Транснациональные цифровые репрессии в Беларуси: от доксинга до дипфейков

Digital Freedoms Lab

Транснациональные цифровые репрессии в Беларуси: от доксинга до дипфейков

Введение

1. Инфраструктура цифровых репрессий: платформы и экосистема Telegram

1.1. Общая характеристика платформ и социальных сетей, применяемых для цифровых репрессий

1.2. Аффилиация Telegram-каналов с государственными органами Беларуси

1.3. Анализ экосистемы каналов

2. Типология кейсов дискредитации, доксинга и разведывательных операций в цифровой среде

2.1. Пропаганда и дискредитация через фабрикацию контента

2.1.1. Создание фейков против активистов и продемократических организаций

2.1.2. Дипфейки как инструмент дискредитации

2.1.3. Фейковые заявления о взломах ресурсов независимых организаций

2.1.4. Пропагандистская дискредитация через материалы уголовных расследований

2.2. Разведывательные операции против диаспоры и гражданского общества

2.2.1. Сбор данных и дезинформация через имитацию доверенных источников

2.2.2. Сбор данных через псевдоработодателей и подставных исполнителей

2.2.3. Попытки онлайн-вербовки членов диаспоры

2.2.4. Сбор данных за денежное вознаграждение

2.3. Онлайн угрозы и преследование в социальных сетях

2.3.1. Угрозы и давление в переписках

2.3.2. Использование родственников в онлайн-кампаниях давления

2.3.3. Публикация видео и фото разгромов имущества

2.4. Атаки на инфраструктуру и деятельность инициатив и организаций

2.4.1. DDoS-атаки на цифровую инфраструктуру

2.4.2. Вмешательство в открытые форматы работы

2.5. Публикация персональных данных активистов и организаций через провластные источники (доксинг)

2.5.1. Публикации призывов от провластных Telegram-каналов явиться к силовикам

2.5.2. Публикация данных активистов в государственных СМИ и провластных источниках

2.5.3. Публикация личной переписки активистов и оппозиционных деятелей

2.5.4. Публикация персональных данных в официальных реестрах

2.5.5. Финансовый доксинг

3. Производство синтетического контента средствами ИИ

3.1. «Людажоры»: пропаганда на основе генеративного ИИ

3.1.1. Технология и форматы производства

3.1.2. Гендерный аспект атак

3.2. «Белорусский фронт»: дипфейк-кампании против лидеров оппозиции

Заключение

Рекомендации

Введение

Данное исследование посвящено цифровым формам транснациональных репрессий, которые беларусские государственные и провластные акторы применяют против беларусской диаспоры после президентских выборов 9 августа 2020 года. В центре исследования - доксинг, дезинформационные и дискредитационные кампании, а также использование технологий искусственного интеллекта (ИИ) в политических репрессиях. Так, данный доклад охватывает как практики, направленные против организаций гражданского общества, так и преследование отдельных лиц (журналистов, активистов, и других публичных деятелей). Эти уровни влияния связаны между собой: компрометация организаций, как правило, реализуется через влияние на конкретного человека, а публичное преследование одного человека зачастую бьет по всей структуре, которую он представляет.

Президентские выборы в Беларуси 9 августа 2020 года и последовавшие за ними массовые протесты обусловили беспрецедентный по масштабу выезд граждан из страны. По оценке исследователей, Беларусь покинули от 500 до 600 тысяч человек. Официальная статистика Белстата фиксирует сокращение населения страны с 2020 года почти на 301 000 человек, однако эти данные не отражают реального масштаба эмиграции: значительная часть уехавших сохраняет прописку в Беларуси, не проходит полную регистрацию в принимающих странах или не попадает в статистику по иным причинам. Параллельно, с 2020 года продолжаются и внутренние репрессии: за пять лет правозащитный центр «Вясна» зафиксировал более 100 000 случаев преследования (обысков, задержаний и допросов). В то же время, статус политического заключенного с 2020 года (и на момент написания этого исследования) получили 4774 человека.

В связи с этим, беларусское гражданское общество вынуждено было переформировать свою деятельность за рубежом: Офис Светланы Тихановской в Вильнюсе, Объединенный переходный кабинет, Координационный совет, независимые медиа, правозащитные организации и фонды солидарности реорганизовались за границей. Деятельность этих структур продолжается в иностранных юрисдикциях, территориях, которые физически недоступны для беларусских государственных органов. В этих условиях власти начали систематически расширять применение транснациональных инструментов воздействия, которые позволяют осуществлять преследование политических оппонентов, активистов и диссидентов даже за пределами территории государства.

Транснациональные репрессии – практика использования государствами инструментов принуждения против своих граждан за рубежом – документируются во многих различных контекстах. С 2014 по 2025 год организация Freedom House в своем докладе зафиксировала 1375 прямых физических инцидентов транснациональных репрессий, совершенных 54 государствами в 107 принимающих странах. В 2025 году 30 государств осуществляли транснациональное преследование своих критиков, и было зафиксировано 126 новых физических инцидентов. Сами составители доклада подчеркивают, что эти цифры отражают лишь видимую часть реальной картины: в базу данных включены исключительно прямые физические случаи воздействия и репрессий (похищения, нападения, депортации), тогда как нефизические тактики систематически не учитываются из-за сложности их распознавания и документирования.

Беларусь регулярно оказывается в числе государств, применяющих транснациональные репрессии. «Freedom House» отмечает, что беларусские власти опираются на глубоко укоренившиеся связи с российским правительством для реализации своих трансграничных репрессивных кампаний. Государственный департамент США в 2024 году также зафиксировал, что власти Беларуси «совершали акты транснациональных репрессий с целью запугивания или преследования лиц, находящихся за пределами страны», перечислив среди жертв таких репрессий лидеров демократического движения, правозащитников, журналистов, профсоюзных

деятелей, адвокатов и студентов, покинувших территорию Беларуси. Аналитическая сеть iSANS в докладе 2024 года описала транснациональные репрессии беларусского режима как «многослойный инструмент подавления инакомыслия», действующий одновременно в правовой, цифровой и информационной плоскостях.

В свою очередь, цифровая среда значительно расширяет возможности для транснациональных репрессий, создавая новые инструменты воздействия на оппонентов. Среди таких инструментов – цифровая слежка, фишинг, онлайн угрозы, разоблачение персональных данных, и так далее. К примеру, по последним данным, не менее 19 правительств применяли коммерческое шпионское программное обеспечение против лиц, находящихся в эмиграции. При этом, авторитарные правительства и связанные с ними структуры редко прибегают к одной тактике в стремлении запугать своих критиков за рубежом: вместо этого они используют комбинацию цифровых методов, которые наслаиваются друг на друга и взаимно усиливают эффект. Таким образом, цифровая инфраструктура и прокси-акторы позволяют государствам проецировать свою власть через границы все более быстро и при меньших затратах, одновременно усложняя установление ответственных за подобные атаки.

В беларусском контексте цифровые транснациональные репрессии охватывают несколько категорий практик, составляющих фокус данного исследования. Доксинг осуществляется через официальные государственные реестры, государственные СМИ и связанные с государственными структурами онлайн каналы. Например, Human Constanta фиксирует, что беларусское «антиэкстремистское» законодательство создало правовую основу, в рамках которой раскрытие персональных данных преследуемых лиц приобретает формально законный характер: в Беларуси действуют несколько отдельных «экстремистских» списков, сведения из которых публикуются открыто и тиражируются различными каналами. Параллельно ведутся дезинформационные и дискредитационные кампании, направленные как против организаций гражданского общества, так и против конкретных лиц: фейковые заявления о взломах баз данных, сфабрикованные материалы с показаниями задержанных людей, атаки на финансовую отчетность организаций, и так далее. Еще одна форма атак – генерация и распространение дипфейков и иного синтетического контента, разведывательные операции и атаки на инфраструктуру. Все эти практики объединяет общая функция: развитие чувства страха и неопределенности в диаспорах.

Чтобы детально показать, как именно работают транснациональные репрессии, доклад разбирает их по составным частям. Материал сгруппирован по типу операций и тому, какие инструменты используются и против кого направлена атака. Такое разделение кейсов условно, так как на практике одна операция часто сочетает в себе и сбор данных, и дискредитацию, и угрозы и давление одновременно. Первая глава описывает платформы и провластную экосистему Telegram: связи между государственными органами и анонимными каналами и количественный анализ публикаций нескольких из таких каналов. Вторая глава направлена на детальный разбор самих практик: фабрикации контента, разведывательных операций, онлайн угроз, атак на инфраструктура и доксинга. Третья глава разбирает производство синтетического контента на примере двух наиболее развитых практик и показывает гендерное измерение таких атак. Заключение обобщает результаты, а завершающая часть содержит рекомендации для гражданского общества, принимающих стран и онлайн-платформ.

Данное исследование сочетает в себе качественный анализ открытых источников и количественный анализ Telegram публикаций, охватывая период с августа 2020 года по июль 2026; количественный анализ Telegram-публикаций охватывает более узкий отрезок – с января 2023 года, что определяется глубиной доступного сбора данных. В качестве основных источников мы используем материалы беларусских и международных правозащитных организаций, независимых медиа, исследования технологического характера, а также официальные публикации государственных СМИ и органов, провластные ресурсы, и свидетельства пострадавших. Данные, опубликованные государственными органами и провластными медиа, используются как свидетельства применяемой риторики и способов давления. Связь каналов с государством определялась по совокупности признаков. Так, это могли быть прямые признаки, такие как официальный статус, известные модераторы, заявления властей или выводы независимых

расследований. С другой стороны, брались во внимание и более косвенные признаки, такие как синхронность с действиями силовых структур, воспроизведение официальных нарративов либо иные технические связи.

Выборка описанных в этом исследовании кейсов не является репрезентативной, так как наше исследование не направлено на измерение общего числа атак. Вместо этого, мы демонстрируем общие повторяющиеся инструменты и то, как государство, провластные ресурсы и медиа дополняют друг друга. У исследования есть и существенные ограничения: использованные данные опираются в основном на открытые источники информации, поэтому задокументированные случаи отражают лишь часть реального масштаба проблемы. Telegram-экосистема также нестабильна: каналы блокируются и восстанавливаются под новыми именами, а часть данных теряется, что мешает точно оценить всю ситуацию. В то же время, анонимность операторов и посредников затрудняют атрибуцию: даже наличие у канала непубличных материалов не всегда говорит, как они были получены и существовало ли прямое поручение. Наконец, доклад сосредоточен на инструментах и моделях и не содержит анализа психологических последствий для пострадавших. Однако, собранного материала достаточно для того, чтобы детально продемонстрировать общую экосистему цифрового давления и служить отправной точкой для дальнейшего диалога гражданского общества.

1. Инфраструктура цифровых репрессий: платформы и экосистема Telegram

1.1. Общая характеристика платформ и социальных сетей, применяемых для цифровых репрессий

Прежде чем перейти к типологии конкретных операций, необходимо описать инфраструктуру, в которой они реализуются: платформы, через которые осуществляется преследование, и экосистему провластных Telegram-каналов, распространяющих материалы, собранные силовыми структурами. Понимание этой инфраструктуры принципиально для интерпретации последующих разделов: одни и те же кейсы читаются иначе, если известно, что публикующие их каналы связаны репостами, синхронным расписанием и общими источниками в органах власти. Так, настоящая глава дает инфраструктурную рамку и результаты сетевого анализа беларусской провластной Telegram-экосистемы.

Цифровизация коммуникаций изменила не только инструменты политической мобилизации и общественной самоорганизации, но и инструментарий государственного контроля. Социальные сети и мессенджеры дают силовым структурам возможность наблюдать за политическими оппонентами, устанавливать их личности и социальные связи, собирать персональные данные, распространять дискредитирующие материалы и оказывать давление на людей за пределами национальной юрисдикции. Как было упомянуто ранее, в беларусском случае цифровые репрессии стали продолжением системы преследования, сложившейся после протестов 2020 года и охватывающей независимых журналистов, правозащитников, представителей гражданского общества, диаспору и в целом оппонентов власти.

Ключевая практика в этом ряду – доксинг. В настоящем исследовании он понимается широко – как публикация или систематизация сведений, позволяющих идентифицировать человека и усилить давление на него: имени, фотографии, места работы или учебы, семейных связей, аккаунтов в социальных сетях, сведений о местонахождении и перемещениях, а также видео задержаний и принудительных «покаянных» записей. Эти сведения регулярно используются для стигматизации, запугивания, травли, создания угрозы последующего преследования и легитимации действий силовых органов. Реализуется эта практика на разных площадках, и функции их внутри системы различаются, поэтому ниже они рассматриваются по отдельности: Telegram как основная среда публикации и координации, Facebook и Instagram как источники идентифицирующих сведений, TikTok и Threads как относительно новая зона государственного мониторинга.

Telegram занимает в этой структуре ключевое место: возможность действовать под псевдонимами, скорость распространения контента и сетевой характер связанных между собой каналов делают платформу удобным инструментом для наблюдения за беларусами за рубежом, доксинга, дискредитации, запугивания и координации кампаний преследования. В отдельных случаях авторы Telegram-каналов также применяют инструменты ИИ для создания и распространения дипфейков и иных синтетических материалов – подробнее об этом будет описано далее, на примере проекта «Нейрокомикс».

Facebook и Instagram используются иначе: они содержат больше биографической и визуальной информации, что позволяет устанавливать личность, анализировать социальное окружение и идентифицировать участников публичных мероприятий, а также вести скрытые информационные операции через поддельные аккаунты. СМИ фиксируют случаи, когда представители беларусских силовых структур предлагали активистам за рубежом сотрудничество от имени фиктивного женского профиля в Facebook: в июне 2025 года об этом сообщал «Белсат», а в других задокументированных случаях отсутствие ответа на подобные обращения сопровождалось последующим давлением на членов семьи активиста в Беларуси.

В отношении платформ компании Meta открытые источники подтверждают как использование связанных с КГБ поддельных аккаунтов в рамках скрытых информационных операций, так и массовый сбор данных об активности пользователей: в 2021 году Meta удалила 41 аккаунт Facebook, пять групп и четыре аккаунта Instagram из сети фиктивных профилей, выдававших себя за журналистов и активистов из стран ЕС, и установила связь этой сети с беларусским КГБ. В мае 2024 года в Telegram-каналах, связанных с ГУБОПиК и государственной пропагандой, были опубликованы массивы персональных данных пользователей Instagram, взаимодействовавших с независимыми беларусскими СМИ: одна из таблиц содержала сведения более чем о 46 тысячах аккаунтов, поставивших отметки «Нравится», другая – более чем о 10 тысячах пользователей, оставивших комментарии.

По мере перемещения аудитории в TikTok и Threads государственный мониторинг распространяется и на эти площадки: в июне 2026 года Следственный комитет Беларуси публично заявил об усилении мониторинга публикаций и комментариев в обеих сетях – с прицелом на материалы, которые власти относят к ложной информации, разжиганию социальной вражды и реабилитации нацизма. Пока эти платформы используются прежде всего для массового поиска критических и быстро распространяющихся публикаций. Объем документированных случаев их применения именно для транснациональных репрессий заметно меньше, чем в отношении Telegram, однако это сопоставление требует осторожности: мониторинг TikTok и Threads был публично заявлен лишь в июне 2026 года, тогда как практики в Telegram документируются с 2020 года.

