Фаріон-Мельник А. І.
к.е.н., доцент, доцент кафедри безпеки та правоохоронної діяльності
Західноукраїнський національний університет.
Винярська Б. П.
студентка НБ-12 юридичного факультету.
Західноукраїнський національний університет.

ЦИФРОВІ СЛІДИ В АНОНІМНИХ МЕРЕЖАХ: КЕЙС-СТАДІ WELCOME TO VIDEO

Сучасна архітектура глобальної безпеки сьогодні стикається з викликами, які ще два десятиліття тому здавалися суто теоретичними моделями з галузі криптопанку. Проблема в тому, що інформаційні технології, які створювалися для захисту приватності та свободи слова, стали ідеальним фундаментом для побудови найбільш закритих і технологічно досконалих кримінальних екосистем. Справа Welcome to Video не просто поповнила список гучних затримань, а стала свого роду вододілом у цифровій криміналістиці, наочно продемонструвавши, як методи Big Data та глибокий аналіз мережевих протоколів здатні пробивати броню багаторівневого шифрування Darknet [6]. Як зазначається в Офіційному звіті Міністерства юстиції США щодо справи «Welcome to Video» (2019) [3], успіх операції базувався на виявленні критичних помилок у налаштуванні сервера. Коли ми розглядаємо структуру цього ресурсу, ми бачимо не просто сайт, а складну інженерну споруду, що базувалася на прихованих сервісах Tor.

Для спеціаліста в галузі права та безпеки важливо розуміти, що анонімність Tor забезпечується цибулевою маршрутизацією, де кожен вузол знає лише попередню та наступну адресу, але не весь шлях. Проте адміністрація WTV пішла далі, створивши повну автоматизацію злочинної

діяльності, що фактично перетворило ресурс на першу у своєму роді e-commerce платформу в тіньовому сегменті мережі. Масштаб монетизації тут вражає навіть досвідчених аналітиків, адже це була повноцінна екосистема, де доступ до контенту купувався через алгоритми, що імітують роботу сучасних легальних стрімінгів. Якщо заглибитися в цифри, то вісім терабайт даних на сервері в середині 2010-х років — це був технологічний виклик. У мережі Tor, яка за своєю природою є повільною через багаторазове перешифрування на кожному вузлі, підтримка такої пропускної здатності вимагала специфічної серверної архітектури. Це підводить нас до каналу «Неразгаданные тайны»(2021р.) [5], де часто наголошується на тому, що головною ілюзією злочинців була віра в абсолютну невидимість Bitcoin. Насправді ж, як показує аналіз WTV, технологія блокчейн, хоч і приховує імена, є публічним реєстром, де кожен крок залишає цифровий відбиток. Крах системи почався не зі зламу самого Tor, а через критичні помилки на рівні прикладного програмного забезпечення. Найбільшим провалом Чон У Чжуна стало ігнорування базової ізоляції серверного середовища. У теорії сервер у Darknet має бути повністю сліпим до зовнішнього інтернету, але через неправильну конфігурацію SSL-сертифікатів стався витік реальної IP-адреси. Це класична помилка, коли сервер на нестандартний запит відповідає не через захищений шлюз, а через відкритий канал. Таким чином правоохоронці отримали справжній паспорт сервера, що призвело їх прямо до звичайної квартири в Південній Кореї. Це звучить іронічно: глобальна кримінальна імперія, що оперувала терабайтами даних і мільйонами доларів, фізично трималася на домашньому комп’ютері, підключеному до звичайного провайдера.

Наступний етап деанонімізації був ще більш витонченим і стосувався блокчейн-розвідки, що підтверджується матеріалами аналітичного порталу Chainalysis (2020) [4]. Агенти IRS-CI застосували метод

кластеризації адрес, який фактично розбив міф про анонімність криптовалют. Вони помітили, що тисячі унікальних гаманців, створених для клієнтів, зрештою акумулювали кошти в одному сховищі. Тут важливо розуміти концепцію точок виходу або ексанчів. Коли злочинці намагалися вивести Bitcoin у фіатні гроші, наприклад у вон чи долари, вони змушені були проходити процедури KYC (Know Your Customer) на біржах. Порівнявши часові мітки в блокчейні з даними про верифікацію на біржах, слідчі отримали реальні імена. Це те, що в професійному середовищі називають цифровим татуюванням: ви можете закрити браузер, але запис у блокчейні залишиться назавжди. Паралельно з цим велася робота з метаданими самих файлів. Кожне відео на сервері було об'єктом для OSINT-аналізу. Слідчі витягували інформацію про моделі камер, часові пояси та навіть GPS-координати, що дозволило ідентифікувати не лише споживачів, а й виробників контенту. Юридичний аспект цієї справи є не менш складним, ніж технічний. Кейс WTV став справжнім випробуванням для міжнародного права, спираючись на механізми, закладені в Конвенції про кіберзлочинність (Будапештська конвенція, Рада Європи, 2001) [1], яка залишається основним документом для міжнародної співпраці. Також це регулюється нормами Закону України «Про основні засади забезпечення кібербезпеки України», який формує актуальну базу для предмету [2]. Це був приклад безпрецедентної співпраці 38 країн, де цифрові докази передавалися в режимі реального часу. Однак тут виникла серйозна колізія між технічною складністю злочину та мірою покарання. У багатьох країнах законодавство просто не було готове до таких масштабів кіберзлочинності. Наприклад, відносно м'який вирок головному адміністратору в Кореї викликав хвилю обурення та став поштовхом до реформування кримінальних кодексів. Ми маємо розуміти, що правова система часто не встигає за розвитком технологій, і WTV став тим болючим досвідом, який змусив держави переглянути свої підходи до кібербезпеки. Підсумовуючи,

