# Звіт за результатами комплексного розвідувального заходу

Встановлення особи фігуранта, атрибуція учасників пов'язаного угруповання та документування їх протиправної діяльності.

**17.12.2025 — 29.12.2025**

# Інцидент

17 грудня 2025 року до нас звернувся клієнт із проханням провести розслідування щодо особи, яка здійснювала погрози та використовувала його персональні дані для психологічного тиску.

Зі слів клієнта, він розмістив оголошення про продаж свого облікового запису в мобільній грі PUBG в одному з Telegram-чатів. Приблизно через 20 хвилин після публікації оголошення з ним зв'язався невідомий користувач із повідомленням:

«Привіт, можеш надіслати огляд акаунта?»

Після перевірки облікового запису співрозмовник перейшов до обговорення умов купівлі. Клієнт запропонував провести угоду через гаранта[1], однак у відповідь невідома особа надіслала йому персональні дані та висунула погрозу:

«Йдемо без гарантів, або я замовляю тобі холодильник за 1 300 000 рублів з оплатою при отриманні».

Після цього зловмисник надіслав додатковий обсяг персональних даних клієнта та продемонстрував процес оформлення фіктивних замовлень на його адресу. Серед них були побутова техніка високої вартості та інші товари, оформлені з післяплатою.

Також невідома особа заявила про намір здійснити так званий «сватинг» — подати від імені клієнта неправдиве повідомлення до правоохоронних органів. Для підтвердження своїх намірів зловмисник надіслав скриншот форми звернення до правоохоронних органів, заповненої від імені клієнта, із завідомо неправдивим повідомленням про тяжкий злочин.

З огляду на характер погроз, використання персональних даних та можливість подальшої ескалації ситуації, було прийнято рішення про проведення комплексного розслідування з метою встановлення особи причетного та документування його діяльності.

[1] Гарант — незалежний посередник між продавцем та покупцем, який забезпечує безпечне проведення угоди. Під час такої угоди гарант тимчасово утримує кошти покупця та переказує їх продавцю лише після підтвердження виконання сторонами своїх зобов'язань.

# Цілі розслідування

Після первинного аналізу інциденту було визначено перелік цілей, необхідних для встановлення особи причетного, документування його діяльності та підготовки матеріалів для подальшого реагування.

1. Встановити особу представника доксинг[2]-спільноти, причетного до погроз та використання персональних даних клієнта.
2. Провести атрибуцію пов'язаних облікових записів, цифрових слідів та контактів фігуранта.
3. Зібрати та систематизувати доказову базу щодо зафіксованих протиправних дій.
4. Встановити законних представників фігуранта та проінформувати їх про його діяльність у інтернеті.
5. Передати зібрані матеріали до правоохоронних органів для подальшої правової оцінки та реагування.

# Команда розслідування

**Маверік —**
Незалежний OSINT-аналітик, керівник розслідування

**Функції в межах розслідування:**

- Планування та координація розвідувальних заходів;
- Проведення OSINT, SOCMINT та HUMINT-аналізу;
- Атрибуція особи фігуранта та пов'язаних облікових записів;
- Збір, верифікація та документування доказової бази; підготовка підсумкового звіту.

Усі етапи розслідування, описані в цьому звіті, були виконані автором самостійно. Окремі дії, пов'язані з передачею матеріалів до правоохоронних органів, виконувалися іншими особами.

[2] Доксинг (doxxing) — збір, пошук та публікація персональних даних особи без її згоди. До таких даних можуть належати ім'я, адреса проживання, номер телефону, дані родичів, місце навчання чи роботи, а також інша конфіденційна інформація.

# Вихідні дані

На момент початку розслідування у розпорядженні команди були наявні такі відомості щодо невстановленої особи:

1. Telegram-акаунт, з якого здійснювалися погрози на адресу клієнта;
2. Історія листування між клієнтом та фігурантом;
3. Матеріали, надіслані фігурантом під час спілкування (скриншоти, відеозаписи, повідомлення);
4. Інформація про використання фігурантом персональних даних клієнта для здійснення психологічного тиску.

Подальші розвідувальні заходи проводилися на основі зазначених вихідних даних.

# Умовні позначення та захист персональних даних

З метою недопущення розкриття персональних даних фігуранта та пов'язаних осіб у звіті використано умовні позначення та псевдоніми.

У подальшому тексті звіту фігурант позначатиметься псевдонімом «Петро». Окремі персональні дані, номери телефонів, адреси, ідентифікатори облікових записів та інша інформація можуть бути частково приховані або змінені без впливу на зміст та результати розслідування.

# OSINT: Комплексний аналіз Telegram-акаунта

Першим етапом розслідування став аналіз Telegram-акаунта, з якого здійснювалися погрози на адресу клієнта.

На момент початку розслідування акаунт використовував username @b*******a та Telegram ID 8********5. Первинний аналіз профілю не дозволив безпосередньо встановити особу власника, однак надав низку цифрових артефактів для подальшого дослідження.

У ході аналізу було встановлено, що акаунт неодноразово змінював username та відображувані імена. Серед виявлених псевдонімів були @vk******, @m*******v, @h******3 та інші. Частина з них надалі використовувалася для пошуку цифрового сліду фігуранта в Telegram та інших сервісах.

