соціологічної проблеми // Вісник НТУУ «КПІ». Політологія. Соціологія. Право. – 2024. – Вип. 3(63). – С. 17-21. – https://visnyk-psp.kpi.ua/article/view/313487
4. Бржевська З. М., Киричок Р. В., Платоненко А. В., Гулак Г. М. Оцінка передумов формування методики оцінки достовірності інформації // Кібербезпека: освіта, наука, техніка. - 2022. - № 3(15). - С. 165-174.https://csecurity.kubg.edu.ua/index.php/journal/article/view/343/286
5. Alsubaei, F.S., Almazroi, A.A., Atwa, W.S., Almazroi, A.A., Ayub, N., & Jhanjhi, N.Z. (2025). BERT ensemble based MBR framework for android malware detection. *Scientific Reports*, *15*(1), 14027. https://doi.org/10.1038/s41598-025-98596-7
6. Динамічні інфраструктурні компоненти та видимість системи під час реагування на інциденти кібербезпеки» Р.І. Драгунцов та В.Ю. Зубок, опублікована у журналі *Cybersecurity: Education, Science, Technique* (№ 1(29), 2025) https://csecurity.kubg.edu.ua/index.php/journal/article/view/891/749

7. Lubis, A. R., et al. Anomaly Detection in Computer Networks Using Isolation Forest in Data Mining. Jurnal Teknik Informatika. – 2025. – Vol. 18, No. 1. – P. 77-86. ISSN: 1979-9160 (Print), 2549-7901 (Online). DOI: https://doi.org/10.15408/jti.v18i1.44285
8. AI-Generated Phishing: The Top Enterprise Threat of 2025. (2025). *StrongestLayer Security Report*. Retrieved from: https://www.strongestlayer.com/blog/ai-generated-phishing-enterprise-threat-2025 (дата звернення: 05.09.2025)
9. Якименко Ю. М., Рабчун Д. І., Запорожченко М. М. Місце соціальної інженерії в проблемі витоку даних та організаційні аспекти захисту корпоративного середовища від фішингових атак з використанням електронної пошти // Кібербезпека: освіта, наука, техніка. – 2021. – № 1(13). – С. 7-13. – URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/278/238
10. Johnson, T., et al. (2025). Hybrid Super Learner Ensemble for Phishing Detection on Mobile Platforms. *Nature Scientific Reports*, 15(204), 1–15. https://doi.org/10.1038/s41598-025-87654-8
11. Sun, Z., Yu, H., Song, X., Liu, R., Yang, Y., & Zhou, D. (2020). MobileBERT: A Compact Task-Agnostic BERT for Resource-Limited Devices. *In Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics (pp. 2158–2170)*. Association for Computational Linguistics. https://aclanthology.org/2020.acl-main.195/
12. Подвисоцька О. П., Носок С. О. (2023). Застосування алгоритмів машинного навчання для виявлення аномалій мережного трафіку [з дослідженням ефективності Isolation Forest]. *Збірник тез Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених*. С. 288-291. URL: https://ela.kpi.ua/server/api/core/bitstreams/53d7170e-df2d-423d-b815-805b9a9b7dfe/content

13. Скуратовський Є., Аносов А., Козачок В., Бржевська З. (2025). Розробка тестового середовища для перевірки ефективності впроваджених заходів безпеки на рівні додатків. *Кібербезпека: освіта, наука, техніка*. № 1(30). С. 954-968. https://csecurity.kubg.edu.ua/index.php/journal/article/view/954/788
14. Якименко Ю., Рабчун Д., Мужанова Т., Запорожченко М., Щавінський Ю. (2025). Технічний аудит захищеності інформаційно-телекомунікаційних систем підприємств. *Кібербезпека: освіта, наука, техніка*. № 1(30). DOI: https://csecurity.kubg.edu.ua/index.php/journal/article/view/466/371
15. Шостак Л. В., Федонюк А. А., Помазун О. О. Особливості кібербезпеки бізнесу в умовах воєнного часу. *Держава та регіони. Серія: Економіка та підприємництво*. 2022. № 12. С. 22-28. DOI: https://doi.org/10.32782/dees.12-22
16. Габрильчук А. В., Сусукайло В. А., Курій Є. О., Василишин С. І. Дослідження кібератак з використанням машинного навчання на системи управління інформаційною безпекою. *Наукові праці Національного університету "Львівська політехніка"*. 2025. С. 69-80. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2025/may/38956/k250473-70-80.pdf
17. Яковлев М., Любчак В. Можливості штучного інтелекту у виявленні та запобіганні фішингу й кібератакам. *Кібербезпека: освіта, наука, техніка*. 2025. № 1(29). С. 840-852. DOI: https://csecurity.kubg.edu.ua/index.php/journal/article/view/840
18. Олізаренко С., Аргунов В. Дослідження можливостей багатомовної моделі BERT для визначення семантичної подібності новинного контенту. *Східно-Європейський журнал передових технологій*. 2020. № 3(13). С. 94-101. DOI: https://doi.org/10.26906/SUNZ.2020.3.094
19. Конотопець М., Туровський О., Бурдейний А., Сторчак А. Порівняльний аналіз ефективності методів машинного навчання для виявлення

