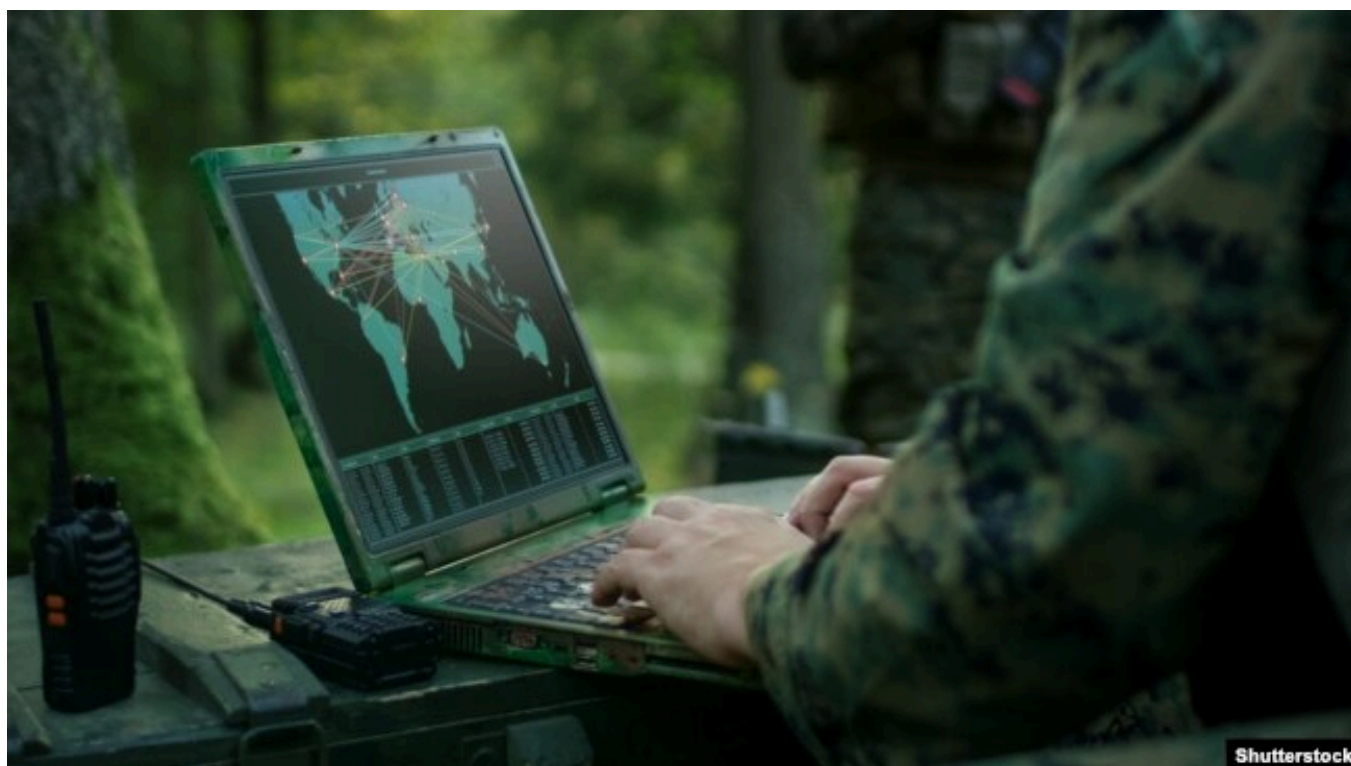


В ДЕТАЛЯХ

"Темная Кларк": как AI-сеть ГРУ в Латинской Америке помогала Кремлю очернять Украину и влиять на местную политику

Александр Дубровский

20 октября 2026 года 06:00 мск



Компания OpenAI, ведущий разработчик в области искусственного интеллекта, разоблачила масштабную скрытую сеть влияния России, получившую кодовое имя Dark Clark ("Темная Кларк"). OpenAI считает, что с ее помощью российские спецслужбы проводили гибридные операции с помощью нейросетей в Латинской Америке, донося до целевых аудиторий свою повестку, но при этом скрывая ее истинный источник. Ранее компания установила, что аналогичным образом нейросети использовали для очернения США спецслужбы Ирана.

