

Основание для проведения расследования

В начале 2025 года поступило обращение, связанное с инцидентом в сфере цифровых активов. Заявитель сообщил о хищении средств в ходе сделки, которая проводилась с участием посредника. Лицо, взявшее на себя функции гаранта¹, злоупотребило доверием сторон: после получения активов на временное хранение оно присвоило их и в одностороннем порядке прекратило коммуникацию.

Данный инцидент был классифицирован как типичный сценарий «Exit Scam²». Учитывая преднамеренный характер действий и прямой финансовый ущерб, основной задачей расследования стала идентификация личности виновного лица. Работа была сфокусирована на анализе цифрового следа и сборе доказательной базы, необходимой для дальнейшего юридического или досудебного разбирательства. Все полученные в ходе проверки данные подтверждают факт мошенничества и позволяют перейти к этапу привлечения ответственности.

Основная цель

Установление личности субъекта, совершившего хищение активов под видом оказания услуг посредничества, а также формирование полной доказательной базы для последующего привлечения лица к ответственности.

Ключевые задачи:

- **Анализ цифрового следа:** Идентификация всех доступных идентификаторов, связанных с деятельностью субъекта в сети, включая профили в мессенджерах, на форумах и торговых площадках.
- **Верификация платежной информации:** Изучение цепочки транзакций и выявление конечных точек вывода средств (биржи, обменные сервисы, личные кошельки) для определения связи с реальными данными пользователя.
- **Сбор компрометирующих материалов:** Документирование факта ведения переговоров, условий сделки и момента присвоения активов для подтверждения мошеннического умысла.
- **Подготовка итогового заключения:** Систематизация полученных данных в отчетный документ, пригодный для передачи в профильные структуры или использования в рамках досудебного регулирования.

Команда расследования



хаупов
OSINT-Specialist



praga
OSINT-Specialist

[1] Гарант — это независимый посредник, который следит, чтобы покупатель получил товар, а продавец — деньги.

[2] Exit Scam — это афера, при которой организаторы легитимного, на первый взгляд, бизнеса, криптообъекта или онлайн-площадки внезапно прекращают работу и исчезают с деньгами клиентов.

Анализ мошеннической схемы



В этом кейсе мошенник разыграл классическую шахматную партию, где главной фигурой стал фейковый гарант. Весь расчет строился на том, чтобы приспать бдительность участников сделки еще до того, как зайдет речь о деньгах. Злоумышленник не просто вклинился в диалог, он заранее создал вокруг своего профиля облако надежности: мелькал в нужных чатах, имитировал бурную деятельность и, скорее всего, использовал накрученные отзывы. Это сработало как социальный инжиниринг — когда люди видят «проверенного» посредника, они перестают задавать лишние вопросы и соглашаются на его условия, даже если те выглядят подозрительно.

Сама ловушка захлопнулась на этапе передачи активов. Вместо того чтобы использовать прозрачные инструменты, где деньги замораживаются до выполнения условий, мошенник убедил стороны перевести всё напрямую на его кошельки. Как только транзакция подтвердились, он моментально включил режим «исчезновения»: заблокировал контакты и удалил переписку. Такая скорость и четкость действий говорят о том, что схема у него поставлена на поток — это не случайная ошибка, а отработанный алгоритм, где каждый шаг от приветствия до финального блока в телеграмме был просчитан заранее. По сути, мы имеем дело с профессиональным игроком, который специализируется именно на таких быстрых «выходах» с чужими средствами.

Весь технический цикл сделки был завязан исключительно на личности посредника и его прямых указаниях. Вместо использования независимых инструментов контроля, вроде смарт-контрактов или кошельков с мультиподписью, мошенник настоял на переводе активов под свое полное управление. В этом и заключалась главная уязвимость: участники передали ему не просто роль арбитра, а физический доступ к средствам. Как только транзакция подтвердилась в сети, у злоумышленника в руках оказались все ключи, и выполнение обязательств перед сторонами стало вопросом исключительно его «доброй воли», которой изначально не планировалось.

