ПУБЛИКАЦИЯ / RU

Иван и Юрий Некулити, Андрей Нестеренко: серверы, санкции и теневая сторона хостинга

Опубликовано 15.10.2026 · Обновлено 15.10.2026



У цифрового подполья есть вполне материальная сторона: серверные стойки, договоры, электричество и компании, которые обеспечивают связь с интернетом. В мае 2026 года нидерландские следователи изъяли более 800 серверов в деле о предполагаемом нарушении санкций. За этой историей — братья Иван и Юрий Некулити, бизнес Stark Industries, смена корпоративных вывесок и MIRhosting Андрея Нестеренко. KARTEL KHIMPROM сопоставил расследования, реестры и

официальные документы, чтобы разобраться, кто за что отвечал и какие вопросы остаются открытыми. [1][2]

Когда расследование приходит в дата-центр

18 мая 2026 года FIOD, нидерландская служба финансовых расследований, задержала двух мужчин — 57-летнего из Амстердама и 39-летнего из Гааги. Следователи обыскали коммерческие помещения в Энсхеде и Алмере, а также дата-центры в Дронтене и Схипхол-Рейке. Предметом дела стало предполагаемое предоставление экономических ресурсов субъектам, находящимся под санкциями ЕС. [1]

Имена в официальном сообщении отсутствовали. Журналист Брайан Кребс назвал задержанных: **Андрей Нестеренко**, связанный с MIRhosting, и **Youssef Zinad**, связанный с WorkTitans. В его публикации операция рассматривается как продолжение истории инфраструктуры Stark Industries Solutions. [2]

Смысл этой истории становится понятнее, если смотреть дальше количества изъятой техники. Преступный интернет-сервис зависит от множества поставщиков. Один продаёт вычислительные мощности, другой предоставляет помещение, третий подключает оборудование к сети. Каждый видит собственный участок работы. Для расследования требуется восстановить всю цепочку, включая то, кто принимал решения и получал доход.

Претензии к провайдеру возникают на пересечении двух вопросов: как использовалась инфраструктура и что было известно людям, которые её предоставляли. В истории Некулити и Нестеренко эти вопросы обсуждаются уже несколько лет.

Иван Некулити: от хостингового бизнеса к международному расследованию

В расследовании CORRECTIV 2024 года Иван Некулити предстаёт предпринимателем из Бендер, построившим бизнес PQ Hosting в Кишинёве. Компания рекламировала недорогие серверы во множестве стран. Для клиента это выглядело как обычное коммерческое предложение: выбрать местоположение, оплатить ресурсы и запустить нужный сервис. [3]

Особое значение имел российский рынок. В интервью, которое разобрали журналисты, Иван объяснял преимущества зарубежных серверов для пользователей, сталкивающихся с ограничениями. Иностранный IP-адрес позволял выходить в сеть с другой географической привязкой. Позднее, отвечая CORRECTIV, он заявил о сокращении деятельности в России после начала войны. [3]

Это важно для понимания продукта: провайдер продавал доступ к распределённой инфраструктуре. Но сведения о продукте ещё не раскрывают состав клиентов. Связи с конкретными злоумышленниками исследователи устанавливают по другим данным — инфраструктуре атак, размещённым ресурсам и реакции на уведомления о нарушениях.

> **Некулити Иван**

История Ивана не ограничивается PQ Hosting. В базе ICIJ Offshore Leaks существует запись о MORENEHOST LTD, где бенефициаром с 24 апреля 2019 года указан IVAN NEKULITSY. CORRECTIV связывает эту запись с Некулити. Это исторический корпоративный след, который позволяет проследить предшествующий проект; само владение офшорной компанией преступления не доказывает. [4][3]

В апреле 2022 года Morphisec исследовал атаку через уязвимость VMware. Аналитики связали сервер одного из этапов загрузки вредоносного кода со Stark Industries и отметили связь этой инфраструктуры с PQ Hosting. Такой результат показывает, где находился технический ресурс. Он не устанавливает, что владелец хостинга сам написал вредоносную программу или управлял атакой. [5]

Юрий Некулити: почему имя в реестре имеет значение

Stark Industries Solutions Ltd зарегистрировали в Великобритании 10 февраля 2022 года. В Companies House у Ивана указана должность секретаря, а у Юрия, записанного как Iurie Neculiti, — директора. В записи о существенном контроле Юрий указан как владелец не менее 75% акций; дата уведомления — 16 февраля 2024 года. [6][7][8]

В схеме CORRECTIV Юрий был младшим братом Ивана и участником бизнеса PQ Hosting. При этом британская Stark формально контролировалась именно им. Поэтому история двух братьев требует раздельного рассмотрения их ролей: публичный представитель бизнеса, директор и зарегистрированный собственник могут выполнять разные функции. [3]

> **Некулити Юрий**

Сам Иван объяснял назначение Stark достаточно предметно: в сведениях об IP-адресах вместо PQ Hosting появлялось нейтральное название. По его словам, британская компания не проводила платежи, а помогала организовать работу. CORRECTIV рассматривал Stark как юридическое звено бизнеса PQ Hosting. [3]

Для внешнего наблюдателя это создаёт несколько слоёв. Название на сайте, контрагент в документах и организация, указанная у сетевого ресурса, могут не совпадать. Такая структура встречается и в законном бизнесе. Вопрос возникает тогда, когда разделение затрудняет установление ответственного за ресурс после обнаружения злоупотребления.

Андрей Нестеренко: кто обеспечивает подключение

Следующее звено — MIRhosting. CORRECTIV описывал компанию Андрея Нестеренко как одного из сетевых партнёров инфраструктуры братьев Некулити. Нестеренко подтвердил журналистам, что Stark Industries является клиентом. В той же публикации отмечалась его работа торговым представителем Serverius в 2014–2016 годах. [3]

У Нестеренко есть и другая публичная профессиональная биография. MIRhosting сообщает о его выступлении на фортепианном конкурсе в Энсхеде в 2002 году, второй премии и последующем обучении у Михаила Маркова. Компания рассказывает о многолетнем техническом сопровождении конкурса. Эти сведения характеризуют его карьеру; они не подтверждают и не опровергают претензий к хостинговому бизнесу. [9]

> **Нестеренко Андрей Владимирович**

Главный вопрос к MIRhosting связан с характером предоставляемых услуг. В мае 2026 года компания объяснила, что обеспечивала WorkTitans размещение оборудования, питание и сетевое подключение. Управление аппаратурой, программами и данными, по её заявлению, оставалось у клиента. [10]

Это принципиальное различие. Прохождение трафика через сеть само по себе не доказывает управление клиентским сайтом. Для оценки осведомлённости поставщика существенны конкретные уведомления, их содержание, сроки реакции и последующие действия. Отдельный вопрос — кому предоставлялись услуги и ресурсы в период действия санкций.

Несколько компаний — несколько разных функций

Чтобы не смешивать участников, полезно разложить опубликованные связи по ролям. Таблица отражает сведения разных лет и не является перечнем действующих договоров на сегодняшний день.

Структура	Роль в опубликованной истории	Основание
PQ Hosting	Хостинговый бизнес братьев Некулити, описанный в расследовании 2024 года.	CORRECTIV [3]
Stark Industries Solutions Ltd	Британское юридическое лицо, связанное с сетевой инфраструктурой бизнеса.	Companies House; CORRECTIV [6][3]
PQ Hosting Plus S.R.L.	Организация, на которую аналитики зафиксировали перенос AS44477 в мае 2025 года.	Recorded Future [11]
WorkTitans B.V. / THE.Hosting	Компания и бренд, фигурирующие в последующей истории переноса услуг.	Recorded Future [11]
MIRhosting	Сетевое подключение; компания также подтверждала услуги размещения оборудования для WorkTitans.	Заявление MIRhosting [10]
Serverius	Оператор дата-центра, упоминаемый в расследовании CORRECTIV.	CORRECTIV [3]

Из таблицы не следует, что все перечисленные структуры имеют одинаковый правовой статус. Она показывает, почему расследование деятельности конкретного сервиса нельзя завершить на первом названии, найденном в сетевом справочнике.

Что находили на серверах: пропаганда, DDoS и финансовая киберпреступность

CORRECTIV подробно разбирал ресурс RRN, связанный с информационной кампанией Doppelganger. По выводам журналистов, он работал через инфраструктуру братьев Некулити в Нидерландах. После вопросов издания Иван сообщил о блокировке соответствующей

учётной записи и сервера. Однако CORRECTIV считал, что ресурс продолжал использовать связанную инфраструктуру, уже скрытую дополнительным сервисом. [3]

В том же расследовании рассматривалась NoName057(16), известная DDoS-атаками. CORRECTIV привёл наблюдения Spamhaus: из 48 обнаруженных управляющих скриптов за два месяца начала 2024 года половина находилась на серверах Stark. Эта повторяемость стала одним из оснований для вопросов к провайдеру. Иван отрицал допустимость атак и утверждал, что компания серьёзно относится к жалобам. [3]

Дальнейшие исследования расширили картину. Recorded Future сообщал, что в середине 2025 года инфраструктуру Stark использовал GrayAlpha — кластер, существенно пересекающийся с финансово мотивированной группой FIN7. Таким образом, круг описанных угроз включал не только политические операции. [11]

Общий коммерческий поставщик может обслуживать разные, не связанные между собой группы. Для анализа это важное предостережение: соседство ресурсов в одной сети ещё не означает общего руководства. Но повторяющееся использование одного поставщика разными злоумышленниками делает его практики работы с клиентами самостоятельным предметом общественного интереса.

Санкции объявлены, инфраструктура меняется

20 мая 2025 года Совет ЕС ввёл санкции против Stark Industries Solutions, Ивана и Юрия Некулити. В официальном сообщении основанием названа поддержка дестабилизирующих действий связанных с Россией акторов, включая информационные операции и кибератаки. Эти меры включают замораживание активов и ограничения на предоставление средств и ресурсов. [12]

Техническое исследование Recorded Future описывает изменения, начавшиеся ещё до объявления санкций. 16 мая 2025 года аналитики зафиксировали перенос AS44477 на PQ Hosting Plus S.R.L. Затем появились бренд THE.Hosting под WorkTitans B.V. и новая автономная

система AS209847. Исследователи оценили перестройку как вероятную попытку сохранить услуги при изменении юридических и сетевых обозначений. [11]

Автономная система — это сеть под единым техническим управлением, которую другие сети распознают по номеру. Изменение такой регистрации может быть существеннее смены логотипа: оно затрагивает то, как инфраструктура представлена другим операторам. При этом назначение конкретного изменения устанавливается по совокупности обстоятельств, а не по одному новому номеру.

16 сентября 2025 года британская Stark Industries Solutions Ltd получила в Companies House статус Dissolved. Это факт о юридическом лице. Он не отвечает на вопрос, что стало с оборудованием, клиентскими данными и услугами, ранее связанными с компанией. [6]

Документ от 8 октября 2026 года: что теперь утверждает Совет ЕС

В обновлённых санкционных записях братьев Некулити Совет ЕС описал перенос инфраструктуры Stark к WorkTitans B.V., названной структурой прикрытия, и роль MIRhosting в обеспечении подключения. Иван и Юрий указаны как бенефициары этой конструкции. По оценке Совета, она отражала попытку скрыть владение и сохранить хостинговые услуги под новыми юридическими и сетевыми обозначениями. [13]

Это уже официальная санкционная оценка, выходящая за рамки ранних журналистских предположений. Однако она не заменяет уголовного приговора каждому человеку или компании, упомянутым в описании. В частности, упоминание MIRhosting в записях братьев не равнозначно персональным санкциям против Нестеренко.

При сопоставлении материалов видно, как меняется предмет публичного обсуждения: от отдельных ресурсов на серверах — к сохранению контроля над инфраструктурой после ограничений. Именно преемственность бизнеса становится центральным вопросом этой истории.

Возражения MIRhosting: спор о том, откуда шли атаки

Нестеренко сообщил KrebsOnSecurity, что переход оборудования и клиентского портфеля к WorkTitans состоялся до санкций и не был направлен на их обход. Он отрицал поддержку киберпреступности. Компания объявила о временной приостановке услуг WorkTitans и сотрудничестве с властями. [2][10]

2 июня 2026 года MIRhosting опубликовала собственный анализ трафика за октябрь–ноябрь 2025 года. По её данным, все 4 468 обнаруженных DDoS-аномалий были входящими: целью были обслуживаемые адреса. Компания утверждала, что её наблюдения не показывают исходящих атак. [14]

При этом MIRhosting указала ограничение: сохранённая детализация некоторых измерений сама по себе не исключает кратковременные всплески. Исходные данные компания обещала предоставить компетентным органам. При подготовке этого материала весь массив независимо не проверялся. [14]

Спор о направлении атак и вопрос соблюдения санкций требуют разных доказательств. Даже исчерпывающий ответ о трафике конкретной недели не установит автоматически, кто контролировал компанию-получателя услуг. И наоборот, корпоративная связь сама по себе не доказывает запуск атаки с конкретного сервера.

В проверенных материалах нет подтверждения обвинительного приговора Нестеренко по описанному делу. Его текущая мера пресечения также не установлена: сообщение о задержании в мае не позволяет утверждать, что он остаётся под стражей в октябре.

Где в этой истории появляется «Химпром»

Для редакции KARTEL KHIMPROM изучение инфраструктуры важно как часть работы о цифровых сервисах, которыми могут пользоваться преступные сети. Но в этом кейсе связь с конкретным картелем требует особенно точной формулировки.

В отчёте Intrinsec *From espionage to PsyOps* разобраны кампании UAC-0050 и UAC-0006. На странице 11 приведён текст угроз, отправитель которых благодарит «Химпром» и администрацию Rutor. В других разделах исследователи рассматривают маршрутизацию и инфраструктурные пересечения, связанные со Stark и MIRhosting. [15]

Упоминание картеля сделано самим автором угроз. Это не подтверждённое свидетельство от его имени и не доказательство договора между картелем и провайдером. Чужое название может использоваться для запугивания, ложного следа или саморекламы. Причину такого упоминания необходимо устанавливать отдельно.

Поэтому имеющиеся материалы позволяют исследовать пересечение тем — преступных сервисов, угроз и поставщиков инфраструктуры, — но не объявлять Некулити или Нестеренко участниками «Химпрома». Документов о прямом обслуживании картеля, его платежах этим людям или их личных договорённостях с Егором Буркиным в изученных источниках нет.

Для продвижения этой части проверки нужен конкретный связующий факт: установленная принадлежность сервиса, подтверждённый поставщик в соответствующий период, договор либо платёж. Обнаружить похожие названия в разных расследованиях недостаточно.

Почему история важнее одной вывески

Сильная сторона этого кейса — возможность сопоставить несколько типов свидетельств. Корпоративный реестр показывает формальные роли. Техническое исследование отслеживает сетевые изменения. Следственный релиз описывает основания операции. Санкционный акт излагает позицию Совета ЕС. Ответы компании позволяют проверить, что именно она оспаривает.

Каждый источник отвечает на свою часть вопроса. Вместе они дают более содержательную картину, чем перечень громких названий. Но и вместе не освобождают от необходимости доказывать каждую персональную связь.

Главный незакрытый вопрос — кто фактически сохранял возможность управлять инфраструктурой и получать от неё доход после корпоративных изменений. Ответ требует сведений о контроле, передаче активов и реальном исполнении договоров. Именно они позволяют отличить обычную продажу бизнеса от конструкции, сохраняющей интересы прежних владельцев.

Когда преступный сервис исчезает с одного адреса, важно понять, исчезла ли его техническая и финансовая основа. История Stark, братьев Некулити и MIRhosting показывает, почему такое расследование должно продолжаться за пределами сайта и его логотипа — до компаний, оборудования и людей, принимающих решения.

Материал подготовлен по открытым документам и опубликованным расследованиям, проверенным на 15 октября 2026 года. Выводы ведомств и исследователей приведены с атрибуцией. Позиции фигурантов изложены по их опубликованным ответам; редакция не представляет эти ответы как полученные на собственные запросы.

Источники

1. FIOD — два задержания и изъятие более 800 серверов по делу о санкциях, 22.05.2026
   https://www.fiod.nl/fiod-houdt-twee-verdachten-aan-wegens-overtreding-sanctiewetgeving/
2. KrebsOnSecurity — задержания Андрея Нестеренко и Youssef Zinad, 25.05.2026
   https://krebsonsecurity.com/2026/05/netherlands-seizes-800-servers-arrests-2-for-aiding-cyberattacks/
3. CORRECTIV — расследование о братьях Некулити, PQ Hosting, Stark и MIRhosting, 31.05.2024
   https://correctiv.org/en/fact-checking-en/2024/05/31/hacks-and-propaganda-meet-the-two-brothers-bringing-russias-cyber-war-to-europe/
4. ICIJ Offshore Leaks / Pandora Papers — MORENEHOST LTD и бенефициар IVAN NEKULITSY
   https://offshoreleaks.icij.org/nodes/240120865
5. Morphisec Labs — исследование атаки через уязвимость VMware и инфраструктуры Stark, 25.04.2022
   https://www.morphisec.com/blog/vmware-identity-manager-attack-backdoor/

6. Companies House — Stark Industries Solutions Ltd, № 13906017; статус и даты регистрации
https://find-and-update.company-information.service.gov.uk/company/13906017

7. Companies House — должностные лица Stark Industries Solutions Ltd
https://find-and-update.company-information.service.gov.uk/company/13906017/officers

8. Companies House — лица со значительным контролем над Stark Industries Solutions Ltd
https://find-and-update.company-information.service.gov.uk/company/13906017/persons-with-significant-control

9. MIRhosting — биографические сведения об Андрее Нестеренко и сотрудничестве с фортепианным конкурсом, 22.02.2026
https://mirhosting.com/mirhosting-international-piano-competition-enschede-livestream

10. MIRhosting — заявление в ответ на публикации СМИ, 22.05.2026
https://mirhosting.com/verklaring-mirhosting-naar-aanleiding-van-recente-mediapublicaties

11. Recorded Future / Insikt Group — One Step Ahead: Stark Industries Solutions Preempts EU Sanctions, 27.08.2025
https://www.recordedfuture.com/research/one-step-ahead-stark-industries-solutions-preempts-eu-sanctions

12. Совет ЕС — санкции против Stark Industries и братьев Некулити, 20.05.2025
https://www.consilium.europa.eu/en/press/press-releases/2025/05/20/russian-hybrid-threats-eu-lists-further-21-individuals-and-6-entities-and-introduces-sectoral-measures-in-response-to-destabilising-activities-against-the-eu-its-member-states-and-international-partners/

13. Совет ЕС — Регламент 2026/2257 от 08.10.2026, записи 27–28; официальный текст на BOE
https://www.boe.es/buscar/doc.php?id=DOUE-L-2026-81528

14. MIRhosting — собственный анализ трафика за октябрь–ноябрь 2025 года, опубликован 02.06.2026
https://mirhosting.com/the-november-2025-danish-election-attacks-what-our-own-network-data-shows

15. Intrinsec — From espionage to PsyOps: Tracking operations and bulletproof providers of UACs in 2025; c. 11, 18, 25–26
https://www.intrinsec.com/wp-content/uploads/2025/10/TLP-CLEAR-From-espionage-to-PsyOps-Tracking-operations-and-infrastructure-of-UACs-in-2025-EN.pdf

Использование материалов

При использовании материалов обязательна активная ссылка на исходную публикацию.

Оригинал материала

https://kartel-khimprom.com/ru/article/ivan-i-yurij-nekuliti-andrej-nesterenko-servery-sankczii-i-tenevaya-storona-hostinga/