можна сказати, що ця історія — це насамперед про помилкову самовпевненість. Злочинці вірили в алгоритми, але забули про людський фактор і про те, що цифрова криміналістика розвивається експоненціально. Кожен рядок коду на сайті був або інструментом захисту, або потенційною діркою, через яку врешті-решт і пройшли спецслужби. Аналізуючи це як студент, я бачу тут не просто детективну історію, а глибокий урок із цифрової гігієни та важливості розуміння того, як працюють мережеві протоколи на найнижчому рівні. Ілюзія анонімності Bitcoin була зруйнована саме завдяки тому, що слідчі навчилися бачити зв'язки там, де інші бачили лише набір випадкових символів. Це фундаментальне нагадування: у цифровому світі кожна дія має свій відгомін, і якщо ви залишаєте фінансовий або технічний слід, рано чи пізно він буде знайдений, незалежно від того, скільки шарів шифрування ви використовуєте.

Справа Welcome to Video назавжди залишиться в підручниках як приклад того, як глобальна мережа правосуддя може бути ефективнішою за будь-який прихований сервер, якщо за справу беруться спеціалісти з блокчейн-аналітики та системного адміністрування. Вивчення подібних кейсів дає нам розуміння, що майбутнє національної безпеки лежить не лише в площині фізичного захисту кордонів, а й у глибокому розумінні архітектури інтернету та вмінні працювати з великими масивами даних, які залишає по собі будь-яка мережева активність. Крах WTV був неминучим саме через те, що адміністрація ресурсу повірила у власну невразливість, ігноруючи той факт, що кожна помилка в SSL-сертифікаті або невдалий скрипт на PHP є прямою дорогою до деанонімізації. Це був технологічний тріумф порядку над хаосом, який показав, що навіть найтемніші куточки Darknet не є безпечними для тих, хто порушує закон у таких масштабах. Досвід розслідування WTV довів, що мережа Tor не є «панацеєю» від деанонімізації. Будь-яка складна система захисту нівелюється помилками в конфігурації прикладного програмного забезпечення. Витік реальної IP-

адреси сервера через некоректні SSL-скрипти підтверджує, що людський фактор залишається найслабшою ланкою в ланцюгу кіберзахисту. Кейс назавжди зруйнував міф про анонімність криптовалют. Використання методів кластеризації та аналітичного ПЗ продемонструвало, що блокчейн є не лише інструментом для транзакцій, а й вічним цифровим архівом доказів. Кожна транзакція, здійснена користувачами WTV, стала незмивним слідом, який дозволив ідентифікувати тисячі осіб через роки після вчинення злочину.

Успіх операції став можливим завдяки поєднанню методів *Big Data* та *OSINT*. Здатність правоохоронних органів аналізувати терабайти неструктурованих даних (метаданих файлів, логів сервера, ланцюжків транзакцій) свідчить про те, що сучасна розвідка перейшла на вищий рівень рівень. Юридичний аспект справи виявив серйозний розрив між швидкістю розвитку IT-технологій та інертністю законодавства.

Транскордонний характер злочину вимагає не лише технічної співпраці, а й створення єдиних міжнародних стандартів покарання за кіберзлочини, щоб уникнути ситуацій, коли адміністратори глобальних мереж отримують мінімальні терміни через локальні правові колізії. Кейс Welcome to Video є наочним підтвердженням того, що в сучасному інформаційному світі анонімність є відносною. Будь-яка дія в мережі залишає цифровий відбиток, а розвиток інструментів аналізу великих даних робить ідентифікацію злочинця лише питанням часу та наявності відповідних обчислювальних ресурсів. Для майбутніх фахівців із права та безпеки цей кейс слугує нагадуванням: технології, що приховують злочин, є тими самими інструментами, які зрештою допомагають його розкрити.

Список використаних джерел*:*

1. Конвенція про кіберзлочинність (Будапештська конвенція). Рада Європи, 2001. (Конвенція про кіберзлочинність — Вікіпедія) (About the Convention - Cybercrime).

2. Закон України «Про основні засади забезпечення кібербезпеки України».(Про основні засади забезпе... | від 05.10.2017 № 2163-VIII).

3. Офіційний звіт Міністерства юстиції США (Department of Justice) щодо справи «Welcome to Video» та деанонімізації Чон У Чжуна, 2019. (Офіс громадських зв'язків | Громадянин Південної Кореї та сотні інших по всьому світу звинуватили у видаленні найбільшого даркнет-сайту з дитячою порнографією, який фінансувався Bitcoin | Міністерство юстиції США).

4. Матеріали аналітичного порталу Chainalysis: «Розслідування в Darknet: роль блокчейн-аналітики у справі WTV», 2020.(Cryptocurrency and criminals: assessing the evidence in Chainalysis' 2020 Report).

5. Відео-розслідування каналу «Неразгаданные тайны»: «Крах Welcome to Video: наймасштабніша операція в історії Даркнета», 2021. (https://youtu.be/p0iJ_2JYKpo?si=pUcb2EzXStCXvW9d).

6. «How the world’s biggest dark web platform spreads millions of items of child sex abuse material — and why it’s hard to stop».