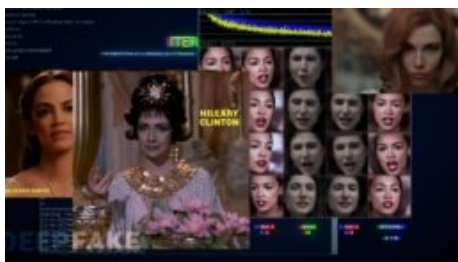
Как работала Dark Clark

В OpenAI считают, что за Dark Clark стоит российская военная разведка ГРУ. Ее сотрудники проводили кампании в Латинской Америке из России через VPN и использовали нейросетевые модели ChatGPT (чат-бота OpenAI) для тонкого администрирования разветвленной агентурной сети и создания фейков. Специалисты по кибербезопасности OpenAI [обнаружили](#) прямые связи между вымышленной сетью аккаунтов и российской организацией под названием "Политология". Она известна в узких кругах как "Компания" (La Compania).

Это структура фактически стала одной из преемниц ЧВК "Вагнер", а также ["Агентства интернет-исследований"](#) ("Фабрики троллей") и других медийно-политических активов, созданных покойным российским бизнесменом Евгением Пригожиным. Их связи подтверждает то, что ее операторы регулярно просили языковые модели переводить на испанский и португальский, анализировать и объяснять для иностранных аудиторий общедоступные публикации о "Политологии" и "ЧВК Вагнер".

Главным вектором усилий российских агентов стали подрыв международной репутации Украины в латиноамериканском регионе и прямое вмешательство во внутривнутриполитические процессы в Аргентине, Боливии, Бразилии, Перу, Эквадоре и Панаме.

При этом большинство операторов сети физически находились на территории Российской Федерации и общались с искусственным интеллектом на русском языке: лишь один из участников регулярно формулировал запросы на испанском. Однако его цифровой след и детали активности также однозначно указывали на то, что он находился в России.



СМОТРИТЕ ТАКЖЕ:

Дипфейки от "Матрешки". Россия делает фейк-видео про украинских беженцев, используя искусственный интеллект – Голос Америки

В OpenAI отдельно отмечают, что из-за действующих блокировок российские агенты не имели легального доступа к передовым западным нейросетям, и поэтому вынужденно использовали коммерческие VPN-сервисы для маскировки своих реальных IP-адресов.

Операторы "Компании" использовали ChatGPT для трех ключевых задач:

- *составление и регулярное обновление подробных внутренних отчетов для своего неизвестного вышестоящего руководителя-куратора;*
- *тонкая языковая калибровка и вычитка пропагандистских материалов для придания им аутентичного местного колорита;*
- *администрирование и координация работы латиноамериканского "Центра социологических исследований" (Social Research Center) – главной и самой опасной ширмы этой операции.*

Нейросети OpenAI стали для них полноценным цифровым секретарем, аналитиком и переводчиком.

По оценкам специалистов OpenAI, вся кампания "Темная Кларк" стала первой в истории детально задокументированной операцией ИИ-влияния, достигшей пятого уровня из шести возможных по так называемой "Шкале прорыва" (см. ниже). Это означает, что созданные в рамках кампании фейки вышли далеко за пределы маргинальных интернет-сообществ и спровоцировали официальные расследования, опровержения на уровне министров и публичные заявления мировых политиков.

Что такое "Шкала прорыва"

"Шкала прорыва" ([IO Breakout Scale](#)) была разработана в 2020 году американским исследователем [Беном Ниммо](#). Она измеряет влияние операции не по трудноизмеримому "изменению настроений" аудитории, а по объективно наблюдаемому, проверяемому и фиксируемому распространению ("прорыву") контента между онлайн-платформами, сообществами и офлайн-средой.

Шкала состоит из шести последовательных уровней, разделенных на две основные группы:

Категория 1: одна платформа, без прорыва. Операция локализована в рамках одной онлайн-платформы и не выходит за пределы одного конкретного сообщества или сети собственных аккаунтов кампании.

Категория 2: выход за рамки одного сегмента. Нарратив распространяется либо в рамках одного сообщества, но на нескольких платформах, либо охватывает несколько разных сообществ, но строго на одной платформе.

Категория 3: множественные платформы и сообщества. Кампания успешно кочует по различным социальным сетям (например, Facebook, X, YouTube, TikTok) и начинает проникать в общие дискуссии обычных пользователей, приобретая вирусный потенциал.

Категория 4: прорыв в центральные СМИ. Информационная операция преодолевает барьер соцсетей и попадает в повестку традиционных авторитетных средств массовой информации (мейнстрим-медиа).

Категория 5: усиление лидерами мнений. Нарратив подхватывают и сознательно или вслепую распространяют крупные публичные фигуры – известные политики, знаменитости или топовые инфлюенсеры – выводя охваты на принципиально новый уровень.

Категория 6: политическая реакция или насилие. Наивысший уровень угрозы. Операция приводит к конкретным реальным последствиям: официальной реакции на законодательном или правительственном уровне, изменению государственной политики, либо провоцирует прямые призывы и акты физического насилия на улицах.

Модель "Шкала прорыва" активно используется исследователями проблем кибербезопасности, аналитическими центрами (например, Институтом Брукинга в Вашингтоне) и технологическими гигантами, в том числе OpenAI. С ее помощью определяют приоритетность реагирования и координации противодействия информационным угрозам в реальном времени.



СМОТРИТЕ ТАКЖЕ:

Open AI вскрыл ИИ-контент в канале "Рыбарь" и нескольких связанных с ним: он использовался для дезинформации в интересах России

Выдуманный институт и ничего не подозревающие эксперты

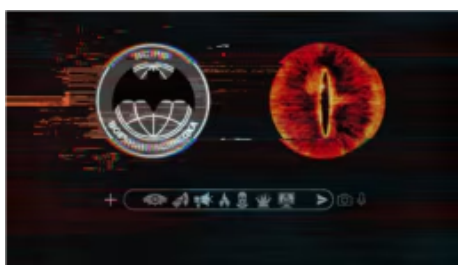
Наиболее изощренным элементом операции Dark Clark стало создание и долгосрочное финансирование вымышленного института, именовавшего себя Центром социологических исследований. Согласно официальному сайту организации, она позиционировала себя как независимая исследовательская платформа.

Для управления этой структурой российские спецслужбы создали глубоко проработанную цифровую личность – вымышленную женщину-руководителя по имени Миа Кларк (от этого имени OpenAI дала название операции – "Темная Кларк").

От имени "Мии Кларк" институт вел официальные аккаунты в социальных сетях, деловую переписку и взаимодействовал с реальными чиновниками на местах.

Уровень проработки легенды оказался настолько высок, что эксперты OpenAI называют созданный российскими агентами институт самой сложной и глубокой попыткой действий под прикрытием вымышленной идентичности – из всех, что были пресечены международными ИТ-гигантами за последние два с половиной года.

Уникальность тактики заключалась в том, что "Темной Кларк" удалось привлечь к реальной аналитической работе ничего не подозревающих жителей Латинской Америки – в том числе профессиональных исследователей, социологов и журналистов.



СМОТРИТЕ ТАКЖЕ:

"Ваше сообщение отправлено в ГРУ". Как военная разведка совместно с неонацистом "Топазом" создает телеграм-ботов для вербовки диверсантов

Российские операторы полностью контролировали деятельность выдуманного института. В запросах к ChatGPT постоянно фигурировали конкретные кадровые решения о найме в него новых сотрудников и увольнении неэффективных специалистов, точные сетки заработной платы в организации, премиальные фонды, а также утверждение текущих и перспективных исследовательских проектов, планов интервью и социологических опросов.

Привлеченные к работе в институте латиноамериканские специалисты искренне верили, что работают на авторитетный международный фонд. Они добросовестно брали интервью у ведущих региональных экспертов, политологов и комментаторов, собирали первичные данные и готовили объемные качественные материалы.

Тематика их исследований при этом была подчеркнута нейтральной и академической: например глобальный анализ общественного мнения о перспективах расширения группы БРИКС или сравнительный анализ макроэкономических показателей Бразилии при президентах Жаире Болсонару и Лулу да Силве.

На сайте "ЦСИ" было опубликовано больше 60 оригинальных статей.

В OpenAI считают, что это была долгосрочная российская стратегия выстраивания доверия у латиноамериканских экспертов. В отличие от других сетей влияния, которые нередко лишь воруют чужие тексты или публикуют дешевые фейки, операция "Темная Кларк" создавала авторитетное аналитическое прикрытия. Обладая легитимным статусом и связями по всей Латинской Америке, центр в нужный момент мог стать каналом для вброса разрушительной дезинформации, которой поверили бы ведущие СМИ региона.

Данная методология весьма напоминает схему работы другой российской операции под названием "PeaceData", также тесно связанной со структурами Евгения Пригожина. Ее международные платформы безопасности, включая Meta, раскрыли и [ликвидировали](#) еще в 2020 году.

Перуанский эксперимент: стравливание Украины и Польши

Самой успешной и изощренной кампанией "Темной Кларк" в Латинской Америке расследователи OpenAI считают операцию в Перу в мае 2026 года.

Российские операторы сперва зарегистрировали фальшивый адрес электронной почты, который визуально и текстуально был не отличим от официального электронного ящика регионального управления образования в столице Перу Лиме.

С этого адреса они провели массовую рассылку по государственным и частным школам столичного округа. В письме содержалось строгое административное указание: в рамках празднования Национального дня культурного и языкового разнообразия (отмечаемого 21 мая) в обязательном порядке провести во всех классах специальные тематические мероприятия и уроки, посвященные солидарности с Украиной. При этом фальшивое распоряжение прямо предписывало учителям многократно упомянуть в ходе уроков фигуру Степана Бандеры, украинского националиста XX века.



СМОТРИТЕ ТАКЖЕ:

Суд в России признал УПА, ОУН и Степана Бандеру "пособниками нацистской Германии"

Некоторые директора школ после проведения мероприятия начали присылать на поддельный адрес электронной почты официальные отчеты об этих уроках и прикреплять к ним реальные фотографии детей на фоне портретов Бандеры.

Аналогичную фейковую операцию в школах в России провел в 2024 году акционист из Беларуси Владислав Бохан: он заставил учителей, которые "купились" на его приказ, выходить на субботник с плакатами с лозунгами Третьего Рейха и делать шапочки из фольги в рамках "патриотического мастер-класса" "Шлем отечества". Составить "инструкцию" акционисту также помог искусственный интеллект:



СМОТРИТЕ ТАКЖЕ:

"Мне этих людей не жалко". Интервью акциониста Владислава Бохана: он заставил учителей в РФ выйти на субботник с лозунгами Третьего рейха

Однако если Бохан просто высмеял учителей и школы в России, которые стали жертвой его пранка, операторы "Темной Кларк", получив отчетные фото, добились публикации подготовленных статей в [перуанских](#) и [польских](#) СМИ (в Польше отношение к Бандере резко отрицательное), а также в англоязычном [издании](#) в Венгрии.

В этих текстах утверждалось, что Украина "экспортирует ультранационалистические идеологии" в латиноамериканские школы и якобы "заставляет детей молиться" на спорных исторических лидеров.

Вброс [сработал](#), отмечает OpenAI, причем дошел даже до высших эшелонов европейской власти. В ряде СМИ тиражировалась жесткая реакция действующего польского депутата Европарламента, который, попавшись в ловушку, официально [предложил](#) объявлять любых лиц, проявляющих подобные "антипольские настроения", персонами нон грата в Польше. Таким образом российская кибергруппировка сыграла на давних исторических противоречиях между Украиной и Польшей, искусственно углубив раскол между ключевыми союзниками на международной арене.

Бразилия: истории "похищенной бразильянки"

В январе 2026 года российские операторы "Компании" зафиксировали во внутренней отчетности запуск полностью сгенерированной с помощью ИИ "трагической истории" о выдуманной бразильской блогерше и топ-модели.

Согласно разработанной дезинформационной фабуле, как пишет OpenAI, молодая гражданка Бразилии якобы стала жертвой международной сети торговцев людьми. В искусственно созданных материалах организаторами выдуманного похищения напрямую назывались действующие сотрудники украинского посольства в Бразилии, которые якобы обманом вывезли девушку в Киев. Финалом сфальсифицированной истории стало сообщение о ее последующем жестоком убийстве.

Этот фейк был призван сформировать образ Украины как опасного, криминального государства, где процветает беззаконие. Это должно было максимально дискредитировать украинские дипломатические миссии в Латинской Америке.



СМОТРИТЕ ТАКЖЕ:

Боливия, Перу и другие. Как Россия вербует на войну в Украине латиноамериканцев под видом работы на стройке

Аргентина: собаки Милей в ошейниках Cartier

Операторы Dark Clark также вели агрессивные точечные кампании против действующих лидеров латиноамериканских стран, чья внешняя или внутренняя политика не устраивала Россию. К примеру, после "шпионского" скандала в Аргентине, связанного с российской прослушкой, обнаруженной в президентском дворце, одной из главных мишеней сети стал радикальный реформатор, президент Аргентины Хавьер Милей.



СМОТРИТЕ ТАКЖЕ:

МИД РФ вызвал посла Аргентины после скандала с прослушкой в президентском дворце и заявлений о причастности к этому России

Киберэксперты OpenAI выявили участие россиян в проведении как минимум двух крупных скоординированных кампаний против аргентинского лидера в 2024 году.

Первый эпизод носил характер классического медийного вброса, бьющего по репутации президента в условиях жесткого экономического кризиса. Россияне разработали и распространили ложную историю о том, что Хавьер Милей, призывающий нацию к тотальной экономии, якобы приобрел для своих любимых собак баснословно дорогие ошейники Cartier, украшенные драгоценными камнями. Фейк был направлен на провоцирование социального взрыва и обвинение президента в лицемерии.



Хавьер Милей и Владимир Зеленский в Буэнос-Айресе в декабре 2023 года

Второй эпизод вышел за пределы цифрового пространства и переместился на улицы Буэнос-Айреса. В отчетах для руководства операторы утверждали, что тайно заплатили местным уличным исполнителям за нанесение серии агрессивных граффити против Милея на стены зданий в центральных районах Буэнос-Айреса. Позже благодаря утечке внутренних документов "Компании" оба этих инцидента – и история с ошейниками, и финансирование уличных вандалов – были [связаны](#) независимыми исследователями с деятельностью российской структуры.

Боливия: паника из-за бензина и снятия наличных

В Боливии в июне 2026 года российские операторы отчитались о создании сфабрикованной аудиозаписи. На ней человек с голосом, практически идентичным голосу высокопоставленного сотрудника Центрального банка Боливии, в панических тонах предупреждал население о якобы неизбежном и скором введении жестких лимитов на снятие наличных денег в банкоматах и кассах.



Протесты в Боливии летом 2024 года

Одновременно было изготовлено и распространено поддельное официальное письмо, исходящее якобы от государственного агентства Боливии по углеводородам. В этом документе содержалось ложное предупреждение о введении строгих ограничений на продажу топлива для частных автомобилей.

В еще одном внутреннем отчете "Компании" описывался фейк, распространенный в Боливии в конце мая, в разгар очередных антиправительственных протестов. С помощью ИИ была создана поддельная аудиозапись сотрудника государственной водоснабжающей компании EPSAS. Он якобы [сообщал](#), что правительство собирается отключить воду в административной столице Ла-Пасе и [ввести](#) в городе чрезвычайное положение.

Целью этой скоординированной атаки было провоцирование массовой паники, штурма отделений банков, искусственного дефицита бензина и, как следствие, масштабного социально-политического кризиса в Боливии. Но, подчеркивает OpenAI, данные вбросы либо были оперативно удалены, либо не смогли набрать критическую массу просмотров для дестабилизации ситуации.

Эквадор: кампания против консула Украины и частной военной компании из США

Еще одним полем для экспериментов Dark Calrk стал Эквадор. Там в июне российские операторы применили тактику, аналогичную перуанской: используя очередной поддельный адрес электронной почты, они разослали по школам распоряжение местного Министерства образования организовать торжественную церемонию. В ходе нее учащиеся должны были [принести](#) коллективную присягу на верность лично действующему президенту страны Даниэлю Нобоа, а также [Эрику Принсу](#), американскому бизнесмену и основателю частной военной компании Blackwater (сегодня она называется [Academi](#)). Ее бойцы задействованы Вашингтоном в Эквадоре в операциях против наркокартелей.



Эрик Принс в 2007 году

Деятельность Academi в Эквадоре сопровождается скандалами. Соответственно, приказ, якобы исходивший от Минобразования, спровоцировал волну возмущения среди родительских комитетов и учителей в Эквадоре. Ситуация накалилась настолько, что министр образования Эквадора [выступил](#) с официальным публичным опровержением. По иронии судьбы, именно это вынужденное заявление [довело](#)

сфабрикованную историю до общенациональной аудитории – чего и добивались российские организаторы атаки.

В Эквадор операторы "Компании" отчитались о создании еще двух фейков. Во-первых, они сгенерировали или смонтировали аудиофайл, приписанный лично почетному консулу Украины в Эквадоре. На этой записи дипломат якобы в крайне пренебрежительной и высокомерной форме высказывался о гражданах Эквадора и их культуре. Запись была залита в TikTok – но широкого резонанса не вызвала.

Во-вторых, в социальных сетях X и TikTok был запущен профессионально смонтированный видеоролик, на который был наложен логотип реального и авторитетного эквадорского новостного телеканала. В сюжете [утверждалось](#), что администрация президента Даниэля Нобоа заключила секретное соглашение с подставной украинской фирмой и начинает принудительно вербовать молодых эквадорских мужчин для отправки в зону боевых действий на Украину. В начале апреля этот ролик стал объектом пристального внимания местных независимых фактчекеров, которые доказали, что это абсолютная ложь, созданная с помощью ИИ.

Кроме того, в июле 2026 года испаноязычный сотрудник "Компании", находившийся в России, передал ChatGPT русскоязычный текст, содержащий вымышленную цитату президента Нобоа, в которой тот якобы грубо оскорблял беднейшие слои населения своей страны. Оператор поставил перед ИИ задачу перевести этот текст на эквадорский диалект испанского языка, внедрив местный сленг и речевые обороты, чтобы у местных жителей не возникло ни малейших сомнений в подлинности цитаты.

OpenAI в своем заявлении подчеркивает, что успех и глубина проникновения операции Dark Clark заставляют экспертов по всему миру полностью переосмыслить систему защиты информационного пространства. Использование в разных странах местных граждан "втемную", создание высококачественных аналитических центров-прикрытий с оригинальным контентом и ювелирная точность перевода ИИ с учетом региональных диалектов делают подобные кампании чрезвычайно опасными: они больше не выглядят как глупый спам в комментариях. Теперь это интеллектуальные операции, способные ссорить дружественные государства, вызывать панику в банковских секторах и заставлять оправдываться министров суверенных стран.

Главный урок "Темной Кларк", как заключает OpenAI, заключается в том, что искусственный интеллект в руках опытных манипуляторов превратился из инструмента автоматизации в мощный усилитель человеческого коварства. Противостоять этой угрозе можно только при полной прозрачности и жестком международном контроле за использованием технологий генеративного искусственного интеллекта.



Читай нас в Телеграме

ПОДПИСАТЬСЯ

МАТЕРИАЛ ИЗ РАЗДЕЛОВ:

В деталях

Видео и статьи

Россия

Украина

Европа

Америка

Актуальное

© Настоящее Время. Все права защищены