Також було встановлено номер телефону, раніше пов'язаний з іншими акаунтами. Аналіз цифрового сліду показав, що номер належить до російського номерного ресурсу та фігурує в окремих телефонних книгах під ім'ям «Петро». На момент виявлення ця інформація розглядалася лише як гіпотеза та була зафіксована для подальшої перевірки в межах розслідування.

Подальший аналіз історичних даних Telegram виявив наявність додаткових акаунтів, пов'язаних із досліджуваним профілем. Це дозволило розширити перелік досліджуваних об'єктів та отримати додаткові точки для атрибуції особи.

Окрему увагу було приділено аналізу активності фігуранта в Telegram-спільнотах. Встановлено, що досліджуваний акаунт та пов'язані з ним профілі брали участь у чатах, присвячених мобільним іграм PUBG Mobile та Standoff 2. У зазначених спільнотах фігурант розміщував повідомлення щодо купівлі, продажу та обміну ігрових акаунтів і внутрішньоігрових предметів.

Крім того, було виявлено зв'язки з низкою Telegram-каналів та спільнот, пов'язаних із діяльністю представників доксинг-середовища. Аналіз цих зв'язків дозволив сформувати початкове уявлення про коло спілкування фігуранта та його можливу належність до відповідних інтернет-угруповань.

# Результати етапу

За результатами комплексного аналізу первинного Telegram-акаунта було встановлено:

- Telegram ID фігуранта: 8********5;
- Основний username на момент початку розслідування: @b*******a;
- Номер телефону, прив'язаний до акаунта, належав до російського номерного ресурсу;
- Виявлено декілька історичних username та псевдонімів, що використовувалися фігурантом у різний час;
- Встановлено наявність двох додаткових Telegram-акаунтів, пов'язаних з фігурантом;
- Виявлено активність у спільнотах, присвячених PUBG Mobile та Standoff 2;
- Встановлено зв'язки з Telegram-каналами та користувачами, пов'язаними з доксинг-середовищем;
- Отримано перший можливий ідентифікатор особи фігуранта — ім'я «Петро», виявлене під час аналізу цифрового сліду телефонного номера.

За підсумками етапу було сформовано такі робочі гіпотези:

| Гіпотеза 1 | Гіпотеза 2 |
|---|---|
| Фігурант є громадянином рф або постійно проживає на її території. | Фігурант активно використовує декілька Telegram-акаунтів для розмежування своєї діяльності та ускладнення атрибуції. |
| **Гіпотеза 3** | **Гіпотеза 4** |
| Основне коло інтересів та комунікації фігуранта пов'язане з ігровими спільнотами PUBG Mobile та Standoff 2. | Фігурант має зв'язки з представниками доксинг-спільнот та може бути інтегрований у відповідне онлайн-середовище. |

Отримані результати стали основою для планування подальших HUMINT-заходів та проведення легендованої взаємодії з фігурантом.

# Соціальна інженерія (18.12–25.12)

## Вступ

Після завершення первинного аналізу Telegram-акаунтів було прийнято рішення провести захід соціальної інженерії.

Метою заходу було отримання додаткових відомостей про фігуранта, його оточення, спосіб життя, цифрову активність та можливі зв'язки з іншими учасниками протиправної діяльності.

На відміну від відкритих джерел, соціальна інженерія дозволяє отримувати інформацію безпосередньо від об'єкта дослідження, оцінювати його поведінку, реакції та перевіряти окремі гіпотези в режимі реального часу.

## План заходу

На момент проведення розслідування автор мав власні розвідувальні інструменти, Telegram-ресурси з багатотисячною аудиторією та певний рівень впізнаваності в профільних онлайн-спільнотах.

Попередній аналіз середовища показав, що для багатьох його учасників важливе значення мають статус, авторитет та репутація всередині спільноти. Саме тому основою заходу стало використання вже наявної репутації та професійного бекграунду для швидкого встановлення довірчих відносин із фігурантом.

План передбачав:

- встановлення довірчого контакту;
- інтеграцію в коло спілкування фігуранта;
- отримання доступу до внутрішніх спільнот та каналів комунікації;
- поступове отримання відомостей про особу фігуранта;
- перевірку раніше сформованих гіпотез;
- виявлення інших причетних осіб.

Окрему увагу було приділено вибору моментів для отримання інформації. Більшість відомостей були отримані не шляхом прямих запитань, а через контрольоване ведення діалогу, створення відповідного контексту та використання поведінкових особливостей фігуранта.

*Візуалізація плану заходу соціальної інженерії

# Реалізація

У період з 18 по 25 грудня було встановлено регулярний контакт із фігурантом.

Після формування достатнього рівня довіри вдалося отримати доступ до закритої спільноти, власником та фактичним керівником якої був досліджуваний об'єкт. Також фігурант представився ім'ям «Петро» (псевдонім, використаний у звіті для захисту персональних даних). Зазначене ім'я повністю співпало з відомостями, отриманими під час аналізу номера телефону, пов'язаного з досліджуваним Telegram-акаунтом, на попередньому етапі розслідування. Це стало першим незалежним підтвердженням правильності обраного напряму встановлення особи та суттєво підвищило достовірність раніше отриманих даних.

Подальший аналіз історії повідомлень, структури спільноти та взаємодії її учасників показав, що діяльність групи не обмежувалася окремим інцидентом щодо клієнта. Було встановлено систематичне використання методів доксингу, погроз, психологічного тиску, спроб сватингу та інших дій, спрямованих проти третіх осіб.

