НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»

НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)
«_____» _____ 2025 р.

Магістерська дисертація

на здобуття ступеня магістра

за освітньо-професійною програмою
«Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека та захист інформації»

на тему:

Застосування OSINT-технологій для оцінки часової активності користувачів Telegram як чинника витоку їхніх поведінкових характеристик

Виконав (-ла): здобувач вищої освіти **II** курсу, групи ФБ-41мп
Сахній Назар Романович _____
(прізвище, ім’я, по батькові) (підпис)

Керівник: Доцент кафедри ІБ, доцент, к.т.н.
Гальчинський Леонід Юрійович _____
(посада, науковий ступінь, вчене звання, прізвище, ім’я, по батькові) (підпис)

Рецензент: Доцент кафедри ФФФФФ, к.т.н.
Прізвище Ім’я По-батькові _____
(посада, науковий ступінь, вчене звання, прізвище, ім’я, по батькові) (підпис)

Засвідчую, що в цій магістерській роботі немає запозичень з праць інших авторів без відповідних посилань.

Здобувач вищої освіти _____
(підпис)

Київ – 2025 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»

НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

Рівень вищої освіти – другий (магістерський)
Спеціальність – 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)
«_____» _____ 2025 р.

ЗАВДАННЯ
на магістерську дисертацію здобувача вищої освіти

Сахнія Назара Романовича
(прізвище, ім'я, по батькові)

1. Тема роботи: Застосування OSINT-технологій для оцінки часової активності користувачів Telegram як чинника витоку їхніх поведінкових характеристик.

керівник роботи Гальчинський Леонід Юрійович, к.т.н., доцент.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом №4797-с по університету від «04» листопада 2025 р.

2. Термін подання здобувачем вищої освіти роботи «16» грудня 2025 р.

3. Вихідні дані до роботи: індикатори онлайн-статусу в месенджері Telegram.

4. Зміст роботи: аналіз можливостей використання індикаторів онлайн-статусу, отриманих із соціальної мережі Telegram, для побудови поведінкових моделей користувачів, розробка алгоритмічної основи збору та візуалізації часових даних активності, а також дослідження хронограм із метою виявлення поведінкових характеристик, періодів підвищеної вразливості користувачів та формулювання рекомендацій щодо мінімізації ризиків витоку конфіденційної інформації.

5. Перелік ілюстративного матеріалу: презентація

6. Дата видачі завдання: «22» вересня 2025 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Формулювання тематики та визначення напрямку написання дипломної роботи	01.09.2025-15.09.2025	виконано
2	Опрацювання наукових публікацій та професійно-технічних матеріалів.	08.09.2025-22.09.2025	виконано
3	Погодження теми та завдання на МД	22.09.2025	виконано
4	Дослідження впливу часових міток на конфіденційність користувачів та аналіз можливостей їх використання для побудови поведінкових моделей	22.09.2025-06.10.2025	виконано
5	Оцінка правових та етичних аспектів використання індикаторів онлайн-статусу як об’єкта OSINT-досліджень	29.09.2025-06.10.2025	виконано
6	Моделювання алгоритмічної основи збору та візуалізації часової активності користувачів Telegram із подальшою реалізацією програмного прототипу.	06.10.2025-20.10.2025	виконано
7	Експериментальний збір та статистичний аналіз хронограм активності користувачів Telegram для виявлення поведінкових моделей та періодів вразливості	20.10.2025-30.11.2025	виконано
8	Аналіз сценаріїв використання одержаних результатів для атак соціальної інженерії	20.11.2025-24.11.2025	виконано
9	Формулювання рекомендацій щодо мінімізації ризиків витоку конфіденційної інформації через індикатори присутності	24.11.2025-08.12.2025	виконано
10	Оформлення магістерської дисертації відповідно до методичних вказівок	08.12.2025-15.12.2025	виконано
11	Передзахист магістерської дисертації	16.12.2025	виконано
12	Захист магістерської дисертації	23.12.2025	

Здобувач вищої освіти _____ Назар САХНІЙ
(підпис) **(Власне ім’я, ПРІЗВИЩЕ)**

Керівник роботи _____ Леонід ГАЛЬЧИНСЬКИЙ
(підпис) **(Власне ім’я, ПРІЗВИЩЕ)**

РЕФЕРАТ

Магістерська дисертація містить 85 сторінок, що складаються із 3-ох розділів, 35 ілюстрацій, 2 таблиці, 1 додаток та 58 посилань на джерела інформації.

Актуальність роботи: в умовах активного використання месенджера Telegram, зокрема як ключового джерела отримання новин, особливої уваги набуває питання приватності індикаторів онлайн-статусу. З цієї причині потребується практична демонстрація того, наскільки подібна інформація може стати об'єктом OSINT-досліджень в соціальній інженерії. Це водночас дозволить не лише розкрити масштаби потенційних ризиків для конфіденційності, а й сформувати рекомендації щодо підвищення цифрової обізнаності користувачів Telegram. Адже наявність лише базових індикаторів «online/offline» може дати змогу досить точно відновити часові шаблони активності людини, визначити її найбільш вразливі періоди та відстежити синхронізацію між поведінковими моделями декількох користувачів.

Зв'язок роботи з науковими програмами, планами, темами: магістерська дисертація виконується у межах науково-дослідних тем кафедри інформаційної безпеки НН ФТІ «КПІ ім. Ігоря Сікорського», зокрема в напрямі «*Створення і дослідження методів і засобів OSINT як складової частини кібербезпеки*» [1]. Обрана тема відповідає також державній науково-технічній програмі розвитку сфери кібербезпеки в Україні та узгоджується з метриками реалізації «*Стратегії кібербезпеки України*» [2]. Роль автора полягає у розробці програмного сервісу для автоматизованого збору часових міток користувачів Telegram, а також подальшої їхньої оцінки із застосуванням методів OSINT та поведінкової аналітики.

Мета дослідження: на основі OSINT-технологій з'ясувати, які ризики носить публічне відображення онлайн-статусу в месенджері Telegram та сформулювати рекомендації щодо мінімізації виявлених ризиків ІБ.

Об'єкт дослідження: побудований на основі методології OSINT процес автоматизованого збору індикаторів онлайн-статусу користувачів Telegram та подальший процес оцінки їхньої часової активності.

Предмет дослідження: загрози конфіденційності інформації про поведінкові характеристики для користувачів Telegram, які виникають у процесі прихованої оцінки їхньої часової активності сторонніми особами.

Методи дослідження:

- Методи OSINT для збору відкритих даних про онлайн-присутність;
- Методи статистичного аналізу та візуалізації даних у вигляді хронограм;
- Методи порівняльного аналізу для побудови поведінкових моделей;
- Програмна реалізація із використанням Python та інтеграцією з Plotly.

Наукова новизна одержаних результатів полягає в тому, що вперше було продемонстровано можливості побудови поведінкових моделей користувачів на основі аналізу індикаторів онлайн-статусу месенджера Telegram, а також було досліджено вплив витоку цієї інформації для атак соціальної інженерії.

Практичне значення одержаних результатів полягає в тому, що в подальшій діяльності результати роботи можуть бути використані у таких сферах, як:

- OSINT – як інструмент збору поведінкових даних із відкритих джерел;
- HUMINT – як допоміжний засіб для непрямого спостереження й фіксації активності підозрюваних осіб під час оперативно-службових розслідувань;
- SOCMINT – як метод вивчення активності публічних осіб у соціальних мережах без порушення приватності їхніх персональних комунікацій;
- HCI – як база для проведення академічних досліджень у сфері взаємодії людини з комп’ютером, зокрема в рамках вивчення людської психології, поведінкових моделей і соціальної динаміки в цифрових середовищах.

Публікації: результати роботи були опубліковані на IX International Scientific and Practical Conference: «Education and science of today: intersectoral issues and development of sciences» (ст. 176-185), (28 листопада, 2025; Кембридж, ВБ).

Ключові слова: OSINT, індикатори онлайн-статусу, онлайн-присутність, конфіденційність, Telegram, поведінкові характеристики, витік чутливих даних.

ABSTRACT

The master's thesis contains 85 pages, consisting of 3 chapters, and 35 illustrations, and 2 tables, and 1 appendix, and 58 references to sources of information.

Relevance of the study: in the context of the widespread use of the Telegram messenger, particularly as a key source of news, the privacy of online status indicators becomes a pressing issue. Therefore, it is essential to practically demonstrate the extent to which such information can serve as an object of OSINT investigations in social engineering. This will not only uncover the magnitude of potential confidentiality risks, but also provide a basis for developing recommendations to enhance the digital literacy of Telegram users. Even basic «online/offline» indicators may allow for accurate reconstruction of individual activity patterns, identification of vulnerable periods, and detection of synchronization between the behavioural models of multiple users.

Connection with scientific programs, plans, and topics: this master's thesis was conducted within the framework of research projects of the academic department of Information Security in IPT, «Igor Sikorsky KPI», specifically in the direction «*Creation and research of OSINT methods and tools as a component of cybersecurity*» [1]. The selected topic also aligns with the state scientific and technical program for the advancement of cybersecurity in Ukraine and corresponds to the performance metrics of the «*Cybersecurity Strategy of Ukraine*» [2]. The author's contribution consists of developing a software service for the automated collection of Telegram users' timestamps and their subsequent assessment through OSINT techniques and behavioural analytics.

Purpose of the research: based on OSINT technologies identify the risks associated with publicly displaying your online status in the Telegram messenger and formulate recommendations for minimizing the identified information security risks.

Object of the research: an automated process for collecting online status indicators (OSI) of Telegram users based on OSINT methodology, followed by an assessment of their activity over time.

Subject of research: threats to the confidentiality of information about the behavioral characteristics for Telegram users, which arise in the process of assessment of their time activity by third parties.

Methods of research:

- OSINT techniques for collecting open data about online presence;
- Statistical analysis and data visualization in the form of chronograms;
- Comparative analysis methods for developing behavioural models;
- Software implementation using Python with integration into the ELK stack.

The scientific novelty of the obtained results lies in the fact that for the first time, this research demonstrates the feasibility of constructing user behavioural models based on the analysis of Telegram messenger online status indicators (OSI) and examines the impact of such information leakage on intelligence during social engineering attacks.

The practical novelty of the obtained results lies in the fact that, the outcomes of this research may be applied in the following scientific and professional areas:

- OSINT – as a tool for collecting behavioural data from open sources;
- HUMINT – as an auxiliary means for indirect intelligence and reporting of suspects' activities during operational and investigative procedures;
- SOCMINT – as a method for analysing the activity of public figures on social networks without intrusion into the privacy of their personal communications;
- HCI – as a foundation for academic research in the human-computer interaction field, particularly in studies of human psychology and social behavioural patterns.

Publications: the results of study were published at the IX International Scientific and Practical Conference: «Education and science of today: intersectoral issues and development of sciences» (p. 176-185), (November 28, 2025; Cambridge, UK).

Keywords: OSINT, online status indicators, online presence, confidentiality, Telegram, behavioural characteristics (and models), sensitive data leakage.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

OSINT – Open-Source Intelligence (Розвідка з відкритих джерел);

HUMINT – Human Intelligence (Агентурна розвідка);

SOCMINT – Social Media Intelligence (Розвідка соціальних медіа);

HCI – Human-Computer Interaction (Людино-машинна взаємодія);

OSI – Online Status Indicators (Індикатори онлайн-статусу);

UI – User Interface (Користувацький інтерфейс);

IM – Instant Messaging (Миттєві повідомлення);

API – Application Programming Interface (Прикладний програмний інтерфейс);

MTProto – Mobile Protocol (Протокол обміну повідомленнями в Telegram);

CSV – Comma-Separated Values (Значення, що розділені комою)

HTML – HyperText Markup Language (Мова розмітки гіпертексту).

ВСТУП

Індикатори онлайн-статусу (OSI) – це елементи користувацького інтерфейсу (UI), які автоматично передають інформацію про те, коли користувач з'являється в мережі або ж виходить з неї. Інформація про присутність виводиться на основі взаємодії із цільовим застосунком. Наприклад, месенджер Telegram автоматично встановлює статус присутності як «онлайн» («online»), коли його застосунок знаходиться на передньому плані, і як «офлайн» («offline»), коли він знаходиться на задньому плані. Крім цього, є функція «останньої активності» («last seen»), при ввімкненні якої ніхто не зможе дізнатися, чи цільовий користувач наразі перебуває онлайн. Проте існують деякі винятки, оскільки іноді очевидно, що користувач все ж перебуває в мережі. Незалежно від налаштувань останньої активності, люди бачитимуть статус «в мережі» протягом короткого періоду (~30 секунд), якщо на цей момент разом взаємодіятимуть в особистому або ж груповому чаті [30].

Коли OSI показує, що користувач активно взаємодіє із застосунком, то це сигналізує іншим, що даний користувач потенційно доступний до соціальних взаємодій. Коли OSI показує, що користувач перебуває офлайн, то це означає, що даний користувач, ймовірно, не зможе швидко відповісти або не доступний для зв'язку. Хоча таке використання OSI дозволяє покращити досвід користування застосунком, однак попередні дослідження показали, що OSI можуть розкривати конфіденційну інформацію, пов'язану із часовою активністю користувача [1], такою як їхній режим сну або навпаки неспання, відволікання на робочому місці, партнери по спілкуванню, а також незвичні відхилення в щоденному графіку.

Незважаючи на те, що OSI, як вже стає зрозуміло, мають проблемні наслідки для конфіденційності користувачів, на даний момент немає чіткого розуміння того, яким чином отримана інформація може бути корисною в рамках атак соціальної інженерії. Тим самим, звичайні користувачі не усвідомлюють всіх ризиків, які виникають під час дослідження часових міток їхніх соціальних мереж. Наскільки

чутливими стають поведінкові характеристики, отримані з хронограм активності? Як OSINT-технології дозволяють автоматизувати процес збору OSI? Чи можливо передбачати життєвий ритм користувача, а також визначити, коли він найбільш вразливий до атак соціальної інженерії? Яким чином і якою мірою користувачі можуть передбачити та контролювати інформацію, яку передають їхні OSI?

Результати досліджень конкретних OSI свідчать про те, що відповіді на деякі з цих питань в певних контекстах можуть бути досить тривожними з точки зору недостатньо вивчених ризиків для користувачів. OSI можуть розкрити, як довго людина залишається на вечірці, о котрій годині прокидається вночі, як часто відвідує свій месенджер в робочий час, який її стиль онлайн-спілкування, чим займається «поза мережею» або ж навіть хто з ким і як задовго розмовляє [1].

Проте OSI є поширеними і цінними компонентами мобільних застосунків, а сама можливість швидко переглянути онлайн-статус інших користувачів стала стандартною функцією, на яку користувачі розраховують і покладаються. Таким чином, постійна відмова від використання OSI через потенційні ризики для конфіденційності є не тільки непрактичною, але й суперечить їхній ключовій особливості, яку ці функції надають користувачам [2]. Натомість необхідно точно визначити ризики, які становлять OSI, і критично оцінити їхнє значення в сучасних реаліях. Зокрема, для українського сегменту користувачів Telegram ця проблема набуває особливої актуальності, адже саме цей застосунок наразі є провідною платформою онлайн-комунікацій і ключовим джерелом отримання новин [42].

На сьогодні, в умовах воєнного часу, будь-яка загроза, пов’язана з витоком поведінкових характеристик користувачів, може мати не лише індивідуальний, але й також суспільно небезпечний ефект. Навіть часткове нехтування подібними налаштуваннями приватності профілю здатне створювати ризик систематичного спостереження не тільки за окремими людьми, але й за цілими спільнотами [1].

1 АНАЛІЗ МОЖЛИВОСТЕЙ ОЦІНКИ ІНДИКАТОРІВ ОНЛАЙН-СТАТУСУ ДЛЯ ПОБУДОВИ ПОВЕДІНКОВИХ ХАРАКТЕРИСТИК

1.1 Цифрова присутність як об’єкт дослідження поведінкових моделей

1.1.1 Призначення та еволюція OSI в застосунках

Індикатори онлайн-статусу (OSI) історично з’явилися як елемент інтерфейсу служб миттєвих повідомлень (IM) для позначення факту присутності користувача у мережі та його доступності до взаємодії. Ще в 2000 році в журналі CSCW було опубліковано статтю, в якій було описано дослідження із використання IM 20 працівниками. Автори на той час визначили «інформацію про присутність інших» як ключову особливість AIM і продемонстрували, що вона полегшує «узгодження доступності» між відправниками та одержувачами у порівнянні з електронною поштою чи очними зустрічами [2]. Одним із практичних висновків була також потреба забезпечити одержувачу простір для правдоподібного заперечення факту перебування онлайн, аби зменшити соціальний тиск на негайну відповідь.

Широкий спектр подальших досліджень був тоді присвячений вивченню можливостей використання «обізнаності» для поліпшення онлайн-спілкування та співпраці. Наприклад, завдяки тому, що інформація про доступність та нові повідомлення стає помітною лише периферійно, то тим самим особові чати можуть менше відволікати увагу користувачів, коли вони зайняті [3, 4]. В інших роботах пропонувалося допомогти користувачам орієнтуватися в онлайн-спілкуванні шляхом включення таких джерел даних, як їхній онлайн-календар та фізичні мітки, щоб дізнатися доступність (або її відсутність), а не тільки присутність [5, 6].

1.1.2 Наслідки використання OSI в месенджерах

З метою виявлення передбачуваних ризиків для конфіденційності при обміні інформацією про онлайн-присутність з мобільних застосунків, дослідники з Ульмського університету провели дослідження в 2013-2014 роках, в ході якого зібрали та проаналізували інформацію про присутність двох незалежних груп користувачів WhatsApp [1]. Дане дослідження стало фундаментальним при написанні автором цієї роботи. Вони розглянули ризики для конфіденційності, що виникають між користувачами, які при наявності лише доступу до інформації про присутність один одного можуть мати непрямий контроль над діями інших осіб. Їхні результати показують, що інформація про присутність мобільних месенджерів є достатньою для того, щоб з достатньою точністю визначити моделі поведінки.

По завершенню експерименту вони провели інтерв'ю зі своїми учасниками, щоб перевірити їхню поведінку в період дослідження та зрозуміти їхнє сприйняття виявлених наслідків для конфіденційності. Результати виявилися показовими: графіки присутності практично один в один відобразили реальні розпорядки дня учасників та їх соціальну активність. Учасники з подивом впізнавали на діаграмах свої щоденні рутини такі, як час засинання і підйому, перерви (наприклад, похід в спортзал щосереди чи «тиша» під час наради), вечірки до пізньої ночі, тощо.

Незважаючи на те, що як приклад досліджувався WhatsApp, проте автори зазначають, що виявлені наслідки для конфіденційності можуть так само стосуватися й інших соцмереж, які відображають мітки онлайн-присутності.

Ці висновки приводять до гіпотези, що OSI з мобільних месенджерів, які надсилаються щоразу, коли застосунок відкривається або закривається, можуть розкривати діяльність та моделі поведінки користувачів, оскільки мобільні месенджери використовуються ними майже регулярно протягом дня [7, 8].

1.1.3 Можливість побудови моделей поведінки

Автор в цій роботі стверджує, що виявлені добові графіки онлайн-активності користувача соцмереж можна безпосередньо пов’язати з циркадними біоритмами. Циркадні ритми – це приблизно 24-годинні денні цикли коливань фізіологічних і поведінкових характеристик організму, що охоплюють добовий сон, гормональну активність, харчування та навіть соціальну поведінку [9]. Наукове значення цього механізму підтверджене тим, що у 2017 році Нобелівську премію з фізіології та медицини було присуджено за відкриття молекулярних механізмів, які здатні контролювати циркадний ритм [10]. Внутрішній біологічний годинник людини з високою точністю синхронізує роботу організму з зміною дня і ночі, регулюючи поведінку, рівні гормонів, цикли сну, температуру тіла та обмін речовин. Якщо ж добовий розпорядок вступає в конфлікт із цим внутрішнім ритмом, погіршується самопочуття і зростає ризик фізичних та психічних розладів [9]. Недотримання природних ритмів призводить до хронічної втоми, зниження мотивації та коливань емоційного стану [11]. Таким чином, циркадні коливання безпосередньо впливають на психоемоційний стан людини та її готовність до взаємодії у той чи інший час доби. Практичні дослідження демонструють, що активність людей у спілкуванні теж підпорядковується добовим пікам і спадам – вечорами соціальна залученість зазвичай максимальна, тоді як у ранні ранкові години вона мінімальна [12].

З огляду на це, врахування циркадних ритмів при моделюванні поведінки користувачів має прикладну цінність під час здійснення OSINT-розслідувань. Профіль вразливості до атак соціальної інженерії можна будувати, беручи до уваги, коли користувач найбільш і найменш уважний та схильний до впливу. Відомо, що когнітивні ресурси людини обмежені та нерівномірно доступні впродовж доби. Наприклад, одразу після пробудження або пізно ввечері, під час природного спаду бадьорості, користувач може діяти менш обачливо [13]. Наукові експерименти підтверджують: втома і високий ментально навантажений стан суттєво знижують

здатність зосереджувати увагу на потенційних загрозах [12]. Іншими словами, людина, яка перебуває не у своїй оптимальній фазі добового циклу, більш схильна пропустити маніпулятивні сигнали. Отже, як стверджує психологія, спеціаліст HUMINT може навмисно обрати час атаки – наприклад, ранкові години, коли користувач ще не увійшов у робочий ритм, або пізній вечір, коли накопичена втома притупляє пильність – щоб підвищити ймовірність успіху соціальної інженерії [14]:

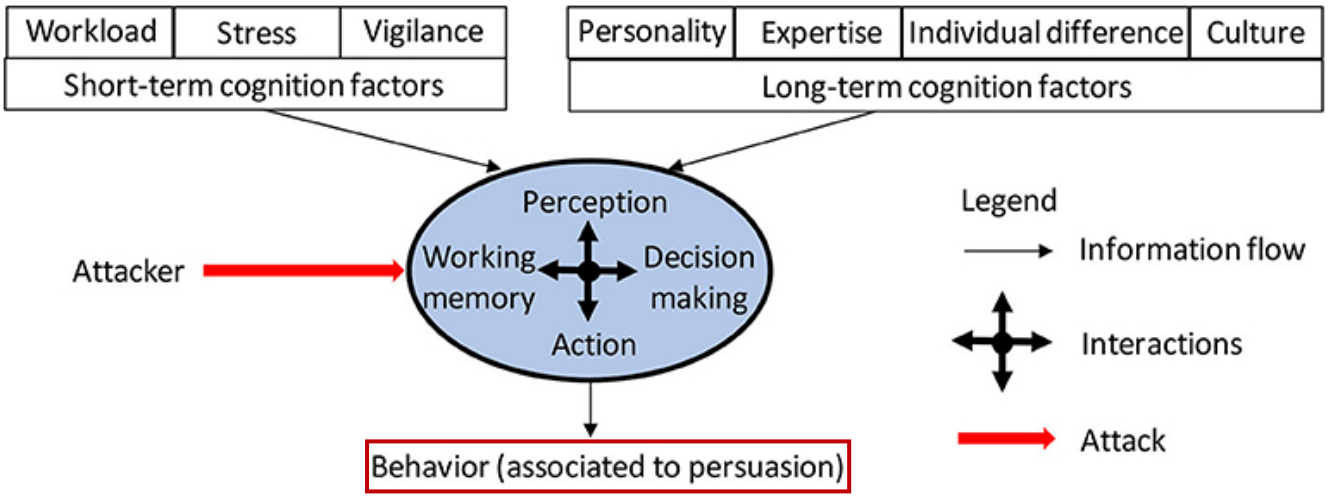

Рисунок 1.1 – Схема людських когнітивних здібностей, де синій фон в овалі вказує на довготривалу пам’ять, з якої формується поведінка в момент атаки

Таким чином, інтеграція циркадних ритмів у моделі поведінки користувачів є обґрунтованою і необхідною. Вона дозволяє глибше зрозуміти добову динаміку онлайн-поведінки та психоемоційний стан користувача, що дає змогу прогнозувати моменти підвищеної вразливості. Тим самим це підсилює як наукову ґрунтовність поведінкових моделей, так і практичну необхідність бути обізнаним з основами ІБ.

1.1.4 Хронограми активності із відомих соцмереж

З огляду на наявні дослідження про Facebook Messenger і WhatsApp, у яких показано можливість відтворення добових патернів за мітками «online/last active», далі наведемо короткий огляд цих підходів як передумову для роботи з Telegram.

- **WhatsApp**

З огляду на результати досліджень науковців з Ульмського університету, месенджер WhatsApp виявився джерелом витоку поведінкових даних тільки на основі аналізу індикаторів онлайн-статусу. Проблема пов’язана із аналогічними до Telegram мітками WhatsApp, які інформують про онлайн-присутність [1].

Таким чином, звичайні на перший погляд, статуси «last seen» та «online» дозволяють дізнатися інформацію про те, як проводите свій час, а особливо про те, коли і скільки спите. Особливо тривожним є те, що практично будь-хто, хто має хоч трохи технічних знань і вільний ноутбук, може зловживати цією вразливістю.

Рисунок 1.2 – Інформація про присутність у месенджері WhatsApp, що показує **a) статус онлайн** та **b) час останньої активності**.

Дослідники візуалізували зібрані дані про присутність, щоб полегшити ідентифікацію потенційних моделей поведінки та наслідків для конфіденційності. Нижче продемонстровано їхню візуалізацію для повного дня однієї з груп. Для кожного учасника (рядки) смуга на часовій шкалі представляє період активного використання WhatsApp. Кожен період використання був визначений парою відповідних міток «доступний/недоступний». Хоча візуалізація подій дозволяє побачити, коли учасники активно використовували WhatsApp, цікавою є додаткова інформація, яку можна було б отримати з цих даних. Тому, крім розрахунку статистики використання, вони досліджували можливість визначення щоденних звичок (наприклад, часу сну або робочих годин), а також партнерів по спілкуванню.

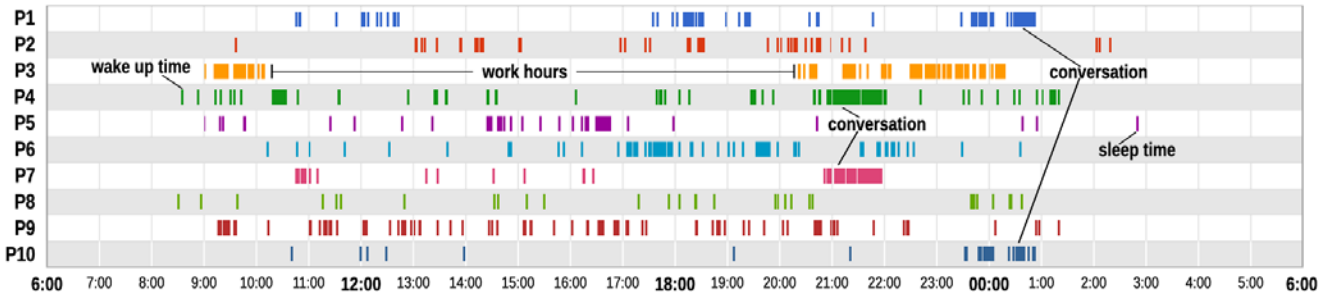

Рисунок 1.3 – Інформація про присутність, що показує активність групи №1 у WhatsApp протягом одного дня. Смуга на часовій шкалі відображає час активного використання WhatsApp. Позначені приклади демонструють, що інформація про присутність може розкривати час пробудження та сну, щоденні звички та розмови.

Якщо порівняти моделі онлайн-активності однієї людини з моделями іншої, то перекриття їхніх хронограм може дозволити з'ясувати, чи спілкуються контакти один з одним. Наприклад, якщо людина заходить в інтернет, щоб написати одному зі своїх контактів, то цей контакт, досить ймовірно, що також з'явиться в інтернеті, щоб відповісти. Як тільки це почне перетворюватися на закономірність, то стане можливим порівняти цю часову активність, щоб з'ясувати, наскільки ймовірно, що ці двоє людей спілкувалися один з одним, і який їхній стиль онлайн-спілкування.

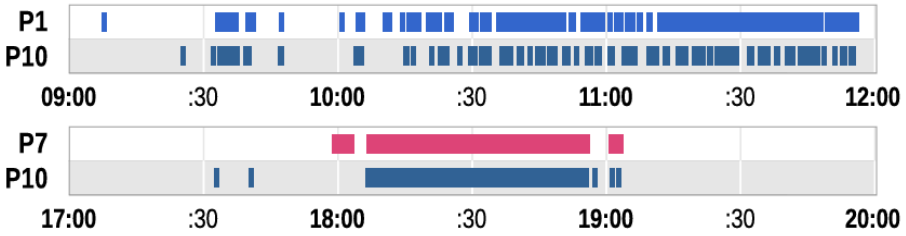

Рисунок 1.4 – Інтенсивна розмова між особами P1 і P10 тривалістю 144 хвилини (вгорі) та зосереджена розмова тривалістю 64 хвилини між P7 і P10 (внизу)

Зібрані статистичні дані про онлайн-активність дозволяють також виявити відхилення від щоденної рутини, наприклад, більш тривале використання вночі або незвично довгі перерви протягом дня. Повторювані відхилення, наприклад, довгі перерви в певні дні тижня, дозволили науковцям Ульмського університету припустити, що учасники екперименту виконували щотижневі заходи, під час яких не можна було користуватися мобільними пристроями, наприклад, під час занять

спортом або репетицій. Під час заключних інтерв'ю учасників попросили пояснити відхилення в їхніх моделях використання за останній тиждень перед інтерв'ю.

Всі учасники були вражені тим, як добре можна було відобразити їхню діяльність: «*так, тут я був у суботу ввечері [...] тут ви бачите, як довго я ходив у спортзал у вівторок і що я грав у баскетбол у середу*» (P1), «*в п'ятницю я ходив по барах до 5 ранку*» (P2), «*тут ви можете побачити мій післяобідній відпочинок і нашу робочу вечірку в суботу*» (P3), «*так, у п'ятницю я був на вулиці до 3:46 ранку*» (P4) і «*тут я катався на лижах і не мав підключення до мережі*» (P5). Учасниця P4 також зазначила, що вона була у відпустці в іншій країні протягом вихідних, що було чітко видно з довгої паузи порівняно з її звичним використанням WhatsApp.

Всі учасники другої групи підтвердили свою присутність на студентській вечірці в ніч з середи на четвер, що було чітко видно з багатьох міток, пов'язаних з онлайн-активністю у 8 учасників після 1 години ночі в звичайний будній день:

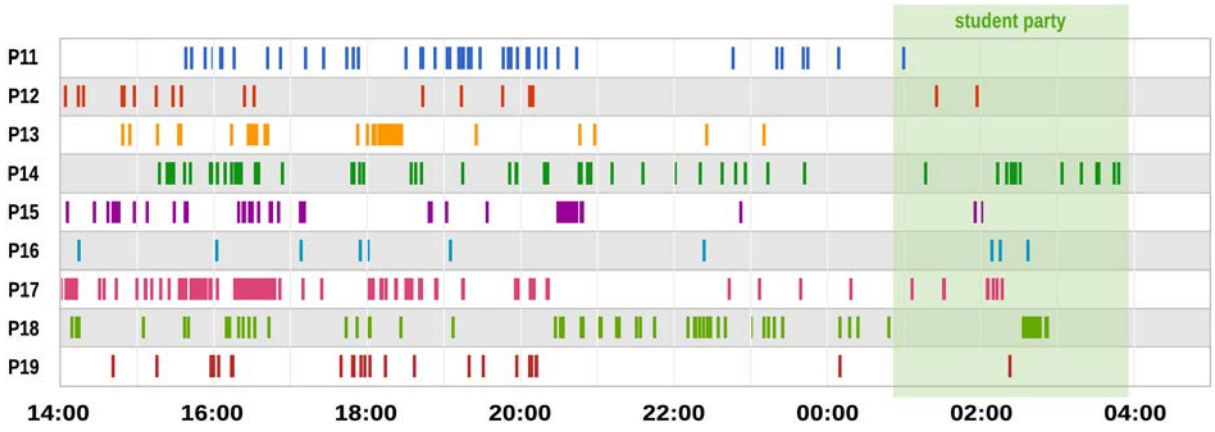

Рисунок 1.5 – Інформація про присутність групи №2, яка демонструє, що 8 учасників все ще були онлайн після 1-ої ночі через студентську вечірку.

Хоча правильне визначення видів діяльності часто залежить від додаткових відомостей про цільову особу (наприклад, інформація хобі чи професія), отримані результати підкреслюють можливість автоматичного виявлення щоденних звичок та їхніх змін, що може мати кілька наслідків для конфіденційності. Знаючи, що хтось зазвичай займається спортом по середах і не використовує месенджери в цей час, легко спостерігати, чи ця людина регулярно тренується (наприклад, коли не

було перерви в активності її месенджера). Хоча успіх ідентифікації таких щоденних звичок і їхніх змін залежить від частоти використання, статистичні результати аналізу часової онлайн-активності демонструють, що більшість учасників дуже часто використовували WhatsApp, а середній час між сеансами становив менше 40 хвилин. Лише двоє учасників (P5, P7) використовували WhatsApp рідше.

Однак навіть для користувачів, які використовують застосунок не так часто, зміни вночі легше вдавалося ідентифікувати, оскільки вони зазвичай спричинені соціальними активностями (наприклад, вечірками або походами по пабах), тому часто передбачали обмін кількома текстовими повідомленнями або фотографіями.

Як підсумок, дослідники зазначили, що ці дані також можна легко збирати у великих масштабах, а потім продавати стороннім компаніям для рекламних цілей. Тут і виникають наслідки для приватності життя, адже це може бути використано для моніторингу часу сну та його змін під час оцінки продуктивності, наприклад співробітників. Людина, яка регулярно лягає спати о 22:00, ймовірно, буде більш відпочилою та продуктивною, ніж та, яка часто «зависає» аж до ранку.

- **Messenger**

Щодо Facebook-месенджера, то на сьогодні відомо як в 2016 році один дослідник у своєму професійному блозі на платформі Tumblr вразливість розкриття поведінкових характеристик завдяки фіксації індикаторів онлайн-статусу [15].

Ця робота була публічно продемонстрована як доповідь «Graphing when your Facebook friends are awake» на PyCon Australia 2016 [16], що підтверджує наукову й практичну релевантність тематики, а також демонструє можливість апробації подібних підходів у дослідженнях про цифрову поведінку користувачів.

Автор статті демонструє, як за допомогою відтвореного мережевого запиту через інструменти розробника (DevTools) можна отримати дані про онлайн-

присутність користувачів Messenger. Ключовим аспектом цього дослідження є те, що попри відсутність офіційного API для доступу до OSI, дослідник реалізував власний недокументований запит до сервісу через функціональний виклик `/pull`.

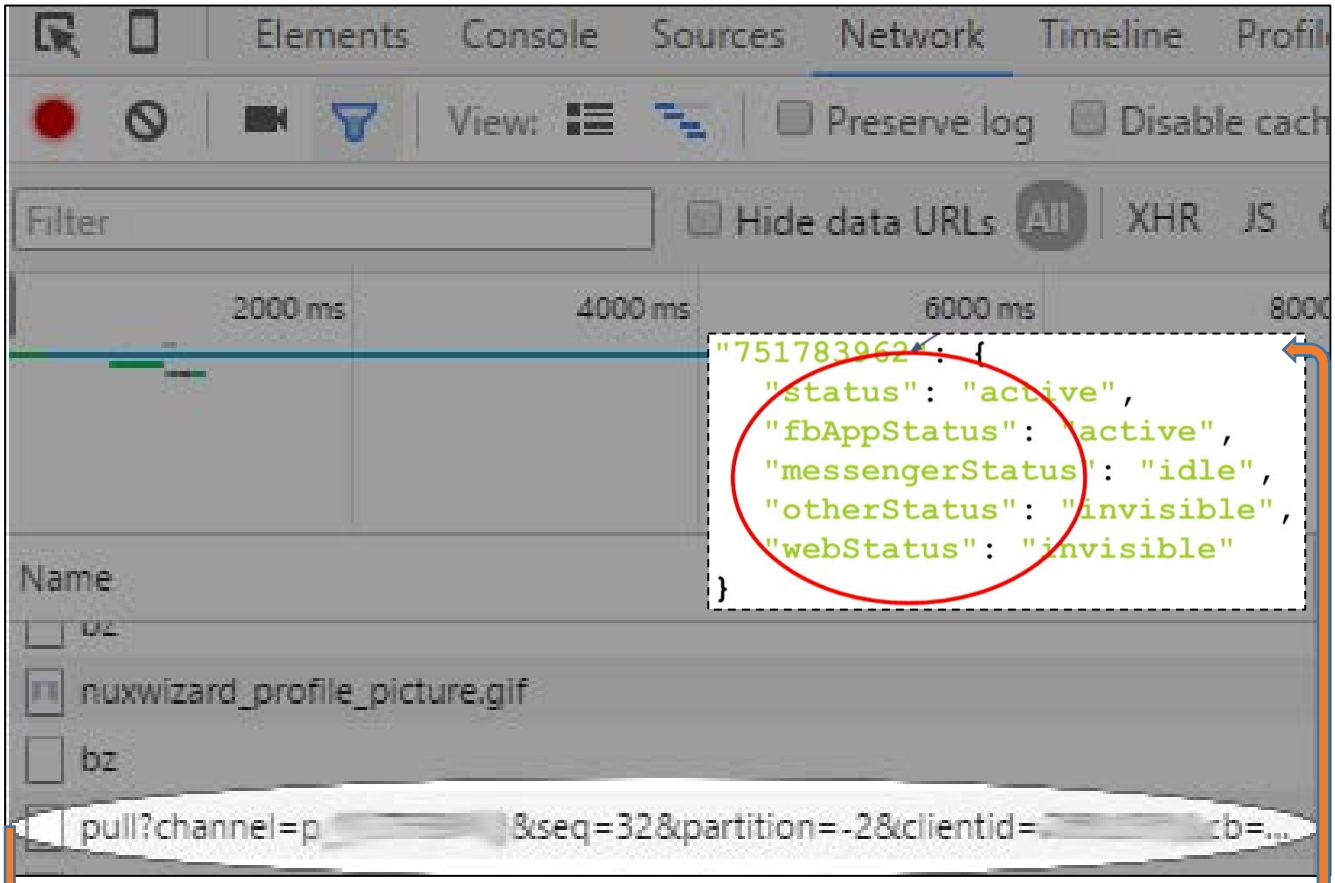

Рисунок 1.6 – Інструменти розробника в контексті Facebook-запитів

Рисунок 1.7 – Фрагмент відповіді `/pull` з полем «last active» (Unix-Time)

На основі зібраних часових серій автор побудував покадрові хронограми, де по осі X – час, а по осі Y – стан («offline», «invisible», «idle», «active») кожного з OSI. З таких графіків він зміг відновити періоди сну та робочої зайнятості.

За результатами продемонстровано високу кореляцію між зафіксованими часовими інтервалами та реальним розпорядком дня. На прикладі одного серед користувачів зафіксовано збіг часу пробудження із налаштуванням будильника на 08:30, що підтверджує достовірність хронограм як проксі-моделі сну та активності. Зроблено висновок, що навіть короткочасна взаємодія з платформою перед сном чи після пробудження забезпечує достатню точність відтворення добових циклів.

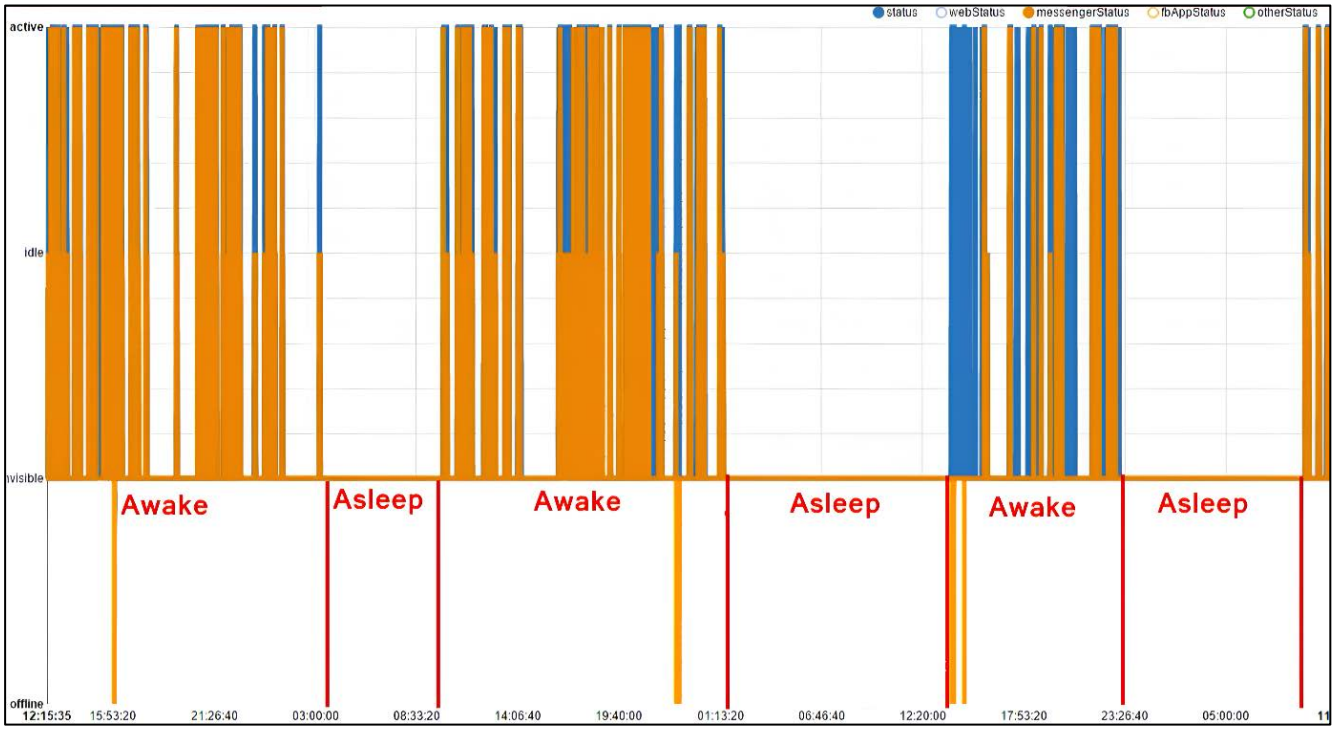

Рисунок 1.8 – Зразок хронограми активності користувача Facebook з інтерпретацією періодів asleep/awake («спить»/»не спить»)

Крім основного аналізу, автор запропонував додаткові напрями оброблення зібраних даних – зокрема, агрегування показників для визначення середніх годин сну та пробудження, пошук аномалій у добових ритмах, а також спроби виявлення потенційних взаємодій між користувачами шляхом аналізу їхньої «синхронності».

1.2 Оцінка правових та етичних аспектів збору міток «online/offline»

1.2.1 Поширеність сервісів моніторингу OSI

Збирання даних про online/offline-статуси набуло поширення завдяки появі сторонніх сервісів моніторингу [17], один із яких наведений нижче. Такі застосунки можуть фіксувати час входу користувача в мережу і тривалість перебування онлайн. На практиці це означає, що третя особа здатна отримувати сповіщення в реальному часі про зміну статусу чужого облікового запису та зберігати ці відомості в хронологічному порядку. Розробники подібних сервісів підкреслюють, що використовують лише відкриті дані, доступні у самих месенджерах, і не збирають конфіденційну інформацію поза офіційними межами платформи [18]. Популярність цих інструментів зумовлена попитом переважно серед пересічних користувачів, зацікавлених «тримати в полі зору» онлайн-активність близьких осіб.

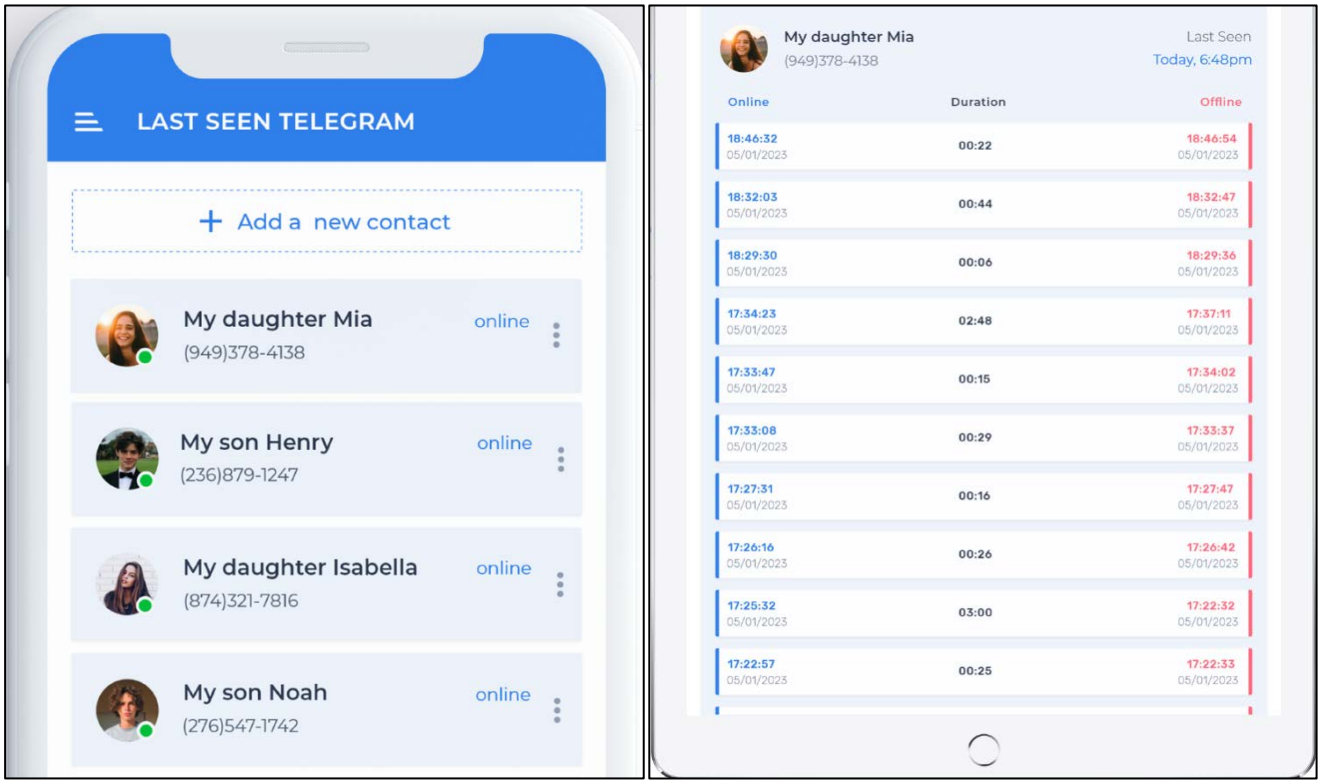

Рисунок 1.9 – Інтерфейс, на якому відображаються періоди останньої активності

Як з’ясували дослідники платформи Traced [17], існують ще також сервіси, які дозволяють будь-кому одночасно відстежувати два номери та порівнювати їхню активність. Таким чином, можна зробити висновок, чи спілкуються прямо зараз ці двоє людей одне з одним в месенджері WhatsApp. Попри цю особливість, подібний застосунок дозволяє своїм користувачам, в контексті WhatsApp, також наступне:

- Бачити «last seen» в мережі контактів, якими стежать.
- Моніторити за декількома контактами одночасно.
- Отримувати миттєві повідомлення про online/offline.
- Переглядати звіти в зручному журналі активності.

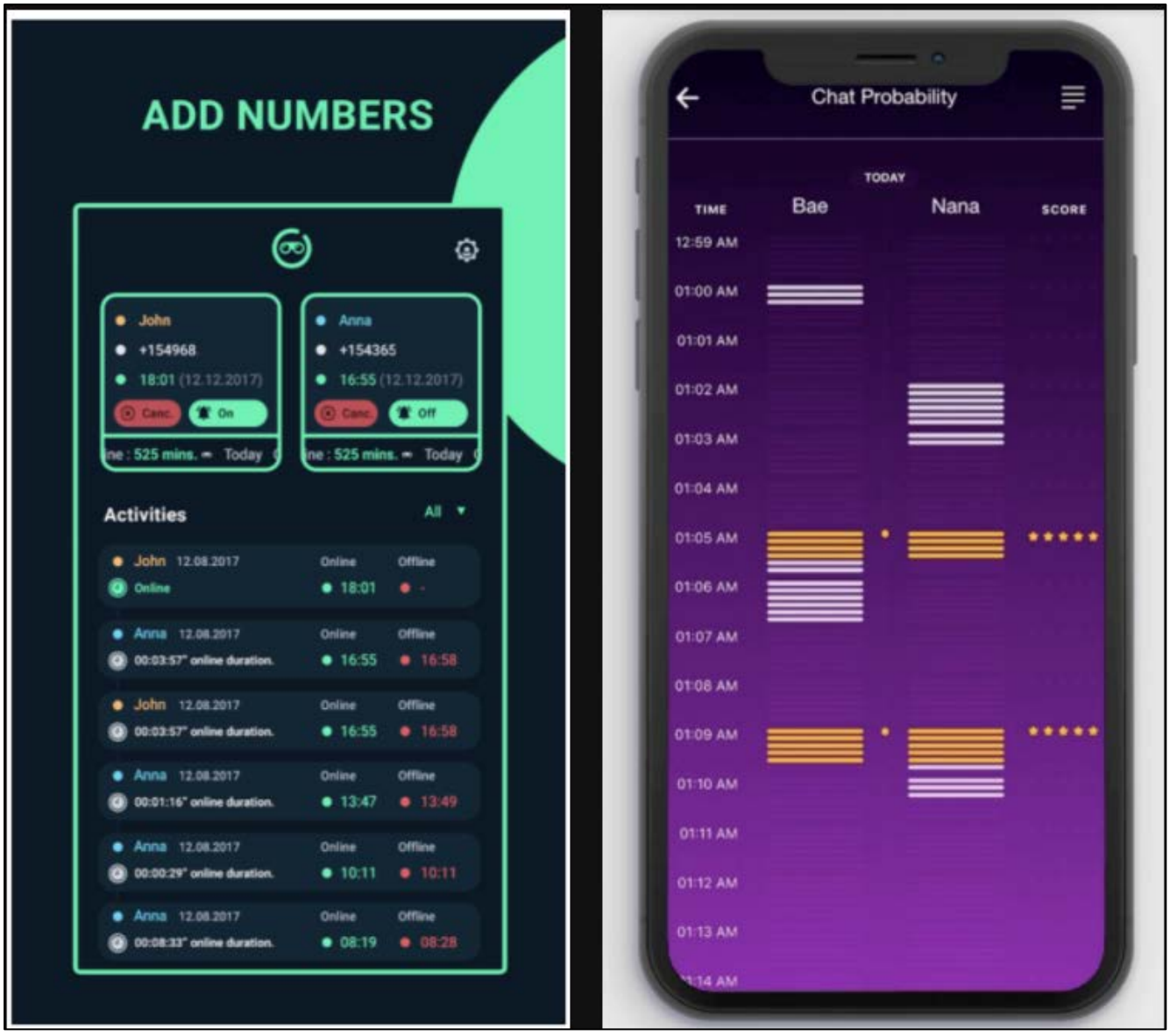

Рисунок 1.10 – Моніторинговий сервіс, що здійснює збір OSI із WhatsApp

Ці функції ілюструють, що навіть проста телеметрія онлайн-присутності формує поведінкові профілі, на підставі яких можливі подальші інтерпретації. На рівні користувацьких практик це підтверджує реальний досвід користування, що був наведений в соцмережі Reddit, де одна користувачка детально описала про власний досвід стеження за своїм партнером завдяки подібним можливостям [17]:

«*Я була вражена тим, наскільки добре працював цей застосунок і скільки розуміння я змогла отримати про психоемоційний стан з таких простих даних, тому я продовжувала спостерігати за його активністю протягом наступного тижня. Оскільки я почала користуватися цим застосунком, коли він спілкувався зі мною лише через WhatsApp, тепер я могла помітити закономірності, коли він справді веде глибоку розмову з кимось, а коли постійно перевіряє, чи є відповідь*».

З огляду на виявлені ризики, експертні спільноти послідовно закликають виробників запобігти зловживанню OSI ще на стадії дизайну. Відповідну позицію висловила Ева Гальперін, одна з провідних світових експертів в цій галузі, а також директорка з кібербезпеки в компанії EFF (Electronic Frontier Foundation) [19]:

«*Це просто недбала робота з боку WhatsApp і типовий приклад того, що відбувається, коли компанії не думають про ризики під час прийняття рішень щодо дизайну. WhatsApp мав би надати користувачам можливість вимкнути свій онлайн-статус з самого початку, і вони повинні виправити це якомога швидше*».

Позиція самої платформи окреслює архітектурні обмеження. Представник WhatsApp на той момент пояснив, що застосунок розроблений таким чином, що користувачі завжди бачать, чи перебувають інші користувачі онлайн. В офіційному FAQ щодо налаштування конфіденційності WhatsApp зазначалося, що «немає способу приховати, коли ви онлайн або друкуєте» [29]. Такий підхід, з одного боку, нормалізує видимість присутності як елемент користувацького досвіду, а з іншого – робить можливим автоматизований збір відповідних сигналів третіми сторонами.

Однак реакція платформи на дії подібних сервісів була показовою: [29]

«*Ми заблокували облікові записи WhatsApp, пов'язані з цим застосунком, а також звернулися до Google із проханням видалити їх застосунок із "Play Store" та надіслали особі, яка стоїть за ним, наказ про припинення подібної діяльності. Автоматизація функцій WhatsApp для збору інформації є порушенням наших умов обслуговування, і ми надалі вживатимемо заходів для захисту конфіденційності*».

1.2.2 Політика конфіденційності Telegram

Офіційні політики та налаштування конфіденційності месенджерів по-різному регламентують видимість OSI. Зокрема, Telegram надає користувачу досить гнучкий контроль – можна обмежити коло осіб, які бачать час останньої активності («last seen» та «online»): <всі>, <мої контакти> або <ніхто>.

Однак існують винятки, адже якщо користувач взаємодіє з кимось у приватному чи груповому чаті, система все одно короткочасно (~30 секунд) покаже його статус «в мережі» незалежно від налаштувань [30]. Водночас Telegram, як і багато інших соцмереж, побудований на принципі взаємності – якщо користувач приховує власний статус, то він не зможе бачити й статуси інших [31].

Автором експериментально підтверджено, що при обмеженні доступу до OSI, навіть із врахуванням щойно згаданих винятків, запити до документованого API (зокрема, Telethon) не повертають навіть короткочасної індикації онлайн-присутності. Це свідчить про те, що при подібних налаштуваннях автоматизований збір OSI є технічно обмеженим і не може бути налаштований у межах офіційних інтерфейсів взаємодії. Проте раніше згаданий приклад про збір OSI із «Facebook Messenger» через DevTools вказує на наявність альтернативних шляхів [15].

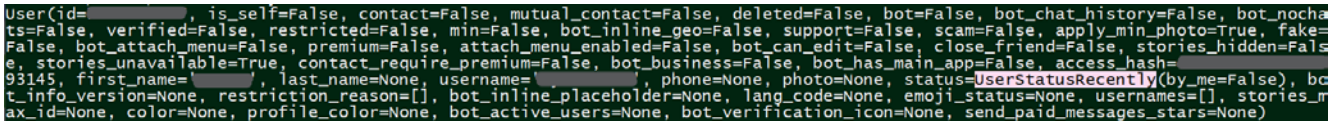

Рисунок 1.11 – Отриманий через API статус в момент взаємодії з користувачем

Потрібно зазначити, що попередні наукові дослідження показали [20], що менше половини застосунків із OSI дозволяють змінити початкові налаштування щодо їх видимості. Іншими словами, у більшості випадків користувач «за замовчуванням» відображає інформацію про себе, навіть не усвідомлюючи цього.

До того ж, щоб мати змогу стежити за чужими статусами, люди часто залишають власний статус відкритим: за даними опитувань [1], дехто вимикав «last seen» через конфлікти (наприклад, з партнером), але більшість тримають його увімкненим, аби відстежувати знайомих. Така асиметрія у контролі підсилює етичну дилему: користувачі можуть одночасно переживати дискомфорт від власної підзвітності і все ж використовувати ці індикатори для спостереження за іншими.

1.2.3 Етичні проблеми та ризики зловживання OSI

Повсюдне поширення індикаторів онлайн-статусу (OSI) породжує певні юридично-етичні питання. Як продемонстровано раніше згаданих академічних роботах, то навіть така базова інформація, як час перебування в мережі, може розкрити чутливі аспекти приватності життя. Зокрема, аналіз даних «online/offline» дозволяє з високою точністю визначити розпорядок дня людини (час підйому та засинання), періоди її активності та відпочинку, факти відволікання під час роботи, а також встановити коло найближчого спілкування. Як наслідок, сторонній спостерігач може зробити висновки про особисті звички чи навіть про взаємодію між двома особами. Так, було продемонстровано, що шляхом порівняння графіків онлайн-активності двох користувачів можна з достатньою ймовірністю припустити факт їхньої розмови між собою (на основі одночасної появи онлайн) [1]:

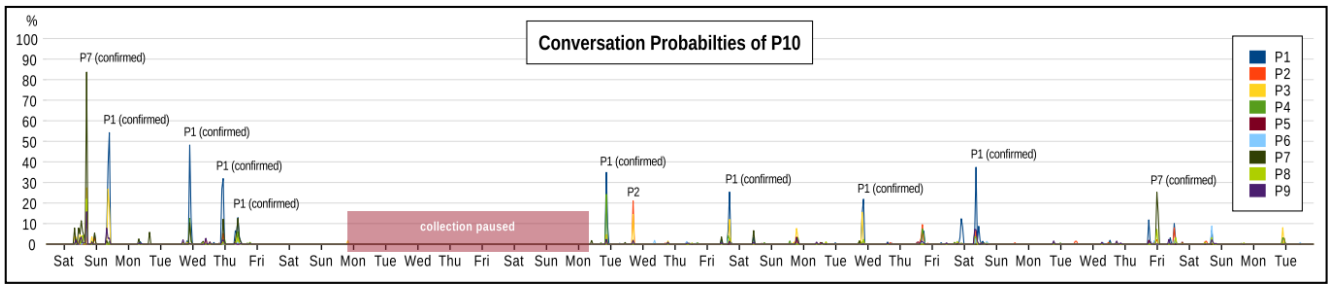

Рисунок 1.12 – Імовірність розмов P10 з іншими учасниками групи №1 протягом усього періоду збору даних. Імовірності були розраховані для годинних часових проміжків. Десять з одинадцяти зображених ймовірних розмов були підтверджені.

Особливе занепокоєння викликає можливість використання цих даних у злочинних цілях або з метою переслідування. Експерти EFF наголошують, що нездатність приховати свій онлайн-статус фактично полегшує роботу шпигунів, тим самим підвищує ризик непрямого контролю над діями інших осіб [19].

1.2.4 Міжнародні стандарти та українське законодавство

З точки зору права, інформація про час та факт перебування особи онлайн розглядається як така, що належить до сфери приватного життя. Міжнародне право з прав людини (зокрема, ст. 12 «Міжнародної декларації про права людини» [21] та ст. 8 «Європейської конвенції з прав людини» [22]) гарантує кожному право на повагу до приватності та таємниці кореспонденції, захищаючи від неправомірного збирання їхніх персональних даних. Разом з тим закон GDPR відносить будь-яку інформацію, що дозволяє ідентифікувати особу, до категорії персональних даних, обробка яких обов’язково потребує правових підстав та згоди суб’єкта [23].

Відповідно до ст. 182 Кримінального кодексу України – незаконне збирання, зберігання, використання чи поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини тягне за собою кримінальну відповідальність. До конфіденційної інформації традиційно відносять відомості особистого характеру, які людина бажає зберегти персонально в таємниці [24].

Однак у випадку з мітками онлайн-присутності виникає правова колізія: з одного боку, користувач власноруч допускає відображення свого статусу (тобто інформація не є повністю прихованою), а з іншого – автоматизований збір цієї інформації стороннім сервісом без згоди може трактуватися як неправомірне її використання. Ключовою ознакою тут виступають спосіб і мета збору: якщо дані агрегуються та зберігаються з наміром передати третім особам або використати на шкоду інтересам суб'єкта, це вже потенційно підпадає під дію ст. 182 ККУ.

Варто розрізняти використання подібних інструментів державними органами та приватними особами. У сфері правоохоронних органів спостерігається інтерес до OSINT-методів, що не порушують таємницю переписки. Моніторинг відкритих цифрових слідів (зокрема, публічних статусів) розглядається як легітимний спосіб отримання розвідувальної інформації про підозрюваних осіб [25]. Так, прототип моніторингового сервісу, який розробляється в межах науково-дослідної роботи, позиціонується як інструмент законного доступу до часових показників активності, що не втручається у зміст повідомлень і приватні чати. Подібні системи можуть бути корисними спецслужбам для оперативного аналізу поведінки – скажімо, визначення розпорядку дня об'єкта спостереження або синхронності онлайн-графіків групи осіб. Зважаючи на вищезазначене, можна зробити висновок, що збір міток «online/offline» знаходиться на межі між публічністю та приватністю. Хоча технічно ці дані є відкритими, проте їхнє використання потребує чіткого правового регулювання та підвищеної відповідальності з боку тих, хто саме їх збирає.

1.3 Практичне значення OSI під час проведення OSINT-розслідувань

1.3.1 OSI як джерело даних для OSINT

Знову ж таки варто згадати, що відстеження інформації про OSI (наприклад, збір даних про те, якими програмами користується людина, як довго і як часто) може бути використано для отримання значно більшої інформації про реальну та цифрову активність цільової особи [26]. Згадані раніше дослідники з Ульмського університету під час своїх експериментів змогли виявити, що онлайн-статус може розкривати час, коли люди прокидаються або лягають спати, а також виявити їхній типовий розпорядок робочого дня, чи відхиляються вони від цього графіку, чи використовують вони застосунки під час роботи, а в деяких випадках які особи спілкуються частіше за інших між собою [1]. Автори повідомляють, що учасники експерименту висловлювали здивування тим, що непряма розвідка дозволила виявити настільки багато правдивої інформації про них. Крім того, автори обговорюють потенційні ризики того, як інформація про OSI може бути дуже чутливою, наприклад, коли вона використовується для спостереження у відносинах або роботодавцями для відстеження продуктивності своїх працівників.

Наукова стаття від ICMI описує, що деякі програми, якими користується людина, дозволяють передбачити її фізичне місцезнаходження, і навпаки [27], тим самим вказуючи на те, що інформація про присутність, яка передається через OSI, може розкривати також інші конфіденційні дані про користувача. Дослідники в рамках своєї статті для MobileHCI додатково вказують на ці та інші закономірності використання застосунків і як наслідок пропонують використовувати їх для створення спеціалізованих інструментів, які рекомендуватимуть користувачам актуальні налаштування конфіденційності своїх даних в застосунках [28].

Індикатори онлайн-статусу (OSI) – це елементи інтерфейсу, які автоматично сигналізують, коли користувач з’являється онлайн чи йде в офлайн. Вони присутні

у багатьох застосунках соцмереж і надають унікальний тип метаданих про активність користувачів, що вже є відкритою інформацією за замовчуванням.

Таким чином, у цій роботі вперше ґрунтовано розглядається трактування індикаторів онлайн-статусів як відкритої інформації, процес збору якої підпадає під методологію OSINT. На відміну від традиційних OSINT-даних (наприклад, контент дописів, зображень чи публічних документів), які несуть змістовну інформацію, під час OSINT-розслідувань інформація про OSI буде розкривати інформацію про поведінкові характеристики – час та частоту присутності користувача онлайн.

Попередні дослідження вже продемонстрували, що ці, на перший погляд, тривіальні дані можуть розкривати конфіденційну інформацію про користувача, оцінюючи його рутину та навіть зв'язки. Зокрема, встановлено, що збір статусів «online/offline» може виявляти режим дня (періоди сну та активності), відволікання на роботі, коло спілкування та інші відхилення від звичного денного ритму.

На прикладі користувачів месенджера WhatsApp було продемонстровано, що регулярний збір даних про мітки статусів «online» та «last seen» перетворюється на цінне джерело розвідки. Зібравши часові мітки, аналітики можуть визначити, коли саме людина зазвичай онлайн, а коли – ні, і чи збігаються ці періоди з активністю інших користувачів. Синхронність виходів онлайн двох чи більше об'єктів може сигналізувати про їх можливу взаємодію (одночасні сеанси зв'язку). Цей прийом фактично дозволяє побічно ідентифікувати коло контактів цілі – якщо двоє абонентів різних номерів систематично з'являються онлайн майже одночасно і офлайн незабаром один після одного, є підстави припустити їхнє спілкування між собою. Попри шифрування повідомлень, сторонній спостерігач, маючи номер телефону, може пасивно відслідковувати ці статуси і робити певні висновки.

На практиці це означає, що OSI-дані доповнюють класичні OSINT-джерела, адже якщо зміст повідомлень чи постів може бути свідомо викривленим або відфільтрованим самим користувачем, то автоматично зафіксовані часові мітки

присутності є більш об’єктивним свідченням активності. Водночас інформація з відкритих джерел загалом потребує критичної оцінки, адже у відкритому доступі трапляються і неточності, і дезінформація, якщо користувач обізнаний в ІБ.

Поєднання OSI-даних з іншими OSINT-відомостями підвищує надійність аналізу. Зокрема, дані про час онлайн-присутності можуть слугувати перехресною перевіркою фактів чи заяв, знайдених у контенті соцмереж, а також виявляти те, чого нема в явному вигляді у публікаціях. Таким чином, інформація про OSI надає поведінковий вимір відкритим джерелам розвідки, дозволяючи бачити не лише що повідомляє об’єкт, але й коли та як часто він проявляє онлайн-активність.

1.3.2 Практичність для національної безпеки.

Інформація з відкритих джерел усе ширше застосовується офіційними структурами безпеки для вирішення розвідувальних і контррозвідувальних завдань [29]. З погляду спеціальних служб, OSINT вже давно перестав бути допоміжним інструментом, адже його інтегрують у повсякденну роботу розвідки поряд із класичними методами. Таким чином, розглянуті в цій роботі методи та технології OSINT можуть потенційно дозволити силам спецслужб (СБУ, Кіберполіції, ГУР) збирати дані про діяльність іноземних агентури на основі інформації із OSI.

Наприклад, публічна цифрова активність підозрюваних осіб (включно з їхнім онлайн-статусом у соцмережах) може виступати додатковим індикатором, що доповнює агентурні дані (HUMINT) при спостереженні за ними. За рахунок OSI-спецслужби можуть отримувати можливість непрямого спостереження. Фіксуючи, коли і як часто ціль виходить на зв’язок, можна зробити висновки про її поведінку без безпосереднього контакту. Практична цінність OSINT-підходів визнана на високому рівні. Наприклад, у кіберпідрозділі СБУ зазначають, що сучасні OSINT-інструменти дають вагомі переваги у боротьбі з агресором, дозволяючи дізнаватися та ідентифікувати ворожі угруповання, не наражаючи на ризик життя людей [31].

OSINT-розвідка в контррозвідувальному контексті здатна добувати навіть таємні відомості про плани чи документи противника за рахунок зіставлення розрізнених відкритих даних, при цьому формально не порушуючи закону і не розкриваючи агентурну мережу. Науковці відзначають, що синтез даних різних видів – відкритих, агентурних, технічних – стає «візитною карткою» високоякісної розвідки, розмиваючи межі між традиційними розвідувальними напрямками [32].

Ілюстративним прикладом взаємодії OSINT-, SOCMINT-, HUMINT-методів є розслідування Bellingcat щодо замаху на Навального [33]. З точки зору поведінки, ключову роль відіграв фактор часу, адже дзвінок до офіцера ФСБ в момент його ранкової когнітивної втоми, коли після пробудження нервова система ще не досягла оптимального рівня активації, а увага й здатність критично оцінювати інформацію залишаються зниженими. Оскільки під виглядом внутрішнього каналу зв’язку цей дзвінок сприймався як службовий, тому це викликало довіру. Саме поєднання низької уваги, поспіху, авторитетної інтонації й часу доби підвищило ймовірність розкриття службової інформації про деталі спецоперації.

З позиції соціального інженера цей приклад підтверджує, що OSI можуть мати прикладну цінність. Зокрема, успішність ранкового контакту (близько 6:30) від імені вигаданого співробітника ФСБ пояснюється зниженою когнітивною пильністю цілі, зумовленою її природним біоритмом [14]. Це демонструє, що знання про нещодавню онлайн-активність (OSI) здатне допомогти визначити момент, коли когнітивний захист людини найслабший, підвищуючи ефективність інформаційного впливу або отримання розвідувальної інформації.

Таким чином, OSI-дані в синтезі різних напрямів OSINT-розвідки зможуть відігравати роль своєрідних “сигналів” активності, дозволяючи підвищити точність та контекст аналітичних висновків. При цьому залишається низка викликів, адже великий обсяг таких даних потребує автоматизації їх опрацювання [34].

Звідси, доцільним буде частковий розподіл функцій між алгоритмічними (Machine/Computer) та аналітичними (Human) етапами. Автоматизовані модулі здатні здійснювати первинне збирання часових метрик і побудову графіків активності, тоді як експерт-розвідник виконувати подальший поведінковий аналіз і контекстну інтерпретацію результатів. Цей процес можна подати у вигляді схеми:

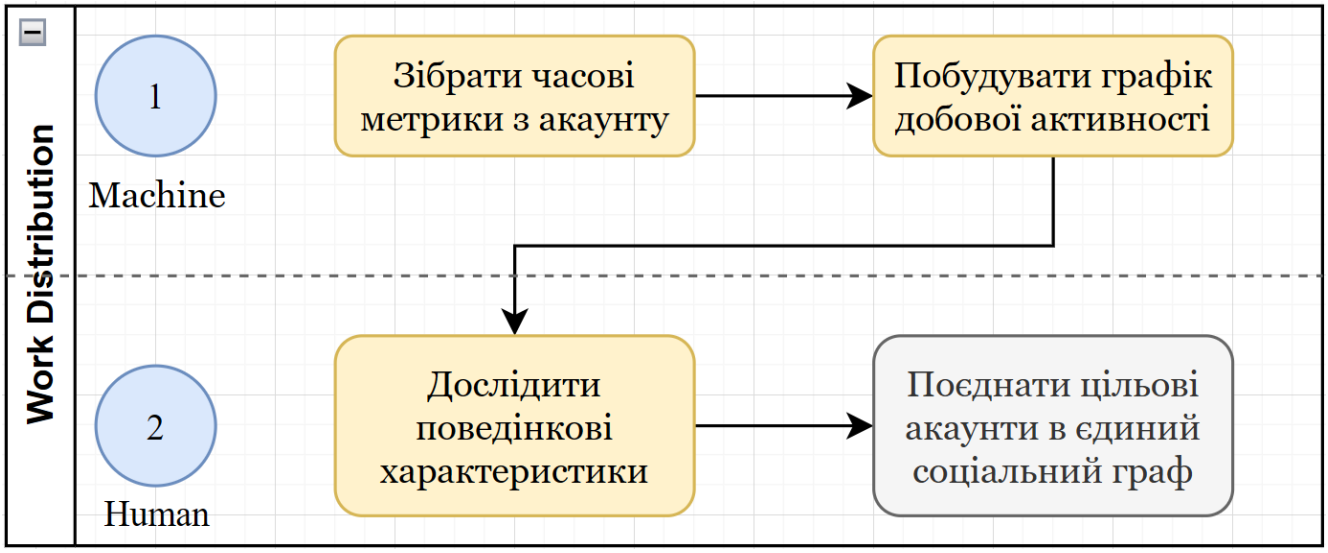

Рисунок 1.13 – Алгоритм HCI під час OSINT-дослідження користувацьких OSI

1.3.3 Значення OSINT-технологій під час війни.

З початком повномасштабної російсько-української війни 2022 року збір інформації з відкритих джерел перетворився на новий фронт бойових дій, де дані стали зброєю [35]. Цифрові сліди противника – дописи в соцмережах, фотографії техніки, геолокації – стали цінними розвідданими для української армії. Наприклад, відомі випадки, коли через необережність російські військові публікували фото або включали геомітки, і їх вираховували; але навіть без явних «засвіток» OSINT-аналітики вичитують із фонових деталей та часу активності багато важливого. За свідченнями українських військових, отриманими під час консультацій, будь-яка дрібниця з відкритих джерел може мати розвідувальну цінність. Водночас вони зазначають, що серед російського населення поступово

зростає популярність федерального месенджера Max. Підтвердження подібній інформації можна знайти в повідомленні телеграм-каналу «OsintFlow» [36]:

«*У вересні аудиторія Max зросла на 30%, досягнувши 41 млн осіб, писали Mediascope. За даними "Агентство. Новости" державний російський месенджер Max завдяки обмеженням конкурентів та різним преференціям на початок жовтня зібрав приблизно половину аудиторії Telegram, але поки що не став серйозним конкурентом, принаймні у сегменті поширення медіаконтенту. Канали Max мають суттєво менше читачів, ніж у Telegram. Виняток становлять деякі канали держорганів, які набирають аудиторію із серйозними аномаліями - короткочасні аудиторні стрибки чергуються з тижнями стагнації*.»

Особливої уваги заслуговує застосування OSI під час військової розвідки, адже завдяки цим індикаторам гіпотетично можливо визначати режим роботи командних пунктів (наприклад, коли офіцери регулярно виходять онлайн або навпаки зникають із мережі), а також розраховувати періоди найвищої або найнижчої активності. Якщо відомо, що опонент щодня має стабільну перерву в цифровій активності о певній годині, це «вікно» може бути використане для проведення раптових операцій чи інформаційних впливів. Отже, відстежуючи, коли і як часто ворожі підрозділи виходять на зв'язок (навіть через ті ж месенджери чи соцмережі), можна робити висновки про їхній режим бойової готовності, цикли відпочинку, зміни чергувань або приховану підготовку до операцій. Все це підкреслює, що аналіз цифрової активності та OSINT стали невід'ємним елементом сучасної військової розвідки, а досвід України у цій сфері – переконливий доказ практичної значущості цих підходів для забезпечення національної безпеки [29].

1.4 Доступність та поширеність комунікаційних сервісів в Україні

- **MS Teams**
  - **Доступність API для OSINT**: Microsoft Teams є закритою корпоративною платформою. Їхній API-функціонал призначений для інтеграції в межах організації (через Microsoft Graph), тому збір даних з відкритих джерел (OSINT) без доступу до внутрішніх облікових записів неможливий.
  - **Популярність в Україні**: Microsoft Teams широко використовується у бізнес-середовищі та державних установах, особливо після переходу на віддалену роботу. Під час війни корпоративний сектор і держоргани перейшли на Microsoft 365, і тим самим Teams став одним з найважливіших інструментів для віддаленої роботи [37]. Серед загального населення Teams мало відомий, адже він є переважно корпоративним «месенджером».

- **Slack**
  - **Доступність API для OSINT**: Slack надає API для розробників, але доступ до даних потребує токену і прив’язаний до конкретного робочого простору. Тобто, публічно отримати дані Slack неможливо без доступу до робочої області – навіть кількість учасників не дізнатися без наявності токена.
  - **Популярність в Україні**: Slack – популярний у IT-компаніях та стартапах інструмент командної роботи, але не настільки масово розповсюджений [40].

- **Gmail**
  - **Доступність API для OSINT**: Gmail надає офіційні API для роботи з поштовими скриньками, однак доступ до них можливий лише за наявності автентифікації власника акаунта. Публічних засобів отримання будь-яких персональних даних або інформації про активність користувача не знайдено.
  - **Популярність в Україні**: Gmail є одним із найпопулярніших електронних поштових сервісів серед українців, частково через прив’язку до Google Play.

- **Outlook**
  - **Доступність API для OSINT**: Outlook (служба електронної пошти Microsoft) також не має відкритого API для чужих даних. Існує Microsoft Graph API для доступу до поштової скриньки Outlook, але лише за наявності облікових даних користувача. Таким чином, контент Outlook із зовні закритий.
  - **Популярність в Україні**: Outlook використовується в корпоративному секторі. Серед приватних користувачів він менш популярний. Багато компаній та держустанов мають домени в Outlook, але для особистого спілкування українці частіше обирають Gmail або локальні поштовики.

- **Viber**
  - **Доступність API для OSINT**: Viber не надає відкритого доступу до контенту особистих переписок – це закритий месенджер з наскрізним шифруванням. Можливостей збору даних про акаунти через публічний API не знайдено.
  - **Популярність в Україні**: Viber – це найпопулярніший месенджер серед українців (особливо старшої аудиторії). За даними дослідження InMind 2025 року, ним користуються близько 45% українських інтернет-користувачів [40]

- **Telegram**
  - **Доступність API для OSINT**: Telegram має відкриті API, які широко застосовуються в OSINT. Існує також документований клієнтський API на основі MTProto (Telethon), що дає змогу розробникам отримувати дані з публічних каналів і груп. Завдяки цьому, попри шифрування приватних чатів, Telegram містить безліч відкритого контенту (публічні канали, групи, профілі) для розвідки [41]. Багато користувачів Telegram беруть участь у відкритих групах, де їхній профіль та попередні повідомлення можна побачити за допомогою пошуку або просто перегляду сторінок.
  - **Популярність в Україні**: Telegram посідає друге місце за популярністю. У 2025 році ним користуються близько 35% українців згідно даних InMind [40],

і ця частка швидко зростає. За останні роки Telegram використовують не лише для особистих повідомлень, а й як джерело перегляду новин [42]. Під час війни Telegram став ключовою платформою для оперативних новин та волонтерських спільнот, що ще більше збільшило його аудиторію.

- **Messenger**
  - **Доступність API для OSINT**: Messenger (від Facebook) не надає окремого відкритого API для отримання інформації про особисті дані користувачів. OSINT обмежується хіба що пошуком профілю людини за ім’ям чи номером.
  - **Популярність в Україні**: Messenger (від Facebook) досить поширений, але поступово втрачає позиції. Аудиторія складає близько 10% користувачів, що менше, ніж у в інших [40]. Популярність Messenger пов’язана з інтеграцією у Facebook – багато хто користується ним, бо має свій акаунт у соцмережі.

- **WhatsApp**
  - **Доступність API для OSINT**: WhatsApp має **Business API** для компаній, що дозволяє надсилати повідомлення клієнтам за їх згодою, але він не дає доступу до загальної інформації або переписок. Через API можна лише перевірити наявність номера телефону в WhatsApp (вручну або через адресну книгу), але отримати контент чи список контактів не вдається.
  - **Популярність в Україні**: WhatsApp в Україні менш популярний, ніж у глобальному масштабі. Лише ~7% українців називали його основним месенджером у 2025 році [40]. Він стабільно входить у п’ятірку, але значно поступається від інших. Історично WhatsApp запізнився на український ринок, де вже закріпилися інші сервіси. Проте, через міжнародні контакти та переселенців, WhatsApp підтримує свою аудиторію і має певне зростання. Адже у світі це #1 месенджер, але в Україні його роль помірна [40].

- **Signal**
  - **Доступність API для OSINT**: Signal побудований навколо найкращих практик із забезпечення приватності, тому він не має відкритого API або публічних даних. Весь обмін повідомленнями наскрізно зашифрований, а сам сервіс мінімізує зберігання інформації про користувачів (не фіксує контакти, список чатів, аватари, OSI [43]). Єдиний доступний метод – перевірити, чи номер зареєстрований у Signal, через функцію додавання контакту в додатку.
  - **Популярність в Україні**: Signal має найменшу частку серед популярних месенджерів – близько 3% користувачів [40]. Він поступово набирає популярності серед тих, хто цінує конфіденційність, особливо в IT-сфері та серед активістів. За останні роки, на хвилі скандалів з приватністю у конкурентів, Signal отримав притік користувачів, але це нішевий продукт. В Україні його рекомендують для безпечного спілкування, проте масовий користувач віддає перевагу менш захищеним, але зручнішим платформам.

- **Instagram**
  - **Доступність API для OSINT**: Instagram після 2018 року досить обмежив будь-які сторонні доступи. Публічно отримати інформацію про чужі профілі можна тільки шляхом скрапінгу (парсингу веб-версії) або через інструменти аналітики, але не через офіційний API. Таким чином, OSINT по Instagram зводиться до аналізу відкритих профілів вручну або через неофіційні інструменти. Контент у відкритих профілях та публічні дописи доступні для перегляду, але автоматизований збір потребує обходу офіційних обмежень.
  - **Популярність в Україні**: Instagram – одна з найпопулярніших соцмереж. На початку 2023 року українська аудиторія Instagram становила близько 11 млн користувачів (~30% населення). У 2024 році цей показник зріс до ~12 млн [44]. Instagram особливо популярний серед молоді та міського населення – це платформа для фотографій, історій та бізнес-просування. Українські бренди та блогери активно присутні в Instagram, а війна посилила використання для

волонтерських зборів та поширення інформації. Хоч офіційно Facebook переважав за охопленням, молодша аудиторія давно мігрувала в Instagram.

- **TikTok**
  - **Доступність API для OSINT**: TikTok не надає повноцінного відкритого API для стороннього аналізу контенту. Таким чином, OSINT по TikTok може здійснюватися лише через веб-скрапінг або сервіси аналітики. Публічні відео та профілі доступні відкрито (якщо профіль не приватний), тому можна вручну чи за допомогою парсерів збирати дані про популярні відео, хештеги, коментарі. Проте, офіційно TikTok API не дає вільно витягати дані, тож доводиться використовувати парсери, які CAPTCHA може блокувати.
  - **Популярність в Україні**: TikTok стрімко набрав популярність. Станом на початок 2023 року в Україні було понад 13 млн користувачів TikTok віком 18+, що дорівнює ~45% повнолітніх інтернет-користувачів. TikTok особливо популярний серед молоді (підлітки, молоді дорослі). За час війни український сегмент TikTok наповнився волонтерськими та інформаційними відео, але основний контент – розважальний. TikTok конкурує з YouTube і Instagram за увагу, часто виступаючи джерелом вірусних новин та медіа-даних.

- **Twitter (X)**
  - **Доступність API для OSINT**: Twitter традиційно був найвідкритішою соцмережею для OSINT. Історично Twitter надавав потужний публічний API для пошуку твітів, аналізу мереж та потокового отримання даних [45].

    Це дозволяло в реальному часі відстежувати події, настрої, геолокацію повідомлень тощо. Проте, після змін у політиці доступу (особливо з 2022–2023 рр. після приходу Ілона Маска) Twitter значно обмежив безкоштовний API-доступ. «Золота ера» відкритих інструментів закінчилась – багато OSINT-інструментів (напр. Twint) перестали працювати [45]. Нині для збору

даних з Twitter потрібно або платити за доступ до API, або використовувати обхідні методи (набори даних, веб-парсинг результатів пошуку).

- **Популярність в Україні**: Twitter ніколи не був масовою платформою в Україні. За оцінками на 2023 рік, Twitter мав лише **близько** 600 тис. користувачів з України [44] – це менше 2% населення. Аудиторія Twitter в Україні – переважно журналісти, IT-спеціалісти, активісти та англомовні користувачі. Широкі верстви населення надають перевагу Facebook, Telegram чи локальним мережам. Втім, Twitter відіграє важливу роль для висвітлення України на міжнародній арені (багато українських посадовців ведуть твіттер англійською для світу). Після початку війни 2022 року український сегмент Twitter дещо зріс, але все одно залишається нішевим.

- **LinkedIn**
  - **Доступність API для OSINT**: LinkedIn має офіційний API, але дані через нього доступні в основному рекрутерам та партнерам за суворими квотами. Публічний пошук профілів реалізований через сам сайт LinkedIn (певну інформацію видно навіть без входу). Для OSINT щодо LinkedIn зазвичай застосовують веб-скрапінг або спеціальні інструменти. Можна збирати дані про місце роботи людей, їх навички, освіту тощо з відкритих профілів.
  - **Популярність в Україні**: LinkedIn – це професійна соцмережа, популярна передусім серед IT, маркетологів, HR та інших спеціалістів, що орієнтуються на міжнародний ринок. За даними реклами LinkedIn, на початку 2023 року в Україні було близько 4,3 млн зареєстрованих користувачів [44]. Це ~15% інтернет-аудиторії країни. Під час війни багато фахівців оновили свої профілі для пошуку роботи за кордоном, що підтримувало активність у мережі.

- **Discord**
  - **Доступність API для OSINT**: Discord надає досить функціональний API для ботів, але контент серверів буде приватний. Індикатори онлайн-статусів (online/idle/dnd/offline) надсилаються через Gateway (WebSocket) як події Presence Update; для автоматизованого доступу до міток онлайн-присутності учасників потрібен привілейований намір PRESENCE INTENT.
  - **Популярність в Україні**: Discord спочатку був популярний серед геймерів, але зараз виходить за ці рамки [40]. В Україні Discord став місцем спілкування для різних спільнот, але масовим месенджером він не став, адже аудиторія переважно геймерська і вимірюється лише сотнями тисяч осіб.

Як емпіричний маркер популярності каналів у поточному інформаційному середовищі України використано щорічне опитування Громадянської мережі ОПОРА (2024). Згідно з результатами, соціальні мережі залишаються головним джерелом новин для 73,4% опитаних (–4,5% порівняно з 2023), а топ-3 платформи виглядають так: Telegram – 78,1%, YouTube – 59,5%, Facebook – 44,6% (частка інших: Viber – 42%+, Instagram – 29,6%, TikTok – 26,8%, Twitter – 7,8%). [42]

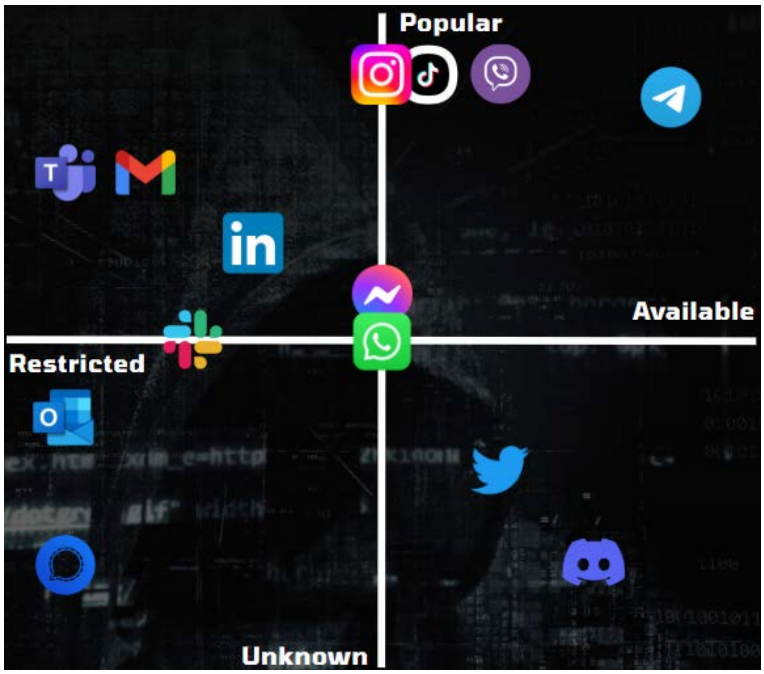

Рисунок 1.14 – Доступність/Популярність застосунка

Нижче представлена таблиця про OSI, яка була опублікована в «sciendo»:

Таблиця 1.1 – Відображення міток онлайн-активності в 40 застосунках [20]

	AUDIENCE			SETTINGS	APPEARANCE *Many apps show online status in more than one way. This table conveys only predominant presentations. Caveats are discussed inline or shown in other figures.*				TIMING	
	TYPE(S) OF OSI (SCOPE)	(DEFAULT) RELATIONSHIP WITH USERS WHO CAN SEE OSI	CAN (OR MUST) SIGN UP WITH OTHER SERVICE *	APP HAS OSI SETTINGS ***	ONLINE APPEARANCE	LAST ONLINE TIME	CLICKS TO SEE AN ONLINE STATUS	VISIBILITY OF SELF	TIME TO ONLINE *	TIME TO OFFLINE *
App *(App description)*	Typical, Sub-area, or Cross-app	● (Friends/connections), ○ (Global), or Other	Yes or No	Yes or No	(Green dot), Text, or Other	Approximate or Exact	0 to 3 or Other	Yes or No	• (A few seconds), ● (A few minutes), -- (Not able to measure)	
Battle.net *(Gaming Chat)*	Cross-app (w/ Hearthstone)	●	Yes	Yes	●	Approximate	0	Yes	•	several hours
Canvas *(Education)*	Sub-area	Anyone w/ access to group chat (restricted)	No	No	●		3	Yes	•	•
Coffee Meets Bagel *(Dating)*	Typical	○	Yes	No	Clock icon and text **	Approximate	Must pay	No	--	--
Discord *(Gaming Chat)*	Typical	●	No	Yes	●		0	Yes	•	●
Facebook *(Social Media)*	Cross-app (FB Grouping)	●	No	Yes	●		0	No	•	●
Facebook Lite *(Social Media)*	Cross-app (FB Grouping)	●	No	Yes	●		0	No	•	10-60 minutes
Google Docs or Google Sheets *(Productivity)*	Sub-area	Anyone w/ access to doc or sheet	Yes	No	Cursor with username appears in doc; username in list of active users		1	No	•	•
(Google) Hangouts *(Chat)*	Typical	●	No	Yes	Text	Approximate	1	No	•	10-60 minutes
	Sub-area	Other person in conversation		No	Opaque thumbnail of profile picture, becomes transparent if not in sub-area		0 once in sub-area	No	•	•
Grindr *(Dating)*	Typical	○	No	No (Android); Yes, "new" for paid users (iOS)	●	Approximate	0	Yes	•	10-60 minutes
Happn *(Dating)*	Typical	○	Yes	No	Text	Approximate	1	No	--	--
Hearthstone *(Gaming)*	Cross-app (w/ Battle.net)	●	Yes	Yes (only via Battle.net app)	Text	Approximate	1	No	•	several hours
Hike *(Chat)*	Typical	●	No	Yes	Text	Exact	1	No	•	•
imo *(Chat)*	Typical	●	No	Yes (Android); "Last Seen" Settings (iOS)	Text	Exact	1	No	•	●
	Sub-area	Other person in conversation		No	Thumbnail of profile picture has teal border if online		0 once in sub-area	No	•	•
Instagram *(Social Media)*	Typical	●	Yes	Yes	●	Approximate	1	No	•	●
JOYRIDE *(Dating)*	Typical	○	Yes	No	●	Approximate	0	Yes	--	--
Jurassic World Alive *(Gaming)*	Typical	●	Yes	No	Orange dot for online, green dot for in-game		1 (Android); 2 (iOS)	No	•	●
LinkedIn *(Employment)*	Typical	No one, but app automatically changes to ● after some use *	Yes	Yes	●		2	Yes	•	●
Marco Polo Video Walkie Talkie *(Video Chat)*	Typical	○	No	No	Text	Approximate	2 (Android); 0 (iOS)	No	•	●
Match *(Dating)*	Typical	○	Yes	No	●	Approximate	0	No	--	--
(Facebook) Messenger *(Chat)*	Cross-app (FB Grouping)	●	Yes	Yes	●	Approximate	0	Yes	•	●
(Facebook) Messenger Kids *(Kids' Chat)*	Typical	●	Yes	No	●	No info (Android); Approximate (iOS)	0	No	●	●
(Facebook) Messenger Lite *(Chat)*	Cross-app (FB Grouping)	●	Yes	Yes	●	Approximate	0	Yes	•	●
MyFitnessPal *(Fitness)*	Typical	●	Yes	No	Text	Approximate	2	Yes	--	--
OfferUP *(Classifieds)*	Typical	○	Yes	No	Text	Approximate	2	No	--	--
OkCupid *(Dating)*	Typical	○	Yes	No	●		0	No	•	10-60 minutes
Plenty of Fish (POF) *(Dating)*	Typical	○	No	No	Text		1	No	--	--
PUBG MOBILE *(Gaming)* *	Typical	●	Yes	No	Text	Approximate	1	No	•	●
ROBLOX *(Gaming)*	Typical	○	No	No	Blue dot for online, green dot for in-game		2 (Android); 0 (iOS)	Yes	•	10-60 minutes
	Sub-area	Anyone w/ access to mini-game (most are public)		No	Presence in list of users in sub-area		1 once in sub-area	Yes	•	•
Skype *(Chat, Video Chat)*	Typical	●	Yes	Yes	●	Approximate	1 (Android); 0 (iOS)	Yes	•	•
Slack *(Chat, Work)*	Sub-area	Anyone w/ access to workspace (restricted)	Yes	Yes	● or other colors if different "theme" chosen; triangle for single-channel guests		1	Yes	•	•
Steam *(Gaming)* *Observed only on iOS*	Typical	●	No (& must sign up in browser)	Yes	Text	Approximate	0	No	•	•
Telegram *(Chat)*	Typical	● (Android); ○ (iOS)	No	Yes (but not functional on iOS)	Text	Exact (Android); Approximate (iOS)	0	Yes	•	•
Tumblr *(Social Media)*	Typical	○	No	Yes	●	Approximate	3 (Android); 1 (iOS)	No (Android); Yes (iOS)	●	10-60 minutes
Twitch *(Gaming, Chat, Livestreams)*	Typical	●	No	Yes	●	Text, grey dot	1 (Android); 2 (iOS)	No	•	10-60 minutes
Viber *(Chat)*	Typical	○	No	Yes	Text	Approximate	1	No	●	●
Waze *(Navigation)*	Typical	●	No	Yes	Text, green line	Approximate	3	No	●	●
WhatsApp *(Chat)*	Typical	○	No	"Last Seen" Settings	Text	Exact	2	No	•	•
Words with Friends (classic) *(Gaming)*	Typical	○	Yes	No	●	Approximate	0	No	●	10-60 minutes
Yubo *(Chat, Social Media)* *	Typical	●	No	No	●	Exact	1	No	•	•
Zoosk *(Dating)*	Typical	○	Yes	No	● with a thin white circle inside		0	No	--	--

* Observed only in original app analysis (Android OS, unless otherwise specified)

** Observed only via other sources (e.g., online image searches, app store screenshots)

*** See Table 2 for additional details about apps with OSI settings

Висновки до розділу 1

Індикатори онлайн-статусу (OSI) було інтерпретовано як специфічний клас відкритих даних про цифрову активність користувачів, які видимі автоматично на рівні UI застосунків і вже за замовчуванням є доступними для спостереження. Такий підхід виводить OSI у фокус OSINT-технологій як поведінкових метаданих, а не як змістовних повідомлень. Підкреслено, що в сучасних системах миттєвих повідомлень інформація про присутність історично виконує роль координатора доступності й взаємодії між користувачами, водночас породжуючи запит на механізми «правдоподібного заперечення» та налаштування видимості статусів.

Окремим підсумковим положенням, що визначає новизну роботи, було таке: «*Таким чином, у цій роботі вперше ґрунтовано розглядається трактування індикаторів онлайн-статусів як відкритої інформації, процес збору якої підпадає під методологію OSINT. На відміну від традиційних OSINT-даних (наприклад, контент дописів, зображень чи публічних документів), які несуть змістовну інформацію, під час OSINT-розслідувань інформація про OSI буде розкривати дані про поведінкові характеристики – частоту онлайн-присутності користувача.*»

Підтверджено, що навіть тривіальні дані про «online/offline» і «last seen» є інформативними для відновлення щоденних шаблонів активності такої, як час підйому/засинання, робочі перерви на обід, вечірня активність), а також для виявлення непрямих соціальних зв’язків через синхронізацію присутності. Це підтверджено ретроспективним аналізом праць, у яких зібрані часові ряди статусів, що відтворювали реальні поведінкові шаблони учасників досліджень.

Акцентовано на контексті інформаційної безпеки, оскільки в умовах витоку поведінкових характеристик з OSI може нести супутні ризики не лише для окремих осіб, а й для спільнот. Навіть часткове нехтування налаштуваннями приватності

здатне полегшити систематичне спостереження. Отже, це посилює актуальність дослідження та зумовлює етичні вимоги до збору/опрацювання таких даних.

Продемонстровано, що баланс між публічністю та приватністю OSI визначається політиками платформ і налаштуваннями користувачів, а також технічними обмеженнями офіційних викликів API. За суворих обмежень видимості автоматизоване збирання через документовані інтерфейси стає недосяжним, що є важливою передумовою коректного проектування інструментів спостереження.

Розділ розмежовує сценарії можливого застосування. Таким чином, для державних органів (або спецслужб нацбезпеки) моніторинг відкритих цифрових слідів (у т.ч. OSI) розглядається як легітимне джерело розвідданих за умови дотримання правового режиму; щодо юридичних та фізичних осіб – потрібні підвищена відповідальність, адже OSI лежать на межі публічності й приватності.

З погляду соціальної інженерії обґрунтовано практичну цінність часових вікон вразливості. Знання про недавню онлайн-активність допомагає обирати моменти зниженої пильності (ранкові години тощо), підвищуючи результативність комунікаційного впливу. Для реалістичного, масштабованого аналізу розділ аргументує поділ процесу на машинні та людські етапи: автоматизовані модулі збирають часові метрики й будують хронограми, аналітик забезпечує контекстну поведінкову інтерпретацію та синтез із іншими джерелами. Таке HCI-подання процесу формує методичний «місток» до подальшого моделювання алгоритмічної основи методики збору й візуалізації, що і становитиме предмет Розділу №2.

Загалом, розділ формулює дослідницькі гіпотези щодо зв’язку виявлених добових графіків активності з циркадними біоритмами та можливості подальшого виявлення періодів підвищеної вразливості користувача на підставі OSI-даних, що задає рамку емпіричного дослідження й верифікації у подальших розділах.

2 МОДЕЛЮВАННЯ АЛГОРИТМІЧНОЇ ОСНОВИ ЗБОРУ ТА ВІЗУАЛІЗАЦІЇ ЧАСОВОЇ АКТИВНОСТІ КОРИСТУВАЧІВ TELEGRAM

2.1 Обґрунтування вибору середовища та методів збору даних

2.1.1 Огляд месенджера Telegram

Офіційні компоненти застосунка Telegram мають відкритий вихідний код за винятком сервера, який має закритий вихідний код і є власністю компанії. Хмарні чати і групи шифруються між клієнтом і сервером, відповідно інтернет-провайдери чи інші треті сторони в мережі не можуть отримати доступ до даних [46].

У січні 2021 року кількість активних користувачів Telegram перевищила 500 мільйонів щомісяця. У червні 2022 року Telegram перевищив 700 мільйонів щомісячних активних користувачів. У серпні 2023 року Telegram перевищив 800 мільйонів щомісячних активних користувачів. Станом на лютий 2024 месенджер налічував 900 млн користувачів, а вже в березні 2025 їх стало близько 1 млрд.

Залученість користувачів також зростає. В середньому кожен користувач відкриває Telegram 21 раз на день і проводить у застосунку 41 хв щодня [47].

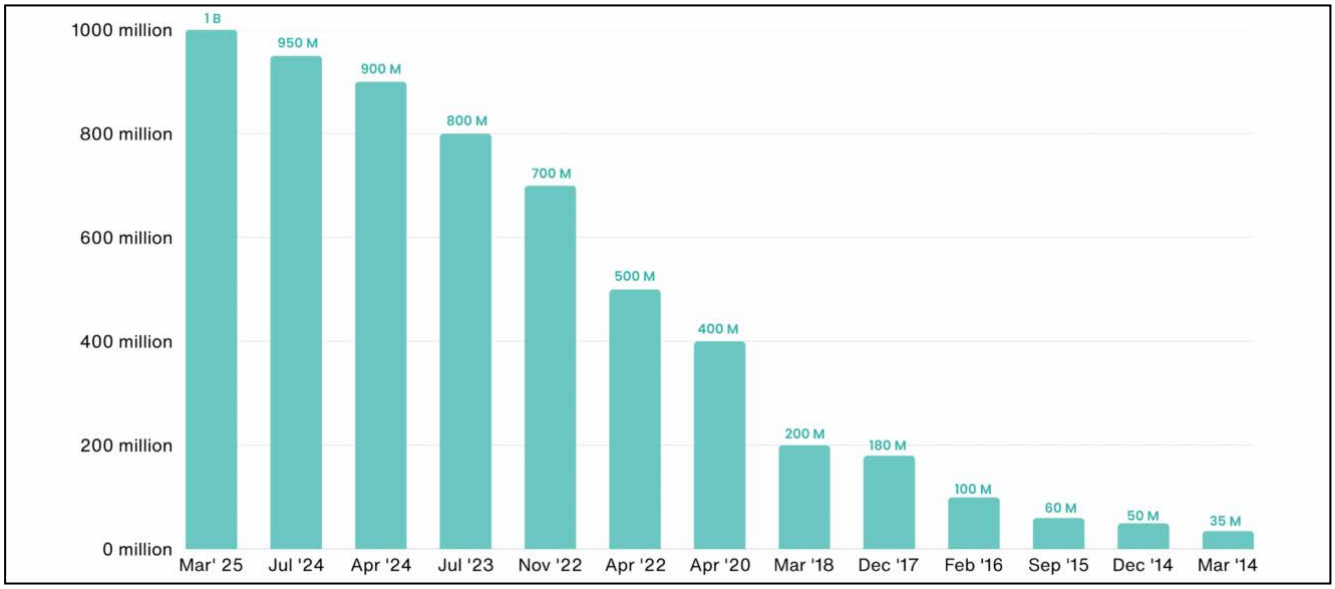

Рисунок 2.1 – Місячна кількість активних користувачів Telegram за роками [48]

2.1.2 Популярність в Україні

За результатами останнього опитування від громадянської мережі ОПОРА, 73,4% респондентів використовують для отримання новин соціальні мережі. І хоча популярність цих платформ уперше з початку повномасштабної війни знизилася на 4,5%, саме вони зберігають лідерство у постачанні інформації українцям.

Понад два роки Telegram упевнено втримує лідерські позиції. Ще у 2021 році, до початку повномасштабного вторгнення, агенція Internews опублікувала [49] результати опитування, згідно з якими Telegram використовували для отримання новин тільки близько 20% користувачів соцмереж. Однак вже в червні 2022 року, цей показник зріс утричі – до 65,7%. А у 2024 році він перевищив показники 2021 року майже вчетверо – тепер новини у Telegram читають понад 78% опитаних.

За останні три роки його аудиторія в Україні відчутно постаршала. Так, якщо у 2022 році лише 24% опитаних, старших за 70 років, споживали новини в Telegram, у 2024 році таких було вже 56%. Збільшилась і частка респондентів в інших вікових проміжках: серед опитаних віком від 50 до 59 років — на 13% (до 71,8%), а серед респондентів віком 60-69 років – на 23% (до 63,3%). Тож тепер Telegram приблизно однаковою використовують для отримання новин усі вікові групи українців [50].

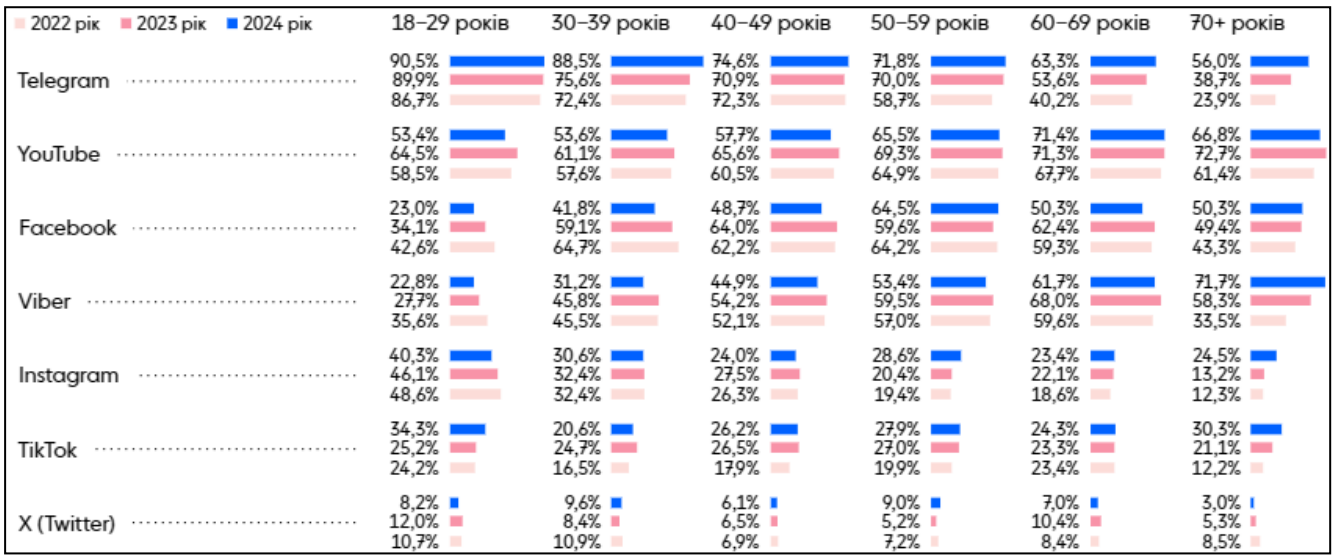

Рисунок 2.2 – Соціальні мережі, які учасники використовували для отримання новин протягом останніх двох місяців в рамках опитування від ОПОРА, 2024 [42]

2.1.3 Конфіденційність міток OSI

Публічність індикаторів онлайн-статусу породжує питання конфіденційності та потенційних ризиків. З одного боку, дані про те, коли користувач був останній раз у мережі, прямо не розкривають зміст його спілкування. З іншого боку, сукупність таких часових міток може видати чутливі поведінкові характеристики: режим дня, розпорядок роботи чи відпочинку, часові проміжки, коли людина найбільш залучена або навпаки – менш уважна. Аналіз OSI здатний доволі точно відновити часові шаблони активності людини, тим самим визначити періоди її вразливості, а також простежити синхронізацію активності кількох користувачів.

Нижче продемонстровано, яким чином в Telegram реалізовано налаштування приватності для «Останньої активності». Таким чином можна обмежити коло осіб, які бачать точний час вашого останнього входу («Усі», «Мої контакти» або «Ніхто»), з можливістю винятків. Якщо користувач приховує статус, інші бачать лише умовне значення, наприклад «був недавно», замість конкретного часу. Відповідно, щоб досягти компромісу в питанні рекомендованих налаштувань, то рекомендовано, щоби за замовчуванням було обрано опцію «Мої контакти» [38].

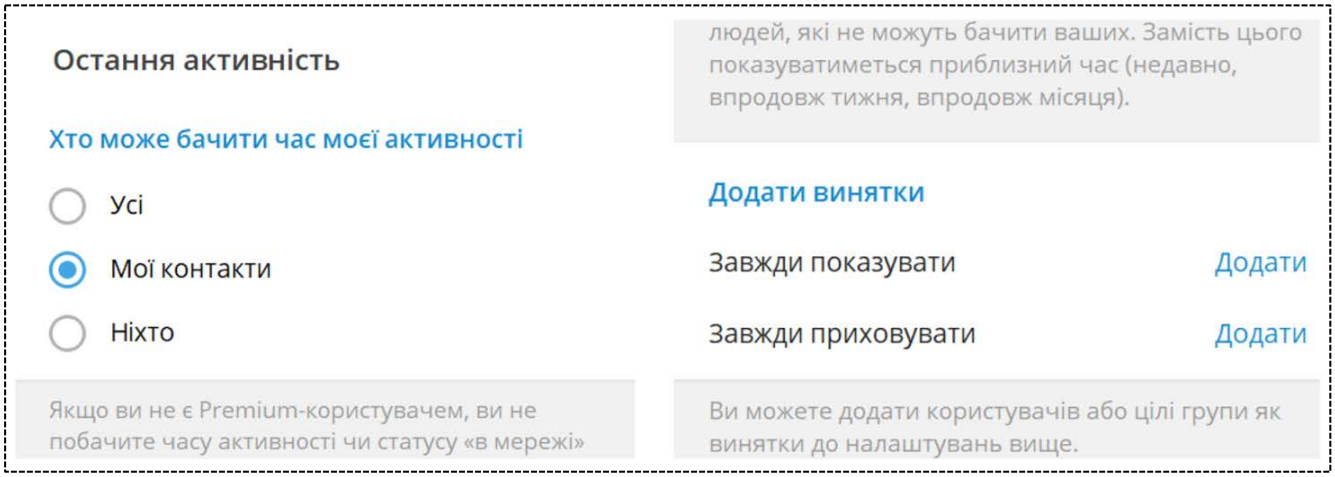

Рисунок 2.3 – Налаштування приватності для «Останньої активності» в Telegram

Проте багато користувачів залишають статус відкритим для всіх, часто навіть через необізнаність про ризики [43]. В контексті OSINT – це означає, що суттєвий обсяг профілів можна моніторити легально, не порушуючи правил платформи.

Методологія OSINT за останні роки набула широкого розповсюдження, для збору та аналізу інформації в мережах, зокрема для боротьби зі зловмисною дезінформацією [39]. Однією з важливих рис методології OSINT є можливість збору персональних даних на різного роду месенджерах на основі відкритих даних.

Автором було проведено суміжне статистичне дослідження, під час якого здійснювався збір із використання скрипта, що отримував по API сутність кожного учасника в чаті («get_entity»), після чого переглядав значення міток OSI («status»).

Таким чином, згідно з даними проаналізованих Telegram-чатів виявлено, що близько 73% користувачів Telegram залишають індикатор «last seen» відкритим для всіх. Даний показник для чатів варіювався в діапазоні від 18% до 92%, оскільки рівень обізнаності в основах цифрової гігієни є різним в профілі кожної аудиторії.

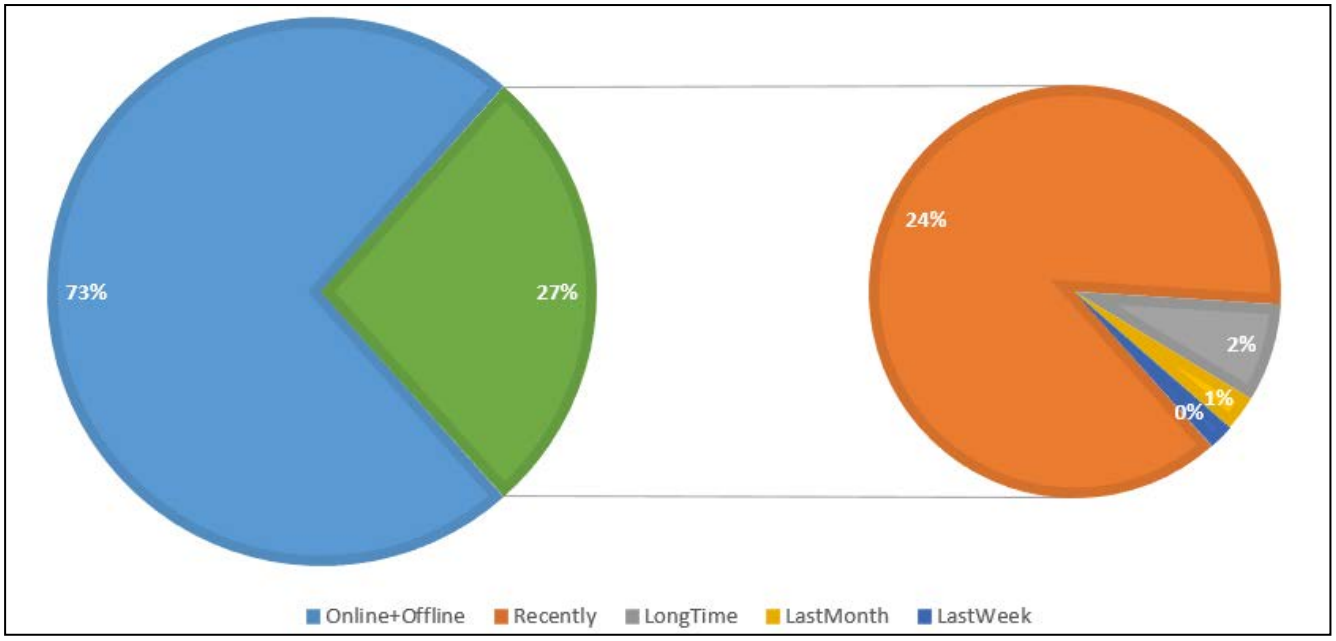

Рисунок 2.4 – Загальний розподіл на **100+ тис.** користувачів із Telegram-чатів

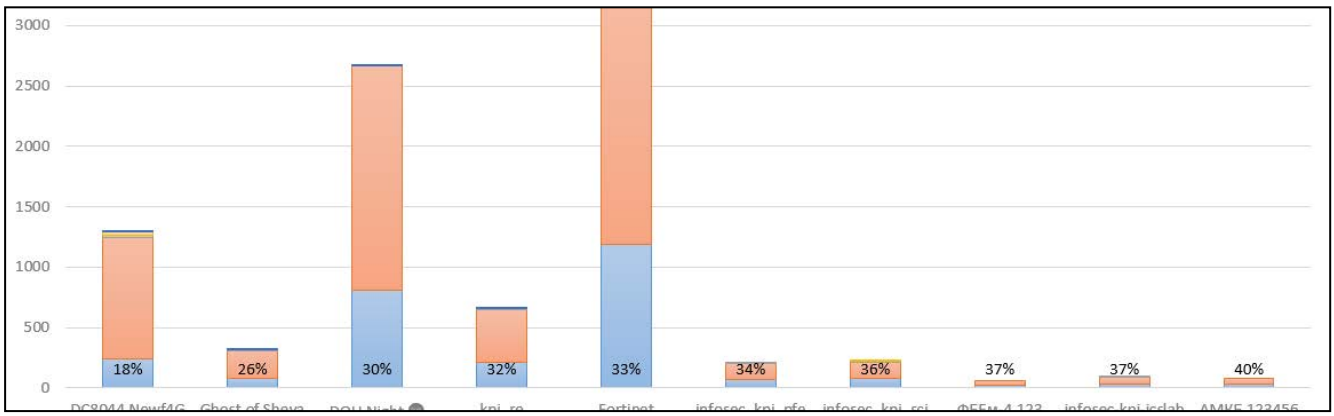

Рисунок 2.5 – Розподіл серед публічних спільнот посеред ІТ та Кібербезпеки. Приблизно **30%** серед усіх учасників чатів мають відкритий статус.

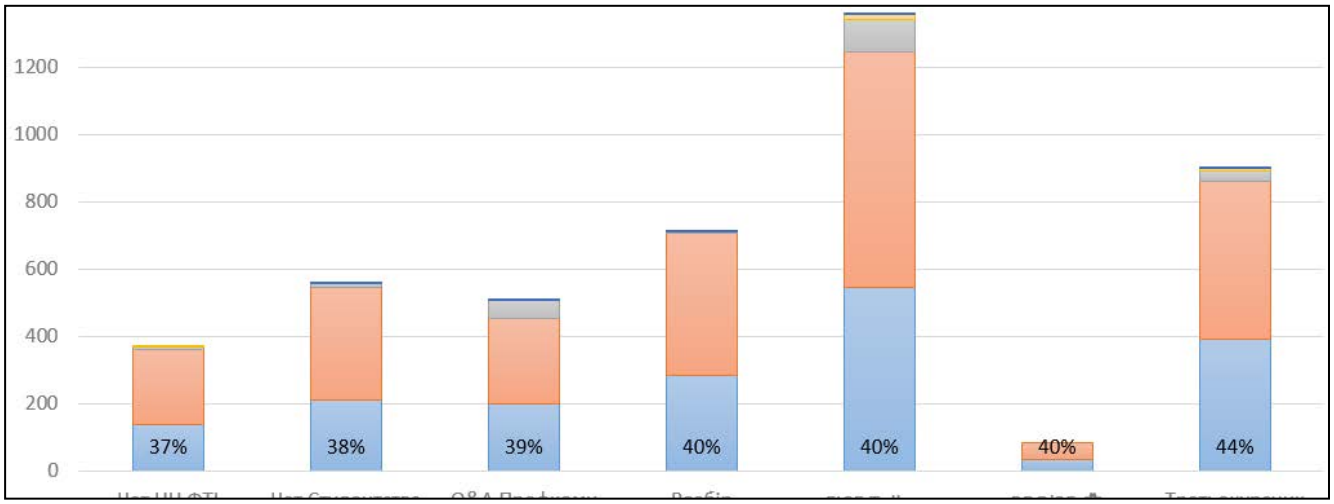

Рисунок 2.6 – Розподіл серед студентських спільнот НТУУ “КПІ ім. Сікорського”. Приблизно **40%** серед усіх учасників чатів мають відкритий статус.

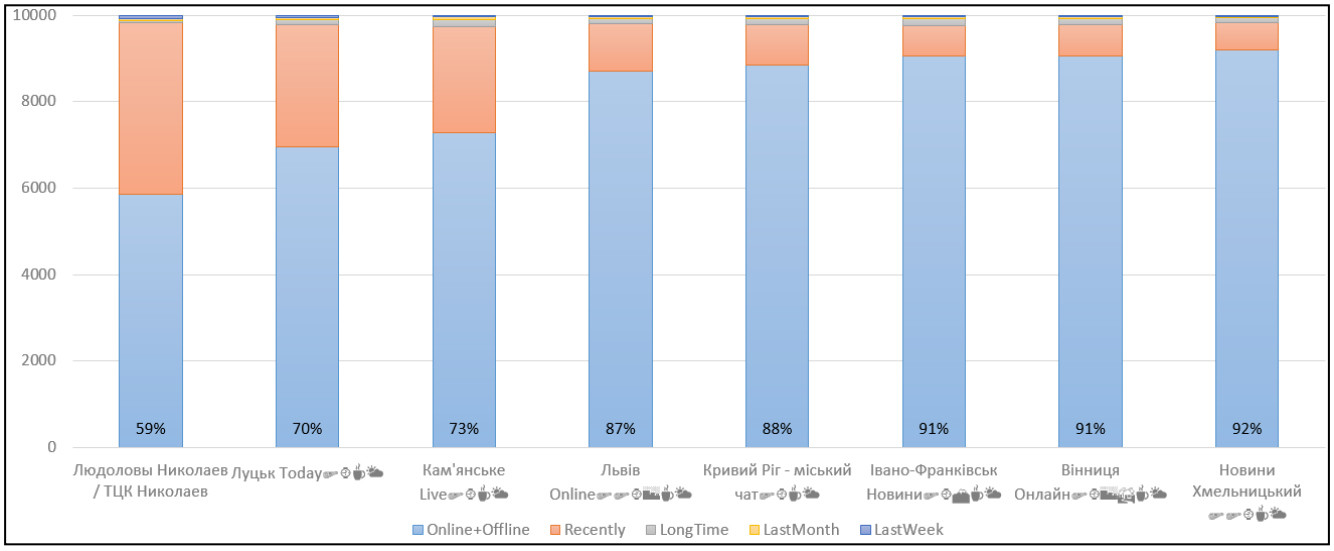

Рисунок 2.7 – Розподіл серед локальних спільнот, в яких публікуються новини. Приблизно **82%** серед усіх учасників чатів мають відкритий статус.

2.1.4 Збір даних через MTProto

Telegram надає офіційний API для розробників, який дозволяє створювати власні клієнти або бот-програми. В основі нього лежить протокол MTProto, що забезпечує авторизацію і обмін повідомленнями з сервером. В рамках дослідження було створено скрипт мовою програмування Python з використанням бібліотеки Telethon – високорівневої обгортки над MTProto API. Ця бібліотека дозволяє увійти в мережу Telegram під обліковим записом користувача або бота і взаємодіяти з об’єктами (користувачами, повідомленнями, статусами) як звичайний клієнт.

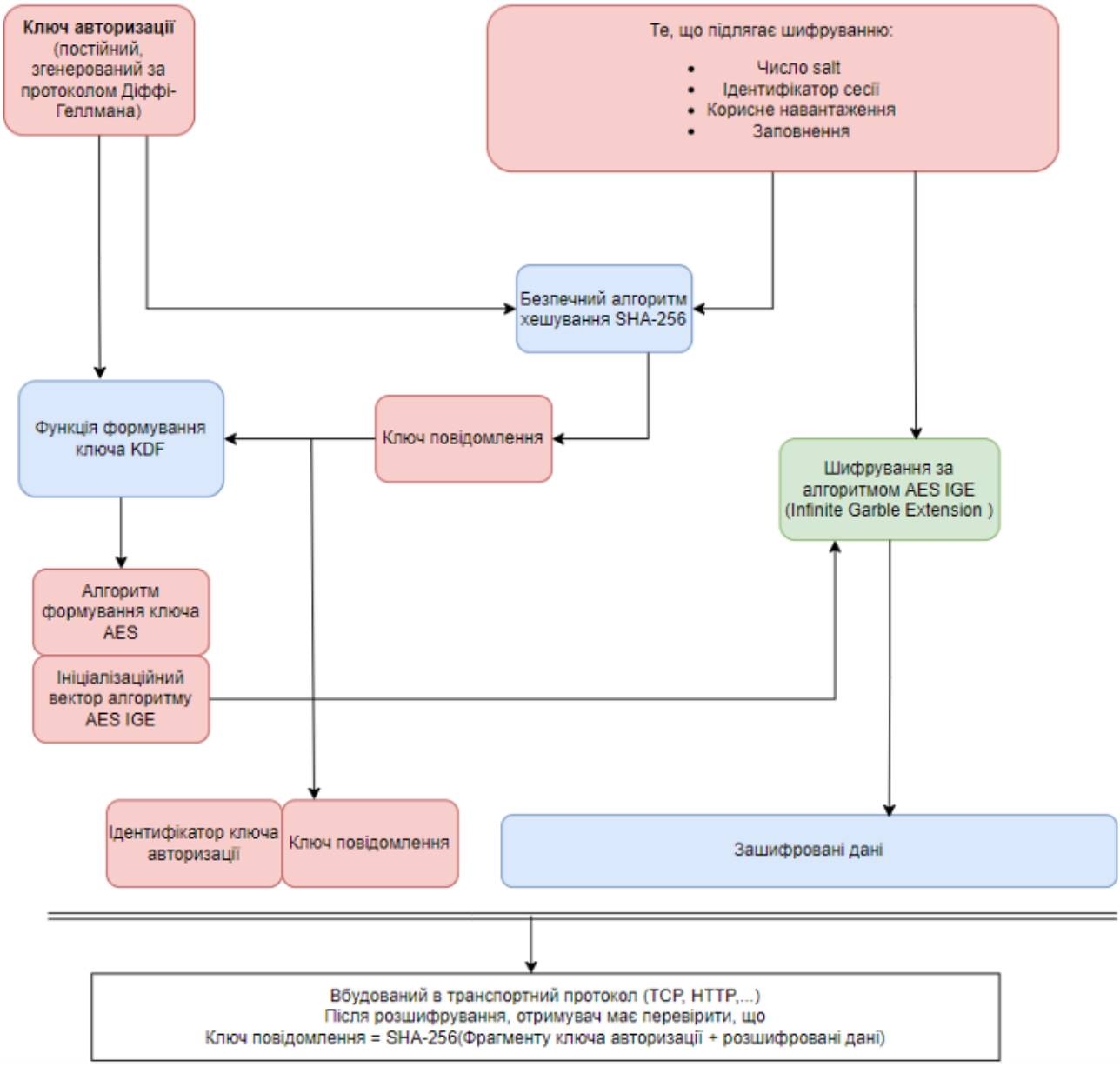

Рисунок 2.8 – Схема роботи MTProto в хмарних чатах [51].

2.2 Розробка архітектури системи програмного прототипу

2.2.1 Можливості Telethon API

Telethon API – це офіційно задокументована бібліотека, яка використовується для написання застосунків на мові Python, що створені взаємодіяти із Telegram. Вона надає зручні асинхронні методи для виконання усіх дій – від надсилання повідомлень до отримання списку діалогів і статусів користувачів. У контексті поставленого завдання ключовими виявились наступні можливості Telethon API:

- Авторизація в Telegram за допомогою бібліотеки Telethon [52]

Перш ніж почати працювати з API Telegram, необхідно отримати власний ідентифікатор та хеш API. Необхідно увійти до свого облікового запису Telegram через номер телефону облікового запису розробника на https://my.telegram.org/apps:

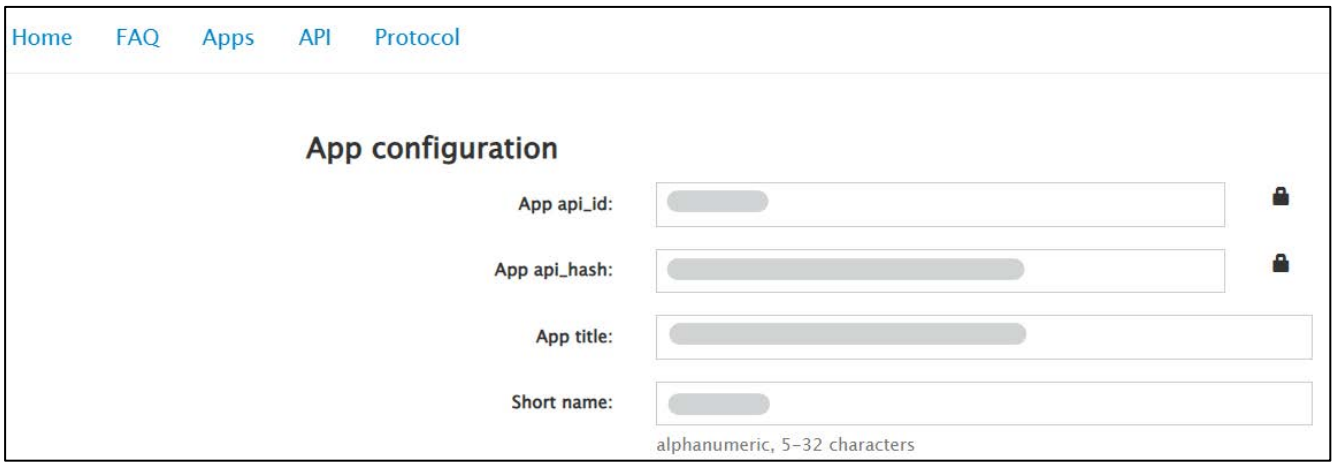

Рисунок 2.9 – Отримання **api_id** та **api_hash** для свого застосунка

Наступний код, що наведений нижче, наочно демонструє як у першому рядку відбувається імпортування імені класу при створення екземпляра клієнта. Потім визначаються змінні для зручного зберігання ідентифікатора та хеша API.

Після цього створюється новий екземпляр TelegramClient із назвою «client». Надалі від імені цього клієнта, наприклад, можна відправити собі повідомлення:

```
from telethon import TelegramClient

# Підставити власні значення із `my.telegram.org`
api_id = 12345
api_hash = '0123456789abcdef0123456789abcdef'

# Перший аргумент – це ім'я файла `.session`.
with TelegramClient('anon', api_id, api_hash) as client:
    client.loop.run_until_complete(client.send_message('me', 'Hello Telegram!'))
```

Також можна використовувати бібліотеку Telethon для своїх Telegram-ботів* (звичайних облікових записів ботів автоматизації, а не користувачів). Для цього все одно знадобиться ідентифікатор та хеш API, але процес аналогічно досить схожий:

```
from telethon.sync import TelegramClient

api_id = 12345
api_hash = '0123456789abcdef0123456789abcdef'
bot_token = '12345:0123456789abcdef0123456789abcdef'

# Якщо нам потрібен явний токен бота,
# то потрібно вручну викликати метод `TelegramClient.start()`.
bot = TelegramClient('bot', api_id, api_hash).start(bot_token=bot_token)

# Надалі можна використовувати екземпляр клієнта як і зазвичай.
with bot as bot_client:
    ...
```

** Для отримання облікового запису бота, необхідно «поговорити» з @BotFather.*

- API методи в бібліотеці Telethon [53]

Існують т.з. «дружні методи», які рекомендовано завжди використовувати для доступу до API Telegram. Їх перелік наводиться в документації Telethon.

Наступний код демонструє, як увійти в Telegram, отримати інформацію про сутність користувача, надіслати повідомлення, файли, увійти до чату, роздрукувати повідомлення та завантажити файли, отримати список користувачів групи:

```python
from telethon import TelegramClient

# Підставити відповідні значення
api_id = 12345
api_hash = '0123456789abcdef0123456789abcdef'
client = TelegramClient('tg_connect', api_id, api_hash)


async def main():
    # Отримати інформацію про користувача
    user = await client.get_entity(<user_id>)

    # `user` - це користувацький об'єкт. Можна красиво надрукувати
    # будь-який об'єкт Telegram за допомогою метода `.stringify`:
    print(user.stringify())

    # Можна отримати доступ до всіх атрибутів сутностей Telegram через
    # атрибути після крапки. Наприклад, щоби отримати нікнейм та статус:
    username = user.username
    print(username)
    print(user.status)  # ☺

    # Можна роздрукувати всі діалоги/розмови, в яких Ви берете участь:
    async for dialog in client.iter_dialogs():
        print(dialog.name, 'has ID', dialog.id)

    # Можна відправити повідомлення самому собі...
    await client.send_message('me', 'Hello, myself!')
    # ... до деякої групи через її ідентифікатор
    await client.send_message(-100123456, 'Hello, group!')
    # ... якимось контактам
    await client.send_message('+34600123123', 'Hello, friend!')
    # ... або навіть на тег будь-якого користувачу
    await client.send_message('username', 'Testing Telethon!')

    # Можна відправляти файли, мелодії, документи, архіви...
    await client.send_file('user', '/home/user/Pictures/holidays.jpg')

    # Можна роздрукувати історію повідомлень будь-якого чата:
    async for message in client.iter_messages('user'):
        print(message.id, message.text)

    # Можна отримати список групи, але потрібно бути її учасником:
    group = await client.get_entity(-100<chat_id>)

    participants = []
    async for user in client.iter_participants(group):
        participants.append([user.username, user.phone])

with client:
    client.loop.run_until_complete(main())
```

- Модуль отримання оновлень користувача [54]

Отримання оновлень – це важлива тема для такої платформи обміну повідомленнями, як Telegram. Завжди виникає потреба отримувати повідомлення, коли надходить нове повідомлення, коли учасник приєднується, коли хтось починає друкувати і т.д. Для цього можна використовувати події («events»).

Зважаючи на те, що в цій роботі досліджуються мітки OSI, то буде розглянуто «events.UserUpdate()». Дана подія виникає завжди, коли цільовий користувач змінює свій статус онлайн-активності, починає писати або надсилати файли і т.д.:

```
from telethon import TelegramClient, events, types

api_id = 12345
api_hash = '0123456789abcdef0123456789abcdef'
client = TelegramClient('tg_connect', API_ID, API_HASH)

# Можна залишити порожнім set() і тоді буде здійснюватися
# моніторинг всіх контактів та одноранговых користувачів
WATCH_USER_IDS = {*********}


@client.on(events.UserUpdate)
async def user_update_handler(event):
    uid = event.user_id

    # Якщо потрібно слідкувати лише за конкретними ID
    if WATCH_USER_IDS and uid not in WATCH_USER_IDS:
        return

    status = event.status  # ☺

    if isinstance(status, types.UserStatusOnline):
        print(f"[ONLINE] {alias} ({uid})")
    elif isinstance(status, types.UserStatusOffline):
        print(f"[OFFLINE] {alias} ({uid}), was_online={status.was_online}")
    elif status is not None:
        # інші статуси: Recently / LastWeek / LastMonth / Empty
        print(f"[STATUS] {alias} ({uid}) → {type(status).__name__}")
    else:
        # подія UserUpdate без статусу (наприклад typing, uploading і т.п.)
        print(f"[UPDATE] {alias} ({uid}) без статусу (typing/uploading тощо)")


with client:
    client.loop.run_until_complete(client.run_until_disconnected())
```

- Поняття сутності в об’єктах Telegram [55]

У бібліотеці Telethon широко використовується поняття «сутності» («entity»). Сутність буде посилатися на будь-який об’єкт User, Chat або Channel, який API може повернути у відповідь на певні методи, такі як GetUsersRequest, тощо.

Завдяки використанню session-файлів бібліотека автоматично запам’ятає ключові властивості сутностей, такі як пара ідентифікатора та access-хеш. Таким чином, викликам API не потрібно знати всю інформацію про об’єкти, а лише їх ідентифікатор та хеш. При виконанні запиту, якщо була надана повна сутність, наприклад User, бібліотека автоматично перетворює його в цільовий InputPeer.

Якщо не вдалося знайти вхідний об’єкт, отримано помилку «*Could not find the input entity for*», то необхідно запитати себе: «*Як би я знайшов цей об’єкт через офіційний застосунок?*». Тепер потрібно зробити те саме з бібліотекою Telethon:

```
# Передбачається, що цей код буде всередині асинхронного визначника
async with client:
    # Якщо є нікнейм користувача ...
    entity = await client.get_entity(username)

    # Якщо є відкрита розмова ...
    await client.get_dialogs()

    # Якщо користувач є учасником якоїсь групи
    await client.get_participants('username')

    # Якщо користувач був першим відправником переадресованого повідомлення
    await client.get_messages('username', 100)

    # Лише зараз, після попередніх викликів, можна використати ідентифікатор
    await client.send_message(123456, 'Hi!')

    entity = await client.get_entity(123456)
    print(entity.status)  # ☺
```

Як тільки бібліотека побачить об’єкт, одразу можна використовувати його цілісний ідентифікатор. Не можна використовувати сутності з ідентифікаторами, яких Telethon не бачив. Потрібно змусити бібліотеку побачити їх хоча б один раз.

2.2.2 Алгоритм отримання міток OSI

З метою проведення експерименту було розроблено прототип програмного застосунку, що призначений здійснювати моніторинг статусів користувачів Telegram із використанням інструментарію мови Python. Таким чином для реалізації було застосовано бібліотеку асинхронної взаємодії Telethon. Отже, такий підхід дозволив автоматизувати збір часових міток про зміну статусів. Фіксувався час, коли цільовий користувач з'являвся «online» та коли переходив в «offline». Моніторинг здійснювався або шляхом активного опитування (періодичного запиту статусу), або через пасивне відстеження оновлень, що надсилаються сервером Telegram. Кожен із методів має свої особливості. Активний метод гарантує фіксацію усіх змін статусу з заданим інтервалом опитування, проте може створювати значне навантаження (часті запити до сервера), через що моніторинг буде призупинятися, сигналізуючи про помилку із кодом 420 FLOOD [56] (час очікування перед наступним запитом). Пасивний метод базується на системних повідомленнях Telegram про зміну статусу (доступних, якщо відкрита відповідна сесія та ціль додана до списку однорангових користувачів, тобто PeerUser), що ефективніше, але можуть фіксуватися незакриті сесії, якщо вони відбулися між інтервалами опитування або не були надіслані як окремі події.

Практична реалізація поєднала обидва підходи*. При появі користувача в мережі: скрипт запускав часте опитування його статусу, щоби точно зафіксувати момент виходу офлайн, а також враховував повідомлення UpdateUserStatus, які надає API-метод. Отримані часові метрики базово зберігалися у CSV-файлі. Зібрані дані представляють собою час входу та виходу кожного користувача з мережі. Серед цільових об'єктів цільового моніторингу було обрано близько 100 реальних користувачів Telegram, що залишили статус видимим для інших.

* *Під час розробки інструмента були спробувані різні підходи моніторингу перед формуванням фінального алгоритму. Оскільки автоматизований збір міток OSI став можливий попри наявні обмеження, то далі розглянуто логіку його роботи.*

- **Активна перевірка статусу (Get User)** – коли періодично надсилається запит «get_entity» до сервера Telegram, щоби отримати поточний онлайн-статус.

- **Пасивне отримання оновлень про статус (Update Events)** – коли сервер Telegram самостійно надсилає повідомлення клієнту про зміну онлайн-статусу однорангового користувача (PeerUser) через подію «UserUpdate».

Нижче представлена таблиця, яка відображає порівняння обох підходів:

Таблиця 2.1 – Відмінності у застосуванні різних підходів до моніторингу

	Активна перевірка	Отримання оновлень
Переваги	• Більш передбачуваний список моніторингу. • Не потрібно додавати користувачів у список контактів Telegram. • Більш придатний для порівняльних тестів.	• Події приходять тільки в момент оновлення даних. • Мінімальна затримка в отриманні точних online. • Відсутній ризик отримати штрафний FloodWait. • Легше масштабується.
Недоліки	• Ризик FloodWait-лімітів (один запит це максимум 200 юзерів; ~0.2 с/запит, але сумарна обробка зростає із довжиною списка > 10-15). • Зайвий мережевий трафік до серверів відповідно можливі затримки в мережі та ріст CPU на постійних запитах.	• Залежність від нюансів мобільного Telegram (т.з. «mobile linger»: ~5 хв можливе фіктивне подовження online або невчасне закриття сесії). • Невідомі ліміти на кількість користувачів (*потрібно досліджувати*)
Доцільність використання	Малі вибірки (~10-15 юзерів), тестові заміри, а також альтернатива при відсутності підписки на отримання оновлень (*якщо її приберуть*).	Довготривалий моніторинг, середні/великі набори користувачів, а також для збереження точності.

Отже, блок-схема моніторингу онлайн-активності має наступний вигляд:

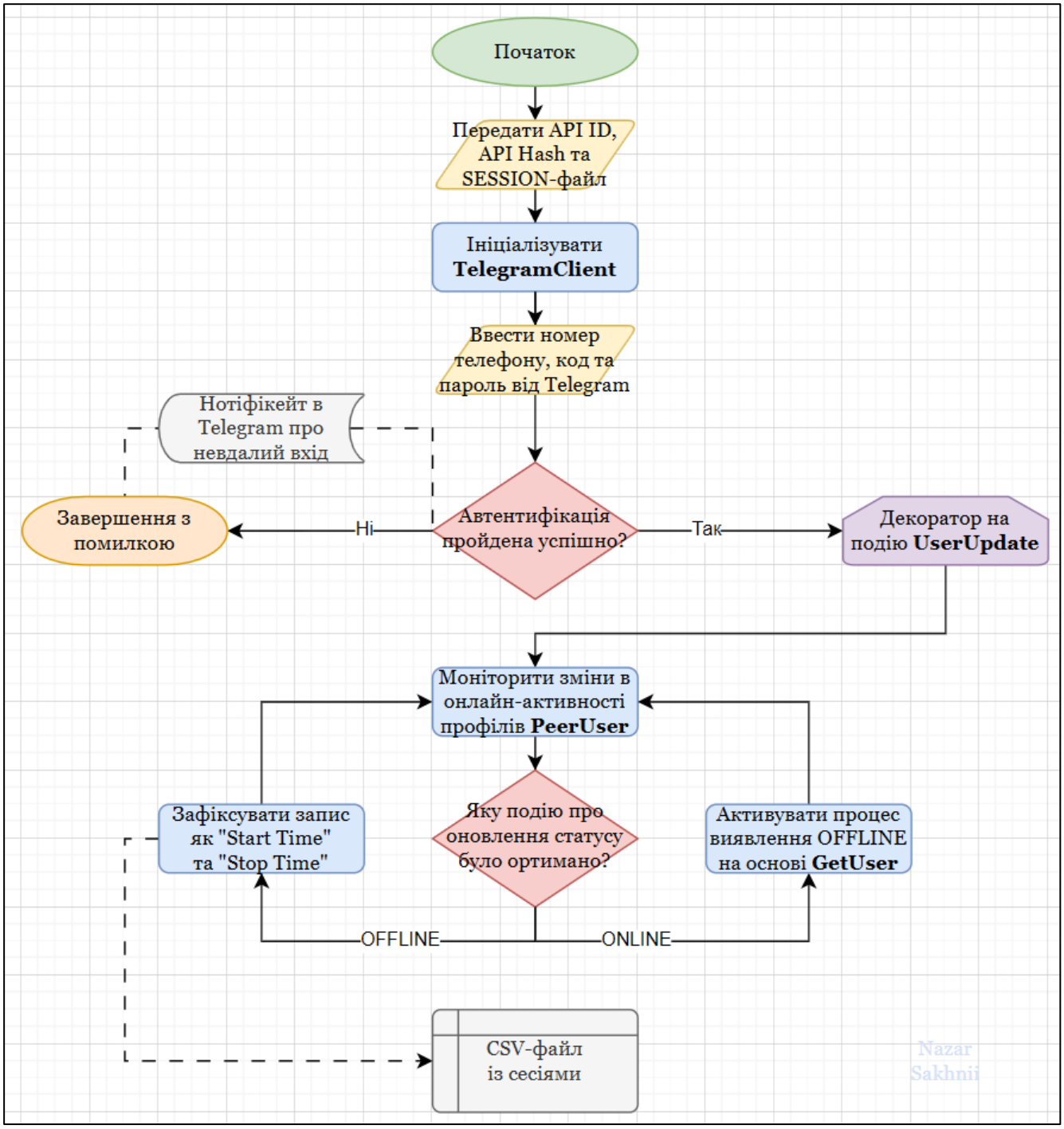

Рисунок 2.10 – Блок-схема моніторингу онлайн-активності.

** Процес виявлення OFFLINE – це запасний механізм із закриття сесії оснований на активній перевірці статусу, що необхідний через можливі затримки в зміні статусу для користувачів, які використовують мобільний застосунок Telegram.*

2.3 Експериментальний збір та кластерний розподіл OSI

2.3.1 Візуалізація зібраних даних

CSV-файл (`sessions.csv`) із переліком всіх зафіксованих сесій під час моніторингу онлайн-активності користувачів Telegram має мінімальну структуру, яка необхідна для збереження відповідної інформації. Таким чином, датасет має такі назви стовпців, як: `user_id`, `username`, `start_time`, `stop_time`, `duration_s`.

Моніторинг було проведено в часовий проміжок **20.10.2025-30.11.2025**, і як результат, було зібрано близько 265 тис. сесій для 100+ користувачів Telegram.

```
RangeIndex: 264738 entries, 0 to 264737
Data columns (total 5 columns):
 #   Column      Non-Null Count   Dtype
---  ------      --------------   -----
 0   user_id     264738 non-null  int64
 1   username    264738 non-null  object
 2   start_time  264738 non-null  datetime64[ns]
 3   stop_time   264738 non-null  datetime64[ns]
 4   duration_s  264738 non-null  int64
dtypes: datetime64[ns](2), int64(2), object(1)
memory usage: 10.1+ MB
```

```
Кількість записів у періоді 20-10-2025 ... 30-11-2025: 264735

Мінімальний start_time у періоді: 2025-10-19 23:58:52
Максимальний start_time у періоді: 2025-11-30 23:59:55
Мінімальний stop_time у періоді: 2025-10-20 00:00:16
Максимальний stop_time у періоді: 2025-12-01 00:01:20
```

sessions.csv - Notepad

File Edit Format View Help

```
user_id,username,start_time,stop_time,duration_s
601[redacted],2025-10-20 00:00:12,2025-10-20 00:00:16,3
414[redacted],2025-10-20 00:00:33,2025-10-20 00:00:37,3
414[redacted],2025-10-20 00:00:48,2025-10-20 00:00:49,0
```

Рисунок 2.11 – Обсяг та структура даних, що були зафіксовані у CSV-файл

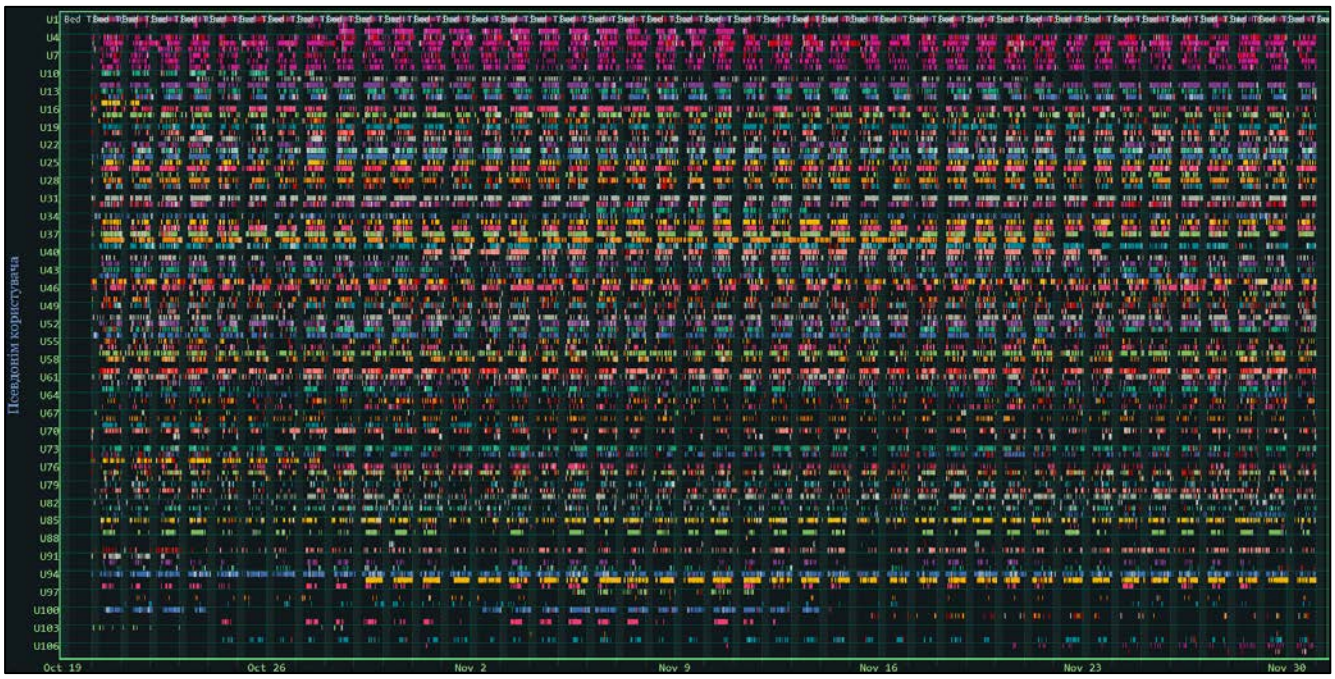

Рисунок 2.12 – Хронограма активності для 100+ користувачів Telegram

Отримані дані часової активності в Telegram можна інтерпретувати таким чином, що кожна сесія – це часовий проміжок між подіями “online” та “offline”. Відповідно, зміни статусу доцільно формалізувати у вигляді автомата станів:

- ***Ідея моделі зміни станів***

  Ми спостерігаємо часовий ряд $x(t)$, де OSI може бути лише у двох станах:

  - **0** – ОФЛАЙН
  - **1** – ОНЛАЙН

  Тоді:

  - *Сесія* – це максимальний відрізок часу, коли $x(t) = 1$ без розривів;
  - *Початок сесії* – це перехід **0** → **1**;
  - *Кінець сесії* – це перехід **1** → **0**.

- ***Формальне означення автомата***

  Нехай існує множина станів $\{S_0, S_1\}$:

  - S_0 = ОФЛАЙН
  - S_1 = ОНЛАЙН

  Час задано із дискретним кроком Δt.

  Таким чином, маємо двостановий автомат $S(t)$ із матрицею переходів:

$$P = \begin{pmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{pmatrix}$$

  де

  - $P_{00} = \mathbb{P}(S(t+\Delta t) = S_0 \mid S(t) = S_0)$ – залишається офлайн
  - $P_{01} = \mathbb{P}(S(t+\Delta t) = S_1 \mid S(t) = S_0)$ – початок сесії
  - $P_{10} = \mathbb{P}(S(t+\Delta t) = S_0 \mid S(t) = S_1)$ – кінець сесії
  - $P_{11} = \mathbb{P}(S(t+\Delta t) = S_1 \mid S(t) = S_1)$ – залишається онлайн

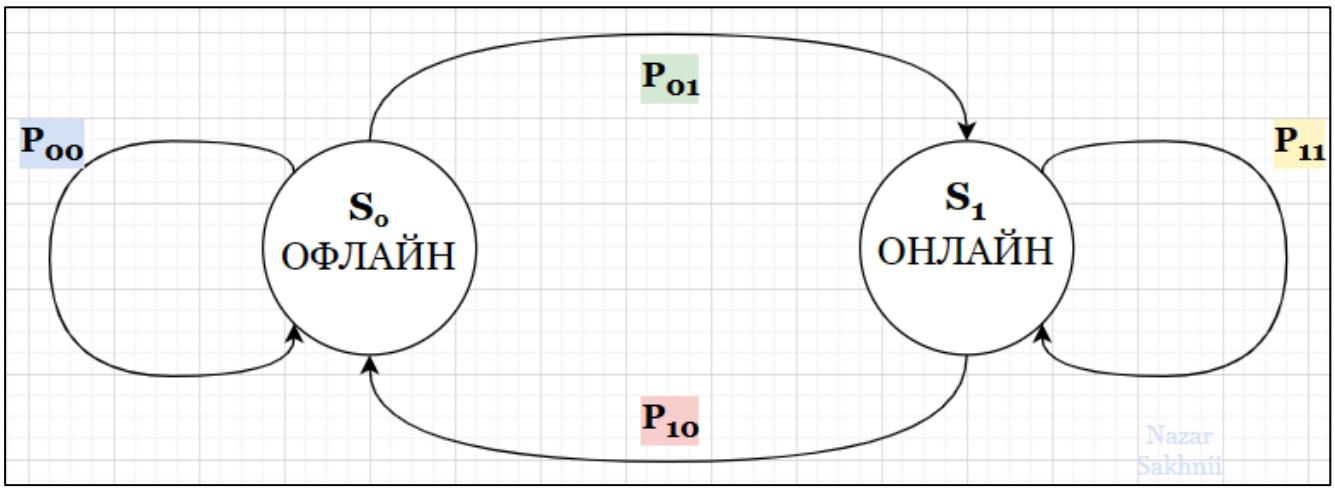

Рисунок 2.13 – Двостановий автомат зміни статусів онлайн-активності

- ***Зв'язок із діаграмою Ґанта***

Таким чином, діаграми Ґанта (на основі Python-бібліотеки «Plotly») наглядно відображають реалізацію процесу $S(t)$. Відповідно, візуалізація сесій на графіку полягає в тому, що інтервали, які відповідають стану S_1 = ОНЛАЙН, штрихуються.

Нижче наводиться хронограма активності для цільової групи з 10 вибірково пов'язаних між собою користувачів, яка більш наглядно демонструє варіативність в стилі використання Telegram. Період спостереження – одна доба (**16.11.2025**).

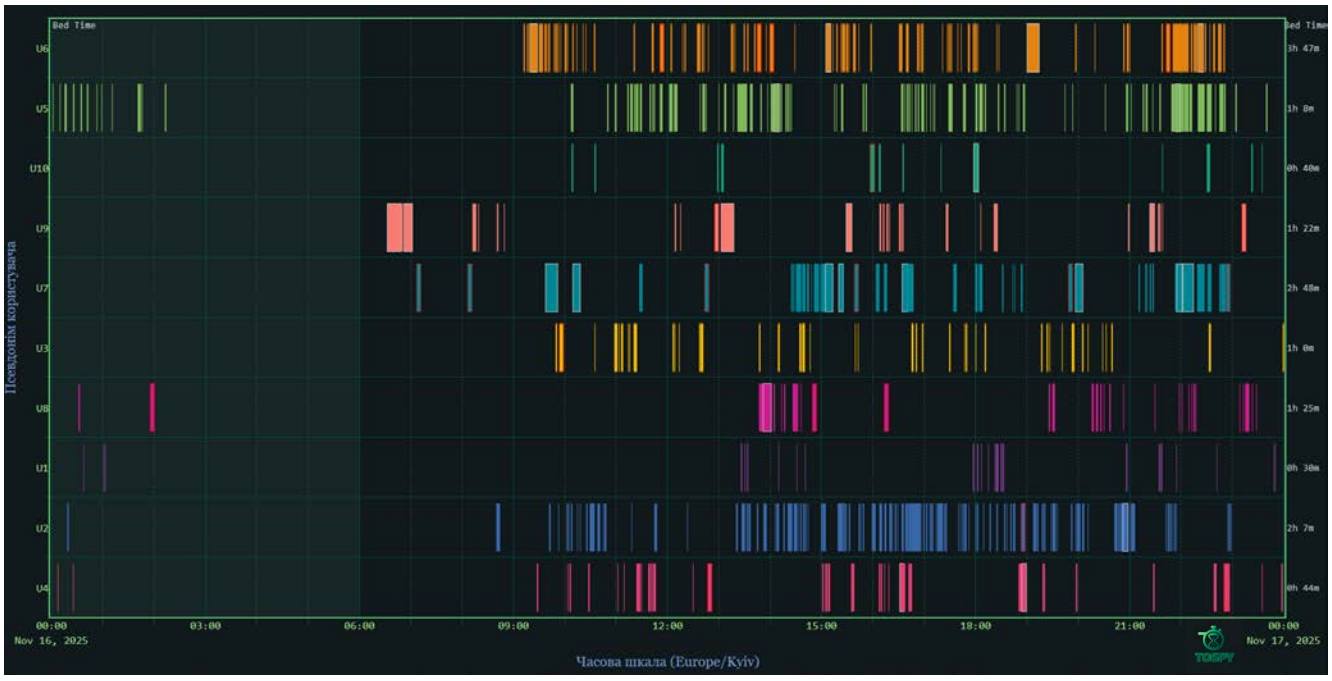

Рисунок 2.14 – Добова хронограма активності для 10 користувачів Telegram

2.3.2 Стиль використання Telegram

Зібравши достатньо даних про входи/виходи в мережу, буде отримано часовий «портрет» – у які періоди дня людина зазвичай активна, коли робить перерви (спить або зайнята справами), наскільки стабільний цей графік по днях тижня. Такий портрет можна співвіднести з відомими циркадними ритмами, визначити хронотип та оцінити вразливість до соціальної інженерії в різні періоди.

Важливо зазначити, що така модель є спрощеною та ймовірнісною. На поведінку впливають і зовнішні фактори (робочий графік, події дня, стрес), і персональні звички (хтось уникає месенджерів, хтось безперервно там зависає).

Таким чином, на основі часових показників онлайн-активності було проведено кластеризацію користувачів за двома ознаками – середньодобова тривалість використання та кількість сесій на день. Оскільки для Telegram були відомі відповідні середньостатистичні показники [47], то межі кластерів було задано методом порогових значень відносно цих границь. Попри узагальнений характер такої моделі, доцільно виокремити характерні стилі взаємодії з Telegram.

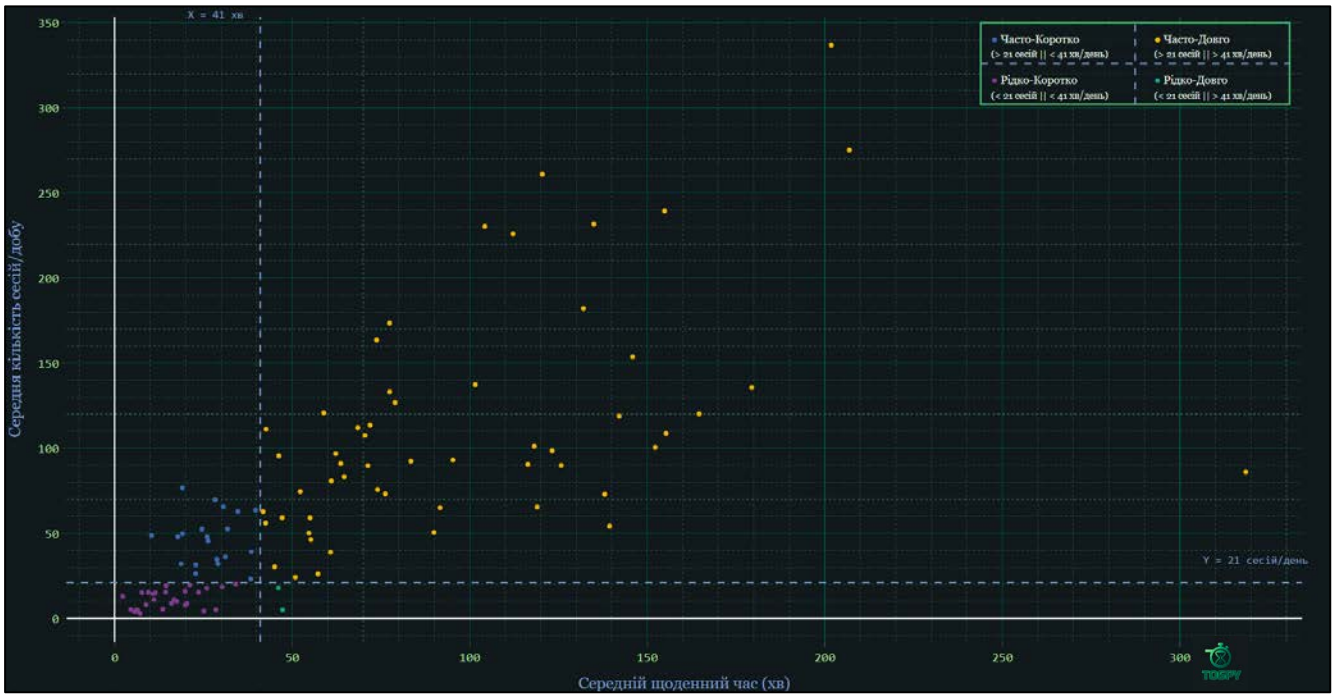

Рисунок 2.15 – Квадрант кластерів для стилю використання Telegram

Висновки до розділу 2

Зважаючи на об’єктивну популярність Telegram в Україні та актуальність проблематики через високий показник (~73%) тих користувачів, що не обмежили доступ у відображенні їхньої онлайн-активності, то особливо доцільним було в цій роботі продемонструвати, яким чином сторонні особи можуть, не порушуючи правових норм та політики конфіденційності, стежити за іншими користувачами.

За результатами проведеного комплексного моделювання алгоритмічної основи збору онлайн-активності користувачів Telegram, можна зробити висновок, що саме відкрита доступність до Telegram API (та відповідно до міток OSI) є ключовим фактором витоку інформації про частоту та тривалість користування. Подібний доступ забезпечує офіційно документована бібліотека Telethon API.

Як результат, було розроблено систему програмного прототипу на основі детермінованої логіки двостанового автомата, який фіксує переходи користувачів між онлайн та офлайн. Таким чином, відповідний алгоритм моніторингу полягає у поєднанні двох підходів таких, як: отримання подій про оновлення статусу через декоратор «**UserUpdate**» та періодична перевірка статусу через метод «**get_entity**».

Із точки зору обчислювальних витрат процес фіксації міток OSI виявився досить легким (операції з часовими даними потребують мінімум ресурсів), а також масштабованим, оскільки було підтверджено, що можна паралельно моніторити значну кількість користувачів. Таким чином, було проведено експериментальний збір, в результаті якого було отримано велику вибірку міток OSI (понад 265 тис.).

Подальше застосування методів статистичної візуалізації дає можливість визначити методику, за якою проводяться аналітичні дослідження характеристик цифрової поведінки. Для окремих користувачів це може означати виявлення регулярних добових циклів, повторюваних патернів активності або специфічних особливостей стилю використання, що й розкривається детальніше у Розділі №3.

3 ДОСЛІДЖЕННЯ ХРОНОГРАМ АКТИВНОСТІ ЩОДО ВИЯВЛЕННЯ ПОВЕДІНКОВИХ МОДЕЛЕЙ І ПЕРІОДІВ ВРАЗЛИВОСТІ

3.1 Застосування методології OSINT для оцінки часової активності

3.1.1 Методика оцінки цифрової активності

Завдяки використанню методів моніторингу часової активності, які були описані в попередньому розділі, стає можливим дослідження цифрової поведінки використання цільовою особою месенджера Telegram. Додаток «А», відповідно, містить програмний код прототипу системи моніторингу, т.з. сервіс авторської розробки «TOSpy»*. Із його використанням сторонній користувач, який проводить дослідження на основі відкритих джерел (надалі OSINT-аналітик), має можливість автоматизовано фіксувати індикатори онлайн-статусів без відома цільової особи.

Мітки OSI користувачів Telegram будуть зібрані та надалі опрацьовані без порушення правових норм про недоторканність приватного життя, а також тих положень про персональні дані, які вказані в політиці конфіденційності Telegram [38]. Чинне законодавство України не містить прямих заборон на збір таких даних, оскільки вони не вважаються конфіденційними через їх добровільне поширення.

OSINT-аналітик, як результат, через надмірну доступність Telegram API, отримує технологічний інструмент цілодобового моніторингу цифрової активності інших користувачів Telegram. Після фіксації достатньої кількості метрик, стає можливим подальше отримання інформації про поведінкові характеристики, тобто таких даних, які доступні лише через персональні сервіси, т.з. «Digital Wellbeing».

** Автор роботи, надаючи програмний код моніторингу OSI та методику оцінки активності, має на меті лише наглядно проілюструвати т.з. «Proof of Concept».*

Таким чином, для наглядного та повноцінного розуміння можливих ризиків витоку чутливої інформації, нижче наводиться BPMN-діаграма*, яка схематично моделює узагальнену методику оцінки цифрової активності користувачів Telegram:

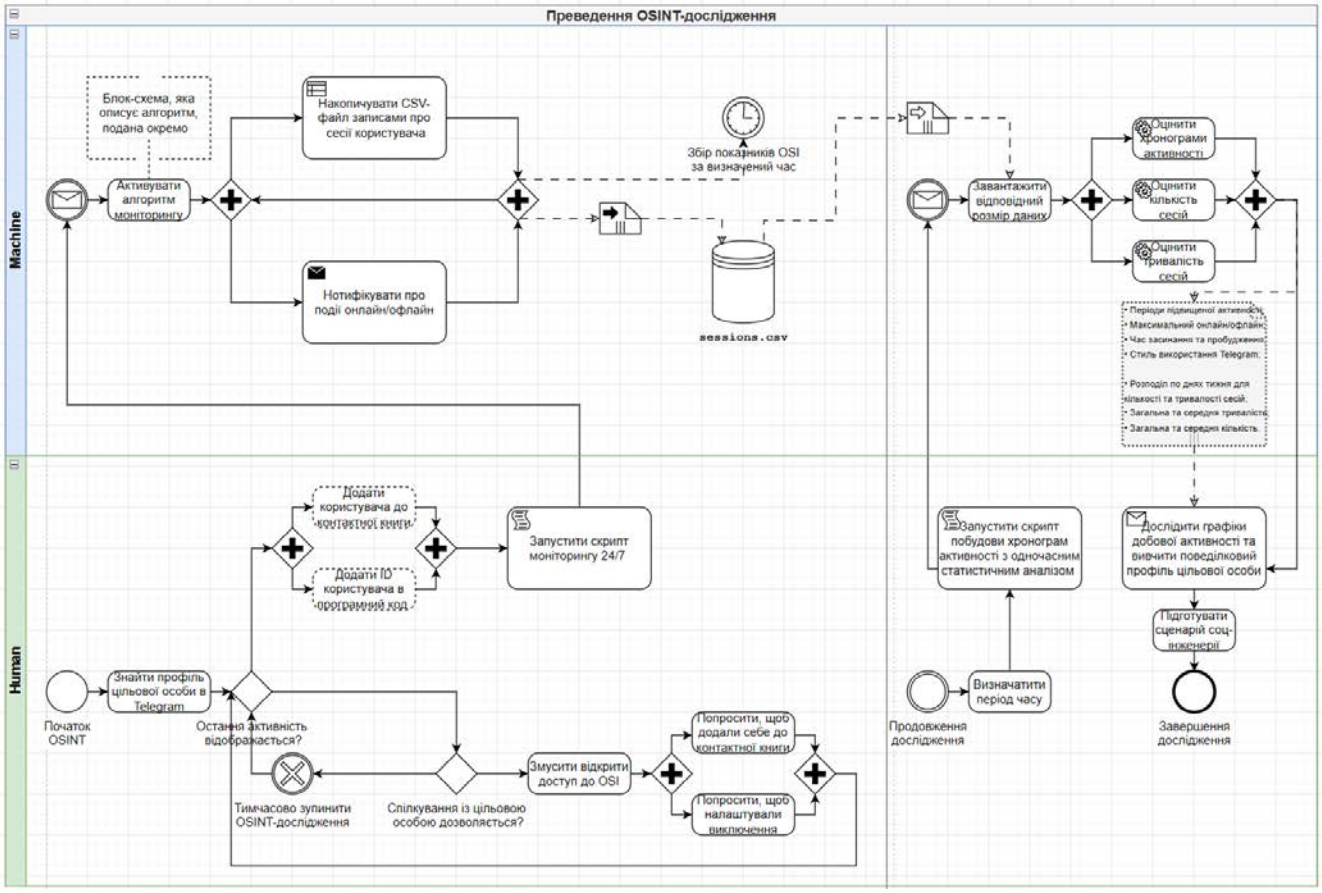

Рисунок 3.1 – BPMN-діаграма методики оцінки цифрової активності. Ключовими етапами в процесі дослідження є збір OSI та їхній аналіз.

Варто зазначити, що розглянута методика потенційно може бути застосована й до інших месенджерів чи соцмереж. Навіть незважаючи, що їх API не настільки доступне для користувацької взаємодії, проте на практиці підтверджено, що існує також інший спосіб. Він полягає в тому, що застосування інструмента «Selenium WebDriver» дозволяє проводити веб-скрапінг OSI-елементів в HTML-розмітці.

Такий підхід буде оснований на активній перевірці статусу із щосекундною періодичністю (якщо не буде лімітів на анти-скрапінг). Це дає можливості для досліджень по відстеженню перебування людини в застосунках різних соцмедіа.

3.1.2 Побудова графіків активності в Telegram

❖ На основі «GanttBased»-діаграм

Збір метрик відбувався протягом півтора місяця (з 20.10.2025 по 30.11.2025). На їх основі було сформовано часові серії та побудовано хронограми активності – т.з. діаграми Ґанта, де по осі X відкладено добовий цикл (з 00:00 до 24:00), а по осі Y – стан користувача (онлайн/офлайн) разом із відповідним днем тижня.

Подібний графік*, водночас, відображає такі статистичні показники, як:

- MAX Онлайн та Офлайн: максимальна та мінімальна тривалість сесії;
- Bed Time + AVG Bed Time: періоди сну та їхнє середнє значення;
- «Частотність-Тривалість»: профіль (стиль) використання Telegram.

Рисунок 3.2 – «GanttBased»-діаграма (т.з. хронограма активності) за часовий період в півтора місяця (20.10.2025-30.11.2025), яка відображає всі сесії в Telegram для окремого користувача (U_i)

** Нанесення часових серій на графік здійснюється із використанням «Plotly» або т.п., проте вимірювання статистичних показників потребує модуля «Pandas».*

❖ На основі «BarBased»-гістограм

Для наочного представлення зібраних даних потребується побудувати дві стовпчасті діаграми, які за своїм змістом мають назву «Сумарна тривалість за день» та «Кількість сесій за день». Вони відображають агреговані показники поведінки користувача в межах обраного періоду спостереження та дозволяють оцінити загальні тенденції використання месенджера Telegram, інтенсивність присутності, частоту входів і характер добових коливань активності. Ці графіки формують основу для подальшого поведінкового аналізу стилю користування Telegram.

- **«Сумарна тривалість за день» (**сумарний час онлайн у год/хв**):**
  - На графіку проведено горизонтальну лінію середнього.
  - Вгорі подається сумарний час і його частка від усього.
  - Фрагменти «контурної» зони, які обведені білим кольором, відображають тривалі сесії за день, що були довші за 5 хв.
  - Надвисокі показники можуть свідчити про певну залежність.

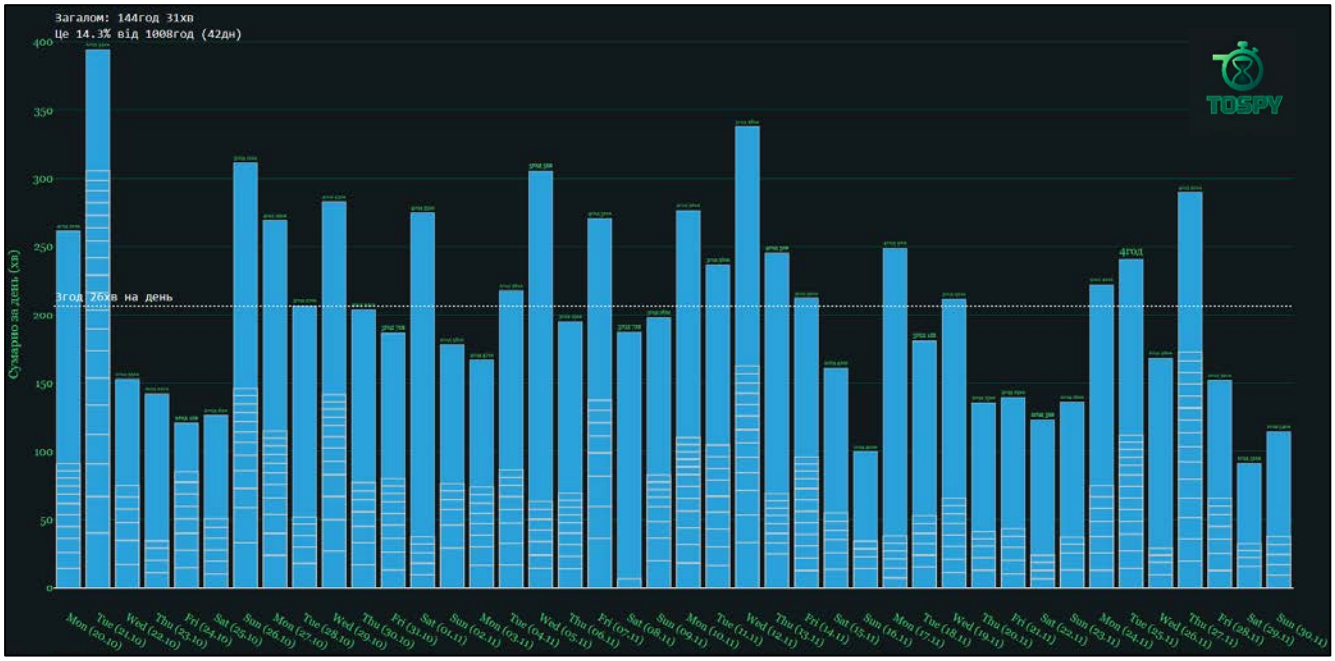

Рисунок 3.3 – Сумарна тривалість за день (20.10.2025-30.11.2025)

- **«Кількість сесій за день» (**кількість окремих сесій за день**):**
  - Нормальні сесії (до 5 хв): типова активність в месенджері Telegram.
  - Фіктивні сесії (295-299 с): т.з. ефект «mobile linger», який випадковим чином (наразі точна інформація відсутня) виникає при користуванні мобільним застосунком Telegram. Відповідно тривалість таких сесій зрізана до 30 с, щоб мінімізувати відхилення від реальної активності.
  - Довгі (>5 хв) сесії – це індикатор тривалої присутності без переривань.

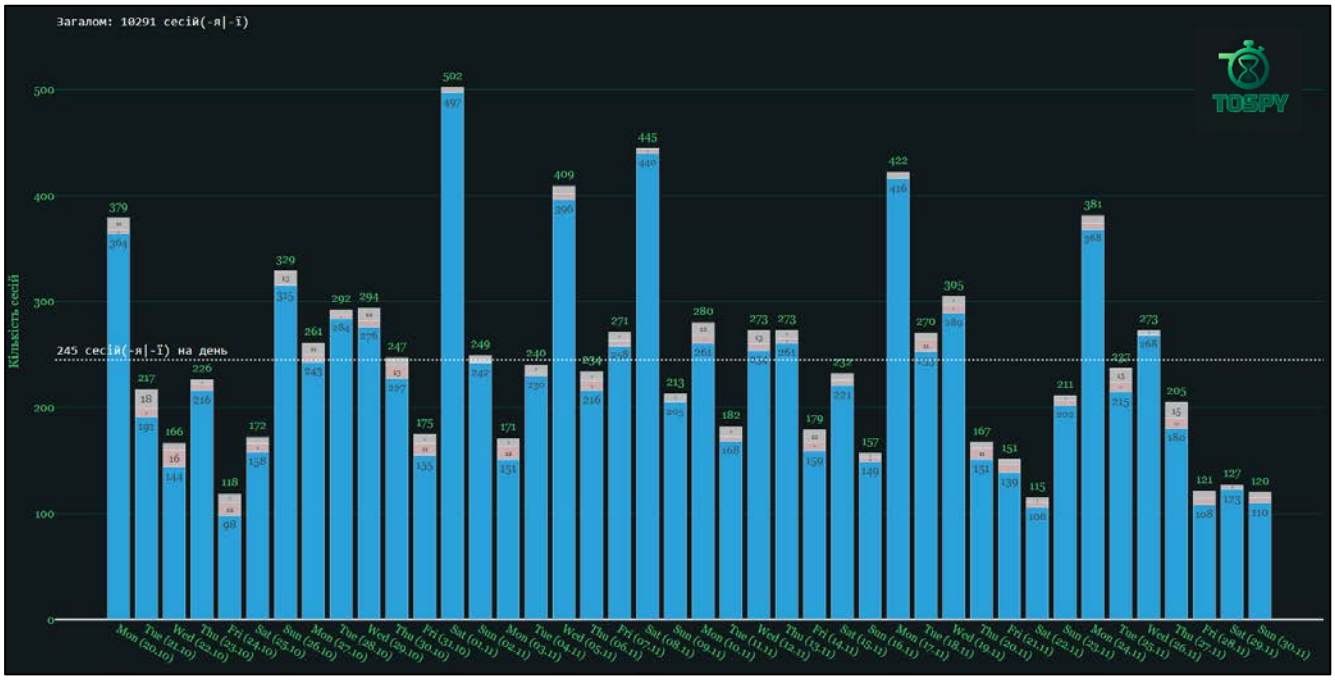

Рисунок 3.4 – Кількість сесій за день (20.10.2025-30.11.2025)

Таким чином, інформація про тривалість та кількість сесій дозволяє OSINT-аналітикам оцінювати, наскільки їхня ціль схильна до залежності від соцмереж та синдрому втрачених можливостей або FOMO (від англ. «Fear of missing out»). Це, в своє чергу, дозволяє передбачати, як користувачі будуть реагувати, коли їм прийде сповіщення в Telegram, тобто наскільки вони швидко відреагують.

Соціальний інженер, знаючи про подібну вразливість користувача, може адаптувати час і форму свого впливу, відповідно, щоб підвищити ймовірність успішного встановлення довірливих відносин під час свого «претекстінгу».

3.2 Побудова поведінкових моделей на основі часової активності

3.2.1 Циркадний ритм людської уважності

Добові коливання активності мозку впливають на увагу та продуктивність людини протягом дня. Дослідження підтверджують фактор ритмічності в окремих компонентах уваги [13]. Ці циклічні зміни рівномірно узгоджуються з коливаннями фізіологічних показників, таких як температура тіла, рівень мелатоніну та ін. – вони теж досягають піку вдень і спадають вночі, задаючи «ритм» організму. Відповідно, увага (і пов'язані з нею когнітивні функції) має циркадну компоненту. Тобто вночі та рано-вранці людині значно складніше зосереджуватися, більше часу потрібно на реакцію і опрацювання інформації, тим самим зростає кількість їх помилок.

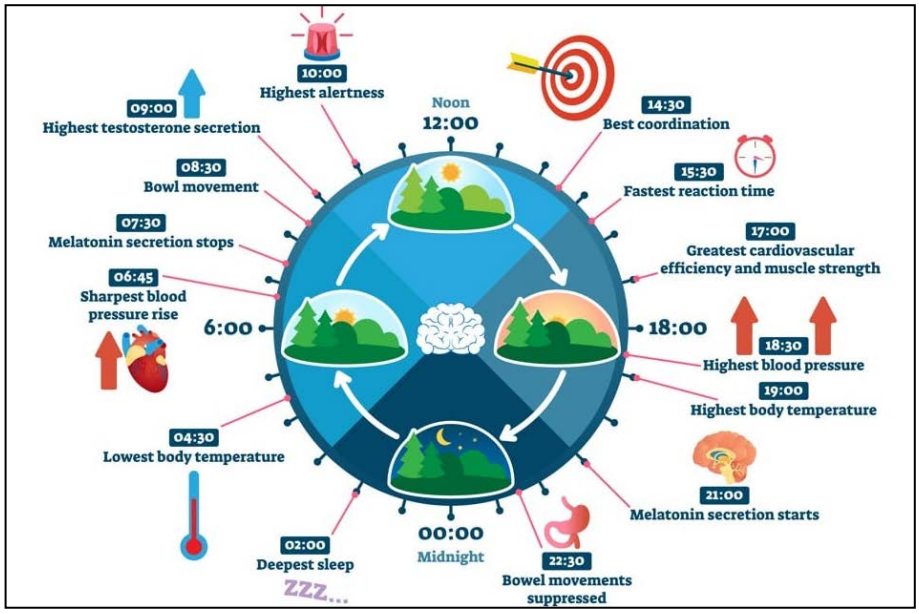

Рисунок 3.5 – Циркадний ритм людини («біологічний годинник») [57]

З точки зору ІБ, зниження уваги означає підвищену схильність не помітити загрозу або діяти «на автоматі», без належної обачності. Наприклад, користувач, перечитуючи повідомлення пізно вночі у втомленому стані, з більшою ймовірністю проігнорує підозрілі ознаки фішингової атаки. Таким чином, знання циркадного ритму уваги дає змогу виділити «вразливі періоди», коли людина природно менш сконцентрована, тобто буде більш вразлива до атак соціальної інженерії.

3.2.2 Хронотип на основі часової активності

Люди різняться у своїх добових біоритмах – це поняття відоме як хронотип. Виділяють класичні типи [58]: «ранковий» (жайворонок) – хто найпродуктивніший вранці і рано лягає спати; «вечірній» (сова) – хто пізно активізується і допізна не спить; а проміжний випадок іноді називають «аритмічний» або «голуб» – без вираженої схильності, рівномірно активні протягом дня. Хронотип визначається ендогенним біологічним годинником, і він є досить стабільною властивістю особистості. Жайворонки мають зсув усіх циркадних ритмів на більш ранній час відносно доби, а сови – навпаки, відстають у фазі (пізніше лягають і встають).

Визначення хронотипу користувача за його розкладом онлайн дозволяє персоналізувати модель. Наприклад, якщо бачимо, що ціль майже не заходить у мережу після 23:00, а зранку активна, то ймовірно це «жайворонок» – очікуємо, що увага буде високою зранку, а ввечері вона буде більш втомлена. Натомість якщо користувач регулярно онлайн до 2–3 ночі і прокидається пізно, можна віднести його до «сов», що значить – у ранкові години (коли його змушують обставини бути активним) він буде особливо неуважним, а також, досить ймовірно, втомленим.

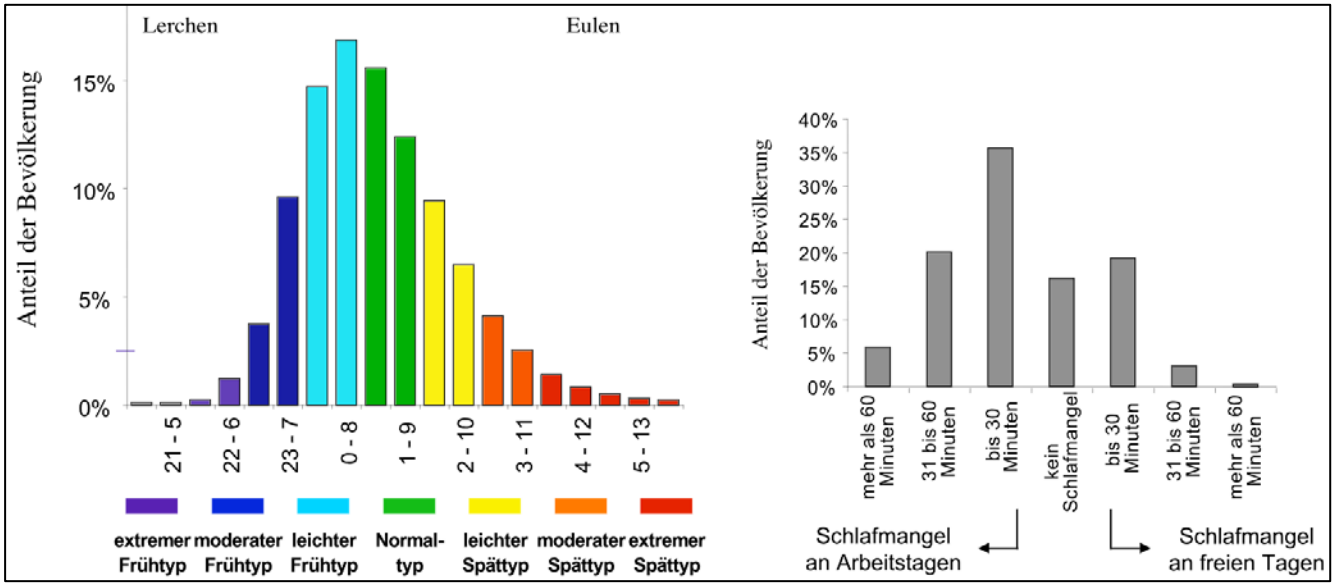

Рисунок 3.6 – Зліва: розподіл населення за хронотипами.
Справа: нестача сну в робочі та вихідні дні відповідно. [58]

3.2.3 Використання одержаних результатів

За результатами дослідження цифрової активності стає доступною додаткова інформація, яка може бути вміло застосована під час атак соціальної інженерії. Варто наголосити, що для отримання точних результатів процес розвідки потребує агрегації інформації на основі двох джерел: люди (HUMINT) та інтернет (OSINT). Таким чином, навіть інформація з міток OSI, яка характеризує цифровий слід, має при можливості бути розглянута для підвищення точності поданих висновків.

Проведення фішингової атаки, передбачає формування повідомлення, яке враховує як поведінкові дані цілі, так і її соціальний контекст. Застосовуються два ключові методи – це контекстуалізація (т.з. претекстінг) та персоналізація [14]:

- *Контекстуалізація* – це різновид підготовки повідомлення, у межах якого здійснюється комунікація таким чином, щоб вона відповідала звичним для користувача моделям взаємодії. Відповідно, розуміння стилю взаємодії під час користування Telegram дозволить синхронізувати свій характер поведінки із цільовою особою для досягнення ефекту «соціального віддзеркалення».
- *Персоналізація* – це ще один метод підготовки, за якого вміст адаптується із врахуванням персональних даних цільової особи. Таким чином, до таких даних належать частота та тривалість онлайн-активності в соцмедіа, типовий час реагування на повідомлення, переважні канали комунікації, а також тематика контенту, що викликає найбільшу зацікавленість. Використання цих даних дає змогу формувати повідомлення, які не лише відображають зацікавлення особи (наприклад, через демонстрацію спільних інтересів або знайомих соціальних зв’язків), але й збігаються з її звичними моделями цифрової поведінки.

Отже, оцінка часової активності перетворює онлайн-статус на інформативне джерело цифрових слідів, що дозволяє соціальному інженеру точно підбирати час і контекст для маніпуляції, експлуатуючи фізіологію та психологію своєї цілі.

3.3 Формулювання рекомендацій щодо мінімізації ризиків витоку

Telegram має достатньо гнучкі налаштування приватності для «Останньої активності». Як вже раніше автором було вказано (в пункті «*Конфіденційність міток OSI*» цієї роботи), то з метою протидії можливості прихованого стеження сторонніми користувачами – потрібно обрати опцію «Мої контакти». Таким чином, навіть ці налаштування обмежать візуальну видимість індикаторів онлайн-статусу та їхню доступність по API міток OSI тільки для списку власних контактів.

Однак використовуючи офіційний Telegram API (через Telethon), як було наглядно продемонстровано, стає зрозумілим те, що наскільки доступним завдяки автоматизації є збір інформації про появу користувачів онлайн та переходу їх в офлайн. Отримані хронограми активності користувачів підтвердили той факт, що як легко стороння особа може отримати детальний профіль цифрової поведінки своєї цілі. Таким чином, рекомендації для розробників Telegram є відповідними [38]:

- *Прибрати API-виклики, які дозволяють отримувати мітки OSI;*
- *Зробити онлайн-статус видимим лише для контактів користувача;*
- *Відмовитися від концепції взаємного приховування онлайн-статусу;*
- *Написати поруч із налаштуванням, які наслідки для конфіденційності*.

«*Кожна функція, яка впливає на конфіденційність користувача, повинна бути ввімкнена лише за вибором цього користувача, а не за замовчуванням*» [38].

Загалом, порушена в цій роботі проблематика може бути інтегрована у навчальні програми фахівців з інформаційної безпеки як складова базових навиків із цифрової гігієни. Врахування подібних аспектів у процесі підготовки дозволяє формувати у користувачів стійкі навички безпечної поведінки в соціальних медіа, включно з усвідомленням ризиків, пов’язаних із залишенням цифрових слідів.

Висновки до розділу 3

Завдяки авторській реалізації програмного прототипу моніторинг-сервісу, стає можливим його застосування, як OSINT-технології, при проведенні цільових досліджень цифрових слідів, залишених під час перебування в Telegram. Такий підхід дозволяє фіксувати індикатори онлайн-статусів без відома цільової особи.

OSINT-аналітик, як результат, через надмірну доступність Telegram API, отримує технологічний інструмент цілодобового моніторингу цифрової активності інших користувачів Telegram. Після фіксації достатньої кількості метрик, стає можливим подальше отримання інформації про поведінкові характеристики, тобто таких даних, які доступні лише через персональні сервіси, т.з. «Digital Wellbeing».

Відповідно, для наглядного та повноцінного розуміння можливих ризиків витоку чутливої інформації, було представлено BPMN-діаграму, яка схематично моделює узагальнену методику оцінки цифрової активності користувачів Telegram.

Варто зазначити, що розглянута методика потенційно може бути застосована й до інших месенджерів чи соцмереж. Навіть не зважаючи, що їх API не настільки доступне для користувацької взаємодії, проте на практиці підтверджено, що існує також інший спосіб. Він полягає в тому, що застосування інструмента «Selenium WebDriver» дозволяє проводити веб-скрапінг OSI-елементів в HTML-розмітці.

Таким чином, інформація про тривалість та кількість сесій дозволяє OSINT-аналітикам оцінювати, наскільки їхня ціль схильна до залежності від соцмереж та синдрому втрачених можливостей або FOMO (від англ. «Fear of missing out»). Це, в свою чергу, дозволяє передбачати, як користувачі будуть реагувати, коли їм прийде сповіщення в Telegram, тобто наскільки вони швидко відреагують.

Соціальний інженер, знаючи про подібну вразливість користувача, може адаптувати час і форму свого впливу, відповідно, щоб підвищити ймовірність успішного встановлення довірливих відносин під час свого «претекстінгу».

ВИСНОВКИ

У магістерській роботі було проведено комплексне дослідження, спрямоване на застосування OSINT-технологій для оцінки часової активності користувачів Telegram як чинника витоку їхніх поведінкових характеристик. На основі огляду наукових публікацій та професійно-технічних матеріалів було досліджено вплив індикаторів онлайн-статусу на конфіденційність користувачів соціальних медіа. Проведений в цій роботі експериментальний збір та статистичний аналіз хронограм активності дозволив підтвердити той факт, що стороння особа завдяки API має можливість моніторити цифрову активність інших користувачів Telegram.

Таким чином, під час проведеного дослідження, в підсумку, вдалося зробити відповідні висновки на основі поставлених завдань, що описують проблематику публічної видимості індикаторів онлайн-статусів (OSI) в соціальних медіа:

- Проведена оцінка правових та етичних аспектів використання міток OSI дозволила підтвердити, що збір та опрацювання інформації про онлайн-активність користувачів Telegram не порушує норм про недоторканність приватного життя і не утворює складу неправомірних дій. Чинне законодавство не містить прямих заборон на збір таких даних, як часові мітки перебування в соцмедіа, оскільки вони не вважаються конфіденційними через їх добровільне поширення. Telegram же в своїй політиці конфіденційності та в умовах використання не встановлює чітких договірних обмежень щодо подібних дій (окрім технічних лімітів). Відповідно, як результат, не було виявлено прямих нормативних або договірних заборон на збір і обробку часових міток онлайн-активності, тому подібні дії є правомірними.

- Розробка моделі алгоритмічної основи збору міток OSI, на основі якої було реалізовано програмний прототип для автоматизованого моніторингу, дозволила підтвердити т.з. «Proof of Concept» надмірної доступності офіційного Telegram API.

Відповідно, для наглядного та повноцінного розуміння можливих ризиків витоку чутливої інформації, було представлено BPMN-діаграму, яка схематично моделює узагальнену методику оцінки цифрової активності користувачів Telegram.

- Зібравши дані про «онлайн/офлайн» близько 100 користувачів Telegram за часовий проміжок в півтора місяця (це понад 265 тис. сесій), було встановлено, що отримана інформація про часову активність розкриває конфіденційні поведінкові характеристики користувачів та їхні періоди вразливості. Завдяки застосуванню методів статистичної візуалізації (хронограми активності) визначено можливість:
  - Класифікації користувачів за профілем використання Telegram, згідно якої стиль «Часто-Довго» може вказувати на ознаки залежності від соцмереж.
  - Використання методики оцінки часової активності з метою вивчення поведінкових характеристик об’єкта дослідження на етапах підготовки (контекстуалізації та персоналізації) сценаріїв атак соціальної інженерії.

- На основі отриманих результатів було сформовано практичні рекомендації для користувачів та розробників Telegram з метою мінімізації виявлених ризиків ІБ:
  - Для всіх активних користувачів головною рекомендацією є обмеження видимості їхньої «Останньої активності» через опцію «Мої контакти».
  - Для розробників Telegram надано рекомендації щодо: видалення API-викликів, які дають змогу отримати OSI; забезпечення видимості онлайн-статусу за замовчуванням лише для контактів користувача; відмови від концепції взаємного приховування, а також чіткого інформування про наслідки для конфіденційності поруч із відповідними налаштуваннями.

Отримані результати та надані рекомендації мають безпосереднє практичне значення для підвищення рівня обізнаності громадян України в ризиках ІБ, які виникають на основі оцінки їхньої часової активності в месенджері Telegram.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

[1] Andreas Buchenscheit, Bastian Könings, Andreas Neubert, Florian Schaub, Matthias Schneider, and Frank Kargl: «Privacy implications of presence sharing in mobile messaging applications». In MUM, 2014.
[Електронний ресурс] – URL-адреса:
https://www.uni-ulm.de/fileadmin/website_uni_ulm/iui.inst.100/institut/Papers/Prof_Weber/2014-MUM-whatsapp-privacy.pdf

[2] Bonnie A Nardi, Steve Whittaker, and Erin Bradner: «Interaction and outeraction: Instant messaging in action». In CSCW, 2000.
[Електронний ресурс] – URL-адреса:
https://dl.acm.org/doi/pdf/10.1145/358916.358975

[3] Daniel Avrahami and Scott E. Hudson: «Responsiveness in instant messaging: Predictive models supporting inter personal communication». In CHI, 2006.
[Електронний ресурс] – URL-адреса:
https://nl.ijs.si/janes/wp-content/uploads/2014/09/avrahamihudson06b.pdf

[4] Edward S. De Guzman, Margaret Yau, Anthony Gagliano, Austin Park, and Anind K. Dey: «Exploring the design and use of peripheral displays of awareness information». In CHI EA, 2004.
[Електронний ресурс] – URL-адреса:
https://dl.acm.org/doi/pdf/10.1145/985921.986035

[5] James "Bo" Begole, Nicholas E. Matsakis, and John C. Tang. Lilsys: «Sensing unavailability». In Proceedings of the 2004 ACM Conference on CSCW’04, 2004.
[Електронний ресурс] – URL-адреса:
https://dl.acm.org/doi/pdf/10.1145/1031607.1031691

[6] Eric Horvitz, Paul Koch, Carl Myers Kadie, and Andy Jacobs: «Coordinates: Probabilistic forecasting of presence and availability». CoRR, abs/1301.0573, 2013.
[Електронний ресурс] – URL-адреса:
https://arxiv.org/pdf/1301.0573

[7] Michael S. Bernstein, Eytan Bakshy, Moira Burke, and Brian Karrer. Quantifying the invisible audience in social networks: «In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems». In CHI’13, 2013.
[Електронний ресурс] – URL-адреса:
https://thoughtcrumbs.com/publications/chi2013_audience_size.pdf

[8] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub: «Keeping a low profile?: Technology, risk and privacy among undocumented immigrants». In CHI, 2018
[Електронний ресурс] – URL-адреса:
https://amcdon.com/papers/lowprofile-chi18.pdf

[9] Буковинський державний медичний університет (БДМУ): «Взаємозв'язок циркадних ритмів та психічного стану людини». In UDC, 2022. [Електронний ресурс] – URL-адреса: https://www.docsity.com/ru/docs/vzayemozv-yazok-cirkadnih-ritmiv-ta-psihichnogo-stanu-lyudini/9743229/

[10] Jeffrey C. Hall, Michael Rosbash, and Michael W. Young in the 2017 Nobel Prize in Physiology or Medicine: «Molecular mechanisms controlling the circadian rhythm» [Електронний ресурс] – URL-адреса: https://www.nobelprize.org/prizes/medicine/2017/press-release/

[11] SportLife: «Циркадні ритми: як працюють і чому віж них залежить ваш сон». [Електронний ресурс] – URL-адреса: https://sportlife.ua/uk/blog/news/tsirkadnie-ritmi/

[12] Cheng Zhang, Chee Wei Phang, Xiaohua Zeng, Ximeng Wang, Yunjie Xu, and Yun Huang: «Circadian Rhythms in Socializing Propensity». In PLoS ONE, 2015 [Електронний ресурс] – URL-адреса: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0136325

[13] Pablo Valdez: «Circadian Rhythms in Attention». In YJBM, 2019 [Електронний ресурс] – URL-адреса: https://pmc.ncbi.nlm.nih.gov/articles/PMC6430172/

[14] Rosana Montañez, Edward Golob, and Shouhuai Xu1: «Human Cognition Through the Lens of Social Engineering Cyberattacks». In Frontiers, 2020. [Електронний ресурс] – URL-адреса: https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2020.01755/full

[15] Alex: «Graphing when your Facebook friends are awake». Blog in Tumblr, 2016. [Електронний ресурс] – URL-адреса: https://defaultnamehere.tumblr.com/post/139351766005/graphing-when-your-facebook-friends-are-awake

[16] Alex: «Graphing when your Facebook friends are awake». Speech on PyConf, 2016. [Електронний ресурс] – URL-адреса: https://www.youtube.com/watch?v=MkSkqMvGBuo

[17] Louisa Stockley: «How a WhatsApp status loophole is aiding cyberstalkers». Blog in Traced (Trustd MTD), 2021. [Електронний ресурс] – URL-адреса: https://traced.app/2021/04/13/whatsapp-status-loophole-is-aiding-cyberstalkers/

[18] Web-Source Ltd: «LastSeen on Telegram. Data Safety». In Play Store from 2021. [Електронний ресурс] – URL-адреса: https://play.google.com/store/apps/datasafety?id=telegram.family.tracker.app

[19] Morgan Meaker, Margi Murphy, and Io Dodds: «WhatsApp records allow stalkers to track you online». In The Telegraph from 2021.
[Електронний ресурс] – URL-адреса:
https://www.telegraph.co.uk/technology/2021/04/16/robinhood-hit-claims-restricting-dogecoin-amid-rally-live/

[20] Camille Cobb, Lucy Simko, Tadayoshi Kohno, and Alexis Hiniker: «A Privacy-Focused Systematic Analysis of Online Status Indicators». In Sciendo, 2020.
[Електронний ресурс] – URL-адреса:
https://petsymposium.org/popets/2020/popets-2020-0057.pdf

[21] Universal Declaration of Human Rights, Article 12.
[Електронний ресурс] – URL-адреса:
https://www.un.org/about-us/universal-declaration-of-human-rights

[22] Європейська конвенція з прав людини, СТАТТЯ 8.
[Електронний ресурс] – URL-адреса:
https://www.echr.coe.int/documents/d/echr/convention_ukr

[23] GDPR, Personal Data.
[Електронний ресурс] – URL-адреса:
https://gdpr-info.eu/issues/personal-data/

[24] LigaZakon: Науково-практичний коментар до ст. 182 ККУ
[Електронний ресурс] – URL-адреса:
https://ips.ligazakon.net/document/KK004687

[25] Дрижакова Д.Ю. та Волинець Р.А.: «Використання відкритих джерел інформації (OSINT) у сфері безпеки держави: технології та перспективи». На конференції «Цифрове наукове суспільство…», 2024.
[Електронний ресурс] – URL-адреса:
https://archives.mcnd.org.ua/index.php/conference-proceeding/article/view/599/601

[26] Camille Cobb, Lucy Simko, Tadayoshi Kohno, and Alexis Hiniker: «User Experiences with Online Status Indicators». In CHI, 2020.
[Електронний ресурс] – URL-адреса:
https://dl.acm.org/doi/pdf/10.1145/3313831.3376240

[27] Trinh Minh Tri Do, Jan Blom, and Daniel Gatica-Perez: «Smartphone usage in the wild: A large-scale analysis of ap plications and context». In ICMI, 2011.
[Електронний ресурс] – URL-адреса:
https://dl.acm.org/doi/pdf/10.1145/2070481.2070550

[28] Matthias Böhmer, Brent Hecht, Johannes Schöning, Antonio Krüger, and Gernot Bauer: «Falling asleep with Angry Birds, Facebook and Kindle: A large scale study on mobile application usage». In MobileHCI, 2011.
[Електронний ресурс] – URL-адреса:
https://dl.acm.org/doi/pdf/10.1145/2037373.2037383

[29] Lorenzo Franceschi-Bicchierai: «You Can’t Hide Whether You Are Online on WhatsApp – And That’s a Problem». In VICE, 2021.
[Електронний ресурс] – URL-адреса:
https://www.vice.com/en/article/you-cant-hide-whether-you-are-online-on-whatsappand-thats-a-problem/

[30] ЧаПи Telegram: «Хто може бачити, що я “в мережі”?»
[Електронний ресурс] – URL-адреса:
https://telegram.org/faq#hto-mozhe-bachiti-scho-ya-v-merezh

[31] ЧаПи Telegram: «Чи можу я приховати час останньої активності?»
[Електронний ресурс] – URL-адреса:
https://telegram.org/faq?setln=uk#chi-mozhu-ya-prihovati-chas-ostanno-aktivnost

[32] Damien Van Puyvelde and Fernando Tabárez Rienzi: «The rise of open-source intelligence». Published online by Cambridge University Press in 2025.
[Електронний ресурс] – URL-адреса:
https://www.cambridge.org/core/journals/european-journal-of-international-security/article/rise-of-opensource-intelligence/21122432399ECB8078BF0D89A76D0586

[33] Bellingcat with Alexey Navalny: «“If it Hadn't Been for the Prompt Work of the Medics”: FSB Officer Inadvertently Confesses Murder Plot to Navalny». In 2020.
[Електронний ресурс] – URL-адреса:
https://www.bellingcat.com/news/uk-and-europe/2020/12/21/if-it-hadnt-been-for-the-prompt-work-of-the-medics-fsb-officer-inadvertently-confesses-murder-plot-to-navalny/

[34] Maxym Zosym: «Розвідка з відкритих джерел (OSINT)». Блог, 2023.
[Електронний ресурс] – URL-адреса:
https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel-osint/

[35] OSINT-бджоли: «Що таке OSINT розвідка?». Блог, 2024
[Електронний ресурс] – URL-адреса:
https://osintbees.com/osint-rozvidka/

[36] OsintFlow ➕: «Аналітика аудиторії каналів месенджера MAX». Допис, 2025.
[Електронний ресурс] – URL-адреса:
https://t.me/osintflow/15502

[37] CEE Multi-Country News Center:
«How technology helped Ukraine resist during wartime». In Microsoft from 2023.
[Електронний ресурс] – URL-адреса:
https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/

[38] Назар Сахній та Леонід Гальчинський: «ЯК ОНЛАЙН-СТАТУС ДОЗВОЛЯЄ РОЗКРИТИ ПРИВАТНІ ДАНІ КОРИСТУВАЧІВ TELEGRAM». From ΛΟΓΟС, in IX International Scientific and Practical Conference: «EDUCATION AND SCIENCE OF TODAY: INTERSECTORAL ISSUES AND DEVELOPMENT OF SCIENCES» (p. 176-185), (November 28, 2025; Cambridge, UK).
[Електронний ресурс] – URL-адреса:
https://archive.logos-science.com/index.php/conference-proceedings/issue/view/42/42

[39] Антон Тихоплав та Леонід Гальчинський: «РОЗПІЗНАВАННЯ ФЕЙКОВИХ НОВИН ШЛЯХОМ МОНІТОРИНГУ НОВИННИХ КАНАЛІВ З ЗАСТОСУВАННЯ КОНТЕКСТНОГО АНАЛІЗУ ПРИРОДНОЇ МОВИ ТА СЕМАНТИЧНИХ МЕТОДІВ». From Collection of Scientific Papers «SCIENTIA» (p. 167–172), (December 8, 2023; Antwerp, Belgium).
[Електронний ресурс] – URL-адреса:
https://previous.scientia.report/index.php/archive/article/view/1434

[40] «Популярні месенджери для спілкування - топ в Україні», 2025.
[Електронний ресурс] – URL-адреса:
https://sitecat.net/review/top-10-popular-messengers/

[41] «OSINT on Telegram: Find Phone Numbers, Emails and User Details», 2025.
[Електронний ресурс] – URL-адреса:
https://www.osint.industries/post/osint-on-telegram-find-phone-numbers-emails-and-user-details

[42] Ольга Снопок (ОПОРА Tech): «Telegram, YouTube чи TikTok: звідки українці дізнаються новини». На замовлення видання “Українська правда”, 2024.
[Електронний ресурс] – URL-адреса:
https://www.oporaua.org/polit_ad/telegram-youtube-chi-tiktok-zvidki-ukrayinci-diznayut-sya-novini-25308

[43] Signal Community: «Optional “Online” / “Last seen” indicator», 2018-2025.
[Електронний ресурс] – URL-адреса:
https://community.signalusers.org/t/optional-online-last-seen-indicator/4375/

[44] Digital 2023: «The state of digital in Ukraine in 2023».
[Електронний ресурс] – URL-адреса:
https://datareportal.com/reports/digital-2023-ukraine

[45] Twitter (X) Strategic OSINT Techniques», 2025
[Електронний ресурс] – URL-адреса:
https://hackers-arise.com/twitter-x-strategic-osint-techniques/

[46] Вікіпедія: «Telegram».
[Електронний ресурс] – URL-адреса:
https://uk.wikipedia.org/wiki/Telegram

[47] Pavel Durov: «User engagement is also rising». Допис, 2025. [Електронний ресурс] – URL-адреса: https://t.me/durov/404

[48] DemandSage: «Telegram Users Statistics 2025». Звіт, 2025. [Електронний ресурс] – URL-адреса: https://www.demandsage.com/telegram-statistics/

[49] InMind (Research & Consulting): «Ставлення населення до медіа та споживання різних типів медіа 2021». Опитування Internews щодо споживання медіа, 2025. [Електронний ресурс] – URL-адреса: https://imi.org.ua/upload/media/2021/11/17/61951144dc1fc-usaid-internews-media-report-2021-ukr.pdf

[50] Ольга Снопок та Анастасія Романюк: «ДОСЛІДЖЕННЯ. Медіаспоживання українців: третій рік повномасштабної війни». ОПОРА+USAID, 2024. [Електронний ресурс] – URL-адреса: https://oporaua.org/viyna/doslidzhennya-mediaspozhivannya-ukrayinciv-tretiy-rik-povnomasshtabnoyi-viyni-25292

[51] Валентина Запорожець та Іван Опірський: «НЕБЕЗПЕКА ВИКОРИСТАННЯ TELEGRAM ТА ЙОГО ВПЛИВ НА УКРАЇНСЬКЕ СУСПІЛЬСТВО». Із елек. фаховому виданні «Кібербезпека: освіта, наука, техніка»: Том 1 №25, 2024. [Електронний ресурс] – URL-адреса: https://csecurity.kubg.edu.ua/index.php/journal/article/view/648

[52] Telethon's Documentation: «TelegramClient». [Електронний ресурс] – URL-адреса: https://docs.telethon.dev/en/stable/modules/client.html

[53] Telethon's Documentation: «Client Reference (Friendly Methods)». [Електронний ресурс] – URL-адреса: https://docs.telethon.dev/en/stable/quick-references/client-reference.html#client-ref

[54] Telethon's Documentation: «Update Events (UserUpdate: UserStatus)». [Електронний ресурс] – URL-адреса: https://docs.telethon.dev/en/stable/modules/events.html#telethon.events.userupdate.UserUpdate

[55] Telethon's Documentation: «Entities». [Електронний ресурс] – URL-адреса: https://docs.telethon.dev/en/stable/concepts/entities.html

[56] About Telegram APIs: «Error handling». [Електронний ресурс] – URL-адреса: https://core.telegram.org/api/errors

[57] https://link.springer.com/chapter/10.1007/978-3-030-13848-6_2

[58] Вікіпедія: «Telegram». [Електронний ресурс] – URL-адреса: https://ru.wikipedia.org/wiki/%D0%A5%D1%80%D0%BE%D0%BD%D0%BE%D1%82%D0%B8%D0%BF

Додаток А

Програмний прототип «TOSpy»

```
import asyncio
from dataclasses import dataclass
from datetime import datetime, timezone
from typing import Dict, Optional, Union

from telethon import TelegramClient, events, types

# TODO: підставити свої значення
API_ID = 12345
API_HASH = "0123456789abcdef0123456789abcdef"
SESSION_NAME = "tg_connect"

client = TelegramClient(SESSION_NAME, API_ID, API_HASH)

# Якщо set() порожній, то моніторинг усіх, інакше лише цих ID
WATCH_USER_IDS = {}

# Параметри анти-лінгер перевірки
PROBE_AFTER_S = 60.0          # коли вперше «пропінгувати» після ONLINE
PROBE_INTERVAL_S = 120.0      # інтервал між наступними перевірками


@dataclass
class SessionState:
    alias: Optional[str] = None
    online: bool = False
    start_utc: Optional[datetime] = None
    close_task: Optional[asyncio.Task] = None
    probe_task: Optional[asyncio.Task] = None

sessions: Dict[int, SessionState] = {}


def log_line(msg: str) -> None:
    ts = datetime.now().strftime("%Y-%m-%d %H:%M:%S")
    print(f"[{ts}] {msg}")


def _normalize_to_utc_datetime(val: Optional[Union[int, float, datetime]]) ->
datetime:
    """Телеграм може віддати timestamp або нормалізуємо datetime до UTC."""
    if val is None:
        return datetime.now(timezone.utc)
    if isinstance(val, (int, float)):
        return datetime.fromtimestamp(val, tz=timezone.utc)
    if val.tzinfo is None:
        return val.replace(tzinfo=timezone.utc)
    return val.astimezone(timezone.utc)


async def _close_session(user_id: int, stop_utc: Optional[datetime] = None) ->
None:
    """Закрити поточну сесію користувача, та записати її в CSV-файл."""
    st = sessions.setdefault(user_id, SessionState())
    if not st.online or st.start_utc is None:
        return
```

```
    st.online = False
    stop_utc = stop_utc or datetime.now(timezone.utc)
    duration = (stop_utc - st.start_utc).total_seconds()

    alias = st.alias or str(user_id)
    log_line(
        f"🔒 {alias} ({user_id}) OFFLINE; "
        f"start={st.start_utc.astimezone(timezone.utc)}, "
        f"stop={stop_utc}, dur_s={int(duration)}"
    )

    # простий CSV-лог: user_id,username,start,stop,duration_seconds
    local_start = st.start_utc.astimezone().strftime("%Y-%m-%d %H:%M:%S")
    local_stop = stop_utc.astimezone().strftime("%Y-%m-%d %H:%M:%S")
    line = f"{user_id},{alias},{local_start},{local_stop},{int(duration)}\n"
    with open("sessions.csv", "a", encoding="utf-8") as f:
        f.write(line)

    # скасовуємо таймери
    if st.close_task and not st.close_task.done():
        st.close_task.cancel()
    if st.probe_task and not st.probe_task.done():
        st.probe_task.cancel()
    st.close_task = None
    st.probe_task = None
    st.start_utc = None


async def _schedule_close(user_id: int,
                          expires_val: Optional[Union[int, float, datetime]]) ->
None:
    """Автозакриття сесії на основі поля expires з UserStatusOnline."""
    st = sessions.setdefault(user_id, SessionState())

    # скасувати попередній таймер автозакриття
    if st.close_task and not st.close_task.done():
        st.close_task.cancel()
        st.close_task = None

    if not expires_val:
        return

    expires_utc = _normalize_to_utc_datetime(expires_val)
    now_utc = datetime.now(timezone.utc)
    delay = (expires_utc - now_utc).total_seconds()
    delay = max(0.0, delay + 2.0)  # невеликий запас

    async def _closer():
        try:
            await asyncio.sleep(delay)
            # якщо досі ONLINE, то закриваємо сесію
            if st.online:
                await _close_session(user_id, stop_utc=expires_utc)
        except asyncio.CancelledError:
            raise
        except Exception as e:
            log_line(f"close loop error for {user_id}: {e}")

    st.close_task = asyncio.create_task(_closer())
```

```
async def _schedule_probe(user_id: int) -> None:
    """Анти-лінгер перевірка: перша через PROBE_AFTER_S, далі кожні
PROBE_INTERVAL_S,
    доки сесія online. Якщо get_entity показує, що користувач вже не online —
закриваємо.
    """
    st = sessions.setdefault(user_id, SessionState())

    if st.probe_task and not st.probe_task.done():
        st.probe_task.cancel()
        st.probe_task = None

    async def _prober():
        try:
            await asyncio.sleep(max(0.0, PROBE_AFTER_S))
            while True:
                if not st.online:
                    return
                try:
                    ent = await client.get_entity(user_id)
                except Exception as e:
                    # при мережевих/рейтових збоях просто перенесемо перевірку
                    log_line(f"probe get_entity error for {user_id}: {e}")
                    await asyncio.sleep(PROBE_INTERVAL_S)
                    continue

                status = getattr(ent, "status", None)

                if isinstance(status, types.UserStatusOffline):
                    stop_dt = _normalize_to_utc_datetime(
                        getattr(status, "was_online", None)
                    )
                    await _close_session(user_id, stop_utc=stop_dt)
                    return
                elif isinstance(status, types.UserStatusOnline):
                    # продовжуємо процес, оновлючи таймер автозакриття сесії
                    await _schedule_close(user_id, getattr(status, "expires",
None))
                    await asyncio.sleep(PROBE_INTERVAL_S)
                else:
                    # Recently/LastWeek/Empty — вважаємо, що можна закривати
                    await _close_session(user_id,
stop_utc=datetime.now(timezone.utc))
                    return
        except asyncio.CancelledError:
            raise
        except Exception as e:
            log_line(f"probe loop error for {user_id}: {e}")

    st.probe_task = asyncio.create_task(_prober())


async def _open_or_refresh_online(
    user_id: int,
    alias: Optional[str],
    expires_val: Optional[Union[int, float, datetime]],
) -> None:
    """Твоя робоча логіка відкриття/оновлення ONLINE-сесії."""
    st = sessions.setdefault(user_id, SessionState())
    st.alias = alias or st.alias
    now_utc = datetime.now(timezone.utc)
```

```
    if not st.online:
        st.online = True
        st.start_utc = now_utc
        log_line(
            f"✅ {st.alias or user_id} ({user_id}) ONLINE; "
            f"start={now_utc.astimezone().strftime('%Y-%m-%d %H:%M:%S')}"
        )

    await _schedule_close(user_id, expires_val)
    await _schedule_probe(user_id)


@client.on(events.UserUpdate)
async def user_update_handler(event: events.UserUpdate.Event) -> None:
    uid = event.user_id

    if WATCH_USER_IDS and uid not in WATCH_USER_IDS:
        return

    try:
        user = await event.get_user()
    except Exception as e:
        log_line(f"get_user error for {uid}: {e}")
        user = None

    username_or_fullname: Optional[str] = None
    if user is not None:
        username = getattr(user, "username", None)

        first = getattr(user, "first_name", None) or ""
        last = getattr(user, "last_name", None) or ""
        fullname = (first + " " + last).strip() or None

        # пріоритет: username -> full name -> None
        username_or_fullname = username or fullname

    status = event.status

    if isinstance(status, types.UserStatusOnline):
        await _open_or_refresh_online(
            uid,
            username_or_fullname,
            getattr(status, "expires", None),
        )
    elif isinstance(status, types.UserStatusOffline):
        stop_dt = _normalize_to_utc_datetime(getattr(status, "was_online", None))
        await _close_session(uid, stop_utc=stop_dt)
    else:
        await _close_session(uid, stop_utc=datetime.now(timezone.utc))


def main() -> None:
    log_line("Starting Telegram OSI monitor...")
    with client:
        # тут відпрацьовує стандартна схема: номер телефону → код → пароль
        client.loop.run_until_complete(client.run_until_disconnected())


if __name__ == "__main__":
    main()
```