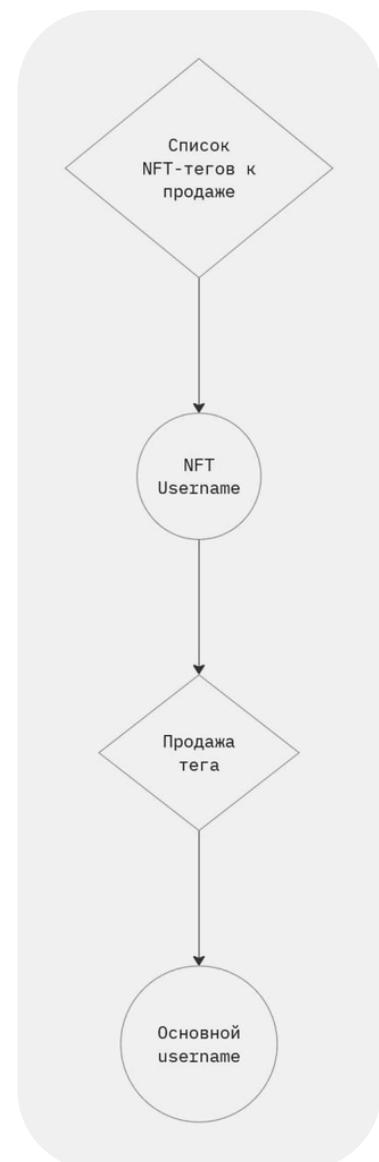
Анализ исходных данных

На начальном этапе оперативного анализа мы столкнулись с классической попыткой фигуранта выстроить эшелонированную систему анонимности. Вместо стандартного номера мобильного оператора для регистрации аккаунта был использован арендованный анонимный номер формата +888 (Anonymous Telegram Numbers). С точки зрения рядового OSINT-подхода это часто считается «тупиковой веткой»: здесь нет физической SIM-карты, нет привязки к конкретному биллингу или паспортным данным в офисе связи. Мошенник явно рассчитывал на то, что отсутствие материального носителя сделает его невидимым для классических методов поиска, таких как HLR-запросы или работа с базами данных сотовых провайдеров. Однако в реальности такая избыточная защита лишь сузила поле нашего маневра, переведя расследование в плоскость высокотехнологичного анализа блокчейн-инфраструктуры.

Логика здесь простая: любая технология анонимизации оставляет специфический след, если понимать механику её работы. Вместо того чтобы тратить ресурс на попытки «пробить» номер-пустышку, мы сместили фокус на операционную деятельность профиля. В рамках реализации методов Threat Intelligence был запущен процесс глубокого аудита через мониторинговые системы. Основная задача заключалась в поиске коммерческих отпечатков субъекта в сети. В ходе сканирования мы обнаружили, что анонимность для фигуранта — это не только способ защиты, но и часть его бизнеса. Было установлено, что субъект активно вовлечен в специфический сегмент рынка — куплю-продажу и холдинг коллекционных юзернеймов. Именно этот массив данных стал критической зацепкой: торговля уникальными цифровыми именами создала тот самый прозрачный след, который невозможно полностью зачистить в публичном реестре.

Выявление конкретного перечня юзернеймов, которые субъект выставлял на продажу или перемещал между подконтрольными аккаунтами, позволило нам инициировать трекинг транзакций непосредственно в блокчейне TON. Здесь вступает в силу жесткая методология: каждое коллекционное имя в Telegram — это полноценный NFT-токен. Каждое его движение, смена владельца или выставление на аукцион фиксируется в распределенном реестре навсегда. Проведя детальный аудит кошелька-холдера через сервисы визуализации блокчейн-связей (например, TonViewer), мы восстановили всю хронологию финансовых операций. Стало очевидно, что арендованный номер +888 служил лишь временной внешней ширмой, в то время как управление основными дорогостоящими активами велось с кошелька, имеющего прямые связи с реальной цифровой личностью мошенника.

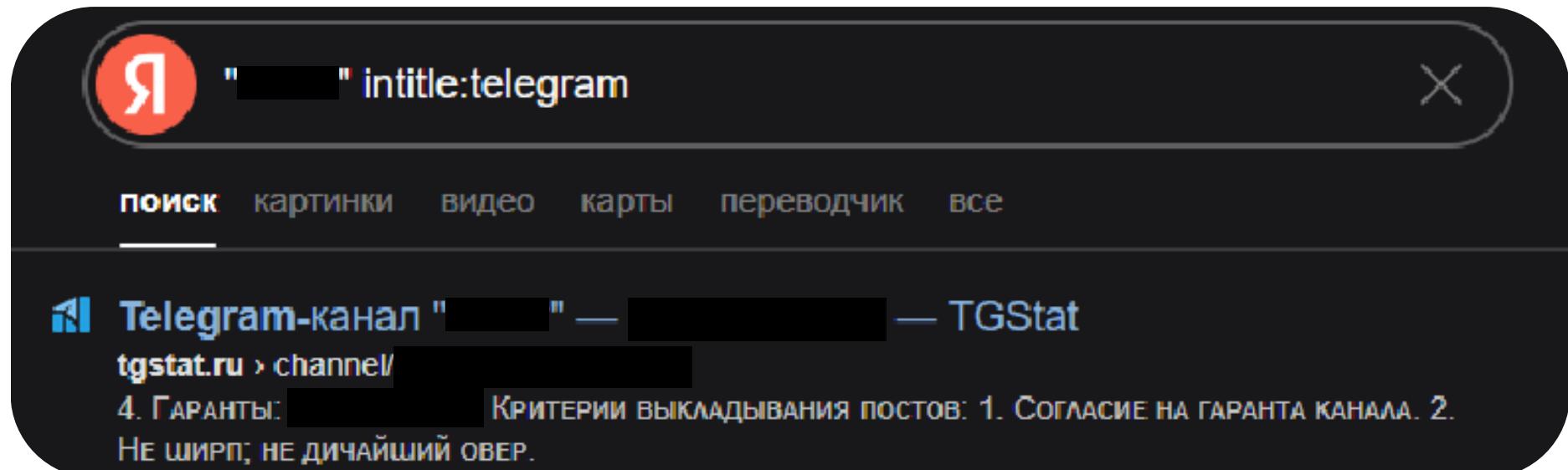
Сопоставление данных из мониторинговых систем с историей перемещений NFT позволило прошить эту анонимную прослойку насквозь. Мы установили прямую связь между «номером-пустышкой» и техническим аккаунтом субъекта с глубокой историей активности. Попытка скрыться за технологиями Web3 обернулась против фигуранта: его коммерческая активность в сфере продажи имен стала фатальной ошибкой, позволив превратить инструменты защиты в неопровергнутую доказательную базу.



Ретроспективный анализ и мониторинг публичной активности

Как только блокчейн-анализ подтвердил связь субъекта с рынком цифровых имен, возникла необходимость восстановить его исторический профиль. Объект пытался мимикрировать под «чистый» аккаунт, но в OSINT-практике полное удаление следов практически невозможно. На этом этапе основным инструментом стал мониторинговый сервис, через который был запущен поиск по архивам публичных сообщений.

Критическим моментом стало использование метода доркинга в плоскости транслитерации. Стандартный поиск по кириллическим запросам часто блокируется фильтрами мессенджера или не индексируется должным образом. Мы перевели поиск в латинское написание никна и применили специфические операторы. Использование дорка в транслите в сочетании с оператором *intitle:telegram* позволило обойти локальные ограничения поисковиков и обнаружить данные в архивах сервисов индексации каналов. Именно там был найден заархивированный ресурс, где в метаданных фигурировал технический юзернейм субъекта. Тот факт, что на момент расследования этот ник уже мог принадлежать другому пользователю, не имел значения — история индексации уже зафиксировала его связь с нашим объектом.

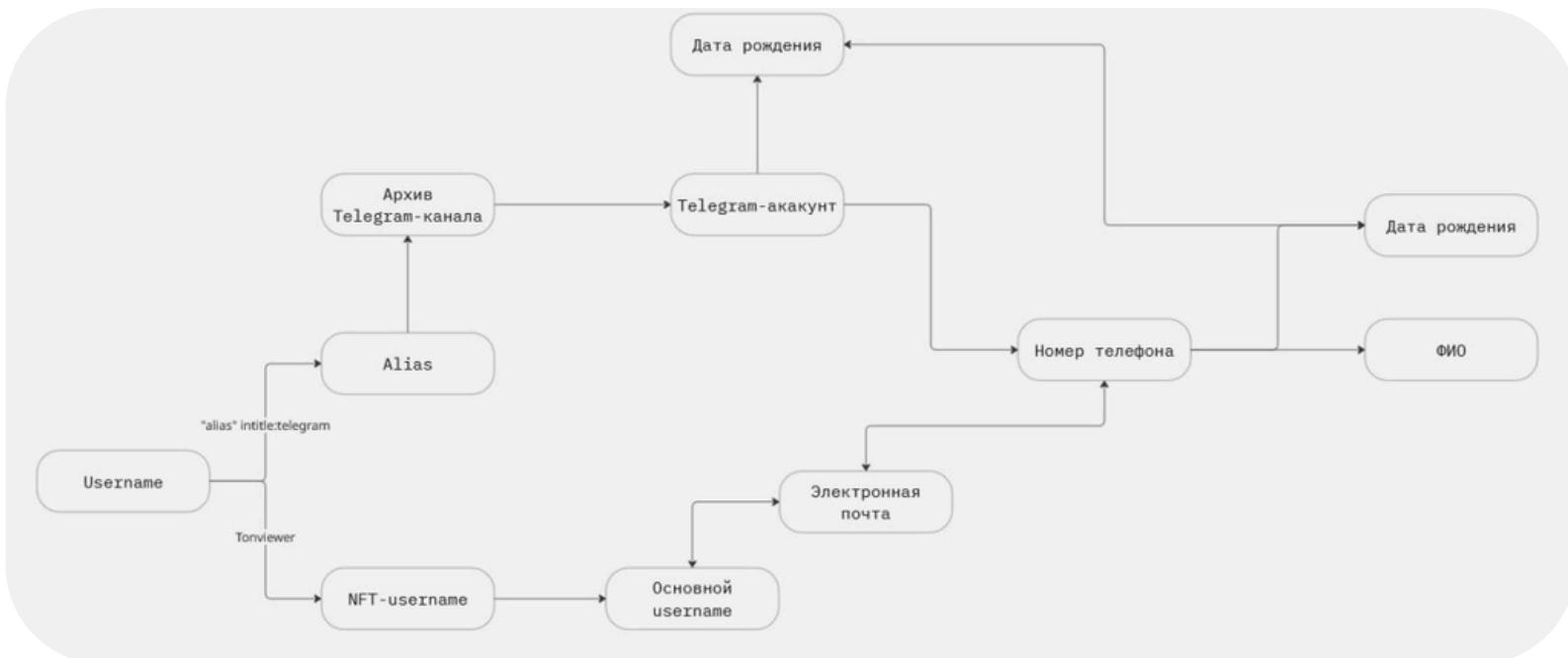


Для окончательной фиксации цифровой личности потребовалось перевести визуальный юзернейм в неизменяемый технический параметр. С помощью того же мониторингового инструментария мы вытащили уникальный идентификатор (UID³) аккаунта. В отличие от юзернеймов, которые можно менять или перепродавать как NFT, UID присваивается один раз и навсегда. Получение этого кода стало точкой невозврата: мы связали архивную активность, старый канал и текущий анонимный профиль в единую логическую цепочку. Это позволило нам зафиксировать конкретный программный объект, который позже был использован для финальной стадии деанонимизации.

Этот этап работы доказал, что любая попытка начать деятельность «с чистого листа» разбивается о системные логи мессенджеров. Комбинация транслит-доркинга и архивного поиска позволила нам восстановить путь субъекта от обычного пользователя до «анонимного» посредника, подготовив все необходимые данные для интеграции с базами финальной идентификации и установления реальной личности.

[3] UID (Unique Identifier, уникальный идентификатор) — это постоянный цифровой или буквенно-цифровой код, присваиваемый пользователю

Финальная идентификация и верификация найденных данных



Заключительный этап расследования был направлен на конвертацию накопленных цифровых идентификаторов в юридически значимые данные о личности. Имея на руках уникальный UID аккаунта и историю его привязок, мы задействовали аналитический инструментарий для поиска пересечений в массивах открытых данных. Основная задача здесь заключалась в том, чтобы найти ту точку, где цифровой профиль неизбежно соприкасается с реальной инфраструктурой — номером телефона или регистрационными данными. Благодаря глубокому синтезу выявленных идентификаторов, нам удалось установить прямую связь аккаунта с абонентским номером диапазона +7.

Получение этого номера позволило провести финальную верификацию и развернуть полный социальный граф объекта. На этом этапе мы не просто получили персональные данные, а выстроили детальный профиль, который подтвердил все предварительные выводы. Сопоставление данных из различных информационных ресурсов позволило однозначно идентифицировать личность фигуранта. Важным моментом стало то, что сведения, полученные в ходе идентификации, полностью совпали с информацией, которую субъект неосторожно оставлял в своих скрытых или архивных профилях — в частности, дату его рождения и регион проживания.

В ходе дальнейшего анализа собранного досье был верифицирован возраст объекта. На момент проведения исследования и совершения анализируемых действий субъект являлся несовершеннолетним. Это обстоятельство добавляет важный штрих к анализу всей схемы: несмотря на использование продвинутых инструментов анонимизации (вроде NFT-номеров и арендованных активов), базовая цифровая гигиена субъекта оказалась недостаточной для противодействия профессиональному анализу. Наличие «хвостов» в архивных записях и пренебрежение правилами разделения личных и технических профилей привели к полной деанонимизации.

Таким образом, цикл расследования был успешно закрыт. Мы прошли путь от анонимного «гаранта» с блокчейн-номером до установления конкретных идентификационных данных. Весь массив собранных доказательств, включая технические идентификаторы, историю транзакций и подтвержденные персональные данные, сформировал базу, достаточную для дальнейшего юридического реагирования или инициирования процедуры возврата активов.

Заключение и аналитические выводы

Проведенное расследование наглядно продемонстрировало несостоительность концепции «абсолютной анонимности» в современных децентрализованных сетях и мессенджерах. Использование субъектом арендованного анонимного номера +888 и оперирование NFT-активами, вопреки ожиданиям фигуранта, не создало непреодолимого барьера для идентификации. Напротив, специфика блокчейн-инфраструктуры TON позволила нам превратить инструменты сокрытия личности в прозрачную доказательную базу. Ключевым фактором успеха в данном кейсе стал не прямой поиск по закрытым базам, а комплексный мониторинг операционной деятельности объекта — от фиксации коммерческих транзакций с цифровыми именами до извлечения архивных метаданных.

Основной вывод по результатам деанонимизации подтверждает типичную ошибку молодых правонарушителей: пренебрежение правилами разделения технической и личной цифровых личностей. Несмотря на техническую подготовленность (использование арендованных мощностей и Web3-инструментария), субъект допустил ряд критических ошибок в «цифровой гигиене». Наличие ретроспективных связей, зафиксированных в ходе мониторинга публичных чатов, и уникальный идентификатор (UID), привязанный к истории транзакций, позволили нам полностью нивелировать эффект от смены аккаунтов. Установление реального номера телефона и ФИО субъекта стало логическим завершением процесса синтеза разрозненных улик в единый профиль.

На текущий момент идентификация личности завершена в полном объеме. Установленный факт несовершеннолетия объекта является важным юридическим аспектом, который необходимо учитывать при выборе дальнейшей стратегии реагирования. Собранный массив данных — включая технические параметры аккаунтов, историю блокчейн-переводов и подтвержденные персональные данные — является достаточным для инициирования процедуры претензионной работы или передачи материалов в соответствующие инстанции.

Результаты расследования подтверждают: любая активность в сети оставляет «хлебные крошки», а использование специализированных аналитических методов и ретроспективного поиска позволяет восстановить цепочку событий даже в условиях намеренной анонимизации. Все выявленные материалы структурированы и подготовлены к использованию в качестве доказательной базы для защиты интересов пострадавшей стороны.