Виявлення організованої групи суттєво змінило масштаб розслідування. Якщо початково основною метою було встановлення особи одного фігуранта, то після отримання доступу до спільноти виникла необхідність документування діяльності всієї групи та ідентифікації її учасників.

У зв'язку з цим перелік цілей розслідування було розширено та доповнено завданням зі збору інформації про всіх встановлених учасників угруповання.

# Результати

Захід соціальної інженерії став ключовим етапом усього розслідування та забезпечив отримання більшої частини відомостей, використаних у подальшій атрибуції особи фігуранта.

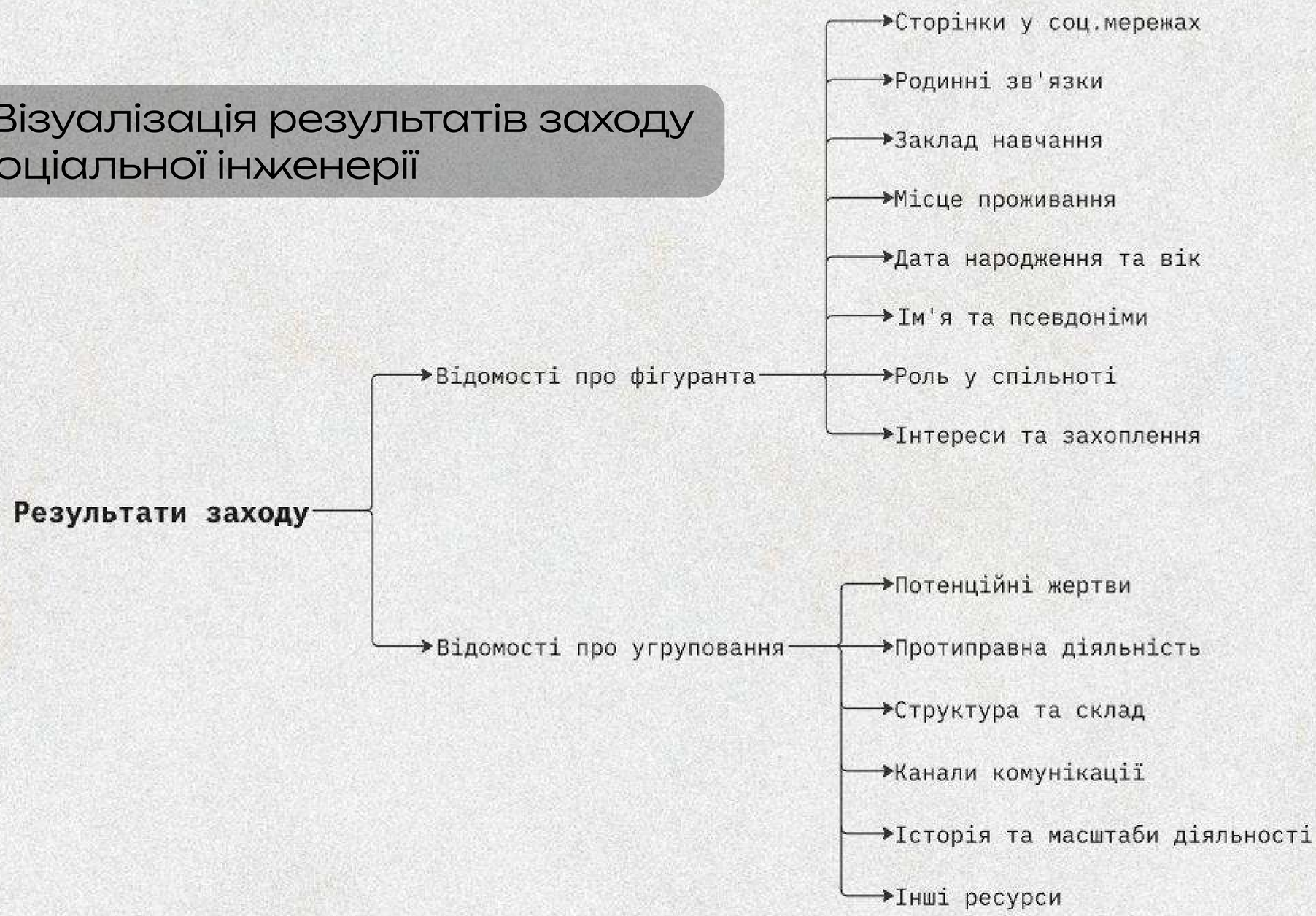
У ході заходу було встановлено та підтверджено:

- ім'я фігуранта: Петро;
- орієнтовний вік;
- дату народження;
- регіон та місто проживання;
- відомості про місце навчання;
- інформацію про членів родини;
- дані про особисте оточення;
- додаткові соціальні мережі та цифрові профілі;
- попередні псевдоніми та історію активності в онлайн-середовищі;
- структуру, склад та внутрішню організацію угруповання;
- роль фігуранта як власника та фактичного координатора діяльності групи.

Крім того, було отримано значний масив допоміжних відомостей, які надалі використовувалися для перевірки окремих гіпотез, пошуку родинних зв'язків, встановлення законних представників фігуранта та збору доказової бази.

Фактично саме результати цього етапу стали основою для всіх подальших заходів розслідування та дозволили перейти від аналізу окремого акаунта до документування діяльності організованої групи осіб.

*Візуалізація результатів заходу соціальної інженерії



# HUMINT: Операція «Замовники»

## Мета заходу

Під час попереднього етапу соціальної інженерії фігурант повідомив, що проживає в місті Митищі Московської області.

Оскільки зазначена інформація була отримана безпосередньо від об'єкта дослідження, виникла необхідність її незалежної перевірки.

Метою заходу стало підтвердження або спростування відомостей щодо місцеперебування фігуранта, а також отримання додаткових технічних індикаторів для подальшого аналізу.

## Планування заходу

Для досягнення поставленої мети було розроблено окремий сценарій взаємодії з фігурантом.

Враховуючи, що під час попереднього етапу між сторонами вже були встановлені довірчі відносини, було вирішено використати цей фактор для створення правдоподібної ситуації, у межах якої фігурант добровільно виконає необхідні дії.

Сценарій передбачав імітацію передачі потенційного «замовлення» від одного клієнта іншому виконавцю. Такий формат взаємодії повністю відповідав звичному середовищу фігуранта та не викликав підозр.

*Візуалізація плавування заходу: Операція “замовники”

# Реалізація

19 грудня фігуранту було запропоновано виконати нібито стороннє замовлення, за яке передбачалася винагорода.

Після отримання згоди фігуранта взаємодія була переведена на окремий контрольований акаунт, що виконував роль замовника.

У межах виконання поставленого завдання фігуранту було передано набір матеріалів для ознайомлення. Під час роботи з ними були зафіксовані технічні індикатори, необхідні для перевірки раніше отриманих відомостей.

Перші результати підтвердили перебування фігуранта на території рф та вказали на місто Митищі як на ймовірне місце його знаходження.

| Дата/час | IP/Провайдер | Країна | Пристрій |
|---|---|---|---|
| 19.12.25<br>19:08:12 | 176.[redacted].[redacted].229<br>NRF SOFTVIDEO Ltd | Russia<br>Mytishchi | Android 15<br>Chrome 143.0 |
| Mozilla/5.0 (Linux; Android 15; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Mobile Safari/537.36 | | | |

Під час подальшої взаємодії було зафіксовано активність ще одного користувача, пов'язаного з виконанням поставленого завдання. Аналіз отриманих даних показав його перебування на території Ізраїлю.

| Дата/час | IP/Провайдер | Країна | Пристрій |
|---|---|---|---|
| 19.12.25<br>19:43:02 | 79.[redacted].[redacted].96<br>Bezeq- THE ISRAEL TELECOMMUNICATION CORP. LTD | Israel<br>Jerusalem | Android 16<br>Chrome 143.0 |
| Mozilla/5.0 (Linux; Android 16; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Mobile Safari/537.36 | | | |

Отримана інформація співпала з відомостями, отриманими раніше під час спілкування з фігурантом, який згадував про одного зі своїх знайомих та учасників угруповання, що проживає в Ізраїлі. Це дало підстави припустити залучення цієї особи до виконання поставленого «замовлення» та дозволило зафіксувати додатковий технічний слід ще одного учасника досліджуваної групи.

Для виключення випадкових збігів через декілька днів було проведено повторну перевірку. Повторний перехід підтвердив раніше отримані результати та засвідчив стабільність зафіксованих даних.

# Результати

За результатами операції «Замовники» було досягнуто основної мети заходу — незалежно перевірено відомості про місцеперебування фігуранта, отримані під час попереднього етапу соціальної інженерії.

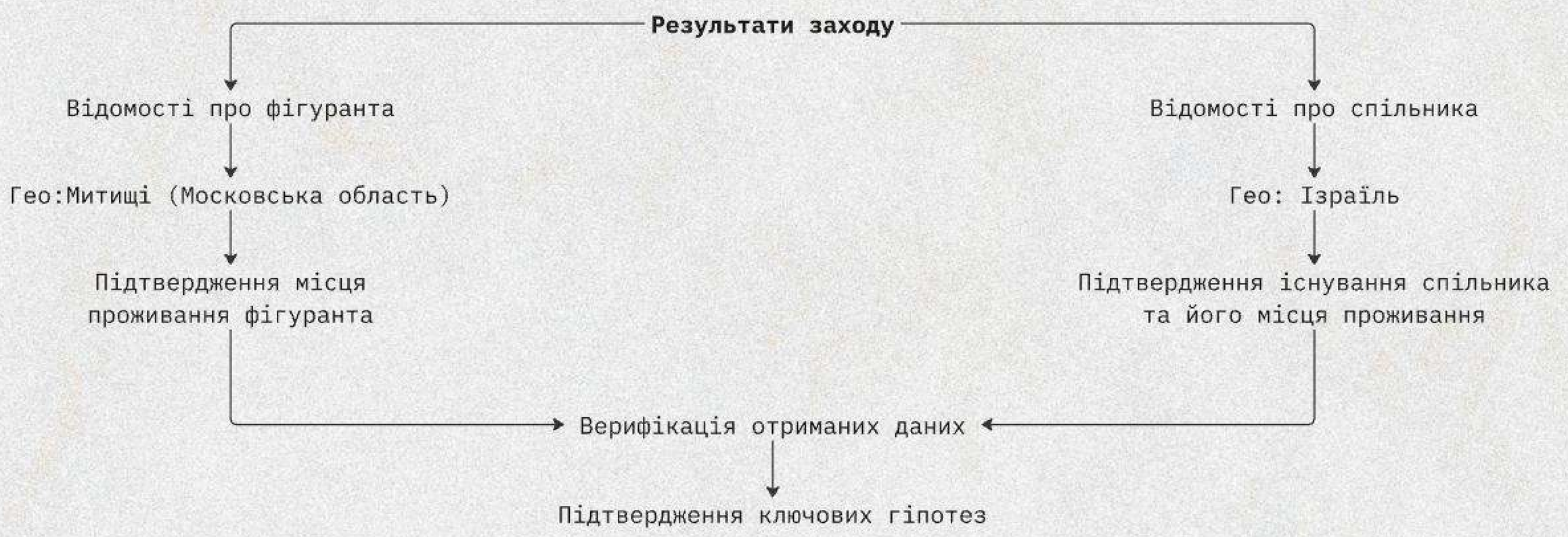
У ході операції було встановлено:

- Фактичне перебування фігуранта в місті Митищі Московської області;
- Відповідність отриманих технічних даних відомостям, які фігурант раніше повідомляв під час спілкування;
- Використання фігурантом пристрою на базі Android для виконання поставленого «замовлення»;
- Наявність щонайменше одного активного спільника, який брав участь у виконанні завдання або мав доступ до переданих матеріалів;
- Перебування зазначеного учасника на території Ізраїлю, що співпало з інформацією, отриманою під час попереднього етапу розслідування.

Окрему цінність становило те, що захід дозволив не лише перевірити раніше отримані відомості щодо основного фігуранта, але й зафіксувати технічний слід іншого учасника досліджуваного угруповання.

Таким чином операція підтвердила достовірність ключових даних, отриманих під час соціальної інженерії, та надала додаткові відомості про структуру, географію та склад досліджуваної групи.

*Візуалізація результатів заходу: Операція “замовники”



# Атрибуція особи

## Вихідні дані

Після завершення попередніх етапів розслідування було сформовано набір відомостей про фігуранта, отриманих незалежними методами збору інформації.

На цей момент було встановлено:

- Ім'я фігуранта («Петро» — псевдонім, використаний у звіті);
- Приблизний вік та дату народження;
- Місто проживання — м. Митищі Московської області;
- Відомості про місце навчання;
- Інформацію про членів родини;
- Додаткові акаунти в соціальних мережах;
- Технічні дані, отримані під час операції «Замовники».

Отримані відомості були достатніми для проведення подальшої атрибуції особи та пошуку збігів у масивах даних.

## Аналіз та пошук збігів

Для встановлення особи фігуранта було проведено зіставлення відомостей, отриманих під час попередніх етапів розслідування.

Основними ідентифікаторами стали:

- Ім'я;
- Дата народження;
- Місто проживання;
- Ймовірний вік
- Відомості про навчальний заклад;
- Дані про родинні зв'язки.

У результаті аналізу було виявлено єдиний профіль, який одночасно відповідав усім встановленим критеріям.

Подальша перевірка показала відсутність суперечностей між знайденими відомостями та даними, отриманими раніше під час заходів соціальної інженерії.

# Результати атрибуції

За результатами аналізу вдалося встановити повні анкетні дані фігуранта, дату та місце народження, адресу реєстрації, контактні відомості та інші ідентифікаційні дані.

Крім того, було встановлено склад найближчого родинного оточення фігуранта, включаючи батьків, молодшу сестру та інших осіб, пов'язаних із ним родинними зв'язками.

Отримані результати дозволили сформувати первинне оперативно-аналітичне досьє на фігуранта та перейти до наступного етапу — незалежної перевірки знайдених відомостей.

Станом на завершення цього етапу особу фігуранта було встановлено з високим ступенем достовірності, однак для виключення ймовірності помилки було прийнято рішення провести додаткову верифікацію отриманих даних.

*Фрагмент досьє, сформованого за результатами атрибуції особи

# Верифікація результатів атрибуції

## Мета етапу

Після завершення атрибуції особи було необхідно незалежно перевірити отримані результати та підтвердити цифровий зв'язок між встановленою особою та Telegram-акаунтом, який використовувався під час вчинення протиправних дій щодо клієнта.

Основною метою етапу стало виключення ймовірності помилки під час атрибуції та отримання додаткових доказів належності досліджуваного акаунта встановленому фігуранту.

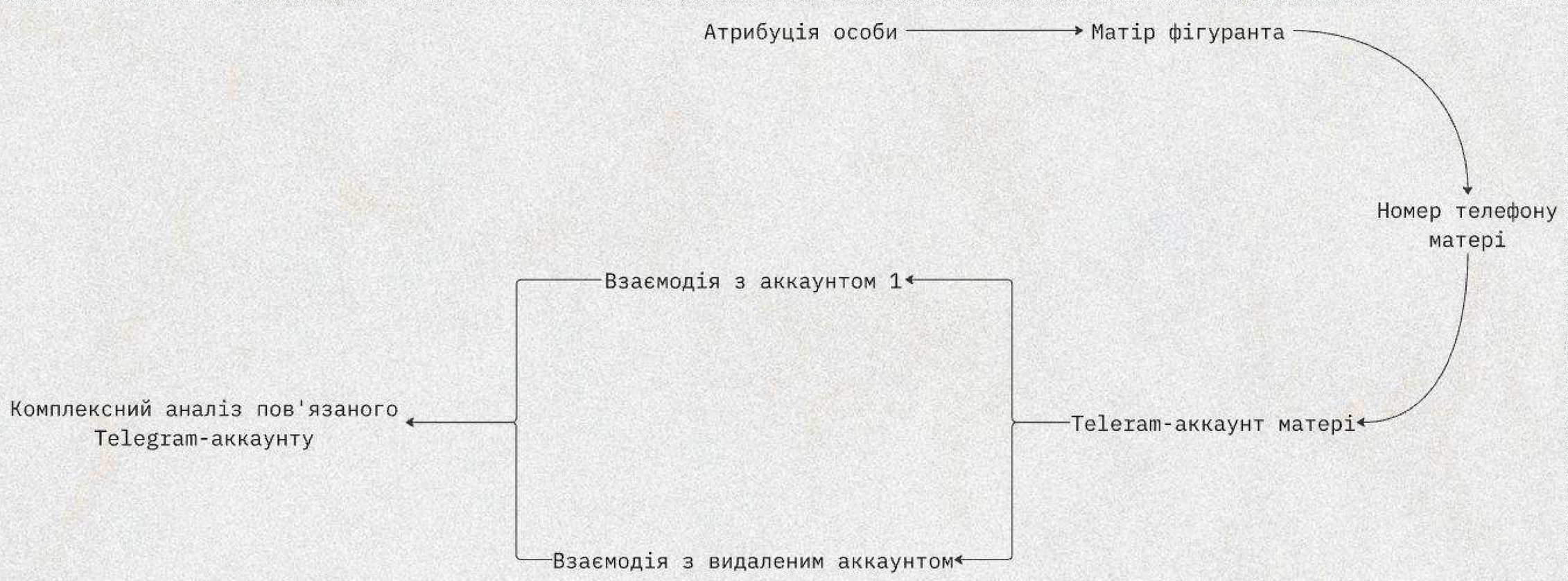
## Аналіз цифрових зв'язків

У межах перевірки було проведено аналіз цифрового оточення членів родини фігуранта.

Через номер телефону матері вдалося встановити її Telegram-акаунт. Аналіз профілю показав наявність взаємодій із декількома пов'язаними акаунтами, серед яких окрему увагу привернув видалений Telegram-профіль.

Подальший аналіз цифрового сліду цього акаунта дозволив отримати відомості про його попередню активність, історію змін псевдонімів та участь у різних Telegram-спільнотах.

*Візуалізація аналізу цифрових слідів



# Виявлені збіги

Під час аналізу було встановлено декілька незалежних збігів із відомостями, отриманими на попередніх етапах розслідування.

Серед історичних псевдонімів акаунта були виявлені варіації ніка «Фігуров», використання якого фігурант раніше особисто підтвердив під час заходу соціальної інженерії.

Крім того, серед історії назв профілю були зафіксовані поєднання псевдонімів, які використовувалися досліджуваним Telegram-акаунтом під час розслідування, а також реальне ім'я фігуранта.

Додатково було встановлено участь акаунта в Telegram-чатах та спільнотах, що відповідали раніше отриманим відомостям про місце навчання, географічне розташування, інтереси та середовище спілкування фігуранта.

Особливу цінність становило те, що кожен окремий збіг не розглядався як самостійний доказ. Висновок було сформовано на основі сукупності незалежних факторів, які взаємно підтверджували один одного.

# Результати

У результаті проведеної перевірки було підтверджено цифровий зв'язок між встановленою особою та Telegram-акаунтом, що використовувався під час протиправної діяльності щодо клієнта.

Збіг імені, псевдонімів, місця проживання, навчального закладу, кола інтересів та цифрового оточення дозволив з високим ступенем достовірності підтвердити правильність проведеної атрибуції.

Таким чином особу фігуранта було остаточно встановлено та верифіковано незалежними методами, а ризик помилкової атрибуції зведено до мінімуму.

На цьому етапі основне завдання зі встановлення особи фігуранта вважалося виконаним.

# Встановлення законних представників

## Мета етапу

Після підтвердження особи фігуранта було прийнято рішення встановити його законних представників для реалізації подальших заходів реагування.

Основними завданнями цього етапу були:

- Встановлення осіб батьків фігуранта;
- Отримання актуальних контактних даних;
- Перевірка достовірності отриманих відомостей;
- Підготовка інформації для подальшого інформування законних представників про зафіксовану діяльність неповнолітнього.

## Аналіз цифрових зв'язків

У межах аналізу родинних зв'язків, встановлених під час попередніх етапів розслідування, було проведено додаткову перевірку відомостей щодо найближчого сімейного оточення фігуранта.

Проведений аналіз дозволив встановити особи матері та батька фігуранта, а також отримати їхні контактні дані, необхідні для подальшої комунікації.

Отримані відомості були додатково перевірені шляхом зіставлення з незалежними джерелами, що дозволило підтвердити їхню актуальність та достовірність.

## Результати

За результатами етапу було:

- Встановлено осіб обох законних представників фігуранта;
- Отримано та верифіковано контактні дані для зв'язку;
- Сформовано довідку щодо сімейного оточення фігуранта;
- Підготовлено інформаційну базу для подальшого інформування батьків про зафіксовану діяльність неповнолітнього.

Таким чином, завдання зі встановлення законних представників було виконано в повному обсязі, а необхідні відомості підготовлено для наступних етапів розслідування.

# Технічна ідентифікація учасників угруповання

## Планування заходу

На момент проведення цього етапу особу основного фігуранта вже було встановлено, однак значна частина учасників угруповання залишалася неідентифікованою.

Проведений аналіз внутрішнього спілкування дозволив зрозуміти інтереси, потреби та характер взаємодії учасників групи. Це дало можливість перейти від пасивного спостереження до активного отримання розвідувальної інформації.

Основною задачею стало встановлення технічних ідентифікаторів усіх учасників угруповання, насамперед їхніх IP-адрес, що могли бути використані для подальшої атрибуції осіб та передачі матеріалів до правоохоронних органів.

З цією метою було розроблено спеціалізований Telegram Web App[3], концепція якого базувалася на попередньо вивчених потребах учасників спільноти.

Зовні застосунок виглядав як повноцінний робочий інструмент та імітував виконання реальних операцій. Користувачеві демонструвався інтерфейс із формами введення даних, процесом виконання запиту та візуалізацією результатів роботи.

Фактично ж основним призначенням застосунку був прихований збір технічної телеметрії користувачів та фіксація їхніх мережевих ідентифікаторів.

Під час проєктування особлива увага приділялася саме збору IP-адрес, оскільки цей тип даних має найбільшу практичну цінність для подальшої роботи правоохоронних органів. Додатково застосунок збирав широкий спектр технічної інформації, необхідної для формування повноцінного цифрового профілю кожного учасника.

Таким чином Telegram Web App фактично виступав платформою технічної розвідки, замаскованою під внутрішній сервіс угруповання.

[3] Telegram Web App (TWA) — вебзастосунок, інтегрований безпосередньо в екосистему Telegram. Запускається всередині месенджера без встановлення окремої програми та дозволяє розробникам створювати інтерактивні сервіси, які взаємодіють із користувачами через Telegram.

# Реалізація

Після завершення розробки застосунок було представлено учасникам угруповання як новий інструмент для внутрішнього використання.

Завдяки попередньо сформованій довірі, успішній інтеграції до колективу та правильному вибору концепції сервісу учасники добровільно почали його тестувати.

Під час кожного запуску Telegram Web App автоматично фіксувався широкий спектр технічних параметрів користувача.

Зокрема логувались:

- Telegram ID;
- Username;
- Ім'я профілю;
- Дата та час взаємодії із застосунком;
- IP-адреса;
- Країна перебування;
- Регіон перебування;
- Місто перебування;
- Часовий пояс;
- Інтернет-провайдер (ISP);
- Автономна система (ASN);
- Тип мережі;
- Модель пристрою;
- Тип пристрою (Android / iOS);
- Архітектура процесора;
- Кількість ядер процесора;
- Обсяг оперативної пам'яті;
- Модель графічного процесора;
- Версія операційної системи;
- User-Agent;
- Роздільна здатність дисплея;
- Щільність пікселів екрана;
- Мова інтерфейсу Telegram;
- Статус Telegram Premium.

Кожна подія автоматично перетворювалася на структурований лог, який містив достатній обсяг інформації для формування технічного профілю користувача.

У результаті правильно спланованого заходу до взаємодії із застосунком вдалося залучити всіх встановлених учасників угруповання, включно з основним фігурантом та його найближчими спільниками.

# Результати

За результатами проведеного заходу було отримано технічні журнали (логи) всіх встановлених учасників угруповання.

Основним результатом операції стала фіксація актуальних IP-адрес кожного учасника з прив'язкою до конкретного Telegram-акаунта та часу взаємодії із застосунком.

У ході заходу було зафіксовано:

- Telegram ID усіх учасників угруповання;
- Username та дані профілів;
- Актуальні IP-адреси;
- Інтернет-провайдерів;
- Географічне розташування користувачів;
- Типи та моделі використовуваних пристроїв;
- Операційні системи;
- Додаткові технічні характеристики середовища роботи.

Отримані логи підтвердили перебування учасників угруповання на території різних регіонів рф а також за її межами. Зокрема було зафіксовано технічний слід одного з учасників, який перебував на території Ізраїлю.

Особливу цінність становить те, що IP-адреси були отримані безпосередньо від самих користувачів у момент взаємодії із застосунком, що значно підвищує достовірність отриманих даних та дозволяє пов'язати конкретний обліковий запис із конкретним мережевим підключенням.

У межах одного централізованого заходу вдалося отримати технічні профілі всіх встановлених учасників угруповання без необхідності проведення окремих операцій щодо кожного з них.

Усі отримані журнали було систематизовано, зведено в окремий документ та долучено до матеріалів розслідування.

На момент завершення етапу технічні профілі учасників угруповання були сформовані та підготовлені для подальшої передачі до правоохоронних органів разом з іншими матеріалами справи.

# Збір доказової бази

Метою цього етапу було документування протиправної діяльності основного фігуранта та інших встановлених учасників угруповання для подальшої передачі матеріалів до правоохоронних органів.

Збір доказів здійснювався шляхом аналізу особистих Telegram-каналів, профілів, групових чатів, архівів повідомлень, а також матеріалів, отриманих під час попередніх етапів розслідування.

У ході роботи було зафіксовано та задокументовано факти:

- Доксингу користувачів та незаконного поширення персональних даних;
- Погроз, шантажу та психологічного тиску на потерпілих;
- Організації та обговорення сватингу (Swatting);
- Координації дій учасників угруповання щодо переслідування третіх осіб;
- Поширення та реклами інструментів, призначених для отримання конфіденційної інформації;
- Розповсюдження навчальних матеріалів із доксингу, сватингу та суміжних напрямів;
- Пропозицій послуг, пов'язаних із завданням матеріальної або іншої шкоди потерпілим;
- Організації масових фіктивних замовлень товарів на адреси жертв з метою створення матеріальних збитків та психологічного тиску.

Окремо було зібрано докази причетності основного фігуранта до інциденту, що став підставою для початку розслідування. Зокрема задокументовано факти використання персональних даних потерпілого, висловлення погроз, спроби економічного тиску шляхом оформлення фіктивних замовлень та погрози здійснення сватингу.

Паралельно із документуванням діяльності основного фігуранта проводився збір доказової бази щодо інших учасників угруповання. У результаті було сформовано окремий архів матеріалів, який містить повідомлення, публікації, медіафайли, технічні журнали та інші відомості, що підтверджують участь встановлених осіб у діяльності спільноти.

За результатами етапу сформовано та систематизовано доказову базу, достатню для подальшої передачі разом із матеріалами розслідування до правоохоронних органів.

# Результати розвідувального заходу та статус виконання цілей

У результаті проведення комплексу OSINT, HUMINT та технічних розвідувальних заходів усі поставлені на початку розслідування цілі були виконані в повному обсязі.

Протягом роботи вдалося не лише встановити особу основного фігуранта інциденту, а й виявити організоване угруповання, учасники якого систематично займалися доксингом, погрозами, сватингом та іншою протиправною діяльністю в мережі Інтернет.

## Статус виконання цілей

- **Встановлення особи фігуранта**

На підставі результатів аналізу цифрового сліду, соціальної інженерії, HUMINT-заходів та подальшої верифікації було встановлено особу користувача Telegram, який здійснював погрози на адресу потерпілого та був безпосередньо причетний до інциденту.

Отримані відомості пройшли багатоетапну перевірку через незалежні джерела, цифрові зв'язки та технічні ідентифікатори, що дозволило підтвердити правильність атрибуції особи.

**Статус: виконано.**

- **Формування доказової бази**

У ході розслідування було задокументовано факти:

- доксингу та незаконного поширення персональних даних;
- погроз і психологічного тиску;
- сватингу;
- організації масових фіктивних замовлень на адреси потерпілих;
- координації діяльності учасників угруповання;
- поширення інструментів та матеріалів, пов'язаних із протиправною діяльністю.

Усі зібрані матеріали були систематизовані та оформлені у вигляді окремого архіву доказової бази.

**Статус: виконано.**

- **Встановлення законних представників**

У ході розслідування були встановлені та верифіковані законні представники неповнолітнього фігуранта.

- 31 грудня 2025 року одному з батьків було направлено повідомлення з інформацією про зафіксовану протиправну діяльність та можливі наслідки її продовження.

- 08 січня 2026 року було отримано відповідь, яка підтвердила отримання повідомлення та ознайомлення із викладеною інформацією.

**Статус: виконано.**

- **Встановлення учасників угруповання**

Під час проведення розвідувальних заходів було встановлено структуру досліджуваного угруповання та ідентифіковано його активних учасників.

Для кожного встановленого учасника були зібрані технічні ідентифікатори, включаючи Telegram ID, IP-адреси, географічні дані, характеристики пристроїв та іншу технічну інформацію.

У результаті було сформовано окремий документ із технічними профілями учасників угруповання.

**Статус: виконано.**

- **Підготовка матеріалів для передачі до правоохоронних органів**

За результатами розслідування було сформовано повний пакет матеріалів, який включав:

- Результати атрибуції основного фігуранта;
- Інформацію про встановлених учасників угруповання;
- Технічні журнали та IP-логи;
- Результати HUMINT та OSINT-заходів;
- Доказову базу щодо протиправної діяльності;
- Інформацію про структуру та діяльність угруповання.

Подальша передача зазначених матеріалів до правоохоронних органів здійснювалася третіми особами, які діяли самостійно та незалежно від автора цього звіту.

**Статус: виконано.**

- **Зафіксовано ознаки реагування правоохоронних органів**

21 лютого 2026 року було отримано непряме підтвердження того, що щодо основного фігуранта проводилися перевірочні заходи.

Під час подальшого спілкування фігурант повідомив про візит співробітників правоохоронних органів за місцем проживання. За його словами, під час перевірки проводилася бесіда із законними представниками, а також перевірялися його цифрові пристрої.

Зазначені відомості не дозволяють достовірно встановити причини проведення перевірки, однак за часом вони співпадають із періодом передачі матеріалів розслідування до компетентних органів.

**Статус: зафіксовано.**

# Підсумок

Усі цілі, поставлені на початку розвідувального заходу, були досягнуті.

У ході розслідування встановлено особу основного фігуранта, проведено його атрибуцію та верифікацію, виявлено учасників пов'язаного угруповання, сформовано технічні профілі його членів, зібрано доказову базу та підготовлено повний пакет матеріалів за результатами проведених заходів.

**Розвідувальний захід завершено.**