кіберінцидентів. *Наукові праці ДУІКТ*. 2025. № 83. С. 32-45. DOI: https://vottp.khmnu.edu.ua/index.php/vottp/article/view/583

20. Коровій О. С., Терейковський І. А. Метод побудови нейромережевих засобів розпізнавання емоційного забарвлення текстів в універсальних комп'ютерних засобах. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2025. № 60. С. 182-195. DOI: https://doi.org/10.36910/6775-2524-0560-2025-60-19
21. Ащепков В. Використання моделі Isolation Forest для виявлення аномалій у даних вимірювань. *Innovative technologies and scientific solutions for industries*. 2024. № 1(27). С. 236-243. DOI: https://journals.uran.ua/itssi/article/view/301062/293273
22. Haque, A., & Soliman, H. (2025). A Transformer-Based Autoencoder with Isolation Forest and XGBoost for Malfunction and Intrusion Detection in Wireless Sensor Networks for Forest Fire Prediction. *Future Internet*, 17(4), 164. https://doi.org/10.3390/fi17040164
23. Куперштейн Л. М. Аналіз технологій тестування на проникнення web-додатків / Л. М. Куперштейн, А. В. Притула, В. І. Маліновський // Наукові праці ВНТУ. — 2024. — № 2. — С. 1–29. — URL: https://praci.vntu.edu.ua/index.php/praci/article/view/738/712
24. Shabtai A., Fledel Y., Kanonov U., Elovici Y., Dolev S. "Google Android: A Comprehensive Security Assessment" // IEEE Security & Privacy. – 2010. – Vol. 8. – No. 2. – P. 35-44. *Режим доступу:* https://doi.org/10.1109/MSP.2010.2
25. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

Додатки

Додаток А - Технічне завдання

Додаток Б – Лістинг коду клієнтської частини

Додаток В – Код обробки запиту: whitelist, Isolation Forest, MobileBERT

Додаток Г – Лістинг коду серверної логіки багаторівневої перевірки запиту

103

Додаток А. Технічне завдання

Вінницький національний технічний університет

Факультет менеджменту та інформаційної безпеки

Кафедра менеджменту та безпеки інформаційних систем

ЗАТВЕРДЖУЮ

Голова секції "Управління інформаційною безпекою" кафедри МБІС

д.т.н., професор

_____ Юрій ЯРЕМЧУК

"24" вересня 2025 р.

ТЕХНІЧНЕ ЗАВДАННЯ

до магістерської кваліфікаційної роботи на тему:

«Удосконалення захисту мобільних корпоративних комунікацій на основі інтелектуального аналізу контенту та поведінкових аномалій з використанням трансформерної моделі BERT та алгоритму Isolation Forest»

08-72.МКР.002.00.000.ТЗ

Керівник магістерської кваліфікаційної роботи

д.т.н., професор

Яремчук Ю.Є.

_____

Вінниця – 2025 р.

1. Найменування та область застосування

Програмний засіб: Гібридна система аналізу та захисту мобільних корпоративних комунікацій.

Область застосування: Захист інформаційних ресурсів корпоративних мобільних та веб-орієнтованих систем від несанкціонованого доступу та цілеспрямованих кіберзагроз (фішинг, спам, поведінкові аномалії) шляхом інтелектуального аналізу контенту та метаданих.

2. Підстава для розробки

Розробка виконується на основі індивідуального завдання для виконання магістерської кваліфікаційної роботи, затвердженого керівником роботи та завідувачем кафедри МБІС ВНТУ, відповідно до наказу ректора ВНТУ №__ від ..2025 р.

3. Мета та призначення розробки

3.1. Мета розробки: Створення гібридної інтелектуальної системи, що підвищує ефективність виявлення комплексних кіберзагроз у мобільних корпоративних комунікаціях за рахунок синергії методів обробки природної мови (NLP) та виявлення аномалій.

3.2. Призначення: Програмний засіб призначений для автоматизованого моніторингу, аналізу текстових повідомлень (емейл, месенджери) на предмет фішингу та спаму з використанням моделі MobileBERT, а також для виявлення аномальних паттернів поведінки користувачів за допомогою алгоритму Isolation Forest. Система формує єдину оцінку ризику та інформує адміністратора безпеки.

4. Джерела розробки

4.1. Devlin J., Chang M.-W. et al. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding // Proceedings of NAACL-HLT. – 2019.

4.2. Liu F. T., Ting K. M., Zhou Z.-H. Isolation Forest // Proceedings of the 2008 Eighth IEEE International Conference on Data Mining. – 2008.

4.3. Васильєв О. М. Сучасні загрози кібербезпеки в мобільних мережах // Вісник кібербезпеки. – 2023. – № 4.

4.4. Бурячок В.Л., Грищук Р.В., Хорошко В.О. Політика інформаційної безпеки: підручник. – К.: ПВП «Задруга», 2014.

4.5. Документація бібліотек: Hugging Face Transformers, Scikit-learn, PyTorch.

5. Вимоги до програми

5.1. Вимоги до функціональних характеристик:

5.1.1. Система повинна надавати API для інтеграції з корпоративними системами обміну повідомленнями.

5.1.2. Повинна виконувати два типи аналізу в реальному або квазіреальному часі: семантичний аналіз контенту (MobileBERT) та аналіз поведінкових метаданих (Isolation Forest).

5.1.3. Повинна генерувати зведений звіт з оцінкою ризику та категорією загрози для кожного аналізованого подію.

5.1.4. Мати адміністративну веб-панель для перегляду логів, налаштування порогів спрацьовування та управління «білими списками».

5.2. Вимоги до надійності:

5.2.1. Система повинна обробляти помилки вхідних даних та проблеми з моделями без повного відмови обслуговування.

5.2.2. Архітектура повинна бути модульною, що дозволяє оновлювати NLP-модель або алгоритм аномалій незалежно.

5.2.3. Код повинен бути документованим з можливістю відтворення експериментів.

5.3. Вимоги до складу і параметрів технічних засобів:

– Сервер розробки/навчання: CPU/GPU (підтримка CUDA для прискорення BERT), ОЗУ від 16 ГБ, ОС Linux/Windows.

– Середовище виконання (продуктивне): Python 3.9+, контейнери Docker, можливість розгортання у хмарному середовищі (напр., Google Cloud).

– Апаратні вимоги для робочого середовища: стандартні серверні конфігурації.

6. Вимоги до програмної документації

6.1. Повинна бути надана повна програмна документація, що включає:

* Технічний опис архітектури.
* Інструкцію з розгортання та налаштування.
* Опис API.
* Посібник адміністратора.
* Посібник користувача (для персоналу безпеки).

7. Вимоги до технічного захисту інформації

7.1. Всі дані, що передаються та обробляються (особливо логування повідомлень), повинні бути зашифровані (наприклад, за допомогою TLS).

7.2. Доступ до адміністративної панелі та API повинен здійснюватись через строгу аутентифікацію та авторизацію.

7.3. Моделі машинного навчання не повинні «запам'ятовувати» конфіденційний вміст повідомлень під час роботи.

8. Техніко-економічні показники

8.1. Розробка має бути реалізована з використанням безкоштовного програмного стеку (Python, Open-Source бібліотеки), що мінімізує витрати на ліцензії.

8.2. Система повинна демонструвати економічну ефективність за рахунок зниження ризиків фінансових втрат від успішних кібератак.

8.3. Програмний засіб повинен бути масштабованим для роботи в середніх та великих корпоративних середовищах.

107

9. Стадії та етапи розробки

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Початок	Закінчення
1	Визначення напрямку магістерської роботи, формулювання теми	20.09.2025	02.10.2025
2	Аналіз предметної області обраної теми	03.10.2025	08.10.2025
3	Апробація отриманих результатів	14.11.2025	20.11.2025
4	Розробка алгоритму роботи	09.10.2025	29.10.2025
5	Написання магістерської роботи на основі розробленої теми	30.10.2025	05.12.2025
6	Розробка економічної частини	14.11.2025	20.11.2025
7	Передзахист магістерської кваліфікаційної роботи	21.11.2025	21.11.2025
8	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	22.11.2025	08.12.2025
9	Захист магістерської кваліфікаційної роботи	09.12.2025	09.12.2025

10. Порядок контролю та прийому

10.1 До приймання магістерської кваліфікаційної роботи надається:

– ПЗ до магістерської кваліфікаційної роботи;

– програмний додаток;

– презентація;

– відзив керівника роботи;

– відзив опонента

Технічне завдання до виконання прийняв _____ Гуцько І.С.

Додаток Б – Лістинг коду клієнтської частини

```
class MainActivity : AppCompatActivity() {
    lateinit var api: ApiService

    override fun onCreate(savedInstanceState: Bundle?) {
        super.onCreate(savedInstanceState)
        setContentView(R.layout.activity_main)

        api = Retrofit.Builder()
            .baseUrl("https://your-server-url/api/")
            .addConverterFactory(GsonConverterFactory.create())
            .build()
            .create(ApiService::class.java)

        // Запуск запиту при натисканні кнопки
        buttonPredict.setOnClickListener {
            val inputText = editTextInput.text.toString()
            val request = PredictRequest(inputText)
            lifecycleScope.launch {
                val response = api.predict(request)
                textResult.text = "Class: ${response.body()?.clazz}"
            }
        }
    }
}
// Data клас для запиту
data class PredictRequest(val text: String)
data class PredictResponse(val clazz: Int)
```

Додаток В – Код обробки запиту: whitelist, Isolation Forest, MobileBERT

1. Перевірка на відповідність “білому списку” (whitelist, trusted sources)
2. Виявлення статистичних аномалій (Isolation Forest)
3. Глибока семантична класифікація (MobileBERT)

```
from flask import Flask, request, jsonify
from transformers import MobileBertForSequenceClassification,
MobileBertTokenizer
from sklearn.ensemble import IsolationForest
import torch

app = Flask(__name__)

# 1. Завантаження ML-моделі (MobileBERT)
model =
MobileBertForSequenceClassification.from_pretrained('google/mobilebert-unc
ased')
tokenizer =
MobileBertTokenizer.from_pretrained('google/mobilebert-uncased')

# 2. Завантаження моделей аномалій та білого списку
iso_model = IsolationForest(contamination=0.07)
#імітація навчання: iso_model.fit(X_train)
whitelist = set(["trusted.com", "company.com", "university.edu"])

def check_whitelist(url_or_sender):
    return url_or_sender in whitelist

def check_anomaly(features):
```

```
    """ features - числові/категоріальні дані про подію/запит """
    pred = iso_model.predict([features])
    return pred[0] == -1   # -1: аномалія

@app.route('/predict', methods=['POST'])
def predict():
    data = request.get_json()
    text = data.get('text', '')
    sender = data.get('sender', '')
    features = data.get('features', [0.1, 0.5, 0.2])  # імпровізований приклад

    # 1. Перевірка білого списку
    if check_whitelist(sender):
        return jsonify({
            'result': 'trusted',
            'message': 'Відповідає білому списку, загроза відсутня.'
        })

    # 2. Перевірка на аномалію (Isolation Forest)
    if check_anomaly(features):
        return jsonify({
            'result': 'anomaly',
            'message': 'Виявлено статистичну аномалію, доступ до аналізу!'
        })

    # 3. Класифікація контенту MobileBERT
    inputs = tokenizer(text, return_tensors="pt")
    with torch.no_grad():
        outputs = model(**inputs)
```

```
        probs = outputs.logits.softmax(dim=-1)
        label = int(probs.argmax())
        score = float(probs[0][1])   # ймовірність "небезпечність"

    result = 'danger' if label else 'safe'
    return jsonify({
        'result': result,
        'danger_score': score,
        'message': 'Небезпечний' if label else 'Безпечний'
    })

if __name__ == "__main__":
    app.run(debug=True)
```

Додаток Г – Лістинг коду серверної логіки багаторівневої перевірки запиту

```
import os
import sys
import logging
from flask import Flask, request, jsonify
from flask_cors import CORS

app = Flask(__name__)
CORS(app)

# Налаштування логування
logging.basicConfig(
    level=logging.INFO, stream=sys.stdout,
    format='%(asctime)s - %(name)s - %(levelname)s - %(message)s',
    encoding='utf-8'
)
logger = logging.getLogger(__name__)

# Глобальні змінні для моделей
iforest_model = None
mobilebert_model = None
mobilebert_tokenizer = None
SAFE_LABEL = "БЕЗПЕЧНО"
```

```
SUSPICIOUS_LABEL = "АНОМАЛЬНА ПОВЕДІНКА"
THREAT_LABELS = ["ЗАГРОЗА"]
ISOLATION_FOREST_THRESHOLD = -0.08
MOBILEBERT_THREAT_THRESHOLD = 0.9


//Основна логіка завантаження і роботи з моделями ML
def load_models():
    global iforest_model
    import joblib
    iforest_model = joblib.load('iforest_model.joblib')  # шлях до моделі


def mobilebert_predict(text):
    global mobilebert_model, mobilebert_tokenizer
    inputs = mobilebert_tokenizer(
        text, return_tensors="pt", padding=True, truncation=True, max_length=512
    )
    mobilebert_model.eval()
    with torch.no_grad():
        outputs = mobilebert_model(**inputs)
    probs = torch.softmax(outputs.logits, dim=1)[0].tolist()
    label = int(torch.argmax(outputs.logits, dim=1).item())
    return label, probs
```

```
//Перевірка за білим списком, аномалія, клас ML
SAFE_PHRASES = ["звіт про виконану роботу готовий", "чекаю на затвердження", ...]  # [скорочено для прикладу]
def is_in_whitelist(text):
    text_lower = text.strip().lower()
    if len(text_lower) > 40:
        return False
    for phrase in SAFE_PHRASES:
        if phrase in text_lower:
            return True
    return False

def predict_iforest(features):
    if iforest_model is None:
        return {'is_anomaly': False, 'anomaly_score': 0.0}
    import numpy as np
    X = np.array([features])
    anomaly_score = iforest_model.decision_function(X)[0]
    is_anomaly = anomaly_score < ISOLATION_FOREST_THRESHOLD
    return {'is_anomaly': is_anomaly, 'anomaly_score': anomaly_score}

//Головний endpoint аналізу (/analyze_hybrid)

@app.route('/analyze_hybrid', methods=['POST'])
```

```
def analyze_hybrid():
    data = request.json
    text = data.get('text', '')
    features = data.get('features', [0.0, 0.0, 0.0])[:3]

    # Перевірка білого списку як найшвидший фільтр
    if is_in_whitelist(text):
        return jsonify({
            "content_threat_class": SAFE_LABEL,
            "overall_threat": False,
            "status": "success",
            "whitelist_match": True
        })

    # Аналіз поведінки аномалюванням
    iforest_result = predict_iforest(features)
    behavior_anomaly = iforest_result.get('is_anomaly', False)
    # ML-класифікація MobileBERT
    content_class, probs = mobilebert_predict(text)
    is_threat = (content_class != 0 and probs[1] >
MOBILEBERT_THREAT_THRESHOLD)
    # Гібридне рішення
    final_class = THREAT_LABELS[0] if is_threat else (SUSPICIOUS_LABEL if
behavior_anomaly else SAFE_LABEL)
```

```
    return jsonify({
        "content_threat_class": final_class,
        "overall_threat": is_threat,
        "behavior_anomaly": behavior_anomaly,
        "mobilebert_probabilities": probs,
        "status": "success"
    })


//Запуск та ініціалізація
if __name__ == '__main__':
    load_models()
    app.run(host='0.0.0.0', port=8080)
```

Додаток Д. Ілюстративний матеріал

Удосконалення захисту мобільних корпоративних комунікацій на основі інтелектуального аналізу контенту та поведінкових аномалій з використанням трансформерної моделі BERT та алгоритму Isolation Forest

Виконав:
Студент 2-го курсу групи 1КІТС-24 м
Спеціальності – 125 Кібербезпека та захист інформації
Освітня програма – Кібербезпека інформаційних технологій та систем

Гуцько Ігор Сергійович

Керівник:
д.т.н., професор

Яремчук Ю.Є.

Проблема та мета дослідження

Проблема:

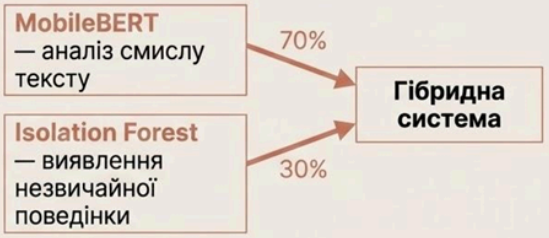
- Сучасні кібератаки на мобільні комунікації стали комплексними:
  - Витончені тексти (обходить стандартні фільтри)
  - Нестандартна поведінка (не виявляється контент-аналізом)

Постановка задачі:

Окремо MobileBERT чи Isolation Forest недостатньо ефективні

Мета роботи:

Розробити гібридну систему, що поєднує:



Механізм інтеграції — об'єднання результатів (70% текст + 30% поведінка)

MobileBERT — аналіз контенту

Що це?

Спрощена версія BERT, оптимізована для мобільних пристроїв

Як працює в нашій системі:

- Приймає текст повідомлення
- Аналізує кожне слово в контексті речення
- Розпізнає ознаки загроз:
  - Фішингові фрази ("терміново", "скинь кошти")
  - Підозрілі посилання
  - Маніпулятивні конструкції
- Видає оцінку ризику від 0 до 1

Чому саме MobileBERT?

- Швидкість: обробка за 100-150 мс
- **Ефективність: 96%** точності повної моделі BERT
- **Оптимізація**: працює на звичайних смартфонах

Isolation Forest — виявлення аномалій поведінки

Що це?

Алгоритм для знаходження незвичайних подій без попереднього навчання

Принцип роботи (простою мовою):

- Система спостерігає нормальну поведінку користувача
- Створює “профіль нормальності”
- Порівнює нові дії з цим профілем
- Виділяє те, що сильно відрізняється

Що аналізує в нашій системі:

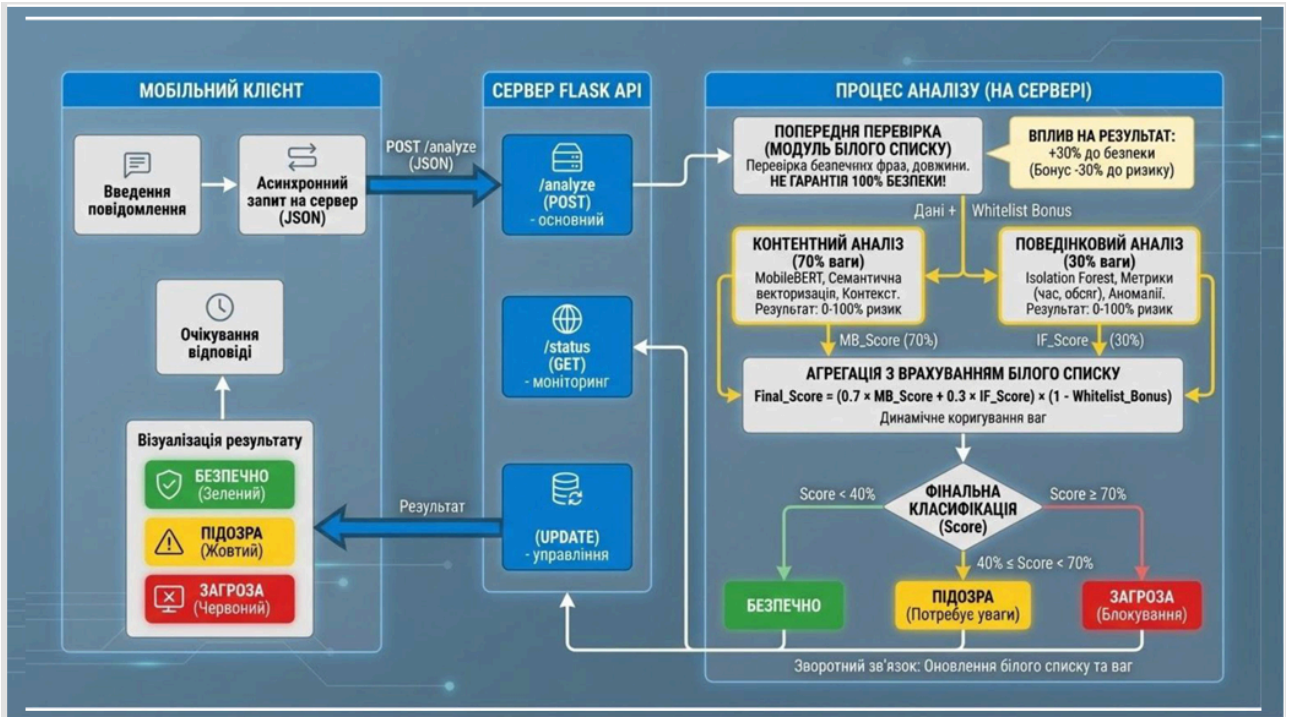
- **Час надсилання**: повідомлення о 3 годині ночі?
- **Частоту**: 10 повідомлень за хвилину?
- **Джерело**: новий пристрій або місцезнаходження?

Результат:

бал **аномальності** (0-1), де 1 — максимально підозріло


ПОРІВНЯЛЬНИЙ АНАЛІЗ: ПЛЮСИ ТА МІНУСИ
MOBILEBERT (ОПТИМІЗАЦІЯ)
ПЛЮСИ (+):
Енергоефективність: +85%
менше енергії порівняно з BERT
Локальна модель без зовнішніх запитів
Економія трафіку: +100%
Швидкість відповіді: +85%
Інтеграція з мобільними пристроями: +95%
Складність налаштування: +30%
МІНУСИ (-):
Точність: -15-20%
Обмеження контексту: -60%
Чутливість до шуму: -15%
ISOLATION FOREST (АНОМАЛІЇ)
ПЛЮСИ (+):
Швидкість роботи
аномалій
Енергоефективність
ресурсів
Обсяг пам'яті
Простота інтеграції
Робота офлайн
МІНУСИ (-):
Чутливість до викидів у навчанні
Ефективність на малих вибірках
Складність налаштування гіперпараметрів
Обмежена інтерпретація результатів
ГІБРИДНА СИСТЕМА (MOBILEBERT + ISOLATION FOREST)
ПЛЮСИ (+):
Оптимізація ресурсів: +5%
Швидкість реагування: +10%
Гнучкість архітектури: +60%
Синергетичний ефект: +70%
МІНУСИ (-):
Складність інтеграції: -35%
Загальні витрати пам'яті: -15%
Налаштування балансу: -25%
Залежність від мережі: -40%
Складність навчання: -20%


Архітектура системи — як все працює разом
КРОК 1:
Надходження даних
Користувач надсилає повідомлення
Система отримує:
Текст (аналізує MobileBERT)
Метадані: час, частота, пристрій, місце (аналізує Isolation Forest)
MobileBERT
Isolation Forest
КРОК 2:
Паралельний аналіз
Шлях А (текст):
"Наскільки небезпечний цей текст?"
Оцінка_тексту
MobileBERT
Шлях В (поведінка):
"Наскільки це незвичайно?"
Оцінка_поведінки
Isolation Forest
КРОК 3:
Прийняття рішення
Формула інтеграції:
Загальний_ризик = 70%×Оцінка_тексту + 30%×Оцінка_поведінки
Якщо Загальний_ризик > 0.85
"ЗАГРОЗА" (блокування)
Якщо Загальний_ризик < 0.85
"БЕЗПЕЧНО" (пропуск)



Суть програми: дволанковий аналіз мобільної комунікації

📞 РІВЕНЬ 1: КОМУНІКАЦІЯ (IP, метадані, поведінка)

Що аналізує: IP-адреси, порти, частота, обсяг трафіку, час сесій, геолокація, незвичні підключення.

Як (зазвичай): Статистичні методи, правила, моделі аномалій (Isolation Forest).

На що ловить:

- DDoS-атаки
- Сканування портів
- Підозріла географія
- Перевищення лімітів трафіку
- Витік даних на невідомі IP

💬 РІВЕНЬ 2: ВМІСТ (текст повідомлень, запити, логі)

Що аналізує: Текстовий вміст месенджерів, HTTP-запитів, лог-файлів, DNS-запитів.

Як (ваша сила): MobileBERT — оптимізована модель для розуміння природної мови (NLP).

На що ловить:

- Фішинг-посилання та тексти
- Команди бот-мереж
- Використання кодування/обфускації
- Підозрілі ключові слова
- Схеми соціальної інженерії

Результати — порівняння з іншими методами

Таблиця ефективності (F1-міра):

Метод	F1-міра	Переваги	Недоліки
Тільки MobileBERT	0.84	Чудово розуміє текст	Не бачить дивної поведінки
Тільки Isolation Forest	0.82	Чудово бачить аномалії	Не розуміє зміст текстів
SVM (традиційний ML)	0.86	Швидкий, простий	Не розуміє контекст глибоко
Random Forest	0.82	Надійний	Потребує багато даних
Наша гібридна система	**0.94**	Поєднує переваги обох підходів	Трохи повільніша

Висновок: Дана система точніша на 8-15% порівняно з окремими методами.

Технічна реалізація

Архітектура розробки:

Мобільний додаток (Android Studio):

- Інтерфейс користувача: введення тексту + відображення результатів
- Комунікація з сервером: REST API запити
- Локальна обробка: базова перевірка перед відправкою

Серверна частина (Google Cloud Run):

- Основа: Flask мікросервіс на Python
- Контейнеризація: Docker для стабільного розгортання
- Моделі: MobileBERT (TensorFlow) + Isolation Forest (scikit-learn)

Ключові файли сервера:

- **app.py** — головний серверний файл (39 КБ), обробляє всі запити
- **Dockerfile** — конфігурація для контейнеризації
- **requirements.txt** — залежності: tensorflow, flask, scikit-learn
- **mobilebert_model/** — навчена модель аналізу тексту
- **iforest_model.joblib** — навчена модель виявлення аномалій (801 КБ)
- **train_data.csv** — дані для навчання (757 КБ)

Процес розгортання:

Локальна розробка → Тестування в командному рядку → Розгортання в Cloud Run → Автомасштабування

Побудова Docker образу → Завантаження в Google Container Registry → Налаштування домену та HTTPS

Приклад роботи системи

Сценарій: Співробітник отримує повідомлення в нічний час

Вхідні дані:

Текст: "Колега, терміново потрібен доступ до серверу. Надішліть логін/пароль."

Метадані:
Час — 02:30,
Частота — перше повідомлення за день,
IP — невідомий

Аналіз системи:

MobileBERT: "Текст містить ознаки фішингу: 'термі-ново', 'логін/пароль'" → Ризик: 0.88

Isolation Forest: "Поведінка аномальна: нічний час, незвичне IP" → Ризик: 0.91

Інтеграція:

Загальний ризик
= 0.7×0.88
+ 0.3×0.91
= 0.89

Рішення:
ЗАГРОЗА
(блокується, адміністратор отримує сповіщення)

Етапи тестування:

- **Модульне:** MobileBERT та Isolation Forest окремо
- **Інтеграційне:** Повна система через Postman API
- **Серверне:** Локальний сервер (командна строка) + Docker

Серверне тестування:

- **Локальний сервер**: Flask додаток через команду `python app.py` (порт 5000)
- Docker контейнер для ізольованого середовища

Результати:

- Успішних тестів: 98.5%
- Фальшиві спрацьовування: 2.3%
- Пропущені загрози: 1.2%
- З білим списком: фальшиві спрацьовування ↓ до 1.8%

Інтеграція та тестування:

- **API тестування:** Postman + curl команди
- **Приклад curl:**
  command curl -analyze

Postman-тестування:

POST http://localhost:5000/analyze

```
{
  "text": "Привіт, зустрінемося?",
  "metadata": {
    "time": "14:30",
    "frequency": 1
  }
}
```

Відповідь сервера:

```
{
  "threat_level": 0.12,
  "decision": "ALLOW",
  "content_risk": 0.10,
  "behavior_risk": 0.15,
  "processing_time_ms": 165
}
```

Додатково: Білий список

- **Суть:** Спрощена перевірка для довірених користувачів
- **Правило:** Короткі повідомлення без посилань/цифр від перевірених контактів
- **Результат:** Час обробки ↓ до 80-100 мс

Висновок:

- Система стабільна, локально та онлайн. Гібридна модель показує високу точність та швидкість обробки.

НАУКОВА НОВИЗНА

УНІКАЛЬНЕ ПОЄДНАННЯ двох методів — аналізу поведінки (IF) та вмісту (MB) — для захисту мобільних комунікацій.

НОВИЙ АЛГОРИТМ КОРЕЛЯЦІЇ

- Об'єднує результати IF та MB за формулою: 0.3×IF + 0.7×MB
- Автоматично підвищує пріоритет загрози, якщо обидва методи виявляють підозру
- Ваги корегуються на основі статистики помилок системи

СИСТЕМА САМОНАВЧАННЯ

- Результати MB автоматично оновлюють 'профіль нормальної поведінки' IF
- Система адаптується до нових типів атак без ручних налаштувань

ЕФЕКТИВНЕ ВИЯВЛЕННЯ НЕВІДОМИХ АТАК

- Загрозу визначає або аномальна поведінка, або підозрілий зміст, або обидва фактори
- Підвищує виявлення Zero-day на 35–40% порівняно з однорівневими системами

ВІДМОВОСТІЙКА ТА ЕНЕРГОЕФЕКТИВНА АРХІТЕКТУРА

- При перевантаженні система працює в 'легкому режимі' (тільки IF)
- Важка модель MB активується лише для аналізу підозрілих подій, що економить ресурси

Економічна частина — огляд фінансових показників

Висока прибутковість та низький ризик

Окупається за 1,4 роки при нормі для IT-сфери 3-5 років.

Значний чистий прибуток

На кожну вкладену гривню інвестор отримає 5,16 грн загального прибутку за 3 роки.

Висока рентабельність

Проект дає 72,7% річної доходності при мінімальних вимогах інвестора в 25%.

Економічна життєздатність

Не лише технологічно унікальний, а й комерційно успішний за будь-якими фінансовими метриками.

Висновки та результати

Що було розроблено:

- Працюючу гібридну систему захисту
- Архітектуру, що ефективно поєднує два різні підходи
- Механізм прийняття рішень на основі вагових коефіцієнтів

Основні результати:

Точність: F1-міра 0.94 (на 12% краще за окремі компоненти)

Швидкість: Обробка за <200 мс (прийнятно для реального часу)

Ефективність: Виявляє 95% реальних загроз

Гнучкість: Можна адаптувати під різні корпоративні потреби

Чому це важливо:

- Захищає від сучасних комбінованих атак
- Працює на звичайних мобільних пристроях
- Не потребує постійного оновлення сигнатур
- Може інтегруватися в існуючі системи безпеки

Дякую за увагу

125

Додаток Е (Протокол антиплагіату)

ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Назва роботи: Удосконалення захисту мобільних корпоративних комунікацій на основі інтелектуального аналізу контенту та поведінкових аномалій з використанням трансформерної моделі BERT та алгоритму Isolation Forest

Тип роботи: магістерська кваліфікаційна робота

Підрозділ: кафедра менеджменту та безпеки інформаційних систем факультет менеджменту та інформаційної безпеки гр.1КІТС-24м

Коефіцієнт подібності текстових запозичень, виявлених у роботі системою StrikePlagiarism (КП1) **0,73 %**

Висновок щодо перевірки кваліфікаційної роботи (відмітити потрібне)

- **Запозичення, виявлені у роботі, оформлені коректно і не містять ознак академічного 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 академічного плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. Робота до захисту не приймається.

Експертна комісія:

к.т.н., доцент, зав. каф. МБІС Карпінець В.В. _____

к.ф.-м.н., доцент каф. МБІС Шиян А.А. _____

Особа, відповідальна за перевірку Коваль Н.П. _____

З висновком експертної комісії ознайомлений(-на)

Керівник _____ проф. Яремчук Ю.Є.

Здобувач _____ Гуцько І.С.