1.2. Аффилиация Telegram-каналов с государственными органами Беларуси

Открытые источники указывают на разную степень связи исследуемых Telegram-каналов с государственными органами Беларуси, поэтому уровень доказанности этой связи следует оценивать отдельно для каждого ресурса. Наиболее надежен он там, где аффилированность подтверждается прямыми и публично доступными сведениями: официальным статусом, публикацией материалов от имени государственного органа, сведениями об администраторах, заявлениями представителей власти либо выводами авторитетных расследований, технологических компаний и правозащитных организаций. В отдельный период аффилированность части подобных ресурсов, прежде всего связанных с ГУБОПиК, не скрывалась и даже прямо указывалась в названиях каналов («ГУБОП», «ГУБОПиК», «#НЕГУБОП»).

Слабее уровень доказанности у формально анонимных ресурсов, организационный статус которых публично не установлен, однако совокупность косвенных признаков может свидетельствовать об устойчивой связи или координации с государственными органами. К таким признакам относятся эксклюзивный или опережающий доступ к материалам задержаний и

обысков, публикация сведений, которые в соответствующий момент могли находиться только в распоряжении силовых структур, синхронность публикаций с официальными действиями, систематическое воспроизведение государственной риторики и участие в согласованных кампаниях против конкретных лиц или организаций. Наличие одного такого признака само по себе не является достаточным доказательством государственной аффилированности: оценка каждого ресурса должна опираться на совокупность данных, повторяемость наблюдаемых практик и качество доступных источников.

Важная методологическая оговорка касается и нестабильности самой Telegram-экосистемы: часть ресурсов, связанных с беларусскими силовыми структурами, неоднократно блокировалась (основная волна блокировок пришлась на 2022-2024 годы) и впоследствии восстанавливалась под новыми именами, юзернеймами и форматами.

Прежде чем разделять эти каналы по степени связи с государством, стоит пояснить и о том, что они собой представляют. Большинство из них распространяет материалы силового происхождения: фотографии и видео задержаний, «покаянные видео», сведения из уголовных дел, данные о преследуемых по политическим мотивам. Роль каналов при этом разная: одни первыми публикуют такие материалы, другие систематизируют их в доксинговые реестры «экстремистов», третьи используют уже опубликованное для травли конкретных людей. Общее у них то, что значительная часть контента поступает из силовых структур и недоступна обычным СМИ, а сами каналы воспроизводят официальную риторику властей. Поэтому вопрос об их связи с государством и оказывается центральным.

Для целей исследования рассматриваемые ниже 11 каналов – «Невольфович», «Книга ГУ «БАЗА»», «Обратная сторона», «ОС Exclusive», «Пульс Гродно», «Первый рубеж», «Людажоры», «ЖС Premium», «КрысолOFF», «Белорусский фронт» и «#знайанархиставлицо» – описываются по двум самостоятельным основаниям, которые важно не смешивать: по уровню доказанности связи с государством и по функциональной роли в доксинговой экосистеме. Первое основание отвечает на вопрос, насколько надежно установлена принадлежность ресурса, второе – какую операцию он выполняет с персональными данными. Эти основания не совпадают: канал может иметь документально подтвержденную аффилиацию и при этом выполнять функцию травли, и наоборот – быть формально анонимным, но систематически выступать первоисточником силовых материалов.

По уровню доказанности связи с государством каналы выборки распадаются на три группы. К первой относятся ресурсы, чья аффилиация подтверждена документально: «Невольфович» (Главное управление идеологической работы Министерства обороны), «Обратная сторона» (Управление информации и общественных связей МВД) и «Людажоры» (обозреватель издательского дома «Беларусь сегодня», учрежденного Администрацией президента). Ко второй – ресурсы, связь которых с силовым блоком следует из самоописания, ведомственных хэштегов, комментариев сотрудников от первого лица и регионального профиля, но документально не подтверждена: «Книга ГУ «БАЗА»», «Пульс Гродно», «Первый рубеж» и «#знайанархиставлицо». К третьей – формально анонимные ресурсы, для которых доступна лишь совокупность косвенных признаков: «ЖС Premium», «ОС Exclusive», «КрысолOFF» и «Белорусский фронт».

По функциональной роли те же каналы распределяются иначе. Первичную публикацию силовых материалов – видео задержаний, фрагментов допросов, оперативных сведений, получаемых раньше или помимо СМИ, – обеспечивают «Обратная сторона», «ОС Exclusive», «ЖС Premium» и «Белорусский фронт». Систематизацию этих материалов в долговременный доксинговый реестр ведут «Книга ГУ «БАЗА»» и «#знайанархиставлицо». Региональную ретрансляцию и локализацию персональных данных выполняют «Пульс Гродно» и «Первый рубеж». Функцию усиления и травли – повторного распространения уже опубликованных сведений с их эмоциональным оформлением и превращением идентификации в кампанию публичного унижения – выполняют «КрысолOFF» и «Людажоры». Более широкие пропагандистские задачи, включая легитимацию силовой повестки, решают «Невольфович» и «Белорусский фронт». Роли не являются взаимоисключающими: «Белорусский фронт» выступает одновременно первоисточником и пропагандистской площадкой,

а «Людажоры» сочетают травлю с самостоятельным производством контента. Ниже представлена характеристика каждого из этих каналов.

«Невольфович» специализируется на новостях и комментариях о беларусском силовом блоке. Доксинг не является его единственной функцией, однако канал участвует в формировании среды, где публикация сведений об «экстремистах» и фигурантах силовых кампаний представляется допустимой и общественно значимой: он репостит официальные ведомства, интерпретирует задержания и распространяет «инсайды», легитимируя силовую версию событий. Связь канала с Министерством обороны Беларуси получила весомое подтверждение в феврале 2024 года, когда канал случайно опубликовал, а затем удалил документ с анализом распространения интервью министра обороны Виктора Хренина: в свойствах файла было указано, что он создан в Главном управлении идеологической работы Минобороны – структурном подразделении военного ведомства, отвечающем за идеологическую и информационную работу. Этот эпизод позволяет с высокой степенью уверенности характеризовать «Невольфович» не просто как провластный ресурс, а как канал, непосредственно связанный с информационной инфраструктурой Министерства обороны Беларуси.

«Книга ГУ «БАЗА»» наиболее близка к формату систематизированного доксингового реестра. В собственном описании канал называет себя «красной книгой вымирающего вида белорусских экстремистов» и прямо обозначает себя как «близкий к силовикам ресурс»; в публикациях систематически используются официальные ведомственные хэштеги (например, #губопик_мвд), а отдельные материалы включают комментарии представителей ГУБОПиК МВД от первого лица. Архив канала также содержит подборки задержаний и материалы, обозначенные как эксклюзивы силовиков, – примером служит публичная лента публикаций. Такая структура позволяет не только разово идентифицировать человека, но и поддерживать долговременное досье, доступное для повторного использования другими каналами. СМИ регулярно характеризуют «Книгу ГУ «БАЗА»» как канал ГУБОПиК или ресурс, приближенный к силовикам, однако открытых данных о его конкретных администраторах нет; самоописание и характер материалов дают высокий уровень уверенности в тесной связи с силовым блоком.

«Обратная сторона» публикует значительный объем криминальной и оперативной информации, включая фотографии задержанных, их возраст, населенный пункт и обстоятельства предполагаемого правонарушения. Открытый архив канала показывает, что он позиционирует себя как площадка, показывающая то, что «не видят другие», и использует отдельного бота обратной связи. Связь канала с Министерством внутренних дел Беларуси получила документальное подтверждение в феврале 2023 года, когда в открытом доступе случайно оказался график дежурств его администраторов: согласно опубликованным данным, канал курировало Управление информации и общественных связей МВД, а в его ведении участвовали сотрудники центрального аппарата и региональных подразделений ведомства, включая работников милицейских пресс-служб.

Канал публикует оперативные материалы правоохранительных органов, сведения и видеозаписи задержаний, в том числе так называемые «покаянные видео», а также информацию о людях, преследуемых по политическим мотивам, что видно по архиву его публикаций. В политически чувствительных случаях такая модель превращает оперативную сводку в инструмент деанонимизации и стигматизации еще до судебного решения, однако значительная часть публикаций относится к обычной криминальной хронике, поэтому квалифицировать весь контент канала как доксинг нельзя. В целом «Обратную сторону» можно характеризовать как неофициальный информационный ресурс, непосредственно встроенный в коммуникационную инфраструктуру МВД Беларуси.

«ОС Exclusive» тематически и стилистически близок к «Обратной стороне» и публикует оперативные криминальные материалы: фотографии подозреваемых и задержанных, возраст, регион проживания и обстоятельства дел; публичная лента канала показывает, что он позиционирует себя как отдельный «эксклюзивный» источник с собственным ботом. Канал

регулярно перепечатывает сообщения МВД Беларуси, публикует сведения о подозреваемых и задержанных, включая их возраст, место проживания, фотографии и обстоятельства уголовных дел, а также распространяет позитивные материалы о работе милиции – это видно по архиву публикаций канала, где наряду с прямыми репостами МВД размещаются тексты, основанные на оперативной информации региональных подразделений.

Политический доксинг в доступной выборке выражен слабее, чем у «Книги ГУ «БАЗА»» или «ЖС Premium», однако публикация идентифицирующих сведений до суда создает риск деанонимизации. Открытых данных о владельцах или формальной принадлежности «ОС Exclusive» конкретному ведомству обнаружить не удалось, однако регулярный доступ к милицейским материалам, систематическое воспроизведение официальной позиции правоохранительных органов и сходство названия с каналом «Обратная сторона» позволяют характеризовать его как ресурс, встроенный в провластный информационный контур. На преемственность указывает и хронология: «Обратная сторона» прекратила публикации 28 января 2026 года, а «ОС Exclusive» начал их 3 февраля 2026 года, то есть спустя шесть дней (см. п. 1.3). Этого, однако, недостаточно, чтобы утверждать, что оба канала управляются одной редакцией. В контексте доксинга «ОС Exclusive» выполняет прежде всего вспомогательную функцию: распространяет идентифицирующие сведения о фигурантах дел и способствует их публичной стигматизации, хотя не является специализированной базой политических противников.

«Пульс Гродно» выполняет функцию регионального узла и, по имеющимся открытым данным, находится в ведении 9-го управления ГУБОПиК по Гродненской области: наряду с общими новостями региона канал распространяет материалы МВД, прокуратуры и государственных медиа, а в политически мотивированных случаях – фотографии и сведения о задержанных. Его роль в доксинговой экосистеме состоит в локализации информации: персональные данные связываются с конкретным городом, местом работы, учебы или местным сообществом, что повышает вероятность оффлайн-давления. Канал присутствует в TGStat под тем же брендом и включался в официальные подборки гродненских информационных ресурсов; независимое исследование провластного беларусского Telegram (Центр новых идей, февраль-март 2025 года, ручная разметка и автоматизированный анализ около 22,5 тысяч постов по 16 каналам) относит «Пульс Гродно» к числу немногих ресурсов, где доля репостов превышает 50% всего контента, то есть по сути к агрегаторам официальных новостей. По собственным данным настоящего исследования доля репостов у этого канала за 2023-2026 годы ниже – 30,6% (см. п. 1.3); расхождение объясняется разными периодами и методиками подсчета: Центр новых идей анализировал выборку за февраль-март 2025 года, тогда как здесь учитывается весь массив публикаций канала за три с половиной года.

«Первый рубеж», по имеющимся открытым данным, находится в ведении 6-го управления ГУБОПиК по Брестской области и прямо определяет свою тематику как «антиэкстремистскую повестку Брестского региона». Канал публикует материалы о задержаниях, фотографии предполагаемых участников протестов и эмигрантов, а также сообщения, подчеркивающие осведомленность правоохранительных органов о местонахождении людей; правозащитные медиа используют публикации канала как источник кадров задержаний – например, «Белсат» ссылался на него при описании репрессий в Брестской области. Канал имеет самую высокую среди рассмотренных ресурсов долю репостов – 56% всех публикаций (см. п. 1.3), то есть работает преимущественно как ретранслятор чужого контента, а не как первоисточник. Это, однако, не отменяет наличия собственного канала доступа: оставшиеся 44% приходятся на самостоятельные публикации с региональной «антиэкстремистской» повесткой и материалами задержаний, получение которых предполагает взаимодействие с силовыми структурами Брестской области.

«Людажоры» – один из ресурсов, чья аффилированность подтверждена документально. Автором «Людажоров», как установили журналисты, выступает обозреватель издания «СБ. Беларусь сегодня» Юрий Терех. Учредителем издательского дома « Беларусь сегодня» выступает Администрация президента Беларуси, что придает связи редакции с государственными структурами формальный, институциональный характер. Сам Терех публично называет себя автором проекта «Нейрокомикс» – сатирического формата с использованием контента,

сгенерированного искусственным интеллектом, регулярно публикуемого в «СБ. Беларусь сегодня» с апреля 2023 года; в одной из публикаций автор указывает редакцию как заказчика этого контента.

«Людажоры» функционирует как многофункциональный инструмент давления, направленного прежде всего против политических эмигрантов, представителей гражданского общества и их родственников: канал сочетает систематическую дискредитацию конкретных лиц, создание и распространение ИИ-контента с образами оппозиционных деятелей, публикацию и систематизацию персональных данных и информационные провокации, а также участвует в легитимации государственного преследования. Отдельные публикации указывают и на участие канала в распространении сведений из взломанных баз данных. С учетом институционального статуса редакции и регулярности проекта «Нейрокомикс» корректно рассматривать его как первый в Беларуси институционализированный формат политической пропаганды на основе ИИ-генерации, а не как личную инициативу отдельного автора.

«ЖС Premium» продолжает линию ранее удаленного канала «Желтые сливы» и использует персонализацию как один из основных способов давления: в публикациях появляются фотографии и видео задержанных, их имена, предполагаемые правонарушения и фрагменты материалов силового контура. Собственная страница канала содержит ссылки на сайт и другие площадки, что указывает на стремление сохранить аудиторию и инфраструктуру за пределами Telegram. Для доксинга канал важен прежде всего как место первичной публикации идентифицирующих сведений: собственный контент составляет около 98% его публикаций (см. п. 1.3), тогда как дальнейшее распространение и эмоциональное оформление этих материалов берут на себя другие участники экосистемы.

На тесную связь канала с государственно-силовым информационным контуром указывает характер его публикаций: он получал видео задержаний, фрагменты допросов и другие материалы, доступные преимущественно правоохранительным органам. В частности, канал одним из первых распространил видео с задержанным Романом Протасевичем. В открытых источниках «Желтые сливы» связывают с сотрудниками государственных медиа, прежде всего с Александром Бенько из издательского дома « Беларусь сегодня»: эта версия возникла после того, как в опубликованном каналом скриншоте была обнаружена аватарка его аккаунта, а после распространения информации изображение удалили. Этот эпизод, однако, указывает лишь на возможную причастность Бенько и не доказывает, что он был владельцем или единственным автором канала. Высказывалось и предположение о возможной причастности бывшего сотрудника ОНТ Андрея Александрова, однако оно основано на свидетельстве бывшей коллеги и документально не подтверждено.

«КрысолOFF» представляет более агрессивный тип доксинговой практики, соединяющий идентификацию человека с травлей, уничижительной лексикой и демонстративным вторжением в личную жизнь: канал публикует сведения об оппозиционных активистах, журналистах и эмигрантах – фотографии, данные о работе, образовании, семейных и личных связях, – сопровождая идентификацию уничижительной и нередко сексуализированной риторикой. Сам канал описывает свою деятельность как высмеивание и преследование «змагаров», что отражено в его публичном архиве.

Роль канала в сети заключается прежде всего в эмоциональном усилении материалов, уже появившихся у силовиков или на крупных провластных площадках, а не в их первичном получении. Формальная принадлежность «КрысолOFF» конкретному государственному органу или редакции публично не установлена. Вместе с тем канал встроен в провластную информационную сеть: его публикации регулярно распространяет сотрудник государственного телеканала СТВ Григорий Азаренок, в том числе размещая прямые ссылки на материалы «КрысолOFF», а материалы канала используются другими пропагандистскими ресурсами в рамках синхронных кампаний против конкретных людей. Поэтому его корректнее характеризовать как анонимный провластный ресурс, выполняющий функцию травли и усиления доксинг-материалов, но не имеющий документально подтвержденной ведомственной аффилиации.

«Белорусский фронт» (до сентября 2025 года – «Три сестры») заслуживает отдельного рассмотрения. По данным СМИ, «Белорусский фронт» связан с Силами специальных операций Вооруженных Сил Беларуси, а в отдельных публикациях прямо утверждается, что его ведут представители этой структуры; прямых подтверждений в открытых СМИ, однако, выявить не удалось, и характеристику следует давать с этой оговоркой. В декабре 2022 года канал сыграл ключевую роль в распространении информации об инциденте с падением украинской ракеты на территории Беларуси, первым сообщив о происшествии и опередив официальные комментарии, что может рассматриваться как косвенный индикатор доступа администраторов к закрытой информации.

Канал демонстрирует устойчивую осведомленность о внутренних процессах диаспорных организаций – доступ к закрытым мероприятиям, переговорам и не опубликованным планам. Так, 12 января 2026 года он опубликовал сведения о распределении пригласительных на прием в Президентском дворце Польши со ссылкой на решения «сверху» от польской администрации президента. Значимым индикатором доступа к оперативной информации стал и эпизод, когда канал опубликовал видео пересечения Ксенией Собчак беларусско-литовской границы до того, как эта информация широко разошлась по СМИ. Одной из ключевых тактик канала является намеренное обострение внутренних противоречий в диаспорной среде: 23 июля 2025 года он опубликовал материал о предполагаемой финансовой схеме в окружении Светланы Тихановской, целью которого была дискредитация фонда взаимопомощи BY_SOL, что соответствует классической тактике транснациональных репрессий, направленной на снижение сплоченности эмигрантских сообществ через информационные вбросы. Практика создания синтетического контента этим каналом подробно рассматривается в п. 3.2.

«#знайанархиставлицо» – канал, аффилированность которого менее очевидна документально, но также не вызывает существенных сомнений на уровне совокупности признаков. Канал «#знайанархиставлицо» воспроизводит официальную риторику властей, называя анархистов «врагами суверенной Беларуси», распространяет материалы о задержаниях и уголовном преследовании и репостит публикации государственных СМИ и провластных каналов; издание Reform.news охарактеризовало ресурс, опубликовавший видео разгромленной квартиры анархиста Романа Халилова, как «приближенный к силовикам». На возможную аффилиацию указывает и доступ канала к материалам, получение которых без взаимодействия с силовыми структурами затруднительно: правозащитный центр «Вясна» сообщал, что канал опубликовал видеозапись с политзаключенным Никитой Емельяновым, снятую внутри могилевской тюрьмы №4. Публикация внутренних тюремных материалов – серьезный признак получения информации от сотрудников правоохранительных органов, хотя открытые источники не позволяют утверждать формальную принадлежность канала конкретному ведомству. По самоописанию в каталоге TGStat и архивным данным Telemetr, канал ближе всего к тематической базе данных: он собирает в одном месте фотографии, имена, политическую биографию и связи конкретных людей, поддерживая их долговременную идентифицируемость, и пересекается по тематике с «Книгой ГУ «БАЗА»».

Рассмотренные каналы различаются и по функциям, и по степени доказанности связи с государством: за одними стоит подтвержденная ведомственная принадлежность, за другими – только совокупность косвенных признаков. При этом все они получают материалы, доступ к которым обычно есть лишь у правоохранительных органов, воспроизводят одну и ту же официальную риторику и действуют согласованно в кампаниях против конкретных людей. Образуют ли они единую сеть или представляют собой разрозненные ресурсы со случайно совпадающей повесткой – это вопрос, который рассматривается в следующем разделе.

1.3. Анализ экосистемы каналов

Описание каналов по отдельности оставляет открытым главный вопрос: перед нами набор независимых ресурсов со схожей повесткой – или единая система распространения. Различие здесь не терминологическое. Если каналы независимы, каждая публикация персональных данных

остается частной инициативой отдельной редакции, а исчезновение ресурса устраняет проблему локально. Если же это связанная система, попадание сведений в один канал автоматически означает их тиражирование в остальных, а выпадение отдельного узла компенсируется другими – именно этим объясняется устойчивость экосистемы к блокировкам, о которой шла речь выше.

Ответить на этот вопрос на уровне содержания невозможно: сходная риторика, общая повестка и синхронное появление одних и тех же сюжетов одинаково хорошо объясняются и координацией, и простым следованием одному официальному источнику. Поэтому связи между каналами проверяются формально – по пересечению публикаций, техническим меткам пересылки и синхронности расписания.

Проверяемая гипотеза состоит в том, что перечисленные ресурсы не являются независимыми друг от друга источниками, а образуют общую сеть распространения контента, технически и содержательно связанную с силовыми структурами Беларуси. Результаты проверки и ее ограничения приведены в конце раздела.

Для целей этой части исследования в выборку вошли следующие каналы: «Книга ГУ «БАЗА»», «Первый рубеж», «Невольфович», «ЖС Premium», «Пульс Гродно», «Обратная сторона», «Белорусский фронт», «Людажоры», «ОС Exclusive», «КрысолOFF», «#знайанархиставлицо». Публикации 11 каналов собирались через клиентский Telegram API (MTProto) за период с 1 января 2023 года по 12 июля 2026 года и сохранялись в базе данных. Один и тот же текст, опубликованный сразу в нескольких каналах, хранится как одна запись, за которой закреплены все каналы, где он появился. Поэтому колонка «Постов» в таблице ниже показывает число публикаций в конкретном канале, а итоговое значение 102 200 – их сумму по всей выборке; самих текстов, без учета повторов в разных каналах, в массиве 96 206.

Таблица 1. Объем собранных публикаций по каналам выборки, 1 января 2023 – 12 июля 2026 года

Канал	Никнейм	Первый пост	Последний пост	Постов	Собственных
«ЖС Premium»	@zheltye_slivy_Belarus	01.01.2023	12.07.2026	39 677	38 817
«Невольфович»	@nevolf	01.01.2023	12.07.2026	23 545	23 191
«Обратная сторона»	@reverse_side2022	01.01.2023	28.01.2026	8 203	7 816
«КрысолOFF»	@ratannihilator	02.01.2023	10.07.2026	6 131	6 120
«Белорусский фронт»	@III_SESTRY	02.01.2023	09.07.2026	5 642	5 637
«Пульс Гродно»	@grodnopuls	03.01.2023	03.07.2026	5 011	3 478
«Людажоры»	@Ludazhors	03.01.2023	11.07.2026	1 194	1 189
«#знайанархиставлицо»	@anarhodnoo	09.01.2023	25.06.2026	116	115
Книга ГУ «БАЗА»	@guBAZA	01.02.2023	11.07.2026	6 951	5 165
«Первый рубеж»	@first_frontier	02.02.2023	07.07.2026	4 404	1 939
«ОС Exclusive»	@reserve_side	03.02.2026	12.07.2026	1 326	1 177
Всего				102 200	94 644

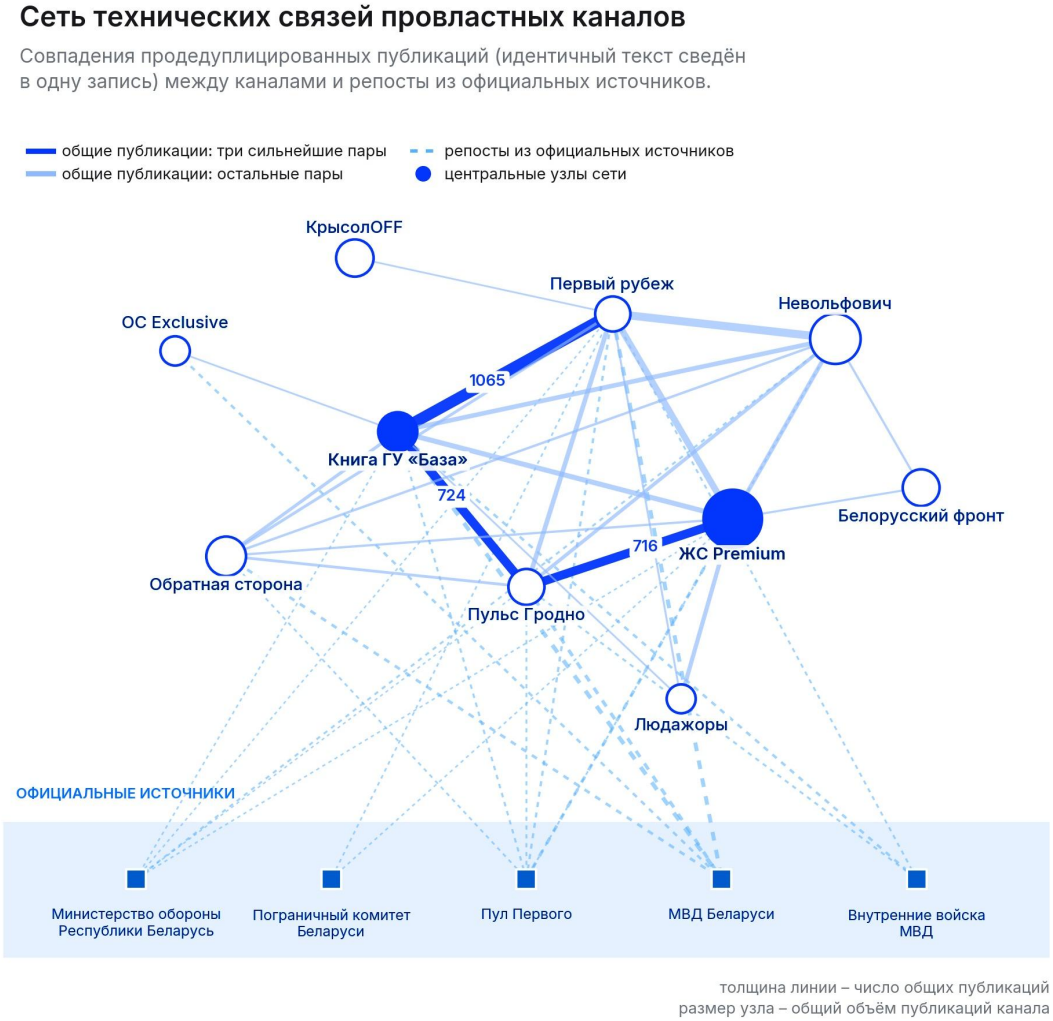
***Справочно**. Даты первого и последнего поста рассчитаны по собственным публикациям канала, без учета репостов: у пересланного сообщения в метаданных сохраняется дата оригинала, а не дата публикации в канале, поэтому по репостам границы периода определять некорректно.*
Колонка «Собственных» приведена отдельно, поскольку доля репостов по каналам различается почти в 600 раз: от 0,1% у «Белорусского фронта» до 56,0% у «Первого рубежа». Расчеты суточной и недельной активности выполнены только по собственным публикациям.
Срез базы: 12 июля 2026 года. Каналы «Обратная сторона» и «ОС Exclusive» наблюдались не весь период: первый прекратил публикации 28 января 2026 года, второй начал 3 февраля 2026 года.

Связанность каналов проверялась двумя способами:

- совпадение текстов публикаций – при обработке сообщения с дословно совпадающим текстом сводятся в одну запись, за которой закрепляются все каналы, где этот текст был опубликован; показателем служит число записей, опубликованных более чем в одном канале выборки;
- атрибуция репостов – у сообщений, пересланных средствами Telegram (признак is_repost=true), сохраняется служебное поле fwd_from – метка пересылки, которую платформа записывает автоматически; в ней указан telegram-id – постоянный числовой идентификатор канала-источника, не меняющийся при смене названия или адреса. Это позволяет построить граф направленных технических связей между каналами.

Оба способа имеют ограничения – совпадение текстов не учитывает пересказ и завышается на шаблонных сообщениях, а граф репостов достроен только для каналов внутри выборки.

Ниже показан граф технических связей ключевых каналов группы. Толщина сплошной линии соответствует числу общих (совпадающих) постов между каналами; пунктирные линии показывают репосты из общего пула официальных силовых источников (МВД Беларуси, внутренние войска МВД, Минобороны, погранкомитет, БЕЛТА, президентский «Пул Первого»).



Источник: собственная база публикаций 11 каналов, Telegram API. Срез: 01.01.2023 – 12.07.2026.
Показаны связи от 20 совпадений.

Рис. 1. Сеть связей между ключевыми каналами группы.

Три пары с наибольшим числом совпадений – «Книга ГУ «БАЗА»» – «Первый рубеж» (1066), «ЖС Premium» – «Пульс Гродно» (740) и «Книга ГУ «БАЗА»» – «Пульс Гродно» (725) – заметно превосходят остальные по силе связи. Чаще других в этих парах фигурируют «Книга ГУ «БАЗА»» и «Пульс Гродно» (по две пары из трех), что позволяет рассматривать их как наиболее связанные узлы выборки. Сила отдельных пар при этом не тождественна центральности: «ЖС Premium» – крупнейший канал выборки, но доля репостов у него минимальна (около 2%), то есть он выступает источником контента, а не его распределительным узлом.

Проверка на уровне отдельных сообщений показывает, что эти совпадения почти целиком созданы штатными репостами: из 1066 общих публикаций пары «Книга ГУ «БАЗА»» – «Первый рубеж» независимыми, то есть опубликованными обоими каналами самостоятельно, оказались лишь четыре, а у пары «ЖС Premium» – «Пульс Гродно» из 740 совпадений – ни одного. Таким образом, внутри группы совпадение текстов и граф пересылок фиксируют одно и то же явление, и самостоятельным доказательством технической связанности остается граф репостов. Исключение составляет пара «Невольфович» – «ЖС Premium», где из 221 общей публикации 54 не связаны пересылкой: эти два канала регулярно публикуют один и тот же текст независимо друг от друга, что указывает на общий источник материалов, а не на заимствование одного канала у другого.

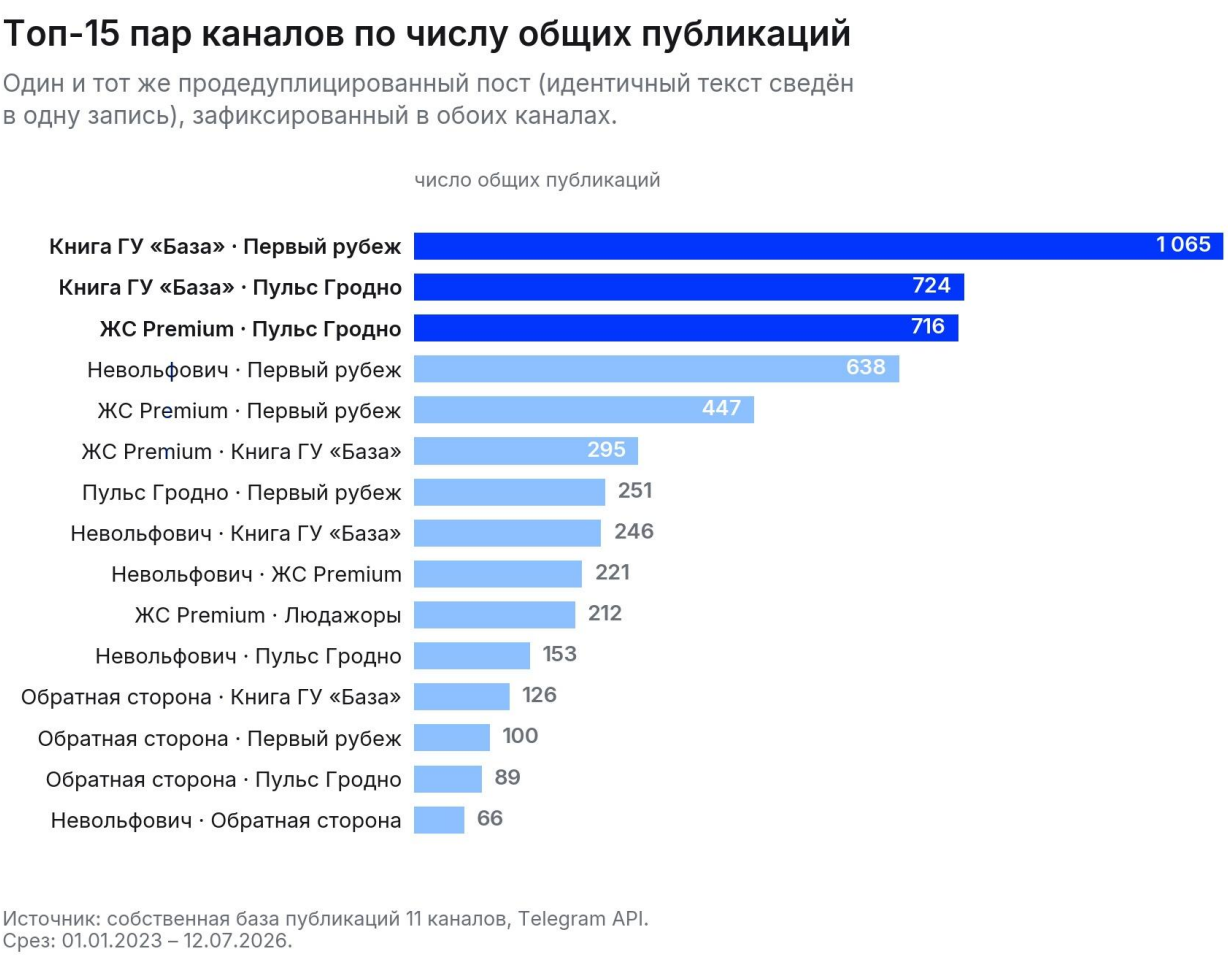
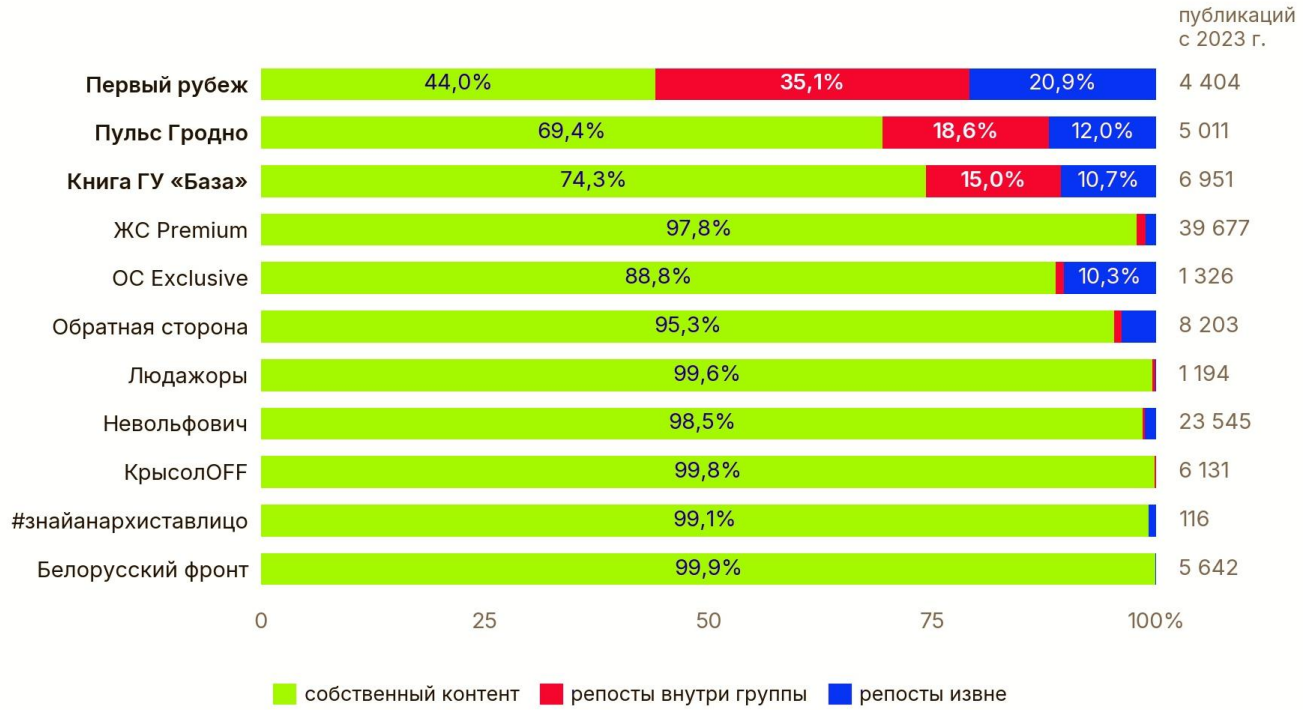


Рис. 2. Топ-15 пар каналов по числу общих (совпадающих) публикаций, 2023-2026 годы.

Для каждого канала рассчитана доля собственного контента, репостов внутри группы (из других каналов выборки) и репостов из внешних источников.

Структура контента каналов

Доля собственных публикаций, репостов из других каналов выборки и репостов из внешних источников. Подписи — для долей от 8%.



Источник: собственная база публикаций 11 каналов, Telegram API.
Срез: 01.01.2023 – 12.07.2026.

Рис. 3. Структура контента каналов.

Для канала «Первый рубеж» репосты внутри группы составляют 35% всех публикаций – это не побочная практика, а основной режим его работы: канал в значительной степени функционирует как ретранслятор контента других участников сети. Аналогичная, хотя и менее выраженная картина наблюдается у «Пульса Гродно» (18,6%) и «Книги ГУ «БАЗА»» (15,0%).

Помимо содержательных и технических связей, проверена синхронность расписания публикаций: совпадение пиков активности – слабый косвенный признак. Оно совместимо с институциональным, штатным ведением каналов, но само по себе не свидетельствует ни о едином администрировании, ни о принадлежности к государственным органам, поскольку сходный график характерен для любой профессиональной редакционной работы.

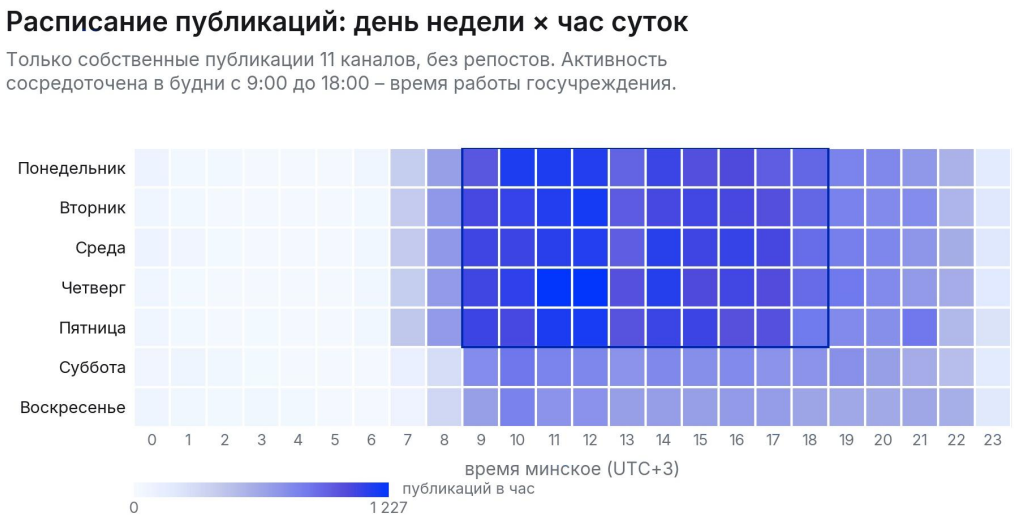


Рис. 4. Суммарное распределение публикаций группы по дням недели и часам суток.

Публикации группы концентрируются в будние дни в интервале 9:00-18:00; после 22:00 активность резко спадает, минимум приходится на 3:00-6:00. В субботу и особенно в воскресенье общий уровень активности заметно ниже. Это профиль штатной работы в рабочие часы: он практически исключает модель ведения каналов волонтерами в свободное время, но сам по себе не отличает государственный орган от любой другой профессиональной редакции.

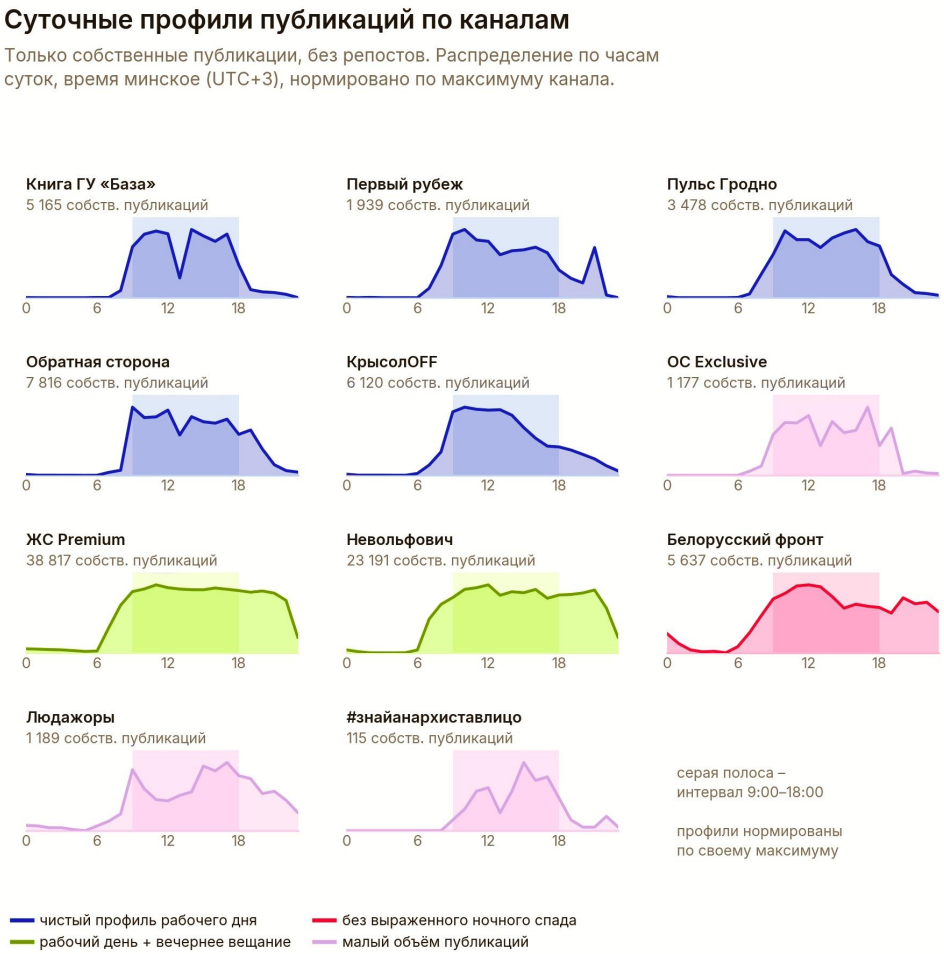


Рис. 5. Распределение публикаций по часам суток для всех 11 каналов выборки, нормировано по максимуму каждого канала.

У большинства каналов группы – «Книга ГУ «БАЗА»», «Первого рубежа», «Пульса Гродно», «Обратной стороны», «КрысолOFF» – схожий профиль рабочего дня: на интервал 9:00-18:00 приходится от 75% до 89% собственных публикаций, с резким спадом к ночи. У «ЖС Premium» и «Невольфовича» профиль шире и включает вечерние часы – эти два канала ведут более «живое» неформальное вещание в дополнение к ретрансляции. «Белорусский фронт» выделяется на общем фоне: заметная активность сохраняется и поздним вечером, без выраженного ночного провала, что отличает его от остальных участников группы. Малообъемные каналы («ОС Exclusive», «#знайанархиставлицо») при небольшом числе публикаций также концентрируются в дневных часах, хотя статистическая значимость их пиков ниже из-за малого объема данных. Отдельно выделяются «Людажоры»: почти треть их публикаций (31,8%) приходится на субботу и воскресенье – самый высокий показатель в выборке, что отличает их от каналов со строгим рабочим режимом.

В совокупности рассмотренные каналы образуют не единую формально оформленную организацию, а функционально связанную экосистему. Первичное поступление силовых материалов обеспечивают «Обратная сторона», «ОС Exclusive», «ЖС Premium» и «Белорусский фронт»; систематизацию этих материалов в долговременные доксинговые реестры – «Книга ГУ «БАЗА»» и «#знайанархиставлицо»; региональную ретрансляцию и локализацию – «Пульс Гродно» и «Первый рубеж»; усиление и травлю – «КрысолOFF» и «Людажоры». «Невольфович» и «Белорусский фронт» решают более широкие пропагандистские задачи, но поддерживают ту же инфраструктуру через легитимацию силовой повестки и распространение оперативных сведений. Роли не являются взаимоисключающими: «Белорусский фронт» одновременно выступает первоисточником и пропагандистской площадкой, а «Людажоры» сочетают травлю с самостоятельным производством контента. Основными признаками связи выступают взаимные репосты, сходная лексика, синхронное появление материалов задержаний, общие региональные рамки и доступ к информации, которая обычно возникает в распоряжении правоохранительных органов.

Интерпретация приведенных данных ограничена рядом факторов. Во-первых, совпадение постов и репосты доказывают информационную и техническую связанность каналов (общую сеть распространения контента), но не доказывают автоматически единое административное управление или общих владельцев. Синхронность расписания публикаций также носит косвенный характер и должна интерпретироваться с осторожностью. Во-вторых, как отмечалось выше, нестабильность Telegram-экосистемы затрудняет учет уникальных акторов: в отдельных случаях одно институциональное ядро последовательно использовало несколько названий («ГУБОП», «ГУБОПиК», «Центр «Э»», «#НЕГУБОП»), поэтому подсчет только уникальных username может искусственно завышать число независимых каналов и занижать роль институциональных центров. Эти оговорки касаются интерпретации данных, но не ставят под сомнение сам факт существования общей экосистемы.

Важно оговорить границы этой выборки. Одиннадцать рассмотренных каналов – не перечень всех акторов цифрового преследования, а срез инфраструктуры распространения: ресурсов, через которые силовые материалы попадают в публичное поле и тиражируются. Значительная часть операций, разобранных в следующей главе, идет по другим маршрутам – через государственное телевидение, официальные пресс-службы, публичные реестры и отдельные специализированные каналы, не входящие в выборку. Инфраструктурный анализ показывает, как устроена среда распространения; типология следующей главы – какие именно операции через нее и помимо нее проводятся.

2. Типология кейсов дискредитации, доксинга и разведывательных операций в цифровой среде

2.1. Пропаганда и дискредитация через фабрикацию контента

Беларусские государственные акторы систематически производят и распространяют сфабрикованный или намеренно искаженный контент для дискредитации оппозиции, гражданского общества и независимых медиа, находящихся за рубежом. Операции этого типа объединяет общая логика: создать нарратив, который выглядит достоверно, распространяется быстро и опровергается медленнее, чем наносит ущерб. Инструментарий варьируется от псевдодокументальных фильмов с показаниями задержанных до синтезированных ИИ медиафайлов и фейковых заявлений о взломах. Во всех случаях цифровые каналы, включая те, что описаны выше, используются как основная среда распространения, позволяющая доставить контент напрямую до целевой аудитории быстро и с широким охватом.

2.1.1. Создание фейков против активистов и продемократических организаций

В отличие от материалов, опирающихся на реальные уголовные дела и показания (раздел 2.1.4), операции этого типа строятся на полностью или частично сфабрикованном контенте. Кампании такого рода преследуют цель подорвать доверие беларусской аудитории к конкретным людям и структурам, создать негативный образ оппозиции в глазах международных партнеров и сформировать у самих активистов ощущение постоянной уязвимости.

Наиболее массовый формат – это вбросы без каких-либо верифицируемых доказательств, которые транслируются через государственное телевидение и радио, после чего тиражируются провластными Telegram-каналами и аккаунтами в социальных сетях.

- Кейс Офиса Светланы Тихановской. В декабре 2025 года пропагандист Григорий Азаренок в эфире СТВ заявил, что офис Тихановской получил от европейских структур €30 млн и купил недвижимость во Флоренции под свой офис. Данную информацию он сопроводил упоминанием гибели беларусских мигрантов в Польше, тем самым создав нарратив о том, что оппозиционное руководство тратит деньги на свое роскошное благополучие, пока рядовые эмигранты умирают на улице. Фактчекеры Беларусского Расследовательского центра (БРЦ) установили, что за громким заявлением стояло открытие двух совершенно разных проектов беларусской диаспоры – шелтера для репрессированных и центра беларусского демократического сообщества. Ни один из проектов не имел отношения к покупке недвижимости. Оба помещения арендованы у итальянских владельцев по официальным договорам, шелтер полностью существует за счет итальянского финансирования, а Офис Тихановской лишь частично участвует в расходах на содержание центра.

Наряду с простыми вбросами широко применяется и более технически сложный формат – псевдодокументальные расследования, в которых срежиссированные съемки скрытой камерой или аудиозаписи с намеренно обрезанным контекстом подаются как неопровержимые доказательства преступной деятельности конкретных людей.

- Кейс Павла Латушко. Павел Латушко – бывший министр культуры Беларуси и посол, один из немногих высокопоставленных чиновников, открыто перешедших на сторону оппозиции после выборов 2020 года. С тех пор он возглавляет Народное антикризисное управление (НАУ) в эмиграции и является одной из ключевых фигур беларусских демократических сил. 6 августа 2025 года ОНТ выпустил фильм, в котором утверждалось, что летом 2020 года Латушко якобы

планировал поджечь объединенный штаб оппозиции, чтобы «создать сакральную жертву». В качестве доказательств пропагандисты показали видео с оперативной съемки низкого качества, на котором человек, похожий на политика, стоит спиной к камере (его лицо не видно) и аудиозапись телефонного разговора с голосом, похожим на голос Латушко. Латушко полностью опроверг обвинения, назвав их абсурдом, и сообщил, что после выхода сюжета получал угрозы убийством. НАУ квалифицировал операцию как «спецоперацию КГБ информационного, пропагандистского и силового характера», указав на то, что фильм вышел одновременно с другими дискредитационными кампаниями против руководства организации.

2.1.2. Дипфейки как инструмент дискредитации

Дипфейки – это синтезированные с помощью искусственного интеллекта медиаматериалы: фотографии, видео или аудиозаписи, в которых внешность, голос или слова реального человека подделываются с высокой степенью правдоподобия. Беларусские власти и связанные с ними акторы используют эту технологию для дискредитации оппозиционных деятелей через фейковые видеообращения от имени лидеров оппозиции и сфабрикованные компрометирующие аудиоматериалы, а также для сексуализированных атак на женщин-активисток с целью их запугивания и вытеснения из публичного поля. Ниже приводятся определенные случаи такого преследования, в то время как более систематическое производство такого контента рассматривается в третьей главе.

- Кейс Светланы Тихановской. За день до президентских выборов, которые проходили в Беларуси 26 января 2025 года, в социальных сетях появилось реалистичное видео, в котором лидерка демократических сил Светлана Тихановская якобы слагала с себя полномочия. Фейк оказался достаточно убедительным, чтобы в его подлинность поверили многие, в том числе другие публичные оппозиционные деятели. Видео было оперативно опровергнуто командой Тихановской.
- Кейс Марины Ментусовой. 9 апреля 2025 года на Pornhub появились фейковые сексуализированные фотографии ведущей YouTube-шоу «Обычное утро» Марины Ментусовой. Сама Ментусова квалифицировала произошедшее как спланированную акцию и цифровое насилие, направленное на запугивание женщин в публичном поле.
- Кейс Алины Харисовой. В июне 2026 года пропагандист Роман Протасевич в эфире СТВ представил аналитика Офиса Тихановской Алину Харисову как агента, якобы завербованного КГБ: по версии сюжета, сотрудники спецслужбы вышли на нее под видом представителей Службы безопасности Украины (СБУ) и убедили передавать внутреннюю информацию об Офисе Тихановской. По данным ASTRA, ключевым инструментом сюжета стали сгенерированные с помощью ИИ аудиосообщения: голос Харисовой был синтезирован на основе ее публичных записей и использован для создания фейковых отчетов перед «кураторами», в которых она якобы сообщала сведения о внутренней работе оппозиционных структур.

2.1.3. Фейковые заявления о взломах ресурсов независимых организаций

Провластные акторы также публикуют скриншоты переписок, видеозаписи внутренних мероприятий и базы данных пользователей оппозиционных платформ, правозащитных центров и фондов солидарности, утверждая, что материалы получены в результате компрометации их систем. При этом в действительности речь может идти о данных из сторонних утечек; материалах, изъятых при задержаниях годами ранее, или о полностью сфабрикованных заявлениях о получении доступа. Механика рассчитана на асимметрию реакции: организация вынуждена тратить ресурсы на опровержение, ее аудитория получает повод усомниться в надежности

структуры, а сам нарратив о взломе живет в информационном пространстве независимо от того, было ли опровержение услышано.

Один из таких сценариев – полностью сфабрикованные заявления об утечке, где предполагаемая база данных содержит технические несоответствия, исключающие ее подлинность.

- **Кейс «Голоса».** В апреле 2021 года в Telegram-канале «Утечки информации» появилось объявление о продаже «SQL-дампа» с номерами телефонов 768 418 пользователей бота «Голоса». Платформа опровергла утечку, указав на технически грубые ошибки в предполагаемой базе: у всех записей был одинаковый chat_id, что невозможно. Разработчики также подтвердили, что вообще не хранят телефонные номера в открытом виде. Показательно, что параллельно неизвестные разослали пользователям Telegram сообщения с фейкового канала, имитирующего «Голос», о том, что они «внесены в некую базу данных».

В некоторых случаях давно известные силовикам данные могут переупаковываться и подаваться как «сенсационный взлом», создавая репутационный ущерб без какого-либо реального инцидента безопасности.

- **Кейс ПЦ «Вясна».** В апреле 2026 года провластные Telegram-каналы распространили видеозаписи семинаров для волонтеров «Вясны» 2019–2020 годов, представив их как результат «взлома» системы правозащитного центра и якобы доказательства спланированной подготовки к протестным акциям. «Вясна» опровергла версию о взломе, пояснив, что речь идет о материалах, которые частично распространялись среди волонтеров в тот период, а часть из них еще в 2020–2021 годах уже находилась в распоряжении силовых органов и использовалась в рамках уголовного дела против Алеся Беляцкого, Владимира Лабковича и Валентина Стефановича. Признаков свежей утечки или взлома, а также угрозы персональным данным обычных людей выявлено не было.

В ряде случаев провластные акторы не фабрикуют утечку с нуля, а берут данные из открытых публичных источников: реестров юридических лиц, открытых сервисов, публичных баз, и представляют их как результат взлома закрытых систем организации.

- **Кейс Павла Либера / «Новая Беларусь».** В мае 2025 года Следственный комитет опубликовал заявление о якобы состоявшемся сливе данных платформы «Новая Беларусь» и идентификации более 1000 пользователей, которых квалифицировали как участников «экстремистского формирования». Операция была многоуровневой: сначала в сети появилась «база данных», которую предлагали купить за $3000, затем некий молодой человек, представившийся стартапером, записал видео с «подтверждением» утечки, читая текст по бумажке со словесными конструкциями, характерными для силовиков; следом появились «покаянные видео» в Instagram от двух девушек. Основатель платформы Павел Либер опроверг утечку: предполагаемая база содержала данные на польском языке из открытых публичных реестров, не пересекающиеся с реальными данными платформы, которая в принципе не собирала персональные данные в идентифицируемом виде. По его оценке, за «слитыми данными» стояли открытые записи беларусских бизнесов из независимого сервиса Bymapka.

В то же время в ряде случаев провластные акторы присваивают себе авторство реальных утечек из посторонних источников, встраивая их в нужный нарратив.

- **Кейс Вадима Кабанчука**. В январе 2025 года Telegram-канал «Книга ГУ «БАЗА»» (см. п. 1.2) опубликовал скриншоты переписок представителя Объединенного переходного кабинета Вадима Кабанчука, заявив об их взломе. Расследование Zerkalo установило, что данные были получены не беларусскими силовиками, а неизвестным хакером и опубликованы на Pastebin еще в декабре 2024 года. Силовики лишь подобрали уже существующую утечку и присвоили себе ее авторство. Сам Кабанчук не зафиксировал никаких проблем со своим аккаунтом.

2.1.4. Пропагандистская дискредитация через материалы уголовных расследований

Государственные СМИ и официальные органы систематически используют уголовные расследования против представителей оппозиции и НКО как основу для пропагандистских материалов. В отличие от тактик использования сфабрикованных данных, описанных выше, материалы такого типа строятся на реальных делах и показаниях людей.

Наиболее популярным инструментом дискредитации организаций гражданского общества такого типа служат документальные фильмы и сюжеты государственных СМИ, построенные на показаниях людей, находившихся под стражей или оказавшихся в Беларуси – добровольно или в результате принудительной экстрадиции. Формат позволяет получить «из первых уст» сведения о внутреннем устройстве организаций, именах участников и предполагаемых связях с иностранными структурами, после чего эти показания интерпретируются государственными СМИ в дискредитирующем ключе. При этом условия, при которых давались показания, и степень их добровольности остаются за кадром.

- Кейс Полка Калиновского. В ноябре 2024 года ОНТ выпустил сюжет «Бесы: как хотят захватить Беларусь» с участием Максима Ралько, представленного как «наемник Полка Калиновского». В кадре Ралько заявлял, что бойцы полка воюют на Украине не ради свободы, а готовятся к вооруженному вторжению в Беларусь: «Когда будет приказ — перейти границу». В январе 2025 года «СБ. Беларусь сегодня» опубликовала интервью с Василием Веремейчиком, доставленным в Беларусь из Вьетнама после экстрадиции. Веремейчик характеризовал полк как «инспирированный спецслужбами информационный проект», называл его командование «тикток-войсками» и описывал бойцов как «расходный материал». Оба материала строились на показаниях людей, находившихся либо под стражей, либо в уязвимом положении после принудительного возвращения в страну.
- Кейс «Радио Свобода». В январе 2025 года ОНТ выпустил документальный фильм «Свобода слова. Андрей Кузнечик» с политзаключенным бывшим сотрудником «Радио Свобода» в главной роли. Кузнечик описывал редакционную политику издания как целенаправленное продвижение западных ценностей и отсутствие реальной свободы слова внутри редакции. Показания бывшего сотрудника подавались как разоблачение организации изнутри.

Отдельно следует выделить и случаи, когда пропагандистские материалы включают не только показания задержанных, но и визуальное сопровождение в виде персональных данных: фотографии из предположительно милицейских баз данных, снимки изъятых личных документов и вещей, а также скриншоты частной переписки.

- Кейс Human Constanta. В декабре 2022 года «СБ. Беларусь сегодня» опубликовала материал «Волонтеры? Крысы! или Как работает агентура зарубежья», содержащий видео допроса задержанной правозащитницы Human Constanta Насты Лойко, который имел целью дискредитировать организацию. Материал содержал поименный список сотрудников с фотографиями (предположительно из официальных баз данных), скриншоты частной переписки Лойко с журналистами, коллегами и партнерами с их именами, а также ее личные документы об образовании. При этом вся опубликованная коммуникация, рутинная правозащитная работа, дипломы с образовательных учреждений и проектов стран Евросоюза и США была представлена как доказательство шпионажа и агентурной деятельности в пользу западных спецслужб.

Наряду с медийными форматами те же нарративы распространяются напрямую через пресс-службы силовых структур. Процессуальные заявления выдержаны в эпатажной, намеренно стигматизирующей лексике и затем тиражируются региональными государственными изданиями, создавая видимость широкого общественного резонанса.

- Кейс Координационного совета. В ноябре 2023 года Следственный комитет распространил через государственные СМИ заявление о возбуждении дела против более ста участников Координационного совета, построенное на показаниях человека, вернувшегося в Беларусь

через «межведомственную комиссию по рассмотрению обращений граждан, находящихся за рубежом, по вопросам совершения ими правонарушений» и передавшего список «ранее неизвестных правоохранительным органам предателей». Заявление было выдержано в намеренно стигматизирующей лексике: Координационный совет назывался «экстремистским муравейником», его участники «беглыми преступниками» и «предателями», а сама деятельность «финансовой пирамидой для спонсирования экстремистской деятельности».

2.2. Разведывательные операции против диаспоры и гражданского общества

Помимо этого, задокументированные случаи указывают и на систематический сбор разведывательных данных о членах диаспоры, оппозиционных структурах и гражданском обществе, в котором цифровые каналы выступают основной средой проведения таких операций. Отнесение ответственности за такие операции к беларусским государственным структурам опирается на характер собираемых данных, публичные заявления силовых органов и выводы правозащитных и технических расследований.

В зависимости от применяемого инструмента степень осведомленности жертвы варьируется: одни операции строятся на полном неведении человека о том, что его данные собираются, другие – на добровольной передаче данных под влиянием ложного доверия к имитируемому источнику, третьи предполагают прямое предложение сотрудничества с режимом. Во всех случаях цифровая среда обеспечивает анонимность операторов, масштабируемость охвата и возможность действовать против целей, находящихся за пределами физической досягаемости беларусских силовых структур.

2.2.1. Сбор данных и дезинформация через имитацию доверенных источников

Общая логика всех операций этого типа – эксплуатация доверия к знакомым организациям и каналам коммуникации. Человек думает, что взаимодействует с настоящим ботом, официальной рассылкой или реальной ссылкой на новость, что делает его уязвимым. В зависимости от конкретного инструмента цели варьируются: сбор персональных данных, деанонимизация через технические параметры устройства, дискредитация организации в глазах ее аудитории или партнеров. Инструменты нередко применяются в связке: ссылка-ловушка фиксирует IP-адрес всех, кто кликнул, а бот собирает данные тех, кто пошел дальше и решил «зарегистрироваться».

Наиболее часто применяемый инструмент для несанкционированного сбора данных оппозиционно настроенных людей – это создание Telegram-ботов, имитирующих официальные каналы оппозиционных структур. Так, человек обращается к боту, полагая, что контактирует с доверенной организацией, и добровольно передает персональные данные. Даже случайное взаимодействие с фейковым ботом беларусские суды квалифицировали как доказательство умысла на сотрудничество с оппозиционными структурами.

- **Кейс BYPOL.** В апреле 2023 года был запущен фейковый бот, имитировавший канал объединения бывших силовиков BYPOL. Ответственность за это впоследствии признали представители ГУБОПиК. Бот предлагал беларусам «проверить себя по базам силовиков». Вышедшим на связь силовики, представляясь сотрудниками BYPOL, предлагали сотрудничество: просили «актуализировать персональные данные», а затем предлагали выполнить «задание по наблюдению за порученным объектом» или «забрать содержимое тайника». За чуть больше часа около 150 человек отправили туда полные персональные данные. Пропагандисты открыто рассказали об этой операции в эфире ОНТ, сопроводив ее «покаянным» видео одного из задержанных.
- **Кейс Офиса Светланы Тихановской.** В январе 2025 года Офис Тихановской предупредил о фейковом боте, отличающемся от официального одной буквой в названии. Бот выглядел идентично официальному каналу коммуникации, при этом собирал персональные данные обращающихся и распространял дезинформацию от имени Офиса.
- **Кейс БРЦ.** В апреле 2026 года пропагандист Роман Протасевич в эфире СТВ заявил о якобы взломе Telegram-бота БРЦ. Сам БРЦ опроверг взлом, однако подтвердил существование клона

своего бота (@NovajaZiamlaBot против официального @NovajaZiamla_bot), который, по всей видимости, администрировали спецслужбы. Люди, писавшие в клон-бот, оказались под угрозой репрессий.

Аналогичные фейковые каналы имитировали правозащитные организации и их горячие линии, формы записи в Полк Калиновского, контактную форму группы «Киберпартизаны» и другие структуры.

Силовые структуры также активно эксплуатируют ссылки-ловушки, которые, в отличие от фейковых ботов, не требуют никакого осознанного заполнения данных со стороны жертвы. Достаточно кликнуть на ссылку: в момент перехода силовики автоматически получают IP-адрес, данные об устройстве, браузере и программном обеспечении. Для пользователей внутри Беларуси это критически чувствительная информация: зная IP-адрес, сотрудники силовых структур могут установить личность человека и его фактическое местонахождение. Технология получила официальное название «Web-капкан» и была описана старшим преподавателем Института повышения квалификации и переподготовки Следственного комитета в научной статье в 2021 году. На практике ловушки и боты используются параллельно в рамках одной операции: ссылка фиксирует всех кликнувших, бот же отбирает тех, кто готов к активному взаимодействию.

- Кейс «Перамога 2.0». 15 марта 2024 года на поддельном канале BYPOL появилось фейковое сообщение о запуске плана «Перамога 2.0» с фальшивыми видеообращениями от имени Светланы Тихановской и Александра Азарова. Пост содержал две ссылки: на «полную версию плана» и на Telegram-бот для «регистрации». Ссылка на план предположительно являлась ловушкой типа Web-капкан: при клике она автоматически фиксировала IP-адрес и данные устройства, при этом внешне вела на обычный контент и никак не сигнализировала жертве о том, что что-то произошло. Ссылка на бот выполняла отдельную функцию: для тех, кто пошел бы дальше, она создавала доказательство умысла. В тот же день силовики опубликовали видео с задержанным мужчиной, который сообщил: «Сегодня, находясь в интернете, увидел ссылку "Перамога 2.0", нажал на нее, ничего не произошло. А вскоре ко мне приехали гости».

Отдельную категорию операций составляют атаки, направленные на полный перехват аккаунта в мессенджере. В отличие от сбора отдельных персональных данных, компрометация аккаунта открывает доступ ко всей переписке жертвы, ее контактам и истории коммуникации, а также позволяет использовать захваченный профиль для дальнейших атак на людей из круга общения жертвы. Основными целями подобных атак становятся аккаунты в мессенджерах, наиболее распространенные в среде оппозиции и гражданского общества: Telegram и Signal.

- Кейс перехвата аккаунтов в Signal. В октябре 2025 года исследователи RESIDENT.NGO зафиксировали кампанию целевых фишинговых атак с использованием мессенджера Signal против беларусских публичных деятелей и медиа работников, проживающих за пределами Беларуси. Злоумышленники создавали профили под названием «Signal Support» с указанием легитимного домена support.signal.org как якобы связанного с ним веб-сайта, имитируя официальную поддержку сервиса. Жертве направлялось сообщение с ложным предупреждением о попытке входа в аккаунт с подозрительного устройства и локации и запросе на смену номера телефона. Для усиления паники в переписке демонстрировался поддельный индикатор скачивания данных с последующим уведомлением об их якобы успешной отправке на сторонний адрес. Жертву просили ввести команду «/cancel» для отмены подозрительного входа, тем самым подтверждая активность номера, после чего у нее запрашивали официальный 6-значный SMS-код верификации Signal. Передача кода приводила к полному перехвату аккаунта. Прямая атрибуция затруднена ввиду характера атаки, однако RESIDENT.NGO указывает на вероятную связь с беларусскими государственными структурами на основании узкой и последовательной направленности кампании против беларусской оппозиции и аффилированных с ней лиц.

Наиболее технически сложные операции направлены на установку вредоносного ПО, обеспечивающего полный удаленный доступ не только к отдельным данным или аккаунтам, но и к всему устройству сразу.

- **Кейс Ghostwriter.** В феврале 2025 года исследователи SentinelLABS зафиксировали кампанию целевых атак против активистов беларусской оппозиции, а также украинских военных и государственных структур. Атаки велись через вредоносные Excel-документы с приманками, подобранными под интересы конкретной аудитории: для беларусской оппозиции файл с названием «Политзаключенные (по судам Минска)», для украинских военных шаблоны отчетности о поставках. При открытии документа и разрешении макросов на устройство жертвы незаметно устанавливалось вредоносное ПО, обеспечивающее удаленный доступ к системе. Кампания находилась в стадии подготовки с июля-августа 2024 года и перешла в активную фазу в ноябре-декабре того же года. Группа, стоящая за атаками, Ghostwriter (UNC1151 по классификации Mandiant, UAC-0057 по классификации CERT-UA) активна предположительно с 2016 года; SentinelLABS напрямую связывает ее с усилиями беларусского правительства в сфере шпионажа.

Под контролем силовиков также регулярно распространяются фейковые рассылки от имени организаций. Вместо того, чтобы заманить человека в поддельный канал, акторы сами выходят на него от имени организации, которой он доверяет. Это позволяет одновременно собирать персональные данные людей, откликнувшихся на предполагаемый запрос, дискредитировать организацию в глазах тех, кто получил фейковое сообщение, и наносить репутационный ущерб, который сложно нейтрализовать постфактум.

- **Кейс рассылки о паспортах.** В декабре 2023 года от имени Офиса Тихановской в Telegram начали рассылаться фейковые сообщения с призывом присылать персональные данные «для нового паспорта Новой Беларуси». Объединенный переходный кабинет квалифицировал это как «провокацию карателей режима с целью сбора данных беларусов».
- **Кейс форума «Шлях да волі».** В марте 2026 года, накануне форума региональной безопасности «Шлях да волі», организованного Объединенным переходным кабинетом Беларуси и аналитическим центром «Украинская призма», неизвестные начали рассылать беларусам личные сообщения в Telegram и социальных сетях от имени оргкомитета, с визуалом, имитирующим официальный, но с измененными графическими элементами и грамматическими ошибками. В сообщении требовалось подтвердить свое участие в форуме. Организаторы форума подчеркнули, что вся коммуникация ведется исключительно через публичные официальные каналы, и квалифицировали рассылку как операцию по сбору персональных данных потенциальных участников.
- **Кейс писем от имени ZMINA.** В октябре 2025 года беларусам начали приходить письма якобы от имени украинской правозащитной организации ZMINA с просьбой присылать информацию о фигурантах «дела Гаюна» и других дел, связанных с поддержкой Украины. Все письма приходили от имени якобы сотрудника организации Николая Оксинюка с адреса на protonmail. Центр прав человека ZMINA сообщил, что такого сотрудника не существует и все официальные письма организации приходят только с адресов на домене @zmina.ua.

2.2.2. Сбор данных через псевдоработодателей и подставных исполнителей

В последние годы силовики все чаще осуществляют сбор данных через псевдоработодателей и подставных исполнителей. Операции этого типа строятся по похожей схеме: неизвестные предлагают оплачиваемую работу от имени реальной организации – СМИ, европейского института, НКО. Исполнитель получает аванс, легендированные документы и задание, выполняет его, искренне убежденный в легитимности работы, и неосознанно передает заказчикам разведывательные данные или материалы для деанонимизации участников акций. Наличие посредника затрудняет установление подлинного заказчика сбора данных.

Наиболее распространенная разновидность – задания под видом журналистской работы: съемка интервью с оппозиционными лидерами или фото и видео с протестных акций. Исполнителей

находят в Telegram-чатах среди людей, ищущих подработку, и снабжают поддельными пресс-удостоверениями с логотипами реальных изданий.

- **Кейс интервью со Светланой Тихановской.** В июле 2025 года неизвестные наняли через Telegram двух человек, гражданина Украины и гражданина Литвы, для съемки интервью с Тихановской, представившись редакцией «Новой газеты Европа». Нанятый 18-летний гражданин Украины получил аванс €100, список вопросов и поддельные пресс-удостоверения с логотипом издания. У команды Тихановской возникли подозрения в реальности «журналистов», после чего они запросили подтверждение у главного редактора «Новой газеты Европа» Кирилла Мартынова, который подтвердил, что эти люди не имеют отношения к редакции. Оба были задержаны литовской полицией.
- **Кейс «Чернобыльского шляха».** В апреле 2026 года в Telegram-чате украинцев, проживающих в Литве, появилось предложение снять фото и видео с беларусской акции «Чернобыльский шлях» (ежегодного марша памяти жертв Чернобыльской катастрофы, который беларусская диаспора проводит 26 апреля в Вильнюсе) за $150 в криптовалюте якобы от имени независимого российского издания «Ходорковский LIVE», однако редакция свою причастность не подтвердила. По аналогичной схеме украинских студентов ранее нанимали снимать акцию на День Воли 25 марта якобы для «Новой газеты Европа». Видео с лицами участников впоследствии показали на государственном телевидении Беларуси. Один из исполнителей подтвердил, что получил оплату криптовалютой, не зная, кому на самом деле передает материалы.

В части операций легенда выстраивается не непосредственно перед заданием, а годами: создаются фейковые аккаунты от имени реальных людей, которые постепенно наполняются контентом и выглядят достоверно к моменту использования.

- **Кейс интервью с НАУ.** В июне 2025 года пресс-служба НАУ получила запрос на интервью с Павлом Латушко от человека, представившегося журналисткой «Новой газеты Европа» Ириной Гариной, с gmail-адреса, не связанного с редакцией. НАУ установило, что журналистка Гарина действительно существует и работает в издании, однако никаких запросов Латушко не направляла. В Facebook был обнаружен фейковый аккаунт на ее имя, созданный в 2022 году, за три года до операции. По оценке Латушко, это свидетельствует о заблаговременно спланированной операции. После просьбы верифицировать личность через мессенджер автор письма прекратил коммуникацию.

В наиболее сложных случаях псевдоработа носила не разовый, а систематический характер: человека вовлекали в длительное сотрудничество, в ходе которого он регулярно передавал данные, полагая, что выполняет легитимную работу для европейской структуры.

- **Кейс «Молодежного хаба» и Олега Аксенова.** В ноябре 2023 года стало известно, что могилевский активист БХД Олег Аксенов более года выполнял задания, полагая, что работает «внештатным аудитором Европейской счетной палаты». На деле за вакансией стоял КГБ: общение велось через Telegram от имени реального депутата Европарламента. За это время Аксенов подготовил четыре отчета со списками участников публичных мероприятий. Операцию КГБ раскрыл публично: 18 ноября 2023 года, во время семинара по безопасности в варшавском «Молодежном хабе», который Аксенов сам организовывал, в эфир по видеосвязи под именем «Фабио Зимера» вышел заместитель начальника следственного управления КГБ Константин Бычек. Он публично поблагодарил активиста за «сотрудничество» и призвал остальных участников явиться с повинной в Беларусь. Сам Аксенов настаивает, что не осознавал, что работает на КГБ, а все переданные им сведения были в открытом доступе.

Наиболее циничной разновидностью этой схемы является использование самого факта выполнения задания как инструмента шантажа. По данным LRT, силовики размещают в Telegram-каналах беларусской диаспоры объявления о подработке – например, перевезти посылку из одной страны в другую. После выполнения задания человеку сообщают, что он якобы перевез взрывчатку или секретные документы, и угрожают сообщить об этом местным спецслужбам, если

он откажется сотрудничать. Силовики указывают, что в таком случае человека либо посадят в тюрьму в стране пребывания, либо экстрадируют в Беларусь, где последствия будут еще серьезнее. Таким образом человек оказывается в ловушке искусственно созданной уязвимости.

2.2.3. Попытки онлайн-вербовки членов диаспоры

Задокументированы систематические попытки использования беларусскими спецслужбами социальных сетей и мессенджеров для вербовки членов диаспоры. В отличие от операций с псевдожурналистами, где исполнитель не осознает, на кого работает, вербовочные контакты предполагают прямое предложение сотрудничества с режимом: человеку открыто предлагают следить за деятельностью диаспоры, передавать информацию об активистах в обмен на прекращение уголовного преследования и возможность возвращаться в Беларусь. Активность сообщений с попытками вербовки заметно возрастает в привязке к конкретным событиям – выборам в Координационный совет или признанию оппозиционных структур «экстремистскими» и «террористическими» организациями. По наблюдениям активистов, перед выходом на контакт силовики, как правило, заранее анализируют социальные сети человека и составляют его психологический портрет, чтобы подобрать наиболее уязвимый заход и выстроить разговор под конкретного человека.

- Кейс вербовки через аккаунт «Марии Пулковской». В 2025 году беларусские активисты за рубежом начали получать сообщения в Facebook и Instagram с предложениями сотрудничества. По данным «Вясны», как минимум пять таких сообщений были отправлены с одного аккаунта под именем Мария Пулковская, предположительно принадлежащего сотруднику КГБ. Все сообщения содержали схожие предложения: следить за деятельностью диаспоры в обмен на содействие в решении личных или правовых проблем.
- Кейс вербовки сотрудников НАУ. По словам лидера НАУ Павла Латушко, КГБ, Главное разведывательное управление (ГРУ) и специальные подразделения МВД регулярно пытаются вербовать сотрудников организации в социальных сетях и мессенджерах через шантаж, денежные предложения и прямые угрозы в адрес членов семей. Вербовщики предлагали «начать жизнь с чистого листа и вернуться в Беларусь в обмен на сотрудничество».

Наряду с прямыми вербовочными предложениями фиксируются и более изощренные операции, в которых силовики заходят на контакт не через открытое предложение сотрудничества, а издалека под видом клиентов, знакомых знакомых или участников диаспорных чатов. Сначала устанавливается доверие, затем начинаются расспросы об активистах и мероприятиях диаспоры, и лишь потом звучит предложение сотрудничества.

- Кейс Александры Мамаевой. В сентябре 2024 года глава Народного посольства Беларуси в Словении Александра Мамаева получила сообщение в Facebook от неизвестного под именем Кирилл, который представился беларусом из Мюнхена и попросил арендовать яхту, сославшись на общего знакомого из диаспоры. Помимо обсуждения вопросов аренды, он постепенно начал расспрашивать об активистах диаспоры и мероприятиях в Германии и Словении, а затем открыто предложил сотрудничество, угрожая родственникам, оставшимся в Беларуси. Как выяснилось позже, аккаунт собеседника был создан после 2020 года, а в диаспоре Мюнхена его никто не знал.

Все чаще вербовочный контакт осуществляется через родственников и друзей эмигранта, остающихся в Беларуси. Силовики приходят к ним, спрашивают о жизни уехавшего, после чего либо берут его контакты для звонка, либо связываются с ним с устройств близких. В ходе этого разговора силовики пытаются добыть сведения о деятельности диаспоры или склонить к сотрудничеству.

- Кейс вербовки через родителей. По данным «Нашей Нивы», в апреле 2024 года к матери девушки, уехавшей из Беларуси в 2020 году, пришли сотрудники КГБ. Они проверили ее переписку и социальные сети, расспросили о жизни дочери за рубежом, после чего попросили мать «повлиять» на нее и передать предложение о сотрудничестве. Затем силовики

взяли у матери контакты дочери и вышли на нее напрямую – обещали помочь с работой и возвращением на родину, однако дали понять, что взамен ожидают информацию об активистах диаспоры. В качестве дополнительного рычага давления упомянули, что если кто-то из близких умрет, она может передумать и захотеть приехать на похороны.

- Кейс вербовки через друга. Также по данным «Нашей Нивы», в мае 2026 года силовики вышли на живущего в эмиграции с 2022 года Антона через его друга. Друга Антона вызвали в одно из государственных учреждений, где его ждали сотрудники КГБ. Затем они позвонили Антону с телефона друга, зная, что звонки с незнакомых беларусских номеров тот игнорирует. В ходе разговора силовики сообщили, что располагают списками донатеров Полку Калиновского и Антон в них значится, после чего стали расспрашивать об организаторах акций диаспоры за рубежом. Затем они трижды предложили помочь с возвращением в Беларусь в обмен на сотрудничество.

2.2.4. Сбор данных за денежное вознаграждение

Отдельную модель сбора персональных данных членов диаспор представляет публичное объявление денежного вознаграждения за сведения, позволяющие установить личность, на конкретных акторов. Провластные каналы открыто и без всякой маскировки предлагают аудитории заработать на передаче персональных данных об оппозиционных деятелях, что фактически превращает деанонимизацию в краудсорсинговую коммерческую услугу. Telegram-канал «Белорусский фронт» (характеристика канала приведена в п. 1.2) систематически публикует подобные объявления с просьбой за плату поделиться информацией об отдельных беларусских гражданах, воюющих на стороне Украины против российской агрессии, а также о деятельности политических активистов за рубежом, после чего публикует полученные данные в этом же канале.

- Кейс вознаграждения за деанонимизацию. 4 октября 2024 года канал опубликовал пост «Сдеанонь белорусского наемника и получи денежный приз», предложив денежное вознаграждение первому, кто предоставит установочные данные (ФИО, дату рождения и иные сведения) человека по присланному фото. Канал обращался к максимально широкому кругу потенциальных информаторов – «журналист, украинский военный, наемник, сосед», гарантируя полную анонимность источника. Подобные предложения публиковались на канале регулярно. 20 ноября 2024 года канал расширил эту модель, объявив вознаграждение уже не за данные отдельных лиц, а за разведывательную информацию более широкого характера: в преддверии президентских выборов 2025 года канал предложил оплату за сведения о «лицах, кураторах и организациях», которые «готовят планы по дестабилизации ситуации в Республике Беларусь», а также информацию об «их финансировании и координации». В этом же посте предлагалась оплата за информацию о людях, причастных к подготовке обращения властей Литвы в Международный уголовный суд, касающегося массовых нарушений прав человека в Беларуси.

2.3. Онлайн угрозы и преследование в социальных сетях

Давление на политических эмигрантов через цифровые каналы строится на том, что у человека за рубежом есть уязвимые точки, доступные для воздействия на расстоянии: личные данные, родственники в Беларуси, имущество. Анонимные сообщения с упоминанием домашнего адреса или материалов уголовного дела, публикация видео разгромленной квартиры родителей, принудительное видеообращение отца с просьбой вернуться являются разными форматами одной операции, цель которой поддерживать постоянное ощущение наблюдаемости и уязвимости. Сдерживающий эффект при этом распространяется не только на определенных адресатов, но и на всю диаспору.

2.3.1. Угрозы и давление в переписках

Анонимные или псевдонимные аккаунты регулярно выходят на связь с эмигрантами в социальных сетях и мессенджерах, чередуя прямые угрозы с уговорами вернуться, предложениями «порешать проблемы» в обмен на информацию и демонстрацией осведомленности о личных данных:

домашнем адресе, паспортных данных, передвижениях, материалах уголовных дел. В подавляющем большинстве случаев авторы угроз не раскрывают принадлежность к силовым структурам, однако осведомленность о непубличных сведениях указывает на их связь с ними.

- **Кейс Анны Красулиной.** Пресс-секретарь Светланы Тихановской Анна Красулина на протяжении нескольких лет после эмиграции в 2020 году получала сообщения от человека, называвшего себя «неравнодушным гражданином», который регулярно делился мнениями об оппозиции. В январе 2023 года он сообщил ей о готовящемся указе Лукашенко о лишении гражданства осужденных мигрантов за десять дней до его подписания, что указывает на осведомленность, несовместимую с заявленным статусом рядового гражданина. Также активистка регулярно получает непрошеные сообщения и звонки по ночам.
- **Кейс Татьяны Ашуркевич.** Журналистка Татьяна Ашуркевич, также не живущая в Беларуси, рассказала BBC в 2025 году, что вскоре после публикации расследования о роли беларусских властей в миграционном кризисе анонимные аккаунты в соцсетях начали перечислять статьи УК, которые теперь могут ей грозить. Один из ее подписчиков в Instagram, представлявшийся машинистом, после прямого вопроса от журналистки о возможных уголовных делах резко сменил тон и предложил обмен: он даст ей информацию о делах, а в ответ на это Ашуркевич должна будет поделиться информацией о бойцах Полка Калиновского.
- **Кейс Кристины Тимановской.** Беларусская спортсменка Кристина Тимановская сообщила AP в 2024 году, что в Варшаве получала угрозы физической расправой в мессенджерах, в том числе сообщение о том, что ей «вспорют живот, если она выйдет на улицу».

Наряду с прямыми угрозами зафиксированы случаи шантажа: неизвестные под псевдонимами пишут активистам по электронной почте, в мессенджерах и социальных сетях, сообщая, что располагают компрометирующими материалами или сведениями личного характера, которые будут преданы огласке, если человек не прекратит свою деятельность.

- **Кейс Риты Гатих.** В июне 2026 года активистка беларусской диаспоры в Чехии и делегатка Координационного совета Рита Гатих получила письмо от неизвестных под псевдонимом «Кастусь Каліноўскі» на электронную почту через Proton Mail. Авторы письма указали, что ее сознательное участие в структурах и мероприятиях, привлекающих внимание соответствующих органов, не останется без последствий, и сообщили, что располагают фотоматериалами и иными сведениями личного характера о ней. Неизвестные заявили, что не намерены использовать эти материалы немедленно, однако предупредили, что в случае продолжения деятельности они могут быть переданы журналистам, тематическим интернет-ресурсам и Telegram-каналам.

2.3.2. Использование родственников в онлайн-кампаниях давления

Одной из форм давления на политических эмигрантов стало использование видеообращений, записанных силовыми структурами с участием их родственников, остающихся в Беларуси. В ходе обысков или задержаний оставшихся близких вынуждают записывать обращения к уехавшим членам семьи с призывами вернуться на родину, прекратить активистскую деятельность или публично осудить своих родных за рубежом. Такие записи затем распространяются через провластные Telegram-каналы и государственные медиа.

- **Кейс Дениса Урбановича.** В марте 2023 года силовики пришли к отцу бойца Полка Калиновского Дениса Урбановича и заставили его записать обращение к сыну с просьбой прекратить участие в боевых действиях и сдаться властям. На видео он говорит следующее – «Отсидишь десятку какую, черт с ним, зато будешь жить на Родине».
- **Кейс «покаянных» видео родственников журналистов.** В июне-июле 2024 года, по данным Беларусской Ассоциации Журналистов (БАЖ), силовики провели обыски по местам регистрации не менее 21 эмигрировавшего журналиста и в ряде случаев принудили их родственников, остающихся в Беларуси, записать «покаянные» видео с осуждением уехавших детей. В частности, родителей ведущих TikTok-канала издания «Зеркало» заставили записать обращения со словами осуждения и возмущения в адрес своих детей.

2.3.3. Публикация видео и фото разгромов имущества

В ряде случаев обыски у беларусских политических эмигрантов и их родственников сопровождались демонстративным уничтожением имущества. Практика публикации фото и видеозаписей разгромленных квартир стала отдельным элементом кампаний давления против беларусской диаспоры. Материалы, распространявшиеся через аффилированные с силовыми структурами каналы, нередко сопровождались монтажом, музыкальным оформлением и визуальными элементами, характерными для телевизионных развлекательных или криминальных программ. Например, в 2022 году силовики разгромили квартиры блогера Андрея Паука, оппозиционных политиков Валерия Цепкало и Вадима Прокопьева, матерей блогера Антона Мотолько и редактора Telegram-канала по деанонимизации правоохранителей Янины Сазанович, после чего опубликовали результаты своих действий в Telegram.

2.4. Атаки на инфраструктуру и деятельность инициатив и организаций

Помимо операций против отдельных людей, провластные акторы атакуют саму инфраструктуру продемократических инициатив, их платформы, сайты и открытые форматы работы. В этих случаях они не собирают данные и не дискредитируют конкретных лиц, а выводят из строя или компрометируют инструменты, на которых держится деятельность организаций.

2.4.1. DDoS-атаки на цифровую инфраструктуру

DDoS-атака (Distributed Denial of Service) – намеренная перегрузка сервера или сайта потоком запросов с множества устройств одновременно, в результате которой ресурс становится недоступен для обычных пользователей. Применительно к оппозиционной инфраструктуре этот инструмент используется для нарушения работы платформ в критические моменты: во время выборов или проведения знаковых мероприятий. В отличие от других инструментов давления, атаки этого типа не собирают данные и не дискредитируют организацию, а лишь лишают ее аудитории тогда, когда доступность ресурса наиболее важна. Атрибуция в большинстве случаев затруднена: используется коммерческая инфраструктура ботнетов, скрывающая заказчика.

- Кейс БРЦ. 12 января 2026 года сайт БРЦ подвергся массированной DDoS-атаке с использованием ботнета примерно из 245 000 уникальных IP-адресов. Атака продолжалась 12 часов и была направлена против конкретной публикации о беларусских политиках, скрывавших средства в швейцарском банке. По оценке RESIDENT.NGO, масштаб и ресурсоемкость атаки указывают на использование коммерческого ботнета, арендованного либо хорошо финансируемой частной структурой, либо актором, аффилированным с государством.
- Кейс выборов в Координационный совет. В мае 2026 года, сразу после старта выборов в КС, платформа для голосования подверглась мощной DDoS-атаке, которая привела к ее временной недоступности и переносу начала приема голосов на резервный сайт. Ранее аналогичным атакам подвергалась платформа «Тры сланы» со списками кандидатов. По оценке разработчика платформы Павла Либера, стоимость атак такого масштаба по рыночным ценам составила от 100 до 200 тысяч евро, что указывает на серьезное финансирование операции.

2.4.2. Вмешательство в открытые форматы работы

Открытость является одновременно политическим принципом и структурной уязвимостью продемократических инициатив. Публичные форматы коммуникации, инклюзивные процедуры голосования и доступные образовательные платформы создаются как демонстрация

демократических ценностей, и именно поэтому не предполагают фильтрации участников по политическому признаку. Провластные акторы систематически эксплуатируют это противоречие: вместо того, чтобы атаковать закрытые системы, они используют то, что открыто по замыслу, превращая инклюзивность формата в инструмент его дискредитации.

- Кейс дискредитации выборов в Координационный совет. В мае 2024 года беларусская диаспора провела онлайн-выборы делегатов Координационного совета, голосование было открыто для всех обладателей беларусского паспорта. Вскоре после завершения голосования, пропагандист Игорь Тур в эфире ОНТ заявил, что сотрудники Белтелерадиокомпании изготовили в Adobe Photoshop поддельные беларусские паспорта и успешно проголосовали по ним, тем самым якобы доказав уязвимость системы идентификации избирателей.
- Кейс звонка Азаренка. Каждую неделю Светлана Тихановская с командой проводила открытые звонки для беларусов, находящихся внутри страны. 5 августа 2022 года стало известно, что пропагандист СТВ Григорий Азаренок воспользовался этим публичным каналом и дозвонился до нее напрямую. В ходе разговора он систематически перебивал Тихановскую, не давая закончить ни одну мысль, и последовательно продвигал нарративы государственной пропаганды: обвинения в получении денег, вопросы о финансах Офиса, призывы к «деятельному раскаянию» и возвращению в Беларусь. Разговор был записан Офисом Тихановской, который, ожидая, что Азаренок использует его на государственном телевидении, самостоятельно передал полную запись независимым медиа, чтобы исключить манипулятивную подачу.
- Кейс Свободного беларусского университета. В декабре 2023 года сотрудник КГБ Константин Бычек подключился к онлайн-занятию Свободного беларусского университета, проводившемуся в Zoom. Подключившись, он объявил участникам: «Все под контролем». По информации Белсата, КГБ мог получить ссылку на занятие, войдя как обычный студент – платформа не требовала верификации участников. Платформа признала это системной уязвимостью: использование ников вместо имен защищает участников, но одновременно делает невозможной проверку, кто именно подключился.

2.5. Публикация персональных данных активистов и организаций через провластные источники (доксинг)

Публикация персональных данных функционирует как инструмент дистанционного давления: человек за рубежом получает сигнал, что его личность, имущество и родственники в Беларуси известны и уязвимы. Сдерживающий эффект распространяется шире конкретных фигурантов – участие в акциях диаспоры становится сопряжено с осознаваемым риском даже для тех, чьи данные пока не раскрыты. Такие публикации охватывают широкий спектр информации: от персональных данных и адресов конкретных людей до финансовой отчетности организаций и юридических лиц, аффилированных с активистами. Данные публикуются через разные каналы: провластные Telegram-каналы, государственные СМИ и официальные органы. Часть практик доксинга также рассмотрена в п. 2.1.

2.5.1. Публикации призывов от провластных Telegram-каналов явиться к силовикам

Канал «Поступи по совести», появившийся в августе 2022 года, опубликовал никнеймы, скриншоты сообщений и личные данные участников протестов с прямым призывом явиться в ГУБОП на «профилактическую беседу». По данным Hrodna.life на сентябрь 2023 года, в канале были размещены данные 630 человек в Беларуси и более 300 за границей. Администрация Telegram неоднократно удаляла канал, однако он создавался заново. Канал содержит бот для доносов и рубрику «Вдали от родины», адресованную эмигрировавшим беларусам с предложением вернуться и покаяться.

2.5.2. Публикация данных активистов в государственных СМИ и провластных источниках

Государственные СМИ используют раскрытие персональных данных как инструмент публичного давления, нередко сопровождая его прямыми угрозами в адрес конкретных людей и их имущества.

- Кейс публикации адресов участников акций. В августе 2025 года пропагандист Игорь Тур в эфире ОНТ зачитал имена, фамилии и адреса объектов недвижимости некоторых из 207 участников зарубежных акций ко Дню Воли, идентифицированных силовиками. Обращаясь к одной из фигуранток, у которой «два дома в Березинском районе, дом в Бобруйске и квартира», Тур произнес в эфире: «Валентина Викторовна, добрый вечер. Оно того стоило?»
- Кейс угроз участникам марша в Вильнюсе. В марте 2026 года Роман Протасевич в эфире СТВ назвал поименно участников марша в Вильнюсе на День Воли с угрозами уголовного дела и конфискации имущества.
- Кейс раскрытия данных руководителя БРЦ. В апреле 2026 года тот же Протасевич в сюжете о БРЦ раскрыл в эфире номер телефона и адрес квартиры в Варшаве руководителя БРЦ Станислава Ивашкевича, находящегося в эмиграции с 2021 года и объявленного в межгосударственный розыск. Сопроводив публикацию данных комментарием о том, что Ивашкевича кто-нибудь может «навестить», Протасевич показал в эфире кадры, на которых неизвестный входит в подъезд его дома и подходит к двери квартиры.

Подобные операции не всегда затрагивают только тех, кто непосредственно связан с гражданским обществом или активистской деятельностью. Под удар могут попасть случайные люди, чье единственное сходство с реальными фигурантами сводится к совпадению имени или отдельных биографических деталей.

- Кейс ошибочной деанонимизации. В вышеупомянутом сюжете о БРЦ пропагандисты также опубликовали персональные данные человека, не имеющего никакого отношения к организации. В редакции БРЦ одна из сотрудниц работает под псевдонимом «Яна Міцкевіч». Пропагандисты разыскали в социальных сетях реальную девушку с таким же именем и фамилией, предположительно ориентируясь на то, что она окончила факультет журналистики Белорусского государственного университета (БГУ), и использовали ее фотографию и дату рождения, представив ее в эфире как автора и редактора материалов БРЦ. На момент выхода сюжета женщина уже около десяти лет жила в Швеции и журналистикой не занималась.

В ряде случаев источником данных для подобных сюжетов служат устройства людей, имевших доступ к чувствительной информации и задержанных внутри Беларуси. Опубликованные на их основе массивы данных затрагивают как людей, остающихся в стране, так и членов диаспоры за рубежом.

- Кейс ByHelp. В августе 2024 года силовики задержали волонтера фонда солидарности ByHelp в Беларуси. На его компьютере находилась база данных получателей помощи. С октября по декабрь 2024 года силовики провели обыски и допросы более чем у 50 человек, бывших политзаключенных и их родственников. В декабре 2024 года Игорь Тур в эфире ОНТ показал таблицы с персональными данными людей, связанных с фондом, представив их как доказательство «коррупции фондов» и якобы состоявшегося взлома. Важный нюанс, задокументированный Еврорадио: данные были получены через физический доступ к компьютеру задержанного волонтера, однако пропаганда намеренно создавала впечатление взлома.

2.5.3. Публикация личной переписки активистов и оппозиционных деятелей

Отдельный прием в арсенале транснационального доксинга – публикация скриншотов личной переписки оппозиционных деятелей и активистов диаспоры. В отличие от доксинга, направленного на раскрытие идентифицирующих данных, здесь объектом атаки становится содержание частных разговоров и личных конфликтов. Подобные публикации преследуют цель спровоцировать или усугубить внутренние конфликты внутри диаспорных и активистских

сообществ, а также дискредитировать членов диаспор в глазах людей внутри Беларуси. Чаще всего силовики получают доступ к переписка как через изъятие личных устройств у людей, задержанных на территории Беларуси (включая самих фигурантов до их освобождения или высылки, а также их знакомых и соратников), так и из старых материалов уголовных дел, накопленных за годы следствия и заключения.

- **Кейс публикации переписки Франака Вечорко.** В январе 2022 года ОНТ опубликовал спецпроект «Кто подставил Романа Протасевича? Публикуем скриншоты переписок», построенный на личной переписке находившегося под арестом с мая 2021 года бывшего главного редактора NEXTA Романа Протасевича с советником Офиса Тихановской Франаком Вечорко, а также фрагментах переписки с упоминанием других диаспорных фигур. Материал выстраивал нарратив о личном конфликте и предательстве внутри штаба Светланы Тихановской.
- **Кейсы, связанные с анархистским сообществом.** Telegram-канал «#знайанархиставлицо» (см. п. 1.2) систематически публикует личную переписку активистов анархистского движения, касающуюся интимных отношений между людьми. 10 августа 2023 года канал опубликовал скриншот переписки активистки Алены Витко (находится в эмиграции в Польше), уничижительно поданный по отношению к Андрею Чепюку – на тот момент политзаключенному (освобожден в апреле 2025 года). 1 декабря 2025 года канал опубликовал скриншоты переписки 2017 года из мессенджера анархиста Николая Дедка с его партнеркой, который к тому времени уже был освобожден и принудительно выслан в Литву. Публикация вышла вскоре после того, как Дедок начал восстанавливать публичную активность в эмиграции.

2.5.4. Публикация персональных данных в официальных реестрах

Отдельным инструментом публичной стигматизации служат официальные государственные реестры, в которых раскрываются персональные данные лиц, признанных причастными к «экстремистской» или «террористической» деятельности. В отличие от провластных Telegram-каналов, здесь речь идет о легализации раскрытия персональных данных через формально правовые механизмы. Реестры содержат полные имена, даты рождения, гражданство и иные идентифицирующие сведения, после чего их содержимое активно тиражируется провластными Telegram-каналами и государственными СМИ. С расширением практики специального (заочного) уголовного преследования все большую долю фигурантов списков составляют члены диаспоры.

Помимо персональных реестров, существует также «Перечень организаций, формирований и индивидуальных предпринимателей, причастных к экстремистской деятельности», в котором все активнее практикуется публикация списков физических лиц, аффилированных с признанными «экстремистскими» структурами.

Параллельно Следственный комитет публикует сведения о лицах, в отношении которых начато заочное производство, в рамках специального списка на официальном сайте и в отдельных постах в специализированном Telegram-канале. В Telegram-канале вместе с персональными данными людей дополнительно публикуются паспортные фотографии преследуемых активистов.

2.5.5. Финансовый доксинг

Публикация финансовой и имущественной информации об активистах и организациях за рубежом составляет еще одну разновидность практики доксинга. Основная цель таких атак – подрыв доверительных отношений между гражданским обществом и его донорской и общественной базой через конструирование образа корыстности и моральной несостоятельности активиста или организации.

Особую роль в таких атаках играют публично доступные реестры юридических лиц. В странах ЕС некоммерческие организации обязаны публиковать финансовую отчетность в открытых государственных реестрах – это стандартный механизм подотчетности гражданского общества

перед донорами и обществом. В контексте беларусской диаспоры этот инструмент прозрачности был переориентирован в инструмент атаки. Провластные акторы систематически анализируют реестры юридических лиц (например, в Литве – сайт rekvizitai.vz.lt) и на основе публичных данных выдвигают обвинения в нецелевом расходовании средств и финансовых злоупотреблениях.

Особую роль в этой схеме играет Telegram-канал «Штаб Оношко», позиционирующий себя как независимый разоблачительный ресурс, специализирующийся на «финансовых и коррупционных скандалах белорусской революции 2020». При этом его материалы системно цитировались и рекламировались государственными СМИ.

Канал скачивает финансовую отчетность организации из публичного реестра, применяет к ней произвольные «рыночные расчеты» и формулирует обвинения в псевдоаналитическом жанре. Обвинения формулируются без независимой верификации, на основе избирательной интерпретации публичных данных. Отдельные публикации канала содержат имена директоров и контактные данные организаций, извлеченные из открытых реестров, тем самым фактически направляя аудиторию к прямым обращениям в адрес конкретных людей.

- Кейс «Наша Нива». 27 апреля 2025 года «Штаб Оношко» опубликовал разбор финансовой отчетности фонда «Наша Нива» за 2023 год. Канал указывал на высокую долю фонда оплаты труда в расходах и акцентировал внимание на договоре подряда с фрилансером, объем работ по которому, по расчетам канала, физически не мог быть выполнен одним человеком за указанный срок – из чего делался вывод о фиктивности договора. Отдельно подчеркивалось, что 1,2% подоходного налога в пользу фонда в 2023 году перечислил лишь один человек, что свидетельствует о том, что поддержка организации среди населения ничтожна. Пост заканчивался угрозой в адрес директора Настасьи Ровдо («ищи работу, денег не будет») и упоминанием «списочка доноров, любезно предоставленного» третьим лицом.
- Кейс Human Constanta. 19 июня 2025 года канал опубликовал разбор отчетности Human Constanta, утверждая, что организация израсходовала на свою деятельность сумму, которая якобы в семь раз превышает «рыночную стоимость» аналогичной работы по собственным расчетам авторов канала. Задекларированные результаты представлялись как несоразмерно скромные относительно потраченных средств, а стоимость волонтерского часа при механическом делении бюджета на число часов подавалась как абсурдная – и тем самым как свидетельство злоупотреблений.

Тактика финансового доксинга часто распространяется и на членов семей активистов. Анонимные провластные каналы регулярно публикуют финансовую и имущественную информацию о родственниках активистов, беря данные о зарегистрированных на них юрлицах из публичных реестров принимающих стран либо, по всей видимости, используя сведения из беларусских государственных баз учета имущества и сделок. На основе этих данных провластные акторы создают нарратив о мошеннических семейных финансовых схемах, косвенно дискредитируя самого активиста.

- Кейс Ольги Зазулинской. В сентябре 2024 года, вскоре после назначения Ольги Зазулинской представителем по социальной политике Объединенного переходного кабинета, провластный канал «Вашы зліўкі» опубликовал скриншоты из литовского реестра rekvizitai.vz.lt с финансовой отчетностью двух юрлиц Hive Media asociacija и Stream Hub MB, зарегистрированных на ее сына Глеба Аникевича. На основе данных о выручке канал построил нарратив о том, что через сына «прошли около полмиллиона долларов», представив это как схему сокрытия средств фондов, связанных с оппозицией.
- Кейс сбора средств для Кристины Черенковой. 17 мая 2024 года канал «#знайанархиставлицо» опубликовал пост, дискредитирующий сбор средств для бывшей политзаключенной Кристины Черенковой в Познани, назвав организаторов «кучкой бывших анархистов» и обвинив их в попытке «выманить бабки» вместо настоящей помощи нуждающимся. В подкрепление этого тезиса канал раскрыл финансовую информацию о муже Черенковой: утверждалось, что осенью 2023 года он продал квартиру и автомобиль в Мозыре и выехал в Польшу с суммой не менее $27 000, что было представлено как доказательство мошеннического характера сбора.

Поскольку подобные сделки в Беларуси подлежат государственной регистрации, источником сведений, вероятно, послужили официальные базы учета имущества, доступ к которым провластные акторы могли получить через силовые структуры.

Все перечисленные в этой главе практики объединяет общая логика: они превращают информацию и данные в средство контроля и дистанционного давления на людей, которые находятся вне физической досягаемости беларусских органов. В то же время, особую и все более растущую роль в таких операциях выполняют инструменты ИИ, чему посвящена следующая глава.

3. Производство синтетического контента средствами ИИ

Распространение и растущая доступность технологий ИИ стимулируют все более широкое их использование в пропагандистских и репрессивных целях. Настоящий раздел рассматривает сдвиг, который ИИ вносит в описанные выше тактики доксинга и дискредитации. Чаще всего объектами подобных атак становятся медийные персоны: представители политических организаций, гражданских инициатив, независимых медиа, экспертного сообщества и беларусской диаспоры. Использование ИИ в таких случаях позволяет быстро создавать визуальные, аудио- и текстовые материалы, имитирующие реальных людей или приписывающие им действия и высказывания, которых они не совершали. Отдельное измерение здесь – гендерное: эротизирующий синтетический контент в проанализированном массиве применяется только против женщин, тогда как в отношении мужчин сексуальные мотивы используются в иной, неэротизирующей функции (см. п. 3.1.2). Анализ ниже строится на двух Telegram-каналах, материалы которых позволяют проследить систематическую практику и развитие таких атак. Отдельные случаи применения дипфейков рассмотрены в п. 2.1.2; здесь речь идет о систематическом производстве такого контента конкретными ресурсами.

3.1. «Людажоры»: пропаганда на основе генеративного ИИ

Telegram-канал «Людажоры» демонстрирует наиболее технологически развитую практику применения генеративного ИИ в беларусской пропагандистской среде. Его главным творческим и пропагандистским продуктом стал «Нейрокомикс» – систематически производимый сатирический ИИ-контент, публикуемый как в самом канале, так и в изданиях холдинга «СБ. Беларусь сегодня»; по состоянию на июль 2026 года, у проекта вышло уже более 150 выпусков.

3.1.1. Технология и форматы производства

На протяжении исследуемого периода автор канала выстроил разнообразный технический арсенал, который детально описывает в своих публикациях. Он включает в себя несколько направлений:

- генерация изображений с помощью нейросетей (упоминаются работа в разрешении 2K, формат fp16, модели LoRA для конкретных лиц);
- создание обучающих датасетов на реальных людях (членах оппозиции) для воспроизведения их внешности;
- клонирование голосов реальных людей для создания видеоматериалов;
- создание «персонажей» на основе конкретных оппозиционных деятелей – Тихановской, Латушко, Карач, Тимановской и других.

При этом автор прямо указывает на политические цели проекта: «В следующем мордобое [имея в виду политическое противостояние – прим.] нейронки будут одним из инструментов, с помощью которого на нас будут нападать в информационной сфере, и отбиваться нам придется ими же».

Применение ИИ здесь можно оценить как систематическое. Так, на это указывают непрерывность использования технологий на протяжении всего исследуемого периода с 2022 по 2026 год, постепенное увеличение количества и сложности материалов, а также расширение набора применяемых инструментов. Если в 2022 году речь шла преимущественно об отдельных экспериментах, то в 2023-2024-м публикация созданного с помощью ИИ контента приобрела регулярный характер, а в 2025-2026-м достигла масштабов устойчивого и серийного производства.

Одновременно наблюдается техническая эволюция: от генерации статичных изображений автор перешел к созданию синтетических видео, видеодипфейков, клонированию голосов и разработке видеоигры с ИИ-персонажами. В 2024 году расширилась практика создания персонализированных моделей реальных людей, преимущественно женщин; в этот же период фиксируются эксперименты с переносом лиц персонажей мультфильмов в фотореалистичные изображения и первые попытки видеогенерации.

Период 2025-2026 годов можно охарактеризовать как качественный переход к более сложным и разнообразным формам синтетического контента: автор освоил видеодипфейки и клонирование голосов, а созданные с помощью ИИ материалы стали систематически встраиваться в политические и пропагандистские нарративы. 11 сентября 2025 года было публично объявлено о «втором раунде» информационной войны; одновременно велась разработка ИИ-видеоигры «Полыханка», в которой прототипами персонажей выступают реальные люди. Стоит отметить, что публичная демонстрация растущих возможностей генерации компрометирующего контента, в том числе сексуализированного, используется как инструмент давления сама по себе.

3.1.2. Гендерный аспект атак

Гендерная принадлежность человека, против которого направлена атака, во многом определяет и саму стратегию таких атак. Дискредитация и публичное унижение применяются ко всем, но средства различаются: в отношении женщин систематически используется эротизирующая сексуализация, тогда как в отношении мужчин преобладают обвинения в предательстве, некомпетентности, алкоголизме и психической неустойчивости. Это различие носит не случайный, