Центральноукраїнський національний технічний університет
Механіко-технологічний факультет
Кафедра кібербезпеки та програмного забезпечення

”Допущено до захисту”
Завідувач кафедри кібербезпеки
та програмного забезпечення
д.т.н., професор
_____ Олексій СМІРНОВ
“____” _____ 2026 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за другим (магістерським) рівнем вищої освіти
на тему
“Дослідження та програмна реалізація системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання”

Виконав здобувач вищої освіти
ІІ курсу, групи КН-25М
ОПП «Комп’ютерні науки»
спеціальності F3 «Комп’ютерні науки»
_____ Протасов Р.Б.
«____» _____ 2026 р.

Керівник проекту
доктор технічних наук, професор
_____ Смірнов О.А.
«____» _____ 2026 р.

Нормоконтроль проекту
_____ Коваленко А.С.
«____» _____ 2026 р.

Рецензент _____
_____

Підписано КЕП
Центральноукраїнський національний технічний університет
Протасов Роман Богданович
Сертифікат: 18DF2C9B93CEA2040400000033E263009C0D7606
Дійсний з 20.11.2026 17:01:32 по 20.11.2027 17:01:31

Центральноукраїнський національний технічний університет
Факультет *Механіко-технологічний*
Кафедра *Кібербезпеки та програмного забезпечення*
Рівень вищої освіти *магістр*
Галузь знань _F_____*"*Інформаційні технології*"*_____
Спеціальність F3 *"*Комп'ютерні науки*"*
Освітньо-професійна (освітньо-наукова) програма _*"*Комп'ютерні науки*"*_

ЗАТВЕРДЖУЮ
Завідувач кафедри
д.т.н., проф.
_____ Олексій СМІРНОВ
« 1 » вересня 2026 року

ЗАВДАННЯ НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗА ДРУГИМ (МАГІСТЕРСЬКИМ) РІВНЕМ ВИЩОЇ ОСВІТИ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Протасову Роману Богдановичу
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження та програмна реалізація системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання*

2. Керівник роботи *Смірнов Олексій Анатолійович, доктор технічних наук, професор*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу № 42-13 від 17.08.2026 року

3. Строк подання студентом роботи до захисту *2.12.2026 р.*

4. Мета та завдання випускної кваліфікаційної роботи*: Метою розробки є дослідження та програмна реалізація системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання*

5. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Призначення та область використання.	*5. Впровадження системи в промислову експлуатацію*
2. Перегляд аналогічних існуючих систем.	*6. Наукова новизна.*
3. Опис і обґрунтування проектних рішень.	*7. Заходи з охорони праці та техніки безпеки.*
4. Етапи програмування системи.	*8. Висновки.*

6. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Наукова новизна	*1 аркуш*
Структурна схема системи	*1 аркуш*
Функціональна схема системи	*1 аркуш*
Діаграма процесів	*1 аркуш*
Блок-схема алгоритму роботи додатку	*2 аркуша*

7. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Марченко К.М., к.т.н., доцент	06.10.2026	16.11.2026

8. Дата видачі завдання « 1 » вересня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти	Строк виконання етапів випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти	Примітка
1.	Аналіз існуючих систем	10.10.2026 р.	
2.	Постановка задачі, оформлення ТЗ	15.10.2026 р.	
3.	Розробка моделі компонента	20.10.2026 р.	
4.	Розробка структур даних	25.10.2026 р.	
5.	Розробка алгоритмів системи	30.10.2026 р.	
6.	Програмування алгоритмів	10.11.2026 р.	
7.	Розрахунки з охорони праці та техніки безпеки	15.11.2026 р.	
8.	Оформлення ПЗ	17.11.2026 р.	
9.	Попередній захист роботи	2.12.2026 р.	

Дата видачі завдання
« 1 » вересня 2026 р.

Підпис керівника

_____ _____
(прізвище та ініціали)

Завдання прийнято до виконання
« 1 » вересня 2026 р.

Підпис здобувача

_____ _____
(прізвище та ініціали)

АНОТАЦІЯ

Протасов Р.Б. Дослідження та програмна реалізація системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання. ФЗ Комп'ютерні науки. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

Метою розробки є дослідження та програмна реалізація системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

Об'єктом дослідження є процес динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

Предметом дослідження є методи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

Методи дослідження базуються на методах машинного навчання, методах математичної статистики, методах розробки програмного забезпечення.

Результат роботи – програмна реалізація системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

Програма може використовуватися на ПЕОМ з ОС Windows 10/11.

Програму розроблено в середовищі PHP фреймворк Yii2.

Ключові слова: комп'ютерні науки, динамічне профілювання, поведінка користувача, кластеризація, глибоке навчання

ABSTRACT

Protasov R.B. Research and Software Implementation of a System for Dynamic User Behavior Profiling Using Clustering and Deep Learning Methods. F3 Computer Science. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

This final qualification thesis, submitted for the second (master's) level of higher education, presents the development of software designed for a system that performs dynamic user behavior profiling using clustering and deep learning techniques.

The objective of this project is to research and implement a software system for dynamic user behavior profiling, utilizing clustering and deep learning methods.

The object of the research is the process of dynamic user behavior profiling based on clustering and deep learning.

The subject of the research consists of the specific methods used for dynamic user behavior profiling via clustering and deep learning.

The research methodology draws upon machine learning techniques, mathematical statistics, and software development practices.

The outcome of the work is a software implementation of a system for dynamic user behavior profiling using clustering and deep learning.

During the development of the software model, an analysis of existing hardware and software tools was conducted. All components of the developed software are described in detail.

A user-friendly interface has been developed, and instructions for operating the software are provided.

The software is designed for use on personal computers running the Windows 10/11 operating system. The program was developed using the Yii2 PHP framework.

Keywords: computer science, dynamic profiling, user behavior, clustering, deep learning

ВІДОМІСТЬ ПРОЕКТУ

		Текстові документи			
1	А4	Пояснювальна записка	93	–	
2	А4	Робоча програма	21	–	Додаток А
		Графічні документи			
3	А4	Наукова новизна	1	–	
4	А4	Структурна схема	1	–	
5	А4	Функціональна схема роботи системи	1	–	
6	А4	Діаграма взаємодії процесів	1	–	
7	А4	Блок-схема основної програми	1	–	
8	А4	Блок-схема роботи підпрограми	1	–	

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ 9
ВСТУП..... 10
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ 12
1.1 Призначення системи..... 12
1.2 Область застосування 13
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ 15
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти..... 15
2.2 Обґрунтування вибору засобів для побудови системи та мови програмування 28
2.3 Розгорнута постановка завдання 29
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ 31
3.1 Опис функціонування системи 31
3.2 Розробка структурної схеми..... 40
3.3 Розробка функціональної схеми 46
3.4 Розробка діаграми процесів 48
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ 50
4.1 Розробка блок-схем та опис алгоритмів функціонування системи 50
5 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ..... 70
6 НАУКОВА НОВИЗНА 74

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ 75
7.1 Вступ 75
7.2 Шкідливі і небезпечні фактори при роботі з комп’ютером 76
7.3 Розробка заходів з умов поліпшення охорони праці 77
7.4 Пожежна безпека 78
7.5 Розрахункова частина 81
8 ОСНОВНІ ВИСНОВКИ 84
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 86

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ЕОМ – електрона обчислювальна машина

ІБ – інформаційна безпека

ІТ – інформаційні технології

КС – комп’ютерна система

КТЗ – комплекс технічних засобів

МЕТОЗ – методичне забезпечення

ОС – операційна система

ОРЗ – організаційне забезпечення

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

ПП – програмний продукт

ППЗ – прикладне програмне забезпечення

ППП – пакет прикладних програм

БД – база даних

DLL – бібліотека динамічної компоновки

UEBA – User and Entity Behavior Analytics

ВСТУП

Актуальність теми. Поширення систем управління навчанням зробило масштабний збір поведінкових даних рутинним побічним продуктом онлайн-освіти, що дозволило застосовувати методи машинного навчання, зокрема кластеризацію без нагляду, для сегментації студентів та аналітики навчання [1]. Онлайн-освіта є невід'ємним компонентом сучасної вищої освіти; в епоху після пандемії моделі змішаного навчання прискорили накопичення детальних записів про взаємодію студентів, включаючи перегляд відео, подання завдань та діяльність на форумах. Програми цифрових медіа, що характеризуються своїм міждисциплінарним характером, що охоплює обробку графіки, відеовиробництво та дизайн взаємодії, генерують особливо неоднорідні поведінкові траєкторії, які звичайні агреговані метрики не можуть адекватно охопити.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

– Дослідження системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

– Програмна реалізація системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

Об’єктом дослідження є процес динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

Предметом дослідження є методи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

Методи дослідження базуються на методах машинного навчання, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

– Розроблено вітчизняний продукт динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання, який має більш широкі можливості, на відміну від існуючих аналогів.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.

Робота апробована на LVIII науково-технічній конференції здобувачів вищої освіти «Наука-виробництву», основні положення випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти надруковані у статті збірника праць молодих науковців ЦНТУ, випуск №17.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Незважаючи на значний прогрес у галузі інтелектуального аналізу освітніх даних (EDM) та аналітики навчання (LA), кілька проблем залишаються невирішеними. Традиційні методи оцінювання, що базуються на результатах іспитів та рівні відвідуваності, не відображають характеристики навчання студентів на рівні процесу [2]. Хоча підходи до машинного навчання з учителем застосовувалися для прогнозування відсіву з помітною точністю [3], виявлення шаблонів без учителя шляхом кластеризації залишається менш систематично дослідженим. Існуючі дослідження кластеризації переважно використовують окремі алгоритми, як правило, K-середні, без перехресного порівняння алгоритмів, що обмежує надійність висновків щодо оптимального методологічного вибору [4]. Інженерія ознак у сучасних дослідженнях, як правило, зосереджується на легко кількісно визначених метриках, таких як кількість входів у систему та час виконання завдання, нехтуючи при цьому показниками якості поведінки, такими як шаблони повторення відео та індекси прокрастинації [5]. Крім того, загальні результати EDM з контекстів STEM або MOOC можуть не застосовуватися до спеціалізованих творчо-технічних дисциплін, таких як цифрові медіа, де шляхи навчання за своєю суттю є нелінійними [6, 7]. Нещодавні огляди літератури підкреслюють необхідність консолідації підходів до великих даних в освіті для покращення методологічної порівнянності та практичної переносимості, що безпосередньо мотивує до більш ретельної міжалгоритмічної оцінки в цьому дослідженні [8]. Попередня робота з кластеризації поведінки навчання в курсах інформатики продемонструвала можливість профілювання на основі K-середніх, але також виявила обмеження, коли вибір алгоритму не перевіряється систематично, що підкреслює необхідність порівняльного тестування в предметно-орієнтованих контекстах

[9]. З точки зору сталості навчальної програми, аналітика навчання на основі штучного інтелекту повинна відповідати довгостроковим освітнім цілям, додатково підтримуючи інтеграцію надійних систем кластеризації в практику цифрової медіаосвіти [10].

Перехід від виявлення закономірностей на основі даних до дієвого педагогічного втручання також залишається недостатньо розробленим [8]. Хоча панелі аналітики навчання були розгорнуті в багатьох закладах, замикання циклу зворотного зв'язку між алгоритмічними висновками та практикою в класі вимагає характеристики закономірностей, специфічної для конкретної предметної області, яку загальні рамки не забезпечують [9, 10].

1.2 Область застосування

Збір та попередня обробка даних

Набір даних було зібрано з онлайн-платформи навчання в університеті та охоплює навчальні записи з вересня 2025 року по червень 2026 року (два повних семестри) за чотирма основними курсами. Досліджувана популяція складалася з 328 студентів бакалаврату; після виключення вибірок з показником відсутніх даних понад 30% для аналізу було збережено 312 дійсних вибірок.

Платформа записувала повні журнали активності, включаючи поведінку під час перегляду відео, завантаження ресурсів, записи про подання завдань, взаємодію на форумах та відповіді на тести. Відсутні значення, що виникли внаслідок вибуття з курсу посеред курсу або системних помилок, були імпутовані з використанням середніх значень на рівні курсу. Викиди в даних про тривалість навчання були виявлені за допомогою методу міжквартильного діапазону (коробчастої діаграми) та перевірені вручну. Усі ознаки були стандартизовані за допомогою нормалізації Z-оцінки (середнє значення = 0, стандартне відхилення = 1) для усунення розбіжностей шкали між вимірами.

Інженерія функцій

Виходячи з унікальних мультимодальних характеристик навчання в галузі цифрової медіаосвіти, було розроблено 18 змінних характеристик за чотирма вимірами: витрати часу, звички навчання, участь у взаємодії та результати навчання.

Змінні ознак для аналізу поведінки навчання

Вимір «Інвестиції часу» фіксує п’ять часових характеристик, що відображають кількість та послідовність залученості. Вимір «Звички навчання» кодує шість показників якості поведінки, зокрема Індекс прокрастинації (розраховується як середня нормалізована затримка здачі для всіх завдань) та Регулярність навчання (обернена величина стандартного відхилення щоденного часу входу в систему). Вимір «Взаємодія» фіксує чотири види співпраці. Вимір «Результати навчання» включає три показники академічної успішності, що використовуються для міжкластерної перевірки, а не як вхідні дані кластеризації, тим самим уникаючи витоку позначень [11].

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

2.1 Огляд існуючих систем, технологій, архітектур, програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти

Програмне забезпечення для аналізу поведінки – це категорія інструментів, які збирають дані про те, як люди взаємодіють з веб-сайтом або додатком, а потім перетворюють ці дані про поведінку користувачів на змістовні висновки, на основі яких команди можуть діяти. Ви можете використовувати його для аналізу поведінки користувачів протягом сеансів та виявлення тенденцій, перш ніж вони перетворяться на втрачений дохід.

Ключовий висновок:

– FullSession: Поєднує відтворення сеансів, теплові карти, відстеження воронки продажів, сповіщення про помилки та зворотний зв'язок в одному робочому просторі, завдяки чому команди розробників продукту та UX отримують повну картину без необхідності використовувати кілька інструментів.

– FullStory: Автоматично фіксує кожну взаємодію та дозволяє командам ретроактивно шукати дані сеансу, що підходить для великих організацій із спеціалізованим персоналом з аналітики.

– Google Analytics: Безкоштовно відстежує тенденції трафіку, залучення та конверсії, що робить його відправною точкою за замовчуванням для широкого звітування.

– Contentsquare: Розбиває сторінки на зони та поєднує їх з аналізом шляху користувача, створений для корпоративних команд, які використовують структуровані програми оптимізації коефіцієнта конверсії.

– Mixpanel: Реєструє певні дії користувачів як події, щоб команди розробників продуктів могли створювати воронки продажів, звіти про

утримання та когортний аналіз на основі точної поведінки.

FullSession вирізняється тим, що замінює кілька окремих підписок одним підключеним робочим простором.

Замість того, щоб отримувати теплову карту з одного інструменту, запис сеансу з іншого, а дані воронки продажів з третього, ваша команда працює з єдиного джерела, яке вже об'єднує ці частини.

Це означає менше часу на узгодження даних і більше часу на фактичне виправлення того, що зламано.

Збір даних у поведінковій аналітиці (і чому це важливо)

Збір даних – це основа, на якій побудовано кожен інструмент поведінкової аналітики. Без точного збору даних звіти, графіки та інформаційні панелі, що на ньому зображені, – це лише припущення, замасковані під аналітичні висновки.

Більшість платформ збирають дані двома способами:

– Кількісне відстеження враховує певні види поведінки: перегляди сторінок, кліки, надсилання форм та події конверсії.

– Якісні дані додають пояснення, чому ці цифри виникають через повтор сеансу, теплові карти та прямі відгуки користувачів.

Інструмент, який виконує лише одне з цих завдань, залишає прогалини. Традиційні інструменти аналітики сильні у підрахунку того, що сталося, але слабкі у їх поясненні. Саме для цього існують повтори сеансів та теплові карти. Ця прогалина також є причиною існування програмного забезпечення для аналітики шляху клієнта: воно об'єднує дві сторони в єдине подання.

Збір даних у режимі реального часу важливий так само, як і глибина. Якщо ваша команда може бачити лише те, що користувачі робили минулого тижня, ви завжди реагуєте із запізненням. Найкращі налаштування показують дії користувачів одразу після їх здійснення, а не через кілька днів.

Те, що збирається, зазвичай поділяється на такі категорії:

Конфіденційність користувачів та безпека даних також мають бути частиною цієї розмови. Будь-який інструмент, що збирає дані про поведінку,

повинен дозволяти маскувати конфіденційну інформацію, виключати певні елементи та дотримуватися регіональних правил конфіденційності за замовчуванням, а не як платне доповнення.

Критерії оцінювання програмного забезпечення для поведінкового аналізу

П'ять критеріїв відрізняють справді корисну програмну платформу для аналізу поведінки від панелі інструментів, яку ніхто не відкриває двічі, і те, наскільки добре вона оцінюється за кожним із них, визначає, наскільки вона насправді сприяє оптимізації продукту в майбутньому.

П'ять основних критеріїв

– Глибина збору даних. Чи фіксуються як кількісні події, так і якісний контекст, наприклад, повтор сеансу, чи лише один?

– Простота налаштування. Чи може нетехнічний член команди отримати реальний потік даних менш ніж за годину, чи існує крутий графік навчання?

– Інформація про ціни. Чи є початкова ціна публічною, чи вам потрібен дзвінок продавця лише для отримання основної інформації про ціни?

– Інтеграції. Чи добре він пов’язаний з Google Tag Manager, вашою CRM та вашими інструментами комунікації?

– Безпека даних та конфіденційність користувачів. Чи функції маскування, отримання згоди та дотримання вимог вбудовані, а не прикріплені?

Якість звітності та швидка самоперевірка

Аналіз даних та звітність також мають значення. Платформа, яка збирає багато даних, але ховає їх у захаращених інформаційних панелях, не допомагає нікому перетворити їх на практичні висновки.

Шукайте чіткі графіки та візуалізацію даних, які ваша команда фактично використовуватиме, а не лише дані, які вони можуть технічно експортувати. Якщо ваша оцінка поширюється на структуровані програми тестування, розбивка категорій інструментів CRO буде корисним наступним кроком.

Розширені функції, такі як зведені за допомогою штучного інтелекту зведення або прогнозоване підрахунок очок, звучать вражаюче, але вони мають

значення лише за умови, що ваша команда дійсно використовуватиме їх щотижня.

Швидка самоперевірка перед тим, як скласти короткий список інструментів:

– Чи може воно точно визначити зони тертя, а не лише повідомляти загальні показники?

– Чи працює це на кількох платформах (веб, мобільні пристрої та додаток)?

– Чи показує він вам конкретну поведінку, пов'язану з реальними сеансами, а не лише з середніми значеннями?

Короткий огляд порівняння найкращого програмного забезпечення для поведінкової аналітики

Вам не потрібно читати п’ять веб-сайтів постачальників, щоб зрозуміти основи. У цьому розділі порівнюються FullSession, FullStory, Google Analytics, Contentsquare та Mixpanel.

Кожен із цих п’яти інструментів використовує різний підхід до однієї й тієї ж проблеми: перетворення сирої поведінки користувачів на щось, над чим ваша команда може реально вдіяти.

FullSession

FullSession поєднує відтворення сеансів, теплові карти, відстеження воронки продажів, збір відгуків та сповіщення про помилки в одному робочому просторі, замість того, щоб розподіляти їх по окремих інструментах.

Команди розробників продукту та UX отримують повну картину шляху користувача, від цільової сторінки до точного кліку, за яким він перейшов на сайт. Їм ніколи не доводиться перемикатися між платформами чи експортувати дані між системами.

Платформа фіксує кожну взаємодію користувача в режимі реального часу та реконструює її як сеанс, який можна переглянути, нашаровуючи дані теплової карти та воронки продажів, отримані з тих самих подій.

Це означає, що ви можете відстежити клік гніву, позначений на тепловій

карті, безпосередньо до запису, який показує причину його виникнення. Для глибшого розуміння того, як це працює, інструменти запису та запису сеансу, а також інструменти теплової карти веб-сайту розбирають кожен елемент окремо.

Найкраще для:

Команди розробки продукту та UX, яким потрібні записи сеансів, теплові карти та дані про конверсії в одному місці, а не об'єднання трьох окремих підписок.

Ключові характеристики:

– Повтор сеансу: Перегляньте реальні сеанси користувачів, щоб точно побачити, де виникають проблеми, клік за кліком.

– Теплові карти: Візуалізуйте місця, де користувачі натискають, прокручують та наводять курсор на будь-яку сторінку, щоб побачити закономірності взаємодії, які ви інакше пропустили б.

– Зворотній зв'язок: Збір контекстних відгуків користувачів, безпосередньо пов'язаних із сеансом, з якого вони виникли.

– Відстеження воронки продажів: Визначте точний крок, на якому користувачі виходять з процесу реєстрації або оформлення замовлення.

– Відстеження помилок: отримуйте сповіщення про помилки JavaScript та пошкоджені елементи, щойно вони впливають на реального користувача.

– Мобільний повтор: Розширте видимість на рівні сеансу на ваш мобільний додаток, а не лише на ваш вебсайт.

– Lift AI: Отримайте рекомендації щодо виправлення, відсортовані за впливом на дохід, а потім перевірте, чи справді кожне з них спрацювало.

– Безпека та захист: вбудовані засоби маскування даних та контролю конфіденційності захищають конфіденційність користувачів за замовчуванням, а не як додатковий товар.

– Сервер MCP: підключайте дані FullSession безпосередньо до робочих процесів штучного інтелекту та інших інструментів, які ваша команда вже використовує.

Ціноутворення:

FullSession пропонує безкоштовний план назавжди, а платні плани починаються від 39 доларів США на місяць (рахунок стягується щорічно) для рівня Growth. Він також включає корпоративні тарифи, які починаються від 500 тисяч сеансів на місяць.

FullStory

FullStory позиціонує себе як ретроактивний пошук, дозволяючи командам запитувати дані сеансу постфактум, не вирішуючи заздалегідь, які події відстежувати. Це подобається великим організаціям зі спеціалізованими аналітичними командами, які хочуть вільно досліджувати дані про поведінку, а не працювати з попередньо встановленими інформаційними панелями.

Платформа автоматично фіксує взаємодії на сайті або в додатку, а потім індексує їх для пошуку. Будь-який член команди може знайти певні моделі поведінки, наприклад, кожного користувача, який натиснув кнопку оформлення замовлення, без попереднього написання запиту.

Найкраще для:

Корпоративні команди зі спеціалізованим аналітичним персоналом, яким потрібно гнучко досліджувати дані сеансів у великих та складних продуктах.

Ключові характеристики:

– Автоматичне захоплення: автоматично записує кожну взаємодію, тому нічого не потрібно позначати заздалегідь.

– Пошук сеансів: запитуйте історичні сеанси за певними поведінковими параметрами або подіями після того, як вони вже відбулися.

– Воронки продажів та шляхи: відстежуйте, як користувачі рухаються багатоетапними потоками в продукті.

– Сегментація: групування користувачів за поведінкою, пристроєм або спеціальними атрибутами для цільового аналізу.

– Зведення StoryAI: Отримуйте автоматизовані, згенеровані штучним інтелектом зведення активності сеансів у великих масштабах.

Ціноутворення:

FullStory пропонує безкоштовний план із 30 000 сеансів на місяць, а також платні рівні Business, Advanced та Enterprise, ціна яких залежить від цінової пропозиції.

Google Analytics

Google Analytics безкоштовно відстежує джерела трафіку, залучення користувачів та поведінку на сайті, що робить його найпоширенішою відправною точкою для збору поведінкових даних в Інтернеті.

Він зосереджується на сукупних закономірностях, таких як звідки приходять відвідувачі та які сторінки вони переглядають, а не на записі окремих сеансів. Ці дані зазвичай безпосередньо враховуються в ширших маркетингових стратегіях, від атрибуції кампаній до бюджетування каналів.

Це працює шляхом розміщення фрагмента відстеження, який часто розгортається через Менеджер тегів Google. Цей фрагмент реєструє перегляди сторінок, події та конверсії у звітах, які команди можуть аналізувати за каналом, пристроєм або сегментом аудиторії.

Якщо сама платформа не покриває ваших потреб, посібник з альтернативами Google Analytics порівнює варіанти, створені для глибшого аналізу поведінки.

Найкраще для:

Команди, яким потрібні широкі, безкоштовні звіти про тенденції трафіку, залучення та конверсії на веб-сайті або в додатку.

Ключові характеристики:

– Відстеження подій: відстежуйте певні дії користувачів, такі як кліки, відтворення відео або надсилання форм.

– Звітування про аудиторію: дивіться, звідки походять користувачі та як поводяться різні сегменти.

– Відстеження конверсій: Вимірюйте ефективність певних цілей, таких як реєстрації чи покупки.

– Інтеграція з Google Tag Manager: розгортання та керування тегами відстеження без зміни коду сайту.

Ціноутворення:

Google Analytics безкоштовний для стандартного використання. Analytics 360, корпоративний рівень, доступний через Google Marketing Platform. Його вартість починається приблизно від 50 000 доларів США на рік.

Contentsquare

Contentsquare зосереджується на структурованих програмах оптимізації коефіцієнта конверсії для великих організацій, поєднуючи теплові карти на основі зон з аналізом подорожі клієнтів у веб- та мобільних додатках.

Він створений для корпоративних команд CRO, які проводять програми постійного тестування, а не для менших команд, які шукають швидкого налаштування.

Платформа розбиває сторінки на зони та відстежує залученість на цьому рівні. Потім вона накладає на них дані про повтор сеансу та шлях користувача, щоб команди могли точно визначити області тертя, які стимулюють або блокують конверсії.

Найкраще для:

Великі підприємства, що використовують структуровані, постійні програми оптимізації коефіцієнта конверсії зі спеціалізованим персоналом з управління конверсією.

Ключові характеристики:

– Теплові карти на основі зон: переглядайте взаємодію, розподілену за певними зонами сторінки, а не лише за кількістю необроблених кліків.

– Аналіз подорожі: відображайте шляхи, якими користувачі користуються під час кількох сеансів та на різних пристроях.

– Повтор сеансу: перегляд записаних сеансів, пов'язаних з певними зонами або подіями.

– Кількісна оцінка впливу: Оцініть вплив на дохід певних точок тертя та підвищення конверсій.

– Аналітика мерчандайзингу: аналіз ефективності на рівні продукту для каталогів електронної комерції.

Ціноутворення:

Contentsquare пропонує безкоштовну пробну версію, а платні плани починаються від 49 доларів на місяць та пропонують 7 тисяч сеансів щомісяця.

Mixpanel

Mixpanel відстежує конкретні дії користувачів як події, а потім дозволяє командам створювати воронки продажів, криві утримання та когортні звіти на основі даних про ці події. Це підходить для команд розробників продуктів, які менше дбають про спостереження за окремими сесіями та більше про вимірювання певної поведінки в масштабі, як-от рівень впровадження функцій або рівень завершення оформлення замовлення.

Mixpanel реєструє кожну дію користувача як окрему подію, пов’язану з профілем цього користувача. Потім команди можуть створювати звіти, які відстежують поведінку людини протягом кількох сеансів та пристроїв з плином часу.

Якщо ви вже переросли це або хочете іншого підходу, посібник з альтернатив Mixpanel порівнює інструменти, побудовані на основі тієї ж моделі відстеження подій.

Найкраще для:

Команди розробників продуктів, яким потрібно відстежувати певні дії користувачів та аналізувати воронки продажів за визначеним набором подій.

Ключові характеристики:

– Відстеження подій: реєстрація певних дій користувачів як структурованих подій з можливістю запиту.

– Аналіз воронки продажів: Вимірювання коефіцієнтів конверсії між будь-якими двома кроками у визначеному потоці.

– Звіти про утримання: дивіться, скільки користувачів повертаються після певної дії або періоду часу.

– Когортний аналіз: групування користувачів за спільною поведінкою або атрибутами для порівняння.

– A/B-тестовий аналіз: вимірюйте вплив експериментів безпосередньо на

поведінкові дані.

Ціноутворення:

Mixpanel пропонує безкоштовний план для команд, які відстежують до 1 мільйона подій щомісяця, а платні плани починаються від 140 доларів на місяць або 0,28 долара за 1000 подій.

Як вибрати правильне програмне забезпечення для поведінкового аналізу

Почніть із найбільшої сліпої зони вашої команди, а не з найдовшого списку функцій. Команда, яка тоне в квитках на кшталт «щось зламалося на касі», потребує відтворення сеансу та відстеження помилок більше, ніж ще однієї панелі інструментів.

Перш ніж використовувати будь-який інструмент, задайте собі три питання, оскільки цей крок прийняття рішення легко зробити поспіхом:

– Яку конкретну поведінку ви намагаєтеся зрозуміти?

– Хто з вашої команди насправді використовуватиме це щодня?

– Який ваш реальний бюджет після переходу на безкоштовний рівень, включаючи будь-які витрати на корпоративний план у майбутньому?

– Який інструмент підходить вашій команді?

Зверніть увагу на кілька поширених проблемних моментів, перш ніж підписувати контракт. Нечітке Ціноутворення: до розмови з відділом продажів, крута крива навчання для нетехнічного персоналу та функції, які здаються просунутими, але приховані за вищим рівнем вартості, – все це тривожні сигнали. Жоден з них сам по собі не є вирішальним фактором, але поєднання двох або трьох разом зазвичай сигналізує про високу вартість володіння в майбутньому.

Чому варто обрати FullSession

Більшість команд зрештою поєднують чотири чи п’ять інструментів, щоб зрозуміти власний продукт: один для повторів, інший для теплових карт, третій для воронок продажів і поштову скриньку підтримки, яка ніколи не спілкується з жодним із них. FullSession існує для того, щоб ви перестали це робити.

Від «Щось не так» до «Ось чому»

Теплова карта позначає місця, де користувачі вагаються або клацають на сторінці в люті. Замість того, щоб залишати вас здогадуватися чому, ця ж аномалія безпосередньо пов’язана зі записом сеансу, який показує точний момент, коли щось пішло не так, аж до кліку.

Відстеження воронки продажів показує, чи ці труднощі призводять до масової втрати конверсій, чи просто дратують кількох користувачів. Відстеження помилок враховує технічну сторону тієї ж історії, попереджаючи вашу команду в той момент, коли помилка стикається з реальним відвідувачем, замість того, щоб чекати на запит у службу підтримки через кілька днів.

А коли користувач залишає відгук, він безпосередньо пов’язаний з його сеансом. Ви читаєте коментар поруч із саме тим досвідом, який його спонукав, а не здогадуєтесь про задоволеність користувачів на основі оцінки опитування.

Щоб детальніше ознайомитися з тим, як працює цей цикл зворотного зв'язку, посібник з інструментів збору відгуків клієнтів розглядає його детальніше.

Менше ручної перевірки, більше пріоритетів

Lift AI йде ще далі, виконуючи пріоритезацію за вас. Замість того, щоб ваша команда вручну переглядала сесії, щоб визначити, що варто виправити, він ранжує проблеми за впливом на дохід, а потім повідомляє вам, чи справді виправлення спрацювало після того, як ви його відправили.

Мобільне відтворення розширює таку ж видимість для вашого додатка, тож ви не будете сліпі на одній платформі, водночас повністю захищені на іншій. А оскільки все відбувається через вбудоване маскування даних та засоби контролю конфіденційності, нічого з цього не відбувається за рахунок конфіденційності користувачів, забезпечуючи дотримання вимог без додаткових зусиль з боку вашої команди.

Що ви насправді отримуєте

– Одне підключене робоче середовище замість чотирьох розрізнених інструментів для узгодження.

– Налаштовувані робочі процеси, які оптимізують робочі процеси між командами підтримки, продукту та маркетингу, замість того, щоб змушувати всіх працювати в рамках одного жорсткого процесу.

– Прямий доступ до ваших існуючих робочих процесів зі штучним інтелектом: сервер MCP надає вам прямий доступ до даних FullSession, замість експорту та повторного імпорту між системами.

– Індивідуальне Ціноутворення: для корпоративних команд з більшим обсягом робіт або специфічними вимогами, щоб вам не довелося вибирати між занадто малим планом та надто складним.

Подивіться на реальні сесії, яких бракує вашій поточній аналітиці

Дивіться реальні сесії та отримуйте підтверджені доказами рішення за лічені хвилини, а не за короткий проміжок часу.

Інтеграції з Google Analytics та операційними системами

Інструменти аналітики поведінки рідко працюють окремо. Більшість команд використовують їх разом із Google Analytics та підключають обидва до решти свого стеку через Google Tag Manager.

Цей інтеграційний рівень зазвичай охоплює кілька поширених категорій:

– Керування тегами: Розгортання фрагментів відстеження через Google Tag Manager без редагування коду сайту для кожної зміни.

– Інструменти комунікації: надсилання сповіщень про сеанси у Slack, електронну пошту або на платформи підтримки, які ваша команда вже використовує щодня.

– Сховища даних: експорт необроблених даних про події до кількох джерел або систем для команд, які хочуть створювати власні звіти в іншому місці.

Ніщо з цього не замінює Google Analytics. Воно працює поряд з ним, додаючи якісне «чому», яке самі лише звіти про трафік не можуть показати, і допомагаючи командам випереджати проблеми, а не реагувати на них через тижні.

Методологія тестування та дослідницькі нотатки

Усі дані про ціни та характеристики в цьому розділі взяті безпосередньо з офіційного веб-сайту та сторінки з цінами кожного постачальника. Ми перевірили кожну з них на момент публікації, а не зі сторонніх сайтів оцінок чи агрегаторів.

Рейтинги G2, на які посилаються в таблиці порівняння, відображають публічно опубліковані оцінки на власній платформі G2. Ціни на плани на основі використання або корпоративні плани можуть змінюватися залежно від обсягу та умов контракту. Розглядайте наведені тут цифри як відправну точку для власної розмови з кожним постачальником, а не як остаточну цінову пропозицію.

Висновок щодо програмного забезпечення для поведінкового аналізу

Кожен інструмент у цьому списку вирішує реальну проблему, але не одну й ту саму. FullSession, FullStory, Google Analytics, Contentsquare та Mixpanel зосереджуються на різних аспектах поведінки користувачів, від загальної звітності про трафік до глибокої деталізації на рівні сеансу.

Вибирайте залежно від того, з чим ваша команда має проблеми сьогодні, чи то швидка діагностика помилок, чи то прагнення збільшити конверсії:

– Швидка діагностика помилок та тертя: FullSession або Contentsquare.

– Гнучке дослідження великих обсягів даних сеансів: FullStory.

– Відстеження певних дій та подій користувачів: Mixpanel.

– Безкоштовна, широка звітність про трафік: Google Analytics.

Якщо ваша команда ще не визначилася, FullSession – це чудовий початок. Він об’єднує повтор сеансу, теплові карти, відстеження воронки продажів, сповіщення про помилки та зворотний зв’язок в одному робочому просторі за нижчою початковою ціною, ніж більшість варіантів, орієнтованих на підприємства, у цьому списку, тому ви не платите за потужність чи робочі місця, які вам ще не потрібні.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Мова програмування та архітектурний фреймворк

Для реалізації серверної частини програмного комплексу динамічного профілювання поведінки користувачів було використано мову програмування PHP (Hypertext Preprocessor) спільно з високопродуктивним веб-фреймворком Yii2. PHP є однією з найпоширеніших інтерпретованих мов веб-розробки, що забезпечує генерацію динамічного контенту на стороні сервера та ефективну взаємодію з реляційними базами даних, де зберігаються параметри поведінкових профілів і результати кластеризації.

Фреймворк Yii2 реалізує архітектурний шаблон MVC (Model-View-Controller – Модель-Вид-Контролер), який забезпечує чітке розмежування відповідальності у проєкті:

– Модель (Model): відповідає за бізнес-логіку, структурування даних користувачів та правила перевірки вхідної сесійної інформації.

– Вид (View): інкапсулює інтерфейс користувача та компоненти візуалізації (аналітичні панелі, графіки поведінкових метрик).

– Контролер (Controller): здійснює координацію між запитами користувача, обробкою подій та викликом алгоритмів аналізу даних.

Використання фреймворку Yii2 обумовлено його швидкою обробкою запитів, підтримкою механізмів кешування, інтеграцією інтерфейсів DAO/Active Record для роботи з базами даних, а також наявністю вбудованих засобів перехоплення помилок і валідації веб-форм, що є критично важливим для надійних веб-систем із великим потоком трафіку.

Середовище розробки

Як інтегроване середовище для розробки програмного забезпечення було обрано JetBrains PhpStorm – кросплатформову IDE, створену на базі платформи IntelliJ IDEA.

PhpStorm забезпечує високу ефективність завдяки розвиненим засобам

інтелектуального редагування коду, підтримці стандартів кодування, аналізу помилок на льоту, вбудованим інструментам рефакторингу, повноцінному SQL-редактору для взаємодії з базами даних та вбудованій підтримці архітектури MVC для фреймворку Yii2. Це дозволяє забезпечити високу якість коду та швидкість розробки аналітичних модулів системи профілювання.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускну кваліфікаційну роботу за другим (магістерським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

В процесі розробки випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти необхідно виконати наступний обсяг роботи:

а) провести аналіз існуючих систем-аналогів для виявлення їх позитивних і негативних якостей. Результати аналізу врахувати в подальших розробках;

б) вибрати та обґрунтувати методику побудови системи контролю роботи технологічного обладнання на виробництві в автоматизованому режимі. Розробити функціональну та структурну схеми системи;

в) розробити програмне забезпечення системи, що дозволить реалізувати поставлену технічним завданням задачу. Побудувати блок-схеми алгоритмів програми та підпрограми;

г) організувати інтерфейс користувача з метою формування та виводу на екран ЕОМ повідомлень про некоректні дії користувача та нестандартні ситуації в роботі технологічного обладнання;

д) розробити рекомендації по організаційних та методичних заходах, які забезпечать впровадження системи в промислову експлуатацію та її подальшу успішну експлуатацію;

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

ж) розробити заходи по охороні праці при впровадженні та експлуатації системи, а також розробити заходи з цивільного захисту;

з) сформувати висновки про виконаний обсяг робіт та одержані результати.

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

В останні роки кібератаки на освітні онлайн-ресурси стали більш витонченими та поширеними, створюючи величезний ризик для підприємств у всьому світі. Експоненціальне зростання цифрової трансформації в поєднанні зі зростаючою складністю сучасних інфраструктур посилило небезпеки, що виникають від зловмисних кібероперацій. Традиційні технології кібербезпеки, такі як системи виявлення на основі правил та методи на основі сигнатур, дедалі менше допомагають протидіяти загрозам, що розвиваються. Ці системи не виявляють ледь помітні, складні та динамічні вектори атак, особливо в контекстах, які потребують аналізу в режимі реального часу та адаптивного реагування.

Однією з найкритичніших труднощів у сучасній кібербезпеці є внутрішні загрози, які часто залишаються непоміченими типовими процедурами безпеки. Внутрішні загрози, що стосуються зловмисних або недбалих, деструктивних або шкідливих дій співробітників або довірених осіб, викликають велике занепокоєння, оскільки вони використовують дозволений доступ до систем і можуть завдати значної шкоди. Недавні дослідження показують, що внутрішні загрози становлять значний відсоток усіх інцидентів у сфері кібербезпеки, маючи потенційно катастрофічні фінансові та операційні наслідки. У 2025 році інциденти, пов'язані з інсайдерами, призвели до середніх витрат у розмірі 15,38 мільйона доларів США на кожне порушення. Це підкреслює необхідність більш складних методів виявлення, які можуть виявляти аномалії, що свідчать про зловмисні наміри або ненавмисну недбалість.

Поява аналітики поведінки користувачів та сутностей (UEBA) забезпечила багатообіцяюче рішення цієї дилеми. Системи UEBA використовують передові моделі машинного навчання для аналізу величезних

обсягів даних про поведінку, встановлення базових рівнів «нормальної» активності та звітування про відхилення, які можуть виявити можливі загрози. Однак типові системи UEBA зазвичай мають труднощі з фіксацією тонкої та динамічної природи поведінки користувачів, особливо в ситуаціях, коли користувачі демонструють різні моделі активності залежно від своїх обов'язків, діяльності та обов'язків.

Щоб усунути ці обмеження, у нещодавніх роботах досліджувалася інтеграція моделей глибокого навчання, зокрема рекурентних нейронних мереж (RNN), таких як LSTM та Gated Recurrent Units (GRU), у структури UEBA. Ці моделі добре підходять для послідовного аналізу даних, що дозволяє їм фіксувати часові тенденції та довгострокові залежності в поведінці користувачів з плином часу. Таким чином, моделі на основі RNN можуть краще виявляти незначні порушення, які можуть бути неочевидними в короткострокових вибірках даних. Однак залишається проблема забезпечення точності та інтерпретованості цих моделей, особливо при розгортанні у виробничих контекстах, де вартість хибнопозитивних та хибнонегативних результатів є значною.

Окрім рекурентних нейронних мереж (RNN), нещодавні розробки в механізмах уваги показали величезний потенціал для підвищення продуктивності систем UEBA. Механізми уваги дозволяють моделям зосереджуватися на найважливіших частинах вхідних даних, підвищуючи їхню здатність фіксувати важливі елементи послідовної поведінки. Інтегруючи механізми уваги в архітектури RNN, такі як моделі LSTM на основі уваги, дослідники продемонстрували покращення точності виявлення та інтерпретованості, що робить ці моделі більш придатними для реальних застосувань у кібербезпеці.

Ще однією важливою особливістю сучасної кібербезпеки є необхідність контекстно-залежного профілювання ризиків та мікросегментації користувачів. Традиційні моделі ризиків часто спираються на статичні, рольові оцінки, які не враховують динамічний та унікальний характер активності користувачів.

Включення контекстної інформації, такої як місцезнаходження користувача, час активності та використання пристроїв, до оцінок ризиків може значно підвищити точність виявлення загроз. Крім того, мікросегментація користувачів допомагає компаніям розробляти більш детальні профілі користувачів, підвищуючи здатність виявляти аномальну поведінку на індивідуальному рівні.

Стандарт ISO/IEC 27001:2022 забезпечує комплексну основу для управління ризиками інформаційної безпеки, підкреслюючи необхідність проактивного виявлення загроз та реагування на них. Управління кібербезпекою підприємства: Огляд ISO/IEC 27001:2022. Міжнародна конференція з кіберменеджменту та інженерії (CyMaEn). Цей підхід підкреслює необхідність систем, які можуть динамічно адаптуватися до змінних ризиків, використовуючи аналітичні дані для покращення прийняття рішень та заходів щодо пом'якшення наслідків. Використання автоматизованих втручань на основі профілів користувачів у режимі реального часу є значним кроком до досягнення цієї мети. Завдяки впровадженню передових моделей машинного навчання, таких як механізми уваги та архітектури глибокого навчання, компанії можуть проактивно передбачати та зменшувати ризики, перш ніж вони призведуть до серйозної шкоди.

Оскільки підприємства швидко використовують хмарні обчислення, периферійні обчислення та Інтернет речей (IoT), прогнозується зростання складності середовищ кіберзагроз. Новітні технології, такі як генеративно-змагальні мережі (GAN) та навчання з підкріпленням (RL), здатні суттєво покращити системи виявлення аномалій, дозволяючи їм постійно навчатися та адаптуватися до нових загроз. Ці досягнення визначають майбутнє кібербезпеки, відходячи від статичних, реактивних систем до динамічних, проактивних та інтелектуальних механізмів захисту.

Кібербезпека значно еволюціонувала протягом останніх кількох десятиліть у відповідь на дедалі складніші кіберзагрози та зростаючу залежність від цифрових інфраструктур. Ранні механізми кібербезпеки в основному спиралися на виявлення на основі сигнатур, брандмауери, антивірусне

програмне забезпечення та системи виявлення вторгнень (IDS), які працювали з використанням заздалегідь визначених правил та відомих сигнатур загроз для виявлення шкідливої діяльності. Хоча ці підходи були ефективними проти відомих атак, їм було важко адаптуватися до нових та раніше невидимих загроз у швидкозмінному кіберландшафті.

Це являло собою зміну в бік більш проактивного підходу до кібербезпеки, оскільки традиційні системи, засновані на правилах, були недостатніми для виявлення цих загроз, що розвиваються. Розширення взаємопов'язаних систем, хмарних обчислень та Інтернету речей ще більше збільшило складність проблем кібербезпеки, тоді як поява APT, експлойтів нульового дня, атак програм-вимагачів та кампаній кібершпигунства викрила обмеження традиційних засобів захисту на основі правил. Як наслідок, дослідники почали досліджувати більш адаптивні та засновані на даних підходи, здатні виявляти невідомі загрози шляхом виявлення аномалій та поведінкового аналізу8 Цей зсув був додатково підтриманий досягненнями в галузі штучного інтелекту та глибокого навчання, включаючи розробку мереж LSTM для послідовного аналізу даних. Початок 2010-х років ознаменувався значною трансформацією в кібербезпеці з впровадженням систем машинного навчання, глибокого навчання та UEBA. Алгоритми машинного навчання, такі як дерева рішень, SVM та ансамблеві методи, дозволили системам безпеки вивчати закономірності з великих наборів даних та виявляти раніше невідомі моделі поведінки атак, тим самим підтримуючи більш проактивні стратегії безпеки.

Одночасно, UEBA виникла як поведінково-орієнтований підхід, який встановлює базові профілі користувачів та сутностей для виявлення відхилень, що свідчать про внутрішні загрози або зловмисну діяльність. Досягнення в глибокому навчанні ще більше розширили можливості кібербезпеки завдяки таким архітектурам, як згорткові нейронні мережі (CNN), механізми уваги, гібридні моделі LSTM на основі уваги та навчання з підкріпленням (RL), що покращило вилучення ознак, контекстне розуміння, виявлення аномалій та адаптивне реагування на загрози.16–20 Зовсім недавно кібербезпека змістилася в

бік проактивних та ризик-орієнтованих підходів, які наголошують на контекстній обізнаності, персоналізованому профілюванні ризиків, мікросегментації користувачів, моніторингу в режимі реального часу та автоматизованих механізмах втручання. Ці розробки тісно узгоджуються з принципами ISO/IEC 27001:2022, який сприяє постійному вдосконаленню, адаптивному управлінню ризиками, стійкості та інтелектуальним засобам контролю безпеки, здатним реагувати на кіберзагрози, що розвиваються.

Внутрішні загрози та аналітика поведінки користувачів і організацій

Внутрішні загрози стали однією з найзначніших проблем кібербезпеки, з якими стикаються сучасні організації, через унікальні права доступу та організаційні знання, якими володіють співробітники, підрядники, постачальники та інші уповноважені користувачі. На відміну від зовнішніх зловмисників, інсайдери працюють у довірених середовищах і часто мають законний доступ до критично важливих систем, мереж та конфіденційної інформації, що ускладнює виявлення та пом'якшення їхньої діяльності. Інсайдерські інциденти можуть призвести до значних фінансових втрат, крадіжки інтелектуальної власності, операційних збоїв, шкоди репутації та проблем із безперервністю бізнесу.

Відповідно, організації дедалі частіше визнають внутрішні загрози як серйозний ризик, що вимагає постійного моніторингу, поведінкового аналізу та проактивних стратегій пом'якшення наслідків. Внутрішні загрози зазвичай класифікуються як ненавмисні або навмисні. Ненавмисні внутрішні загрози виникають через недбалість, людську помилку або недотримання встановлених процедур безпеки. Прикладами є втрата пристроїв, що містять конфіденційну інформацію, перехід за шкідливими посиланнями, неправильне налаштування систем або ненавмисне розголошення конфіденційних даних.

Однак навмисні внутрішні загрози включають навмисні дії, спрямовані на завдання шкоди організації з особистих, фінансових, ідеологічних або репресивних причин. Ці загрози, внутрішні чи зовнішні, Зловмисники-інсайдери часто володіють широкими знаннями про організаційні системи, засоби

контролю безпеки та операційні процедури, що дозволяє їм уникати виявлення, використовуючи свій авторизований доступ. Організації також повинні боротися зі змовними внутрішніми загрозами, коли інсайдери співпрацюють із зовнішніми зловмисниками, а також зі загрозами третіх сторін, що стосуються підрядників, постачальників або ділових партнерів, які мають доступ до ресурсів організації. Фінансові та операційні наслідки інсайдерських інцидентів можуть бути серйозними. Нещодавні галузеві звіти свідчать про те, що інциденти, пов'язані з інсайдерами, продовжують спричиняти суттєві витрати для організацій через витоки даних, крадіжку інтелектуальної власності, перебої в обслуговуванні, заходи з реагування на інциденти, регуляторні штрафи та репутаційну шкоду. Окрім прямих фінансових втрат, організації часто несуть значні витрати на відновлення, пов'язані з судово-медичними розслідуваннями, відновленням систем, юридичними зобов'язаннями та відновленням довіри зацікавлених сторін. Оскільки організації стають дедалі цифровішими та взаємопов'язаними, складність та потенційний вплив внутрішніх загроз продовжують зростати, що підсилює потребу в більш інтелектуальних та адаптивних механізмах безпеки. Одним з найперспективніших підходів до пом'якшення внутрішніх загроз є інтеграція UEBA в ширші програми кібербезпеки та управління внутрішніми загрозами. UEBA використовує машинне навчання, поведінкову аналітику та методи виявлення аномалій для встановлення базових моделей поведінки користувачів та об'єктів, а також виявлення відхилень, які можуть свідчити про зловмисну діяльність або порушення політик. Завдяки постійному моніторингу взаємодії користувачів, моделей доступу, системної активності та переміщення даних, системи UEBA можуть виявляти підозрілу поведінку, таку як спроби несанкціонованого доступу, незвичне використання привілеїв, аномальні передачі даних та потенційні витоки даних. У поєднанні з моніторингом у режимі реального часу, прогнозною аналітикою та засобами контролю безпеки організації UEBA підвищує здатність організації виявляти нові загрози, підтримувати проактивне управління ризиками та зміцнювати загальну стійкість кібербезпеки.

Огляд нейронних мереж та глибокого навчання

Здатність виявляти та пом'якшувати внутрішні загрози стала першочерговим завданням для організацій. Традиційні заходи безпеки, такі як виявлення на основі сигнатур та системи на основі правил, дедалі більше виявляються неадекватними для виявлення складної та динамічної природи нових кіберзагроз. Методи штучного інтелекту, зокрема машинне навчання (ML) та навчання з навчання (DL), набули популярності завдяки проактивному вирішенню цих проблем шляхом навчання та адаптації до аномальних моделей поведінки в режимі реального часу. Для виявлення аномалій у поведінці користувачів, особливо в контексті виявлення внутрішніх загроз, було застосовано кілька традиційних алгоритмів машинного навчання. Ці методи аналізують історичні дані, щоб встановити базовий рівень нормальної активності, а відхилення від цього базового рівня позначаються як потенційні загрози. Деякі з найбільш широко використовуваних традиційних алгоритмів машинного навчання:

Випадкові ліси (RF) – це метод ансамблевого навчання, який поєднує кілька дерев рішень для підвищення продуктивності класифікації. Вони чудово справляються з обробкою великих, зашумлених наборів даних, що робить їх особливо корисними для виявлення внутрішніх загроз. Алгоритм може аналізувати різноманітні ознаки та ефективно позначати аномалії. Однак одним із обмежень є відсутність інтерпретованості, що є критично важливим у кібербезпеці, оскільки аналітики повинні розуміти, чому певні моделі поведінки позначаються як аномальні. Метод опорних векторів (SVM) – потужний класифікатор, який добре працює для високовимірних даних. При виявленні внутрішніх загроз SVM можуть виявляти складні межі, що розділяють нормальну та аномальну діяльність. Вони широко використовуються в застосунках, де існує чіткий контраст між звичайними та шкідливими операціями. Однак SVM потребують значної кількості маркованих даних і можуть мати проблеми з незбалансованими наборами даних, де зловмисна діяльність трапляється значно рідше, ніж звичайна поведінка.

K-найближчі сусіди (KNN) – це базовий, простий метод, який класифікує елементи даних на основі їхньої близькості до інших. У кібербезпеці він може виявляти аномальну поведінку користувачів, порівнюючи дії окремої особи з діями порівнянних користувачів. Хоча KNN простий у побудові, він має проблеми з обчислювальною ефективністю при роботі з величезними наборами даних, а міра відстані може не завжди фіксувати складні поведінкові взаємодії.

Нейронні мережі (НМ): Нейронні мережі – це алгоритми машинного навчання, засновані на людському мозку, що складаються з взаємопов'язаних нейронів, які обробляють та інтерпретують дані. Ці нейрони структуровані за шарами: вхідний шар приймає необроблені дані, приховані шари виконують складні обчислення, а вихідний шар генерує кінцевий результат. Нейронні мережі успішно виконують такі завдання, як ідентифікація аудіо/зображень, обробка природної мови та прийняття рішень.

У 1950-х–1960-х роках Френк Розенблатт винайшов перцептрон, різновид штучного нейрона, який аналізує двійкові входи. Перцептрон видає 1 або 0 на основі порогового значення, що застосовується до суми зважених входів. Хоча перцептрони корисні для лінійно роздільних даних, вони обмежені у виконанні складніших завдань. Щоб вирішити цю проблему, у 1980-х роках були винайдені сигмоїдні нейрони, які дозволяють видавати вихідні значення від 0 до 1. Це допомагає їм моделювати складніші шаблони. Вихід обчислюється шляхом пропускання зваженої суми входів через сигмоїдну функцію.

Навчання сигмоподібних нейронів використовує градієнтний спуск, який коригує ваги для мінімізації похибки між очікуваним і фактичним результатом. Нейронні мережі, особливо з сигмоподібними нейронами, стали вирішальними в глибокому навчанні. У нейронних мережах нейрони групуються в шари, кожен з яких виконує перетворення вхідних даних для вилучення відповідної інформації. Кінцевий результат створюється за допомогою функції активації, яка вносить нелінійність у модель, дозволяючи їй фіксувати складні кореляції в даних.

Пряма нейронна мережа (ПМП) – один із найпростіших типів нейронних мереж, у якому дані передаються від вхідного шару через приховані шари до

вихідного. Нейронні шари використовують зважені суми та функції активації для перетворення вхідних даних.

Зворотне поширення помилки – це основний алгоритм, який використовується для навчання нейронних мереж та усунення помилок шляхом зміни ваг. Він складається з двох основних фаз: прямого проходу та зворотного проходу. Під час прямого проходу мережа обчислює свій вихідний сигнал, тоді як під час зворотного проходу для обчислення градієнтів помилок з урахуванням ваг використовується ланцюгове правило диференціювання. Ці градієнти потім використовуються для коригування ваг, спрямовуючи мережу на досягнення меншої помилки. Помилка на вихідному шарі зазвичай вимірюється за допомогою функції втрат середньоквадратичної помилки (MSE):

Архітектура нейронної мережі

Архітектура нейронної мережі зазвичай складається з трьох типів шарів: вхідного шару, прихованих шарів та вихідного шару. Вхідний шар отримує необроблені дані та передає їх прихованим шарам, де дані зазнають складних перетворень. Нарешті, вихідний шар створює результат прогнозування або класифікації мережі. Оскільки нейрони в середньому шарі не є ні входами, ні виходами, це називається прихованим шаром. Деякі мережі містять більше прихованих шарів, ніж мережа яка має лише один.

Глибокі нейронні мережі (ГНМ)

ГНН (глибинні нейронні мережі) – це клас нейронних мереж, що містять кілька шарів нейронів, що дозволяє їм навчатися та моделювати дуже складні закономірності в даних. На відміну від поверхневих нейронних мереж, які складаються лише з одного або двох шарів, ГНН містять кілька прихованих шарів між вхідним та вихідним шарами, що дає їм можливість фіксувати складні зв'язки у великих наборах даних. Кожен шар у ГНН складається з нейронів, які обчислюють, використовуючи свої вхідні дані, ваги та функції активації. Здатність мережі вивчати глибокі представлення даних дозволяє їй виконувати складніші завдання, такі як ідентифікація зображень, обробка природної мови та розпізнавання мовлення. ГНН значною мірою покладаються на алгоритм

зворотного поширення для навчання, який коригує ваги на основі різниці між очікуваними та істинними виходами. ГНН зазвичай складається з вхідного шару, одного або кількох прихованих шарів та вихідного шару, причому вхідний шар отримує необроблені дані, а кожен прихований шар поступово навчається абстракціям даних вищого рівня. Вихідний шар створює кінцевий результат прогнозування або класифікації, де ? позначає кількість шарів. Кожен прихований шар збирає ознаки вищого рівня.

Для оптимізації глибоких нейронних мереж (DNN) використовується безліч стратегій, включаючи градієнтний спуск або його похідні, такі як стохастичний градієнтний спуск, для зменшення функції втрат. Нелінійність вводиться за допомогою активаційних функцій, таких як ReLU (випрямлена лінійна одиниця) або сигмоїда, що дозволяє мережі моделювати складні функції, тоді як методи регуляризації, такі як відсів або L2-регуляризація, допомагають мінімізувати перенавчання та забезпечують, що мережа добре узагальнюється на нові дані.

3.2 Розробка структурної схеми

Опишемо структурну схему системи.

Структурний блок завдання «виявлення»

Можливість оперативного виявлення сучасних кібератак має першорядне значення, оскільки швидкість реагування безпосередньо впливає на масштаб можливих збитків. У представленому нижче списку наведено завдання UBA-аналітики, які забезпечують підвищену ефективність виявлення загроз у будь-яких ситуаціях.



Рисунок 3.1 – Структурна схема системи.

– **Блок компрометації облікового запису користувача:** Це необхідна, але недостатня умова для UBA-аналітики. Система має легко виявляти факти захоплення облікових записів мережевих користувачів хакерами, незалежно від вектора атаки чи наявності шкідливого ПЗ (зокрема, атаки типу *pass the hash* і *golden socket*). Механізм виявлення повинен коректно працювати з будь-якими

комбінаціями користувачів, пристроїв та IP-адрес. Ключовою вимогою є здатність оперативно фіксувати компрометацію облікового запису будь-якого співробітника чи підрядника всередині організації.

– **Блок компрометації облікового запису привілейованого користувача:** Компрометація облікових записів привілейованих користувачів (адміністраторів баз даних чи системних адміністраторів) є складнішим завданням для виявлення. Через специфіку своєї роботи (реагування на критичні інциденти) такі співробітники часто не дотримуються стандартних поведінкових шаблонів, що ускладнює їх профілювання. Системи UBA-аналітики мають ефективно розпізнавати типові атаки на привілейовані облікові записи, які надають доступ до критично важливих систем. Якщо зловмисники захоплюють такий акаунт і отримують прямий доступ до ключових ресурсів, засоби UBA зобов'язані миттєво ідентифікувати цю загрозу.

– **Блок доступу до ресурсів керівництва:** Очевидними мішенями для зловмисників є пристрої топ-менеджменту – зокрема, ноутбуки виконавчих чи фінансових директорів, які містять стратегічні дані про власністю, злиття, поглинання та конфіденційну бізнес-інформацію. Наприклад, щороку шляхом шахрайства з електронною поштою та маніпуляцій керівництвом з рахунків компаній викрадаються сотні мільйонів доларів через підтвердження фальшивих переказів. Ефективні системи UBA-аналітики мають автоматично будувати моделі ресурсів для ідентифікації пристроїв керівництва, після чого здійснювати постійний моніторинг на предмет несанкціонованого чи аномального доступу до них.

– **Блок визначення внутрішніх загроз:** Хоча більшість резонансних уразливостей спричинені зовнішніми атаками, інсайдерське шахрайство залишається суттєвим джерелом витоку даних. Системи UBA-аналітики мають ефективно виявляти ситуації, коли як привілейовані, так і звичайні користувачі здійснюють ризиковані операції, що виходять за межі їхнього стандартного профілю поведінки.

Кожне з перелічених завдань фокусується на виявленні певних типів кіберзагроз. Оскільки ці загрози не є взаємовиключними, ефективні рішення UBA-аналітики повинні забезпечувати паралельний і комплексний захист від них усіх одночасно.

Структурний блок завдань «пріоритезації й реагування»

Хоча чимало вендорів UBA-рішень заявляють про можливості виявлення загроз, не кожна така система здатна реально підвищити ефективність роботи SOC та IT-персоналу. Наведені нижче завдання UBA зосереджені на точнішому визначенні пріоритетів і раціональнішому реагуванні на інциденти. Для досягнення цього результату рішення UBA мають одночасно підтримувати весь спектр зазначених операцій.

– **Блок блокування облікових записів:** Процедура блокування облікових записів зазвичай вимагає значних трудозатрат на адміністрування. У великих компаніях цілі штатні одиниці можуть увесь рік займатися виключно розслідуванням таких інцидентів – з'ясовуючи, чи спричинене блокування звичайною помилкою під час введення пароля, чи є наслідком спроби злому акаунта. Аби оцінити рівень загрози, адміністратори витрачають по 4–5 годин на аналіз логів кожного заблокованого облікового запису. Системи UBA-аналітики мають автоматизувати цей процес та самостійно визначати ступінь ризику для акаунта. Завдяки цьому впровадження UBA дозволяє суттєво скоротити витрати на утримання профільних IT-фахівців.

– **Блок створення облікових записів:** Класичний сценарій атаки передбачає початкове зараження окремого вузла з подальшим генеруванням нових облікових записів, не пов'язаних із первинним вектором входу. Через це переписування образу скомпрометованої системи втрачає сенс – зловмисники продовжують контролювати мережу через нові акаунти. Платформи UBA-аналітики зобов'язані контролювати динаміку створення облікових записів, виявляючи несанкціоновані дії та відхилення від прийнятих процедур.

– **Блок спільного використання облікових записів:** Багато організацій потерпають від порушень безпеки, пов'язаних із використанням єдиного

облікового запису кількома особами – зокрема, спільного застосування адміністраторами БД загального акаунта для рутинних операцій. Ефективні платформи UBA-аналітики зобов'язані фіксувати подібні практики, персоналізувати реальних користувачів спільних облікових записів та спрощувати оптимізацію цього процесу.

– **Блок класифікації сервісних облікових записів:** Зазвичай фахівці з інформаційної безпеки мають обмежені можливості для контролю сервісних облікових записів із розширеними повноваженнями, через що такі акаунти стають привабливою мішенню для зловмисників. Яскравим прикладом є обліковий запис «Firefighter» («пожежний») у системі SAP, який надає повний доступ до критично важливих додатків. Системи UBA-аналітики мають автоматично ідентифікувати подібні сервісні акаунти й позначати їх спеціальними мітками у разі фіксації будь-якої аномальної поведінки.

– **Блок роботи з неактивними обліковими записами:** Багато компаній мають внутрішні політики щодо неактивних облікових записів. Якщо співробітник не авторизувався у системі протягом 30 днів, це може свідчити про те, що він звільнився, а процедуру деактивації акаунта не було завершено належним чином. Системи UBA-аналітики мають забезпечувати безперервний моніторинг персоналу та підрядників, чиї облікові записи залишалися неактивними протягом заданого періоду.

– **Блок розслідування оповіщень системи безпеки:** Платформи UBA-аналітики функціонують в інфраструктурі підприємства паралельно з іншими засобами кібербезпеки – антивірусами, системами DLP, інструментами контролю мережевого доступу (NAC) тощо. Ці системи генерують сповіщення, які потребують опрацювання, проте часто містять мінімум даних (наприклад, лише IP-адресу без імені власника чи назви відділу), що суттєво ускладнює розслідування. Рішення UBA мають збагачувати такі алерти від сторонніх систем повноцінним контекстом про користувачів та ресурси. Завдяки цьому співробітники SOC зможуть за ідентифікатором стороннього сповіщення переглядати в UBA всю вичерпну інформацію щодо інциденту.

– **Блок розслідування облікових записів:** Зазвичай юридичні та кадрові відділи компаній регулярно запитують звіти щодо історій дій користувачів. Збір та об'єднання цих даних з усіх систем, пристроїв, мереж, IP-адрес і акаунтів вимагає значних ручних зусиль. Рішення UBA-аналітики мають автоматично формувати хронологічну шкалу всієї мережевої активності – включно з підключеннями через VPN та змінами облікових записів у межах однієї системи, а також підсвічувати аномальну поведінку із зазначенням рівня ризику. Завдяки цьому правильна автоматизація дозволяє заощадити кілька днів роботи на кожне розслідування.

– **Блок огляду порушень безпеки:** Після виявлення інциденту на кшталт витоку даних чи зламу мережі внутрішні та зовнішні команди розслідування можуть витратити тижні й місяці на ретельне зіставлення таймлайнів усіх порушень безпеки, відновлення дій зловмисників, точного часу атак та переліку постраждалих систем. Рішення UBA-аналітики повинні автоматично опрацьовувати великі масиви даних, щоб будувати цілісні часові шкали із відображенням усіх користувачів та систем, залучених до інциденту.

– **Блок інтеграції з рішеннями Red Team:** З метою виявлення вразливостей і підготовки аналітиків до реальних загроз чимало Центрів моніторингу безпеки (SOC) залучають команди етичних хакерів (Red Team). Системи UBA-аналітики мають підтримувати такі тестування, повністю візуалізуючи весь ланцюжок атаки як під час моделювання порушень, так і після нього. За правильного впровадження UBA дає змогу глибше зрозуміти внутрішні слабкі місця та вразливості інфраструктури.

Red Team

Термін Red Team походить із військової сфери та позначає команду «дружніх» антагоністів, якій протистоїть захисна група – Blue Team. Головна відмінність Red Team операцій від класичного тесту на проникнення (пен-тесту) полягає в регламенті процедур та відсутності попередження для команди захисту. Крім того, традиційні пен-тести зазвичай передбачають використання «білих списків», часові обмеження та суворі рамки взаємодії з системою.

Натомість Red Team практично не має обмежень і передбачає імітацію реальної атаки на інфраструктуру – від штурму зовнішнього периметра й спроб фізичного проникнення до складних методів соціальної інженерії (наприклад, використання повноцінного реверс-шеллу замість простого відстеження кліків по посиланнях).

3.3 Розробка функціональної схеми

Функціональна схема визначає шляхи реалізації заданих завдань програмним забезпеченням, відображаючи характер перетворення даних і взаємозв'язки між окремими елементами системи. Вона формується на основі структурної декомпозиції і слугує для детального опису архітектури майбутнього програмного продукту. На основі визначеної структури та функцій складових компонентів було побудовано функціональну схему розроблюваної системи, яку наведено на рисунку 3.2.

Головна програма комплексу охоплює чотири основні функціональні блоки:

– блок головної сторінки системи динамічного профілювання;

– блок сторінки профілю користувача;

– блок сторінки запитань для аналізу поведінкових особливостей;

– блок бази даних системи.

Характеристика функціональних блоків та модулів

1. Блок головної сторінки Забезпечує первинне ознайомлення користувачів із можливостями вебсервісу та містить такі підмодулі:

– модуль реєстрації користувачів: реалізує форму введення облікових даних (email та пароля), перевірку їхньої коректності та збереження нового запису в базі даних;

– модуль авторизації: здійснює перевірку автентичності користувачів за введеними реквізитами, керування рівнями доступу до сервісу та валідацію вхідних даних;

– модуль актуальних запитань: забезпечує відображення останніх поведінкових тестів, анкетних завдань або запитань для аналізу;

– модуль інформації про розробника: містить довідкові дані та форму зворотного зв'язку для надсилання користувацьких пропозицій і зауважень.



Рисунок 3.2 – Функціональна схема системи

2. Блок сторінки профілю користувача Надає інтерфейс для моніторингу та аналізу персональної активності. Блок відображає профільну інформацію, історію відповідей, коментарів, часові мітки останньої активності та пов'язані теги. Окрім цього, передбачено функції редагування основних параметрів облікового запису та його видалення за потреби.

3. Блок сторінки запитань Складається з таких взаємопов'язаних модулів:

– модуль окремого запитання: забезпечує перегляд повного змісту запитання, додавання та перегляд коментарів, керування рейтингом відповідей і призначення відзнаки найкращого коментаря як вирішення;

– модуль тегів**:** реалізує структурований виведений перелік тегів та повнотекстовий пошук за ними.

Інтерфейс розробленого програмного забезпечення спроєктований з урахуванням ергономічних вимог, є інтуїтивно зрозумілим для користувача та забезпечує ефективну взаємодію з аналітичними компонентами системи.

3.4 Розробка діаграми процесів

Процесну діаграму розроблюваної системи наведено на рисунку 3.3. Її детальний аналіз дозволяє простежити характер взаємодії внутрішніх компонентів та маршрутизацію інформаційних потоків у межах платформи динамічного профілювання. У процесі проєктування застосовується модель графічного представлення потоків даних (*Data Flow Diagram, DFD*), яка відображає рух, трансформацію та збереження інформації в інформаційній системі (зокрема, параметрів поведінкових сесій, результатів кластеризації та моделей глибокого навчання).

Діаграми взаємодії процесів є базовим інструментом структурного проєктування для візуалізації обробки даних. Традиційно розробка розпочинається з побудови контекстної діаграми потоків даних, яка ілюструє загальну взаємодію системи з користувачами та зовнішнім середовищем. У подальшому ця модель деталізується шляхом поетапної декомпозиції процесів і потоків даних з метою повної та всебічної демонстрації архітектури розроблюваного комплексу профілювання.

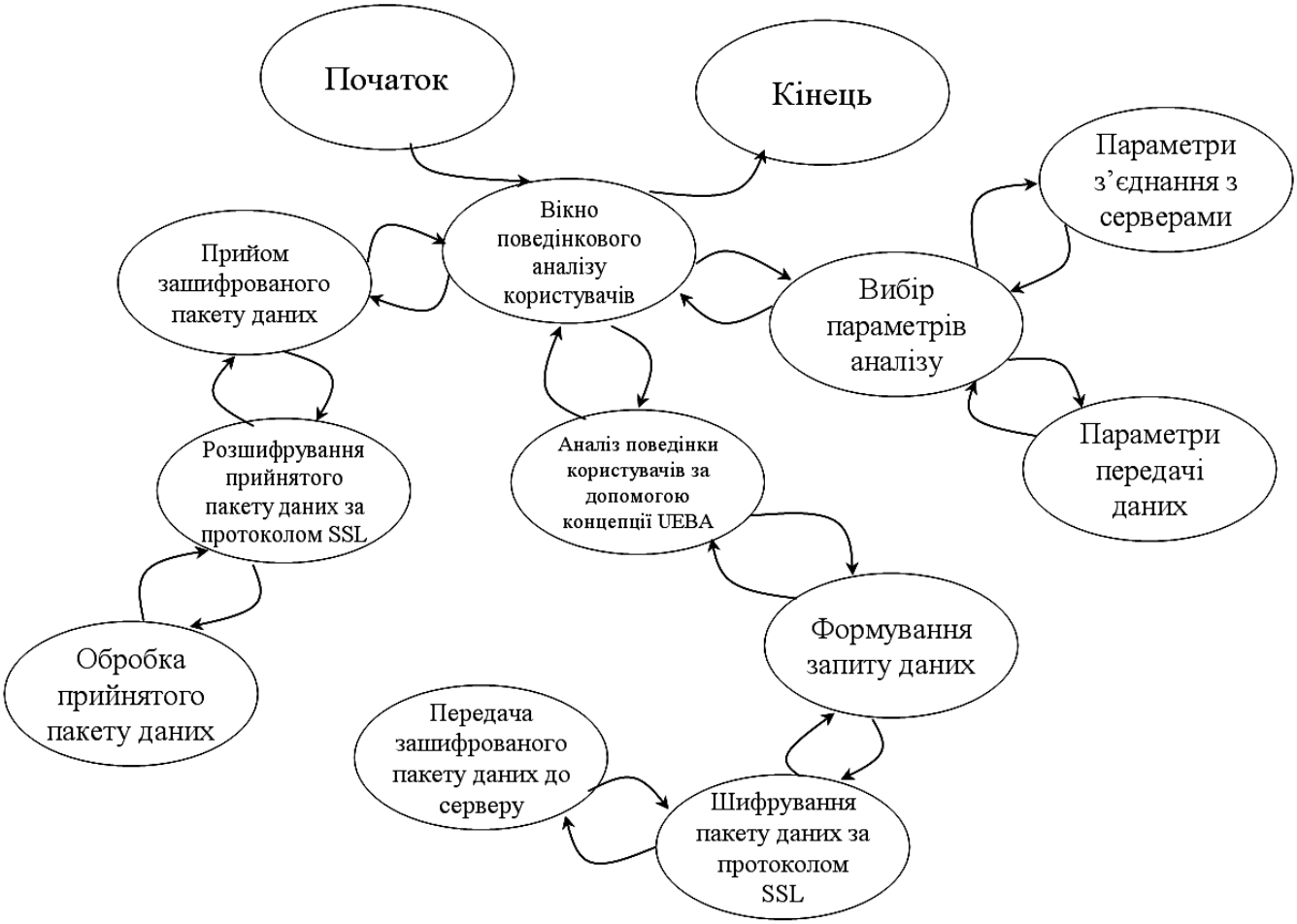

Рисунок 3.3 – Діаграма взаємодії процесів

Таким чином, розглянувши опис системи, структурну, функціональну схеми системи, та діаграму взаємодії процесів перейдемо до опису блок-схем основної програми, та підпрограм, які використовуються, для реалізації системи.

4 РЕАЛІЗАЦІЯ ПРОЕКТУ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ПРОЕКТНИХ РІШЕНЬ

4.1 Блок-схеми та опис алгоритмів функціонування системи

Алгоритмічне забезпечення системи динамічного профілювання поведінки користувачів призначене для автоматизованого аналізу їхньої активності, визначення характерних моделей взаємодії з інформаційними ресурсами та виявлення відхилень від установлених поведінкових профілів. Основним завданням є формування індивідуальних і групових характеристик користувачів на основі послідовностей зареєстрованих подій. Для цього передбачається поєднання методів кластеризації, які дозволяють визначати групи подібної поведінки, та моделей глибокого навчання, які аналізують складні залежності між характеристиками активності. Динамічний характер системи забезпечується регулярним уточненням профілів відповідно до нових спостережень із контролем можливих аномалій.

Загальну послідовність функціонування системи відображено на рисунку 4.1. Основний алгоритм передбачає отримання подій користувацької активності, їхню нормалізацію, формування поведінкових ознак і визначення відповідності поточних дій раніше встановленим профілям. На основі підготовлених даних виконується кластеризація користувачів за характером взаємодії з інформаційними ресурсами. Додатково модель глибокого навчання аналізує поведінкові характеристики та визначає ступінь відхилення нових спостережень від засвоєних закономірностей. Отримані результати використовуються для формування оцінки аномальності. Після перевірки допустимості нових даних здійснюється оновлення відповідного поведінкового профілю.

Для реалізації зазначених функцій доцільно передбачити модульну архітектуру програмного комплексу. Компонент збору даних відповідає за

отримання подій із контрольованих інформаційних систем. Модуль попереднього оброблення забезпечує перевірку, нормалізацію та формування послідовностей активності.

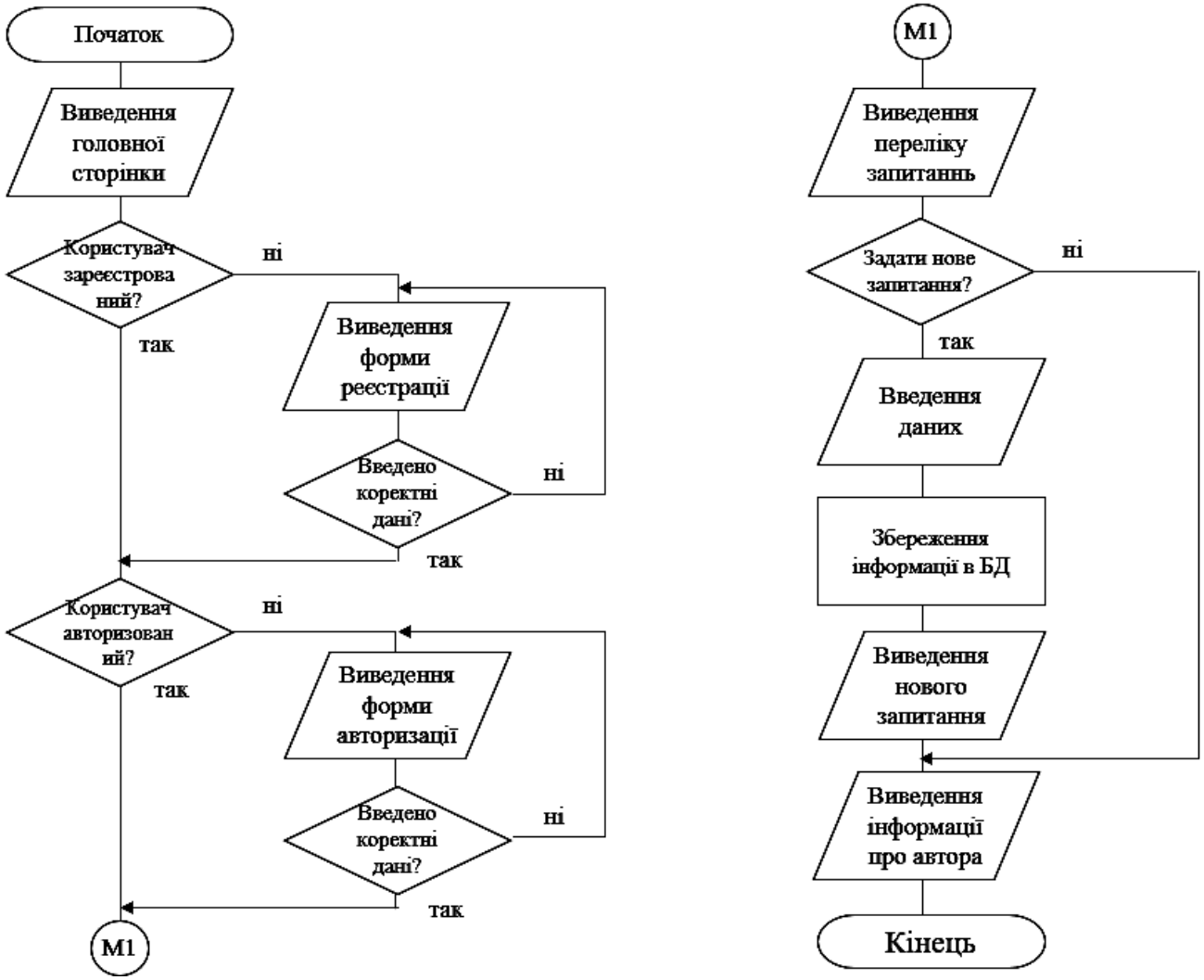

Рисунок 4.1 – Блок-схема основної програми

Аналітичний компонент виконує побудову поведінкових ознак, кластеризацію та обчислення результатів нейромережевого аналізу. Окрема служба профілів забезпечує зберігання індивідуальних характеристик користувачів і керування їхніми версіями. Модуль оцінювання аномалій формує підсумкові результати, які можуть передаватися до користувацького інтерфейсу або зовнішньої системи моніторингу.

Особливістю поведінкових даних є їхня неоднорідність. Активність користувача може характеризуватися часом входу до системи, тривалістю сеансів, частотою звернень, кількістю виконаних операцій, типами використаних ресурсів та послідовністю дій. Частина характеристик має числове представлення, інші визначаються категоріальними значеннями або часовими залежностями. Тому безпосереднє застосування алгоритмів кластеризації до початкових журналів не забезпечує коректного порівняння користувачів. Необхідно сформувати узгоджений простір поведінкових ознак, який враховує особливості різних типів активності.

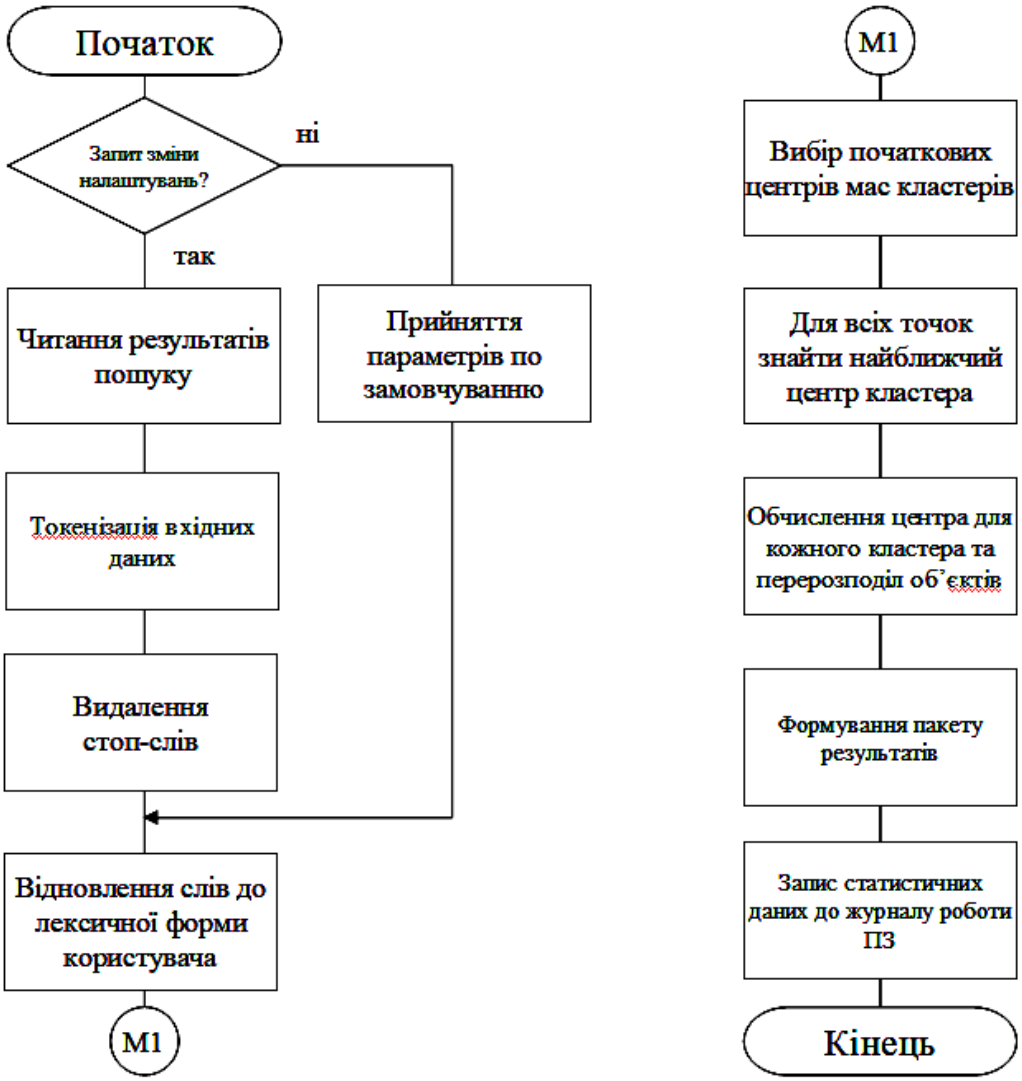

Рисунок 4.2 – Блок-схема роботи підпрограми

Окремим функціональним блоком є підпрограма оцінювання поточної поведінки користувача. Принцип її функціонування представлено на рисунку 4.2. Підпрограма отримує нормалізований вектор характеристик активності, визначає відповідний кластер поведінки та обчислює відхилення від індивідуального і групового профілів. Додатково використовується результат нейромережевої моделі, яка оцінює відповідність спостереження засвоєним закономірностям. Після об'єднання результатів формується оцінка аномальності. Якщо вона перевищує встановлений поріг, подія передається до компонента поглибленого аналізу. Звичайні спостереження можуть розглядатися як кандидати на подальше оновлення профілю.

Під час проєктування алгоритмічного забезпечення необхідно розрізняти зміну поведінки та порушення інформаційної безпеки. Нетипова активність може бути наслідком зміни службових обов'язків, нового робочого графіка або використання раніше недоступного програмного забезпечення. Тому система повинна визначати насамперед статистичні й поведінкові відхилення, а не автоматично ототожнювати їх зі зловмисними діями. Подальша інтерпретація результатів може виконуватися з урахуванням контексту інформаційної системи, характеристик облікового запису та додаткових джерел інформації.

Алгоритм збору подій користувацької активності

Початковим етапом функціонування системи є отримання інформації про взаємодію користувачів із програмними та мережевими ресурсами. Джерелами можуть бути журнали автентифікації, вебзастосунки, корпоративні інформаційні системи, сервери прикладних програм та засоби контролю доступу. Конкретний перелік визначається призначенням досліджуваного програмного комплексу.

Вхідними даними алгоритму є повідомлення, сформовані контрольованими системами. Для кожної події можуть визначатися ідентифікатор користувача, час виникнення, тип операції, інформаційний ресурс і результат виконання. Додатково можуть використовуватися характеристики пристрою або сеансу, якщо їхнє отримання відповідає встановленим правилам оброблення даних.

На першому етапі перевіряється доступність джерела. Далі визначається формат повідомлень і спосіб їхнього передавання. Для інтеграції можуть використовуватися програмні інтерфейси API, системні журнали або спеціалізовані агенти. Отримані події передаються до компонента попереднього оброблення.

Для кожного повідомлення необхідно фіксувати час виникнення та час надходження до системи. Ці значення можуть відрізнятися через затримки передавання або оброблення. Під час подальшого аналізу поведінкових послідовностей доцільно використовувати початковий час події з урахуванням достовірності відповідної часової позначки.

Окремо контролюється правильність визначення користувацької ідентичності. Один користувач може працювати з декількома корпоративними застосунками, які використовують різні внутрішні ідентифікатори. Для формування спільного профілю необхідно встановити відповідність між такими обліковими записами. Якщо ця відповідність не підтверджена, події не повинні автоматично об'єднуватися.

Результатом алгоритму є структурований потік користувацьких подій із визначеним походженням. Він використовується для подальшого формування поведінкових характеристик.

Алгоритм нормалізації та перевірки поведінкових даних

Інформація, отримана з різних джерел, може мати неоднакові назви полів, формати часу та способи представлення операцій. Для забезпечення сумісності необхідно застосувати єдину внутрішню модель події.

На початковому етапі визначається тип повідомлення. Далі застосовується відповідний аналізатор, який виділяє необхідні поля. Для кожної події формується узгоджений набір атрибутів, що включає користувача, час, категорію активності, ресурс та результат операції.

Особливу увагу необхідно приділити часовим характеристикам. Для розподілених систем доцільно приводити часові позначки до UTC. Це дозволяє

правильно зіставляти дії, виконані в різних часових поясах або зареєстровані незалежними серверами.

Наступним етапом є перевірка коректності значень. Події з відсутніми обов'язковими полями позначаються як неповні. Некоректні часові позначки, невідомі категорії операцій та неправильні типи даних обробляються відповідно до визначених правил.

Окремо необхідно контролювати дублювання. Повторна доставка одного повідомлення може призвести до штучного збільшення кількості дій користувача. Для усунення таких випадків використовуються ідентифікатори подій та інші стабільні характеристики.

Водночас дві однакові операції, виконані послідовно, не повинні помилково вважатися дублюванням. Тому алгоритм враховує джерело, час та доступні службові ідентифікатори.

Результатом є нормалізований набір подій, придатний для побудови часових послідовностей та числових характеристик активності.

Алгоритм формування користувацьких сеансів

Для аналізу поведінки недостатньо розглядати кожну операцію незалежно. Важливе значення має послідовність дій, виконаних протягом певного періоду взаємодії з інформаційною системою.

Вхідними даними алгоритму є нормалізовані події, впорядковані за користувачем і часом виникнення. На першому етапі визначається наявність ідентифікатора сеансу, сформованого джерелом. Якщо він доступний і достовірний, події можуть групуватися за цим значенням.

За відсутності явного ідентифікатора застосовується часовий спосіб сегментації. Для кожного користувача визначається інтервал між сусідніми діями. Якщо він перевищує встановлене значення, наступна подія може вважатися початком нового сеансу.

Однак часовий підхід не завжди точно відображає фактичну структуру роботи. Користувач може одночасно використовувати декілька застосунків або залишати активний сеанс без виконання операцій. Тому бажано враховувати

доступні ідентифікатори пристрою, застосунку та автентифікованого підключення.

Після формування сеансу визначаються його початок, завершення, тривалість і кількість дій. Додатково зберігається впорядкована послідовність категорій операцій.

Для подій, які надходять із запізненням, передбачається контрольований механізм уточнення сеансів. Якщо повідомлення належить до вже сформованого інтервалу, відповідні характеристики можуть бути перераховані.

Результатом алгоритму є набір користувацьких сеансів, які використовуються для статистичного та послідовнісного аналізу.

Алгоритм формування векторів поведінкових ознак

Наступним етапом є перетворення отриманих подій на числове представлення, придатне для методів машинного навчання. Для цього кожному користувачу або його окремому часовому інтервалу зіставляється вектор характеристик.

Вхідними даними є сформовані сеанси, історія активності та доступні метадані інформаційних ресурсів. На першому етапі визначається перелік ознак, які мають практичне значення для аналізу.

До кількісних характеристик можуть належати загальна кількість операцій, середня тривалість сеансу, частота автентифікацій, частка невдалих входів і кількість різних ресурсів. Для аналізу різноманітності дій можуть використовуватися кількість унікальних категорій або показники ентропії.

Часові характеристики дозволяють визначати звичайні періоди активності. Для представлення часу доби доцільно враховувати його циклічну природу. Наприклад, активність поблизу завершення доби повинна бути близькою за часовою характеристикою до активності на її початку.

Категоріальні ознаки можуть перетворюватися за допомогою One-Hot Encoding або інших відповідних способів кодування. Для великої кількості ресурсів доцільно використовувати узагальнені категорії або компактні представлення.

Оскільки різні характеристики мають неоднакові масштаби, перед застосуванням кластеризації необхідно виконати нормалізацію. Для цього можуть використовуватися стандартизація або робастне масштабування. Параметри перетворення визначаються на навчальному наборі та надалі застосовуються до нових спостережень без довільного переналаштування.

Результатом алгоритму є поведінковий вектор фіксованої структури. Для кожного вектора зберігаються ідентифікатор користувача, часовий інтервал і версія процедури формування ознак.

Алгоритм побудови початкового поведінкового профілю

Для аналізу нової активності необхідно мати базове представлення звичайної поведінки користувача. Воно формується на основі історичних спостережень, які відповідають визначеному періоду навчання.

На початковому етапі перевіряється достатність наявної інформації. Якщо користувач має лише декілька зареєстрованих дій, побудований профіль може бути статистично нестійким. У такому випадку доцільно застосовувати групову модель або позначати профіль як недостатньо сформований.

Для користувачів із достатньою кількістю спостережень обчислюються характерні значення поведінкових ознак. До них можуть належати середні або медіанні значення, діапазони звичайних коливань і розподіл категорій активності.

Окремо враховується неоднорідність поведінки в різні періоди. Наприклад, користувач може виконувати адміністративні операції лише в певні дні, а звичайну прикладну роботу протягом решти часу. Тому доцільно підтримувати декілька контекстних станів профілю.

Після обчислення характеристик створюється запис поведінкового профілю. Він містить узагальнені показники, кількість спостережень, часові межі та версію використаної моделі.

Результатом алгоритму є початковий профіль користувача. Він використовується для визначення індивідуальних відхилень і подальшого динамічного оновлення.

Алгоритм кластеризації поведінки користувачів

Кластеризація дозволяє визначати групи користувачів із подібними характеристиками активності без необхідності попереднього призначення кожному користувачу певної поведінкової категорії.

Вхідними даними алгоритму є нормалізовані вектори поведінкових характеристик. На першому етапі перевіряється їхня розмірність і наявність некоректних значень. Далі визначається спосіб обчислення подібності між спостереженнями.

Для початкового групування може використовуватися K-means. Алгоритм формує визначену кількість кластерів, кожний із яких характеризується центром у просторі ознак. Під час навчання спостереження відносяться до відповідних груп, а центри послідовно уточнюються.

Перевагою такого підходу є відносно проста процедура визначення найближчого кластера для нового поведінкового вектора. Водночас K-means потребує попереднього вибору кількості груп і не завжди правильно описує складні кластери нерегулярної форми.

Як альтернативний або додатковий метод може використовуватися HDBSCAN. Він дозволяє знаходити області різної щільності та виділяти спостереження, які не належать до достатньо стійких груп. Це доцільно під час дослідження неоднорідних поведінкових даних.

Після виконання кластеризації визначаються характеристики кожної групи. Наприклад, один кластер може об'єднувати користувачів із короткими регулярними сеансами, інший характеризуватися тривалою роботою з великою кількістю ресурсів.

Отримані групи не повинні автоматично ототожнюватися з посадовими ролями або рівнями довіри. Кластер відображає насамперед подібність спостережуваної активності. Його зміст потребує подальшої інтерпретації.

Результатом алгоритму є групова структура поведінкових профілів, яка використовується для оцінювання нових спостережень відносно користувачів зі схожим характером роботи.

Алгоритм визначення належності до поведінкового кластера

Після навчання кластерної моделі необхідно визначати, до якої групи належать нові поведінкові спостереження. Для цього використовується збережена модель групування та параметри нормалізації ознак.

На першому етапі новий вектор приводиться до тієї самої структури, яка використовувалася під час навчання. Якщо структура ознак змінилася, безпосереднє застосування попередньої кластерної моделі не допускається.

Для K-means виконується обчислення відстані до центрів кластерів. Спостереження відноситься до найближчого центру. Додатково може визначатися ступінь віддаленості від характерної області відповідної групи.

Для HDBSCAN необхідно враховувати особливості застосування моделі до нових точок. Звичайна процедура кластеризації формує групи на основі всього навчального набору. Тому визначення належності нового спостереження потребує окремого механізму наближеного прогнозування або повторного групування.

Якщо поведінковий вектор суттєво віддалений від відомих груп, його доцільно позначити як невизначений. Примусове віднесення до найближчого кластера може приховати появу нового типу поведінки.

Результатом алгоритму є визначений або невизначений груповий контекст, який надалі використовується для оцінювання аномальності.

Алгоритм навчання нейромережевої моделі поведінки

Методи кластеризації дозволяють визначати подібність користувачів за сукупністю ознак, але не завжди виявляють складні нелінійні залежності. Для їхнього аналізу доцільно передбачити модель глибокого навчання.

Одним із можливих варіантів є автоенкодер (Autoencoder). Він складається з компонентів кодування та відновлення вхідного представлення. Під час навчання модель отримує поведінкові вектори та намагається відтворити їхні значення.

Вхідними даними алгоритму є набір попередньо оброблених поведінкових векторів. На першому етапі формується навчальна вибірка. Для побудови моделі

звичайної поведінки необхідно обмежити вплив підтверджено аномальних або явно некоректних спостережень.

Далі визначається структура нейромережі. Для числових векторів може використовуватися багатошаровий повнозв'язний автоенкодер. Внутрішній шар зменшеної розмірності формує компактне представлення характеристик активності.

Під час навчання обчислюється різниця між початковими та відновленими значеннями. Параметри моделі уточнюються методом оптимізації, спрямованим на зменшення помилки реконструкції.

Після завершення навчання модель перевіряється на окремій валідаційній вибірці. Важливо використовувати часовий поділ даних, який не допускає потрапляння майбутніх спостережень до навчального набору.

Як можливі технологічні засоби програмної реалізації можуть використовуватися Python і PyTorch. Вибір конкретного фреймворку визначається фактичною реалізацією та вимогами до продуктивності.

Результатом алгоритму є навчена модель, здатна формувати компактні поведінкові представлення та оцінювати помилку реконструкції нових спостережень.

Алгоритм аналізу послідовностей користувацьких дій

Агреговані характеристики не завжди дозволяють визначати порядок операцій. Два сеанси можуть мати однакову кількість входів, переглядів і змін даних, але відрізнятися послідовністю виконання.

Для врахування таких закономірностей доцільно застосовувати нейромережеву модель послідовностей. Як можливі архітектури розглядаються Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU) або модель на основі механізму уваги.

Вхідними даними є впорядковані послідовності категорій операцій, часових інтервалів та доступних характеристик ресурсів. Перед навчанням визначається спосіб числового кодування подій.

Для кожної категорії операції може формуватися векторне представлення. Далі послідовність передається нейромережі, яка аналізує залежності між її елементами.

Модель може навчатися прогнозувати наступну категорію дії або відновлювати послідовність. У першому випадку аномальність визначається за низькою відповідністю фактичної дії прогнозу. У другому використовується помилка реконструкції.

Необхідно враховувати різну довжину користувацьких сеансів. Для цього можуть застосовуватися доповнення послідовностей і маскування неінформативних елементів. Під час оцінювання модель не повинна враховувати штучно додані елементи як реальні дії.

Результатом алгоритму є додаткова характеристика поведінкової аномальності, яка відображає незвичність порядку виконання операцій.

Алгоритм комплексного оцінювання аномальності

Для підвищення інформативності оцінювання доцільно поєднувати результати кластеризації та глибокого навчання. Перший компонент характеризує віддаленість спостереження від групової поведінки. Другий визначає, наскільки нові дані відповідають закономірностям, засвоєним нейромережевою моделлю.

Вхідними даними алгоритму є поточний поведінковий вектор, характеристики відповідного кластера та результат нейромережевого аналізу.

На першому етапі обчислюється відстань до характерної області поведінкового кластера. Для кластерів, сформованих K-means, може використовуватися відстань до центру з урахуванням розподілу навчальних спостережень.

Далі отримується помилка реконструкції автоенкодера або результат аналізу послідовності. Значення повинні приводитися до порівнянного масштабу, оскільки їхні початкові діапазони можуть суттєво відрізнятися.

Для нормалізації можуть застосовуватися порогові значення, визначені на валідаційних даних. Наприклад, оцінка відхилення може характеризуватися відношенням поточного значення до допустимої межі відповідного показника.

Після нормалізації результати можуть об'єднуватися за допомогою вагової моделі. Ваги визначаються на основі експериментального оцінювання та не повинні призначатися довільно як остаточні параметри системи.

Окремо необхідно враховувати випадки суперечливих результатів. Якщо кластерна модель визначає звичайну поведінку, але нейромережевий компонент виявляє значне відхилення, таке спостереження може потребувати додаткового аналізу.

Результатом алгоритму є узагальнена оцінка аномальності з відомостями про внесок окремих моделей.

Алгоритм динамічного оновлення індивідуального профілю

Поведінка користувачів змінюється протягом експлуатації інформаційної системи. Незмінний профіль може поступово втрачати актуальність і формувати зростаючу кількість хибнопозитивних спрацювань. Для врахування таких змін необхідно передбачити контрольоване оновлення поведінкових характеристик.

Вхідними даними алгоритму є поточний профіль користувача, нові поведінкові спостереження та результати їхнього оцінювання.

На першому етапі перевіряється придатність нових даних. Події з некоректними атрибутами або невизначеною ідентичністю користувача не повинні використовуватися для автоматичного навчання.

Далі аналізується результат оцінювання аномальності. Якщо спостереження належить до допустимої області поведінки та не має інших підтверджених ознак порушення, воно може бути використане для оновлення профілю.

Для числових характеристик може застосовуватися експоненційне згладжування. Новий профіль формується з урахуванням попереднього стану та останнього допустимого спостереження. Коефіцієнт оновлення визначає швидкість адаптації.

Надмірно швидке оновлення може призвести до втрати історичних закономірностей. Занадто повільне оновлення не дозволятиме своєчасно

враховувати зміни звичайної роботи. Тому параметри адаптації необхідно визначати експериментально.

Особливу небезпеку становить включення зловмисної активності до навчальних даних. Якщо система автоматично засвоює кожне нове спостереження, тривала підозріла поведінка може поступово перетворитися на нову норму. Для зменшення цього ризику доцільно використовувати відкладене оновлення, підтвердження допустимості даних і обмеження швидкості зміни профілю.

Результатом алгоритму є актуалізований поведінковий профіль із збереженням попередньої версії та відомостей про використані спостереження.

Алгоритм виявлення зміни поведінкового розподілу

Оновлення окремих характеристик не завжди достатнє для опису суттєвої зміни поведінки. Наприклад, користувач може перейти на іншу посаду, отримати новий набір службових функцій або почати працювати за іншим графіком.

Для виявлення таких ситуацій може використовуватися аналіз зміни статистичного розподілу поведінкових ознак. Вхідними даними є історичні та нові спостереження, отримані протягом визначених часових інтервалів.

На першому етапі формуються статистичні характеристики попереднього й поточного періодів. Далі виконується перевірка їхньої відповідності.

Для автоматизованого виявлення зміни розподілу може застосовуватися підхід Concept Drift Detection. Одним із можливих алгоритмів є Adaptive Windowing (ADWIN), який використовує адаптивне часове вікно для визначення статистично значущих змін.

Під час використання такого механізму важливо правильно вибрати контрольовані показники. Ними можуть бути частота операцій, інтенсивність користувацьких сеансів або значення оцінки аномальності. Виявлення зміни одного показника не завжди означає зміну всього поведінкового профілю.

Якщо зміна розподілу підтверджується, система формує повідомлення про необхідність перегляду профілю або повторного навчання моделі. Безпосереднє

оновлення може виконуватися після додаткової перевірки допустимості нових даних.

Результатом алгоритму є визначення потреби в адаптації поведінкової моделі без автоматичного закріплення потенційно небезпечних змін.

Алгоритм повторної кластеризації користувачів

Зі зміною характеру роботи користувачів початкова структура кластерів може втрачати актуальність. Тому необхідно передбачити періодичний перегляд групових профілів.

Вхідними даними алгоритму є актуальні поведінкові вектори та результати контролю зміни розподілу. На першому етапі визначається необхідність повторного навчання кластерної моделі.

Якщо зміни не перевищують установлених меж, може продовжуватися використання поточної структури. Якщо кількість невизначених спостережень зростає або групові характеристики суттєво змінюються, ініціюється повторна кластеризація.

Нова модель навчається на підготовленому наборі даних. Після цього перевіряється стабільність отриманих груп і можливість інтерпретації їхніх характеристик.

Необхідно враховувати, що числові ідентифікатори кластерів не мають постійного семантичного значення. Після повторного навчання кластер з попереднім номером може відповідати іншій групі користувачів. Тому для збереження історії необхідно зіставляти групи за їхніми характеристиками, а не лише за номером.

Перед заміною діючої моделі доцільно виконувати порівняння результатів на контрольному наборі. Якщо нова структура не забезпечує прийнятної якості, попередня версія може залишатися активною.

Результатом алгоритму є оновлена групова модель із контрольованим переходом між версіями.

Алгоритм формування повідомлень про поведінкові аномалії

Після визначення підвищеної оцінки аномальності система повинна сформувати результат, придатний для подальшого аналізу. Для цього передбачається механізм реєстрації та групування підозрілих спостережень.

Вхідними даними є оцінка аномальності, характеристики користувацького профілю, результати кластеризації та відповідні події.

На першому етапі визначається, чи пов'язане нове спостереження з уже зареєстрованою групою підозрілої активності. Якщо відповідний запис існує, нова інформація додається до його історії.

Якщо пов'язаного запису немає, створюється нове повідомлення. Воно містить ідентифікатор користувача в дозволеному представленні, часовий інтервал, категорію аномалії та основні чинники відхилення.

Для підвищення пояснюваності доцільно зберігати окремі оцінки кластерної та нейромережевої моделей. Додатково можуть зазначатися характеристики, які найбільше відрізняються від індивідуального профілю.

Оскільки результат автоматизованого аналізу має ймовірнісний або статистичний характер, повідомлення повинно описувати виявлену аномалію, а не безпідставно стверджувати факт порушення.

Результатом алгоритму є структуровані повідомлення, які можуть використовуватися для перевірки, формування звітів та уточнення моделей.

Алгоритм зворотного зв'язку та уточнення результатів

Для підвищення практичної придатності системи доцільно передбачити можливість перевірки результатів відповідальним користувачем або аналітиком.

Вхідними даними є сформоване повідомлення, пов'язані події та результат експертного розгляду. Після перевірки спостереження може бути позначене як підтверджена аномалія, допустима зміна поведінки або випадок із недостатньою інформацією.

Такі рішення можуть використовуватися під час формування наступних навчальних наборів. Проте їх необхідно перевіряти на узгодженість і

достовірність. Помилкове підтвердження може негативно впливати на якість майбутніх моделей.

Для контрольованого оновлення доцільно зберігати версію профілю та модель, які використовувалися під час первинного оцінювання. Це дозволяє відтворювати причини попередніх спрацювань.

Окремо необхідно передбачити можливість скасування некоректних змін. Якщо нова модель починає формувати значну кількість помилкових результатів, система повинна підтримувати повернення до попередньої перевіреної версії.

Результатом алгоритму є накопичення перевірених відомостей, придатних для подальшого вдосконалення поведінкового аналізу.

Особливості програмної реалізації та зберігання даних

Програмна реалізація може передбачати окремі служби отримання подій, формування ознак, виконання кластеризації та нейромережевого оцінювання. Такий розподіл дозволяє незалежно керувати навантаженням і оновленням аналітичних компонентів.

Для реалізації алгоритмів оброблення даних як можливе технологічне рішення розглядається Python. Для підготовки числових характеристик можуть застосовуватися NumPy та pandas. Алгоритми кластеризації можуть реалізовуватися за допомогою scikit-learn, а нейромережеві моделі через PyTorch. Ці засоби становлять можливу технологічну основу, а не підтверджений перелік використаних бібліотек.

Для зберігання поведінкових профілів необхідно передбачити структуроване сховище. Воно повинно забезпечувати зв'язок між ідентифікатором користувача, версією профілю, характеристиками ознак і відповідною версією моделі.

Окремо зберігаються результати оцінювання та повідомлення про аномалії. Необхідно забезпечити можливість відтворення рішення на основі доступних історичних даних.

Для потокового оброблення значної кількості подій може застосовуватися брокер повідомлень. Це дозволяє відокремити надходження інформації від її

подальшого аналізу. При цьому необхідно контролювати затримку та можливе повторне доставлення подій.

Забезпечення конфіденційності поведінкової інформації

Система профілювання накопичує інформацію, яка може характеризувати робочі звички користувачів, їхню активність та особливості використання інформаційних ресурсів. Тому необхідно передбачити обмеження складу зібраних відомостей і контроль доступу.

На початковому етапі визначається мінімальний набір даних, необхідний для побудови поведінкових профілів. Не слід автоматично накопичувати вміст особистих повідомлень або іншу конфіденційну інформацію, якщо для аналізу достатньо технічних метаданих.

Для зменшення ризику розкриття особистих даних можуть застосовуватися псевдонімізовані ідентифікатори користувачів. Відповідність між ними та реальними обліковими записами повинна зберігатися окремо із належним розмежуванням доступу.

Окремо встановлюються правила зберігання історичних подій. Детальні журнали можуть мати інший строк зберігання, ніж агреговані поведінкові профілі або результати аналізу.

Необхідно враховувати можливість використання алгоритмів профілювання для необґрунтованого оцінювання працівників. Тому результати автоматизованого аналізу доцільно застосовувати для визначених завдань моніторингу та безпеки, не використовуючи окрему оцінку аномальності як безумовну підставу для висновків про поведінку конкретної особи.

Алгоритм оброблення помилок та відмов компонентів

Під час роботи системи можливі порушення доступності джерел, затримки надходження повідомлень, помилки формування ознак та недоступність нейромережевої моделі.

Для кожного компонента необхідно визначити стан виконання. Якщо дані неповні, алгоритм не повинен формувати результат із необґрунтованою впевненістю.

У разі недоступності нейромережевого компонента система може продовжувати обмежений аналіз на основі кластерної моделі, якщо такий режим передбачений політикою. При цьому результат повинен містити відомості про часткове оцінювання.

Якщо відсутній актуальний поведінковий профіль, може використовуватися групова модель. Такий підхід дозволяє аналізувати нових користувачів, але потребує обережного визначення порогів аномальності.

За порушення доступності сховища нові події можуть тимчасово накопичуватися в проміжній черзі. Після відновлення з'єднання вони передаються до оброблення з контролем повторної доставки.

Результатом алгоритму є контрольована робота системи за часткової недоступності компонентів із відповідним відображенням обмежень аналізу.

Перевірка коректності алгоритмів та оцінювання ефективності

Для експериментального дослідження запропонованого алгоритмічного забезпечення необхідно передбачити перевірку як окремих моделей, так і всієї послідовності оброблення поведінкових даних.

Початковим етапом є перевірка збору й нормалізації подій. Для цього використовуються контрольовані набори повідомлень із відомими ідентифікаторами користувачів, часовими позначками та категоріями операцій.

Після цього перевіряється формування користувацьких сеансів. Особливу увагу необхідно приділити правильності впорядкування подій, визначенню меж сеансів і обробленню повідомлень, отриманих із затримкою.

Для оцінювання кластеризації можуть використовуватися показники Silhouette Score та Davies-Bouldin Index. Вони дозволяють аналізувати структуру отриманих груп, хоча не підтверджують безпосередньо здатність моделі виявляти загрози.

Окремо необхідно оцінювати стабільність кластерів після зміни навчального набору. Якщо незначне додавання спостережень призводить до повної перебудови групової структури, це може ускладнювати інтерпретацію результатів.

Для нейромережевої моделі перевіряється помилка реконструкції або якість прогнозування послідовностей на окремому наборі даних. Необхідно контролювати можливість перенавчання, за якого модель добре відтворює навчальні спостереження, але неправильно оцінює нову активність.

Якщо доступні достовірно розмічені приклади звичайної та аномальної поведінки, можуть використовуватися Precision, Recall, F1-score та площа під кривою Precision-Recall. Для незбалансованих наборів даних важливо оцінювати кількість хибнопозитивних спрацювань.

Для визначення ефективності комплексного підходу доцільно порівнювати кластерну модель, нейромережеву модель та їхню комбінацію. Випробування повинні виконуватися на однакових контрольних наборах.

Окремого дослідження потребує динамічне оновлення профілів. Для цього можуть використовуватися часові послідовності, що містять поступові зміни звичайної поведінки. Необхідно перевірити, чи зменшується кількість помилкових спрацювань після адаптації та чи не відбувається засвоєння небезпечних спостережень.

Запропоноване алгоритмічне забезпечення формує послідовний процес динамічного профілювання поведінки користувачів від отримання початкових подій до формування індивідуальних і групових моделей активності. Методи кластеризації дозволяють визначати подібні поведінкові структури, а нейромережеві моделі забезпечують аналіз складніших залежностей між ознаками та послідовностями дій. Центральне значення має комплексне оцінювання аномальності та контрольоване оновлення профілів із запобіганням засвоєнню підозрілої поведінки. Сукупність розглянутих алгоритмів створює основу для програмної реалізації системи, здатної адаптувати поведінкові моделі до змін користувацької активності та формувати результати для подальшого аналізу.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Програмне забезпечення системи динамічного профілювання поведінки користувачів призначене для автоматизованого аналізу їхньої активності, формування індивідуальних і групових поведінкових профілів та виявлення аномальних відхилень із використанням методів кластеризації та глибокого навчання. Система забезпечує оброблення користувацьких подій, визначення характерних моделей поведінки та поступове уточнення профілів відповідно до нових спостережень. Результати аналізу можуть використовуватися для моніторингу інформаційних систем і формування повідомлень про підозрілу активність. Головне вікно програми показане на рисунку 5.1.

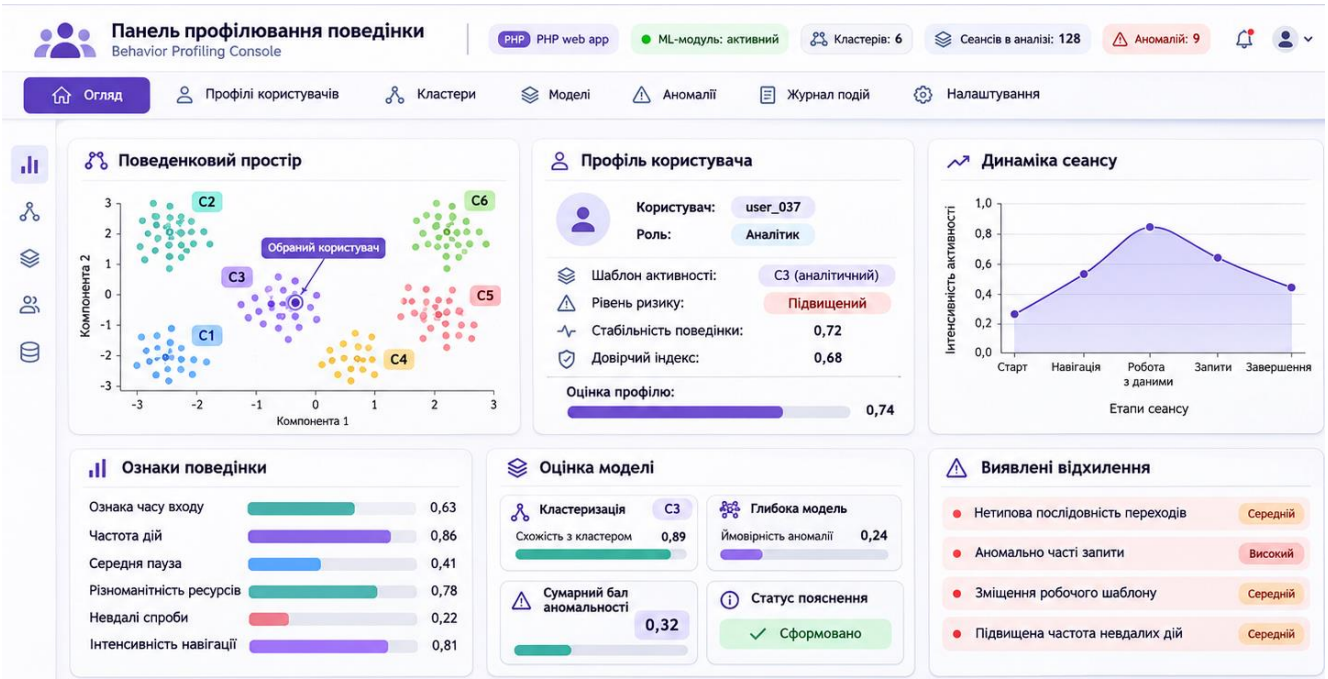

Рисунок 5.1 – Головне вікно ПЗ

Практичне впровадження програмного комплексу передбачає підготовку середовища виконання, налаштування джерел поведінкових даних, розгортання

аналітичних компонентів і перевірку правильності функціонування моделей машинного навчання. Архітектура включає модуль отримання подій, компонент попереднього оброблення, службу формування поведінкових ознак, модулі кластеризації та нейромережевого аналізу. Окремо передбачається зберігання профілів користувачів, параметрів навчених моделей і результатів виявлення аномалій. Наступним етапом є підключення джерел користувацької активності. До них можуть належати корпоративні вебзастосунки, сервери автентифікації та інформаційні системи, які формують журнали операцій. Для кожного джерела визначаються параметри доступу, формат повідомлень і перелік доступних атрибутів. Необхідно забезпечити отримання ідентифікатора користувача, часу події, категорії операції та відомостей про відповідний ресурс. Конкретний набір полів залежить від можливостей інтегрованої системи.

Перед початком збору подій необхідно визначити правила оброблення персональної інформації. Для поведінкового аналізу доцільно використовувати лише ті характеристики, які необхідні для формування профілів. За можливості застосовується псевдонімізація користувацьких ідентифікаторів. Доступ до відповідності між внутрішніми ідентифікаторами та реальними обліковими записами повинен бути обмежений.

Після підключення джерел налаштовується нормалізація повідомлень. Для кожного формату визначаються правила виділення полів і приведення часових позначок до узгодженого представлення. Окремо контролюється повторне надходження однакових подій. Записи з відсутніми обов'язковими атрибутами повинні позначатися як неповні. Для подій, які надходять із затримкою, необхідно передбачити правильне віднесення до відповідного часового інтервалу користувацької активності.

Для зберігання інформації необхідно підготувати сховище подій і поведінкових профілів. Воно повинно підтримувати пошук записів за внутрішнім ідентифікатором користувача, збереження часових характеристик та зв'язок результатів оцінювання з відповідною версією моделі. Конкретна система керування базами даних визначається програмною реалізацією. Важливо

передбачити окреме зберігання початкових подій, агрегованих ознак і результатів аналітичної обробки.

Наступним етапом є налаштування формування поведінкових векторів. Для цього визначаються контрольовані часові інтервали та перелік числових характеристик. До них можуть належати кількість операцій, тривалість сеансів, частота автентифікацій і різноманітність використаних ресурсів. Після формування ознак виконується їхнє масштабування. Параметри нормалізації необхідно зберігати разом із відповідною моделлю, щоб під час експлуатації використовувалося однакове перетворення навчальних і поточних даних.

Для підготовки кластерної моделі формується набір історичних поведінкових векторів. Як можливий алгоритм розглядається K-means, який дозволяє визначати групи подібної активності. Кількість кластерів доцільно уточнювати за результатами перевірки структури даних. Альтернативно може застосовуватися HDBSCAN для визначення груп різної щільності. Після навчання модель і параметри її попереднього оброблення зберігаються для подальшого використання. Для HDBSCAN необхідно окремо врахувати підтримуваний механізм віднесення нових спостережень до сформованих груп.

Підготовка нейромережевого компонента передбачає визначення архітектури та завантаження параметрів навченої моделі. Для аналізу числових поведінкових векторів може використовуватися автоенкодер. Якщо необхідно враховувати послідовність дій, можуть застосовуватися LSTM або GRU. Навчання доцільно виконувати окремо від постійного оброблення подій. Перед введенням моделі в експлуатацію необхідно перевірити сумісність вхідних ознак, правильність відновлення її параметрів та відтворюваність результатів.

Після підготовки моделей налаштовується механізм комплексного оцінювання аномальності. У його конфігурації визначаються способи нормалізації оцінок кластеризації та нейромережевого аналізу. Окремо встановлюються порогові значення для формування повідомлень. Їх необхідно визначати за результатами перевірки на валідаційних даних. Використання

довільних порогів без оцінювання кількості хибнопозитивних спрацювань може призвести до некоректної роботи системи.

Рекомендована послідовність запуску починається з перевірки доступності сховища та джерел поведінкових подій. Після цього активується модуль нормалізації й формування ознак. Далі завантажуються збережені параметри кластерної та нейромережевої моделей.

Після підтвердження їхньої працездатності запускається компонент оцінювання аномальності. Завершальним етапом є активація механізмів формування повідомлень і користувацького інтерфейсу.

Для перевірки виявлення аномалій можуть використовуватися тестові послідовності, які відрізняються від характерної активності. Наприклад, незвичне збільшення кількості операцій або зміна послідовності звернень до ресурсів. Необхідно перевірити формування повідомлення та збереження чинників, які вплинули на оцінку. Такі спрацювання повинні відображатися як поведінкові аномалії, а не як автоматично підтверджені порушення інформаційної безпеки.

Для документування програмного продукту передбачається представлення відомостей про його розробника. Вони забезпечують ідентифікацію авторства системи динамічного профілювання поведінки користувачів і можуть використовуватися під час її подальшого супроводження. Відомості про автора програмного забезпечення представлені на рисунку 5.2.

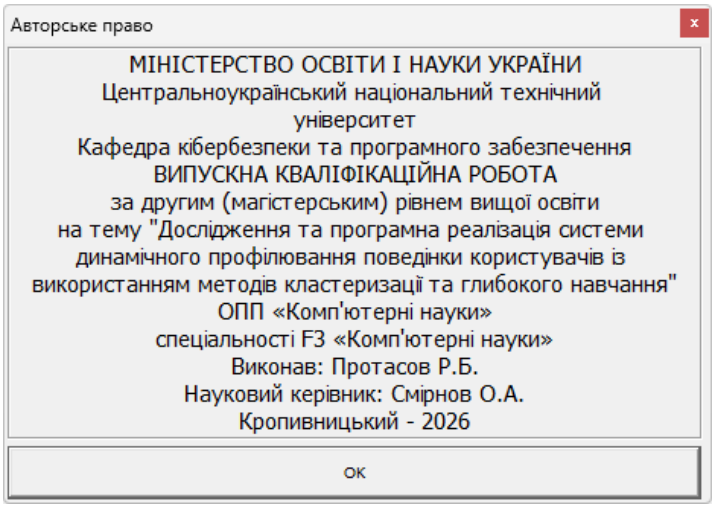

Рисунок 5.2 – Форма авторського права

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

Метою розробки є дослідження та програмна реалізація системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

Об'єктом дослідження є процес динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

Предметом дослідження є методи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

Методи дослідження базуються на методах машинного навчання, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

– Розроблено вітчизняний продукт динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання, який має більш широкі можливості, на відміну від існуючих аналогів.

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

7.1 Вступ

Охорона здоров'я працівників, забезпечення безпеки умов праці, ліквідація професійних захворювань і виробничого травматизму повинна складати одну з головних завдань роботодавця.

Основою охорони праці є науковий аналіз умов праці, технологічних процесів, виробничого обладнання, робочих місць, трудових операцій, організації виробництва з метою виявлення шкідливих і небезпечних виробничих факторів, їх властивостей, особливостей виливу на організм людини. На підставі такого аналізу розробляються заходи та засоби, спрямовані на мінімізацію несприятливого впливу виробничих факторів, створення безпечних та нешкідливих умов праці.

Основою охорони праці є науковий аналіз умов праці, технологічних процесів, виробничого обладнання, робочих місць, трудових операцій, організації виробництва з метою виявлення шкідливих і небезпечних виробничих факторів, їх властивостей, особливостей виливу на організм людини. На підставі такого аналізу розробляються заходи та засоби, спрямовані на мінімізацію несприятливого впливу виробничих факторів, створення безпечних та нешкідливих умов праці

Для того, щоб об’єктивно проаналізувати відповідність умов праці діючим нормативно-правовим актам, необхідно здійснити санітарно-гігієнічну характеристику умов праці відділу, в якому працює програміст, над розробкою даного програмного продукту. В зв’язку з цим необхідно сконцентрувати увагу на небезпечних і шкідливих чинниках пов’язаних з постійною роботою за комп’ютером. Електробезпека є одним із критичних питань для співробітників, що працюють із технікою, яка одержує живлення з електричної мережі. При невиконанні норм електробезпеки можливе враження електричним струмом.

7.2 Шкідливі і небезпечні фактори при роботі з комп’ютером

Електронно-обчислювальна машина (ПЕОМ) та інше обладнання є джерелами небезпеки ураження електричним струмом. Так як робота програміста характеризується істотним зоровим навантаженням, то вимагає належного освітлення. У приміщенні, в якому працюють програмісти необхідно створити належний мікроклімат, параметри якого регламентуються, Державними санітарними правилами і нормами, зокрема ДСанПіН 3.3.2.007-97.

При роботі з використанням ПЕОМ відзначають наступні небезпечні та шкідливі фактори:

– ризик виникнення надзвичайних ситуацій природного або штучного характеру на об’єкті або території;

– ризик виникнення пожежі;

– негативний вплив на органи зору людини;

– ризики ураження електричним струмом;

– недостатня, або надмірна освітленість робочого місця;

– електромагнітні (у тому числі високочастотні) випромінювання (коливання);

– несприятливі мікрокліматичні умови;

– нервово-емоційна напруженість праці;

– інтелектуальні навантаження;

– монотонність праці;

– невідповідність ергономічних показників робочого місця діючим вимогам;

– шум;

– статичні навантаження на кістково-м’язовий апарат;

Відповідно до ст.14 Закону «Про охорони праці» [1] на роботодавця покладено обов'язок забезпечити: безпеку працівників при експлуатації устаткування; застосування засобів індивідуального захисту працівників; відповідні вимоги охорони праці, умови праці на кожному робочому місці;

дотримання режиму праці та відпочинку працівників; навчання безпечним методам і прийомам виконання робіт; інструктаж з охорони праці; організацію контролю над станом умов праці на робочих місцях; проведення атестації робочих місць за умовами праці.

Максимально зменшити кількість шкідливих впливів на людину при високій продуктивності праці, створити комфортні умови для роботи людей – одна з головних задач охорони праці.

7.3 Розробка заходів з умов поліпшення охорони праці

Згідно аналізу умов праці в розглянутому приміщенні, ми одержали наступні результати:

– розмірі приміщення, у розрахунку на одному працюючого, відповідають нормативам;

– мікроклімат відповідає нормативному значенню;

– акустичні умови роботи не перевищують нормативних значень;

Таким чином можна припустити, що основною причиною можливого зниження працездатності програміста є психофізіологічний фактор, тому основна пропозиція буде така: дотримання позитивної психологічної атмосфери в колективі та регламентованого режиму праці та відпочинку, організація робочого місця з урахуванням ергономічних вимог.

Рекомендовані заходи: регулярні періодичні наочні огляди персоналом шляхів для евакуації людей із приміщення, відповідно до плану евакуації (який повинен розташовуватись на видному місці у приміщенні), включення до колективного договору мінімально можливого вмісту аптечок з обов'язковою наявністю масок-клапанів, або іншого спорядження для штучного дихання. Регулярна періодична перевірка параметрів заземлення та занулення (вимірювання опору ланцюга) [9].

Регулярна наочне знайомство персоналу із шляхами для евакуації людей із приміщення відповідно до плану евакуації, забезпечення розподільних щитів

спеціальними розетками з заземлюючими контактами; організація заземлення всіх приладів і пристроїв, які працюють при напрузі вище 36 В.

Так як при ураженні електричним струмом у людини може статися фібриляція шлуночків серця, в організації бажано мати дефібрилятор і підготовлений персонал для роботи з ним.

7.4 Пожежна безпека

Вимоги до пожежної безпеки на підприємстві неухильно повинен дотримуватися кожен співробітник, а організаційна складова при цьому покладається на посадових осіб за відповідним рішенням керівництва і прописується в посадових інструкціях і положеннях по структурним підрозділам.

Зокрема, вказуються конкретні території, ділянки, зони, об’єкти, цілі будівлі і їх частини, поверхи, на яких відповідальний співробітник повинен проводити такі організаційні роботи.

Відповідальні особи зобов’язуються розробити, впровадити та підтримувати виконання певних інструкцій і положень на ввірених їм об’єктах. протипожежний режим відповідно до вимог, викладених в нормативних актах.

Передбачено також створення підрозділу добровільної пожежної охорони та пожежно-рятувальної команди в його складі.

Встановлений режим включає порядки з описом місць спеціального призначення та правила їх використання та утримання, наприклад:

– евакуаційних шляхів;

– так званих «курилок»;

– місць складування продукції та сировини;

– стоянки транспорту.

Також встановлюється порядок роботи та технічного обслуговування:

– вентиляційного устаткування;

– засобів пожежогасіння і захисту від загорянь;

– нагрівальних приладів;

– електрообладнання.

Розробляються і впроваджуються правила роботи з відкритим вогнем і горючими матеріалами. Створюються графіки проходження інструктажів з пожежної безпеки співробітників, а також порядок і терміни перевірок знань пожежно-технічного мінімуму, в тому числі, тих працівників, які відповідальні за цю ділянку роботи на підприємстві. При цьому можуть передбачатися внутрішні лекції, семінари, тренінги та практичні заняття на підприємстві, а також зовнішні – на базі спеціалізованих навчальних центрів з професійними викладачами.

Важливою складовою протипожежного режиму на будь-якому об’єкті є розробка і впровадження порядку дій при виникненні пожежі. Неодмінно має бути план евакуації, описано, як повинні відключатися електроустановки, що і в якій послідовності необхідно робити співробітникам.

Відповідно, для кожного об’єкту, кожного приміщення (крім коридорів, санвузлів, басейнів і подібних приміщень), окремих видів робіт складаються інструкції, за якими повинен працювати персонал, залучений на певних ділянках і в виконанні окремих видів робіт. За інструкціями проводиться навчання (інструктаж) персоналу з подальшим контролем знань.

Детально про те, як розробити протипожежний режим, прописати порядки та інструкції, пояснюють на тематичних курсах і семінарах. [4]

Відповідно ДБН В 1.1-7-2016 «Пожежна безпека об’єктів будівництва» будинок можна віднести до II групи за ступенем вогнестійкості й до категорії Д за ступенем пожежонебезпеки.

Від розподільного щита по праву й ліву сторони встановлені кондиціонери, зовнішня електропроводка поміщена в ізольований кабель. Висота проводки становить 2,2 м від рівня підлоги. Біля кожного столу організований розподільний щит, розташований на текстолітовій пластинці, закріпленій на стіні на рівні 1м від підлоги. Усього до складу входять п'ять розеток і дві клеми заземлення. Всі обчислювальні машини з'єднані із клемами

заземлення. Чотири з п'яти розеток забезпечують подачу напруги 220 V, а одна, забезпечує подачу напруги в 36 V. Про це є відповідні написи на кожному розподільному щиті.

Робота обслуговуючого персоналу полягає в інсталяції необхідного програмного забезпечення й наступному його використанні в діалоговому режимі роботи з ЕОМ. Іноді може виникати необхідність написання допоміжних програм для поліпшення роботи вузла або для зниження витрат. З погляду забезпечення умов праці й вимог техніки безпеки для роботи програміста необхідно наступне: достатнє висвітлення екрана дисплея й робочого місця; повна технічна справність устаткування, його електробезпечність; достатня пожежна безпечність приміщення; оптимальний мікроклімат, що сприяє продуктивній роботі; відповідність робочого місця вимогам ергономіки. До небезпечних і шкідливих факторів, дії яких піддається програміст, можна віднести: можливість поразки електричним струмом, при електронесправності устаткування, порушенні заземлення або техніки безпеки; робота в мікрокліматі з неприпустимими параметрами; робота при недостатній освітленості екрану дисплея й робочого місця.

Відповідно НПАОП 40.1-1.21-98 “Правил безпечної експлуатації електроустановок споживачів” [6], приміщення можна віднести до приміщень без підвищеної небезпеки, оскільки це приміщення сухе, з нормальною температурою й ізолюючими підлогами, що не має заземлених металоконструкцій.

Персональні ЕОМ можна віднести до першого класу електротехнічних виробів за способом захисту людини від поразки електричним струмом, оскільки їхні корпуси зроблені з ізолюючої пластмаси й кожен пристрій має заземлення. Відповідно правилам пристрої електроустановок ЕОМ можна віднести до електроустановок з робочою напругою до 1000 В.

Однією з достовірних причин пожежі в приміщенні з обчислювальною технікою може бути коротке замикання, що спричиняє спалах електропроводки. Для його попередження вся обчислювальна техніка, а також інші електричні

пристрої повинні бути обладнані плавкими запобіжниками, а на вході електромережі повинен бути передбачений автомат захисту. Не слід користуватися електричними подовжувачами й трійниками, що не мають сертифікатів відповідності вимогам безпеки.

Необхідно передбачити наявність у межах досяжності первинних засобів гасіння пожежі (вогнегасників) для локалізації вогню власними силами до приїзду команди пожежної охорони. Повинен бути розроблений план екстреної евакуації персоналу при виникненні загоряння. Кількість евакуаційних виходів повинне бути не менш двох. Допускається використання одного евакуаційного виходу, якщо відстань найбільш віддаленого робочого місця до цього виходу не перевищує 25 м.

7.5 Розрахункова частина

Запорукою безпечної роботи в ІТ-сфері є виконання вимог електричної безпеки, оскільки все офісне обладнання заживлюється від електричної мережі. Одним з необхідних засобів електричної безпеки є встановлення захисного заземлення.

Початкові дані, необхідні для розрахунку захисного заземлення:

– допустимий опір розповсюдженню струму в землі від заземлювального пристрою $R_{зн}$ = 10 Ом;

– питомий опір грунту в місці встановлення заземлювача $\rho_з$ = 100 Ом/м;

– тип ґрунту – суглинок;

– тип заземлювача – труба, діаметром d=0.058 м і довжиною l =2.1 м; – конструкція заземлювача – розташування заземлювачів по контуру. Розрахунок проводимо за стандартною методикою [7].

Визначимо розрахунковий опір землі:

$$\rho_{рз} = \phi \cdot \rho_З$$

де ϕ – коефіцієнт сезонності, що враховує коливання питомого опору при зміні вологості ґрунту протягом року; при використанні заземлювача довжиною l = 2.1

м при глибині закладання від вершини h = 0.4 м ϕ = 1.1 для четвертої кліматичної зони.

Схема розташування заземлювачів показана на рисунку 7.1.

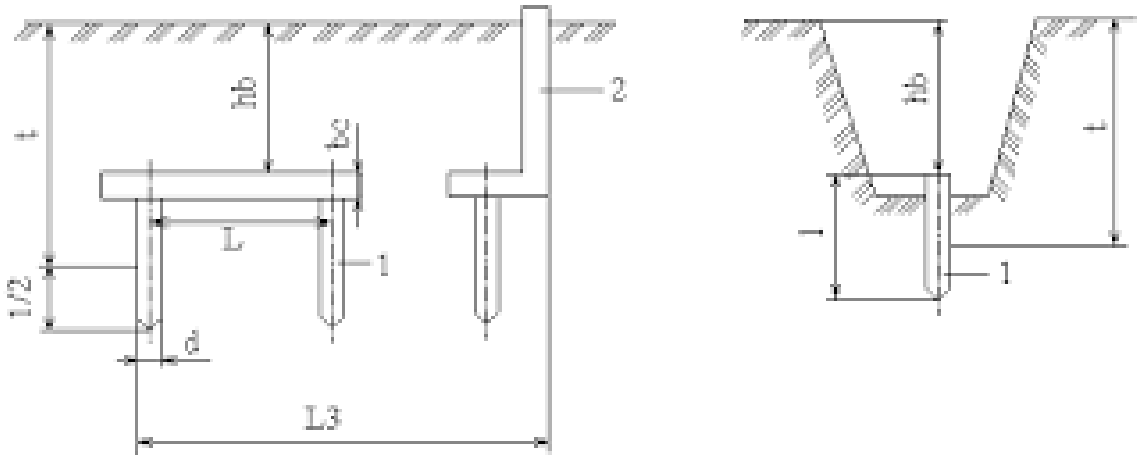

Рисунок 7.1 – Схема розташування заземлювачів

Опір землі:

$$\rho_{рз} = 1{,}1 \cdot 100 = 110 \text{ Ом·м}$$

Опір Rв, розповсюдженню струму в землі від одного вертикального заземлювача:

$$R_B = \frac{\rho_{рз}}{2\pi \cdot l}\left(\ln\frac{2 \cdot l}{d} + 0.5\ln\frac{4t + l}{4t - l}\right)$$

де

l – довжина заземлювача (l = 2.1 м);

d = 0.058 м – діаметр заземлювача при U<1 кВ та при S<100 кВА;

t – відстань від поверхні до середини заземлювача:

$$t = h + l/2 = 0.4 + 2.1/2 = 1.45 \text{ м.}$$

$$R_в = \frac{110}{2 \cdot 3.14 \cdot 2.1}\left(\ln\left(\frac{2 \cdot 2.1}{0.058}\right) + 0.5 \cdot \ln\left(\frac{4 \cdot 1.45 + 2.1}{4 \cdot 1.45 - 2.1}\right)\right) = 38.72 \text{ Ом}$$

Визначаємо потрібну кількість заземлювачів:

$$n' = \frac{R_в}{R_{зн}} = \frac{37.72}{10} = 3.9 \approx 4 \text{ шт.}$$

Коефіцієнт використання вертикальних заземлювачів враховує ефект екранування. При вибраному значенні k = a/l, де a – відстань між вертикальними заземлювачами, м; k = 1 при a = 1.5 м. Коефіцієнт використання вертикального заземлювача за довідковими даними дорівнює $\eta_В = 0,6$.

Кількість вертикальних заземлювачів з урахуванням коефіцієнту використання $\eta_В$ приблизно складає

$$n = \frac{R_в}{R_{зн} \cdot \eta_в} = \frac{38.72}{10 \cdot 0.6} = 6.45 \approx 7 \text{ шт.}$$

Довжина горизонтального заземлювача, необхідна для розміщення вертикальних заземлювачів по контуру

$$L = a \cdot n = 1.5 \cdot 7 = 10.5 \text{ м}$$

Опір горизонтального заземлювача $R_Г$, Ом, прокладеного на глибині h = 0.4 м від поверхні землі буде

$$R_г = \frac{R_{рз}}{2 \cdot 3.14 \cdot L} \cdot \ln \frac{2 \cdot L^2}{b \cdot h} = \frac{110}{2 \cdot 3.14 \cdot 10.5} \cdot \ln \frac{2 \cdot 10.5^2}{0.058 \cdot 0.4} = 15.7 \text{ Ом}$$

де b = 0.04 м – ширина сталевої смуги, з якої виготовлений заземлювач.

Обчислюємо загальний опір:

$$R_з = \frac{R_в \cdot R_г}{n \cdot R_г \cdot \eta_в + R_в \cdot \eta_г} = \frac{38.72 \cdot 15.7}{6 \cdot 15.7 \cdot 0.6 + 38.72 \cdot 0.34} = 8.13 \text{ Ом}$$

де $\eta_Г$ – коефіцієнт використання горизонтального заземлювача ($\eta_Г$ = 0.34).

Маємо 7.13 Ом < 10 Ом, отже нормативне обмеження для потужності генераторів та трансформаторів 100 кВт і менше $R_з < R_{з.норм}$ виконується.

8 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти, призначено для системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

В межах України в недостатній мірі представлені вітчизняні розробки в цій області.

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти наведені теоретичне узагальнення й рішення наукового завдання дослідження методів динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

– Досліджена система динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

– На основі отриманих результатів досліджень створена програмна реалізація системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання.

Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань.

При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем.

Програма реалізована на мові високого рівня PHP фреймворк Yii2. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

Програма призначена для виконання під управлінням багатозадачної операційної системи Windows 10/11.

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Протасов Р.Б. Дослідження та програмна реалізація системи динамічного профілювання поведінки користувачів із використанням методів кластеризації та глибокого навчання // Збірник праць молодих науковців ЦНТУ. – Вип. 17. – Кропивницький: ЦНТУ, 2027.
2. Foreman J.W. Data Smart: Using Data Science to Transform Information into Insight 1st Edition. – Wiley, 2013. – 432 p.
3. Hurbans R. Grokking Artificial Intelligence Algorithms. – Manning, 2020. – 631 p.
4. Gusfield D. Algorithms on Strings, Trees, and Sequences: Computer Science and Computational Biology 1st Edition. – Cambridge University Press, 2008. – 556 p.
5. Kotu V., Deshpande B. Data Science: Concepts and Practice. – Elsevier Science, 2018. – 953 p.
6. Knowledge Base A Complete Guide – 2021 Edition // The Art of Service – Knowledge Base Publishing, 2020. – 306 p.
7. Knuth D. The Art of Computer Programming, Vol. 1: Fundamental Algorithms, 3rd Edition 3rd Edition. – Addison-Wesley Professional, 2019. – 672 p.
8. Mattmann C. Machine Learning with TensorFlow, Second Edition. – Manning, 2020. – 1124 p.
9. Mueller J.P., Massaron L. Machine Learning For Dummies. – Wiley, 2016. – 714 p.
10. Teofili T. Deep Learning for Search. – Manning, 2019. – 695 p.
11. Rungta K. TensorFlow in 1 Day: Make your own Neural Network. – Publishdrive, 2019. – 587 p.
12. Weidman S. Deep Learning from Scratch: Building with Python from First Principles. – O'Reilly. 2019. – 252 p.
13. Rajasekaran S., Vijayalakshmi Pai G.A. Neural networks, fuzzy logic,

and genetic algorithms: synthesis and applications (with cd-rom) Kindle Edition. – PHI, 2013. – 628 p.

14. Vintenko, B., Myronets, I., Smirnov, O., Smirnova, T. «Enhancing the Reliability of Input Data for Nuclear Power Plant Operator Support Systems». *International Conference on Sensors, Devices and Systems. SDaS 2025. Lecture Notes in Electrical Engineering,* 2026. vol 1617. pp 3-12 Springer, Cham.

15. Богаченко, С., Смірнов, О., Буравченко, К., Смірнова, Т., Конопліцька-Слободенюк, О., Якименко, Н., Смірнов, С. «Обмеження ресурсів мобільних та edge-платформ при розробці програмного забезпечення для реалізації та оптимізації моделей машинного навчання». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2026, т. 2 № 34, С. 677-686.

16. Смірнов, О., Ткачук, Р., Козірова, Н., Константинова, Л., Конопліцька-Слободенюк, О., Якименко, Н., Смірнов, С.. «Дослідження застосування векторних баз даних у генеративному штучному інтелекті». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2026, Том 1 № 33, 667-682.

17. Вінтенко Б.Ю., Смірнова Т.В., Миронець І.В., Смірнов О.А., Буравченко К.О. «Метод оцінки функціональної стійкості комп'ютерно-орієнтованих процедур системи підтримки оперативного персоналу АЕС». *Системи управління, навігації та зв'язку*, 2026, вип. 2(84), С. 62-69.

18. Смірнов О., Заріцкий В., Буравченко К., Конопліцька-Слободенюк О., Константинова Л., Якименко Н., Смірнов С. «Оптимізація розпізнавання облич за допомогою CUDA прискореної бібліотеки dlib». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»,* 2026, Том 4, № 32, С. 573-582.

19. Лисенко, І., Минайленко, Р., Смірнов, С., Буравченко, К., Якименко, Н., Смірнов, О. «Дослідження інструментів штучного інтелекту для інтелектуального аналізу даних». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»,* 2025, № 3(31), С. 227–241.

20. Kuznetsov O., Frontoni E., Arnesano M., Smirnov O., Khruskov B. «Biometric Authentication in TinyML: Opportunities and Challenges». *Tiny Machine Learning: Design Principles and Applications*, 2026, pp. 587-633.

21. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». *Cybersecurity Defensive Walls in Edge Computing*, 2025. pp. 21-61.

22. Вінтенко, Б.Ю., Миронець, І.В., Смірнов, О.А., Коваленко, О.В., Усік, П.С., Буравченко, К.О., Лисенко, І.А. «Логіко-структурна модель комп'ютерно-орієнтованої процедури системи підтримки оперативного персоналу АЕС». *Кібербезпека: освіта, наука, техніка*. 2025. Том 2 № 30. С. 413-427, 2025.

23. Смірнова, Т.В. «Дослідження методів, моделей та сучасних ІТ-рішень для підтримки технологічних процесів у критичній інфраструктурі держави». *Кібербезпека: освіта, наука, техніка*. 2025. Том 2 № 30. С.195-208, 2025.

24. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». *Кібербезпека: освіта, наука, техніка*. 2025. Том 1 № 29. С.704–716, 2025

25. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 193–224.

26. Kuznetsov, O., Smirnov, O., Akhmetov, B., Alimseitova, Z., Imoize, A.L. «Deep Learning Frontiers in Copy-Move Forgery Detection: Advances, Challenges, and Future Directions». *Advancements in Cybersecurity Next Generation Systems and Applications*, 2025. 202-229.

27. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details».

International Review on Modelling and Simulations 18 (1), 2025. pp. 32-42.

28. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». *Центральноукраїнський науковий вісник. Технічні науки.* 2025. Вип. 11(42), ч. II. С.52-62.

29. Смірнов, О.А., Константинова, Л.В., Конопліцька-Слободенюк, О.К., Козірова, Н.В, Якименко, Н.М., Доренський, О.П., Буравченко, К.О. «Дослідження інструментів штучного інтелекту для роботи з базами даних та аналізу даних». *Кібербезпека: освіта, наука, техніка.* 2025. №3(27), С. 429–448.

30. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». *8th International Symposium on Intelligent Informatics, ISI 2023*, 2025. vol 389. pp 377-389. Springer, Singapore.

31. Smirnov O., Fedorov E., Neskorodieva A., Neskorodieva T. «Intellectual Classification method of Gymnastic Elements Based on Combinations of Descriptive and Generative Approache». *CEUR Workshop Proceedings* Volume 3664, 2024, Pages 11-23.

32. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.

33. Malyukov V., Bebeshko B., Lakhno V., Smirnov O., Malyukova I., Mohylnyi H. «Managing the Purchase-Sale Process of Digital Currencies Under Fuzzy Conditions». *Lecture Notes in Networks and Systems,* 2023, 729 LNNS, pp. 104–112.

34. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56.

35. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev,

S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings,* Volume 3530, 2023, pp. 256-265.

36. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.

37. Smirnov, O., Karapetyan, A., Fedorov, E., «Creating Neural Network and Single Solution Human-Based Metaheuristic Methods of Solving the Traveling Salesman Problem». CEUR Workshop Proceedings, Volume 3312, 2022, pp. 47-58.

38. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022, pp. 1-12.

39. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheroz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». Sensors (Basel, Switzerland) Volume 22, Issue 16, 6223, 2022.

40. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp. 21-34.

41. Kuznetsov, A., Oleshko, I., Chernov, K., Bagmut, M., Smirnova, T. «Biometric authentication using convolutional neural networks». Lecture Notes in Networks and Systems. Volume 152, 2021, Pages 85-98.

42. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. https://doi.org/10.1007/s42979-021-00739-w.

43. Smirnov O., Neskorodieva T., Fedorov E., Rymar P. «Neural Network

Modeling Method of Transformations Data of Audit Production with Returnable Waste». CEUR Workshop Proceedings Volume 3101, 2021, Pages 192-207.

44. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.

45. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.

46. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.

47. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.

48. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.

49. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.

50. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.

51. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.

52. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.

53. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». CEUR Workshop Proceedings, Vol 2588, P. 215-227, 2019.

54. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.

55. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.

56. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.

57. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.

58. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova,

K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.

59. Smirnov, S., Bulekbaeva, G., Kikvidze, O.G., Lakhno, V., Brzhanov, R., Tabylov, A. «Computer simulation in the MathCAD package of plastic deformation of the deposited layer on the flat surface of the part». Journal of Theoretical and Applied Information Technology Volume 97, Issue 20, 2019, Pages 2467-2484.

60. Smirnov A.A., Kuzne tsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.

61. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». Сучасні інформаційні системи. 2021. Т. 5, № 4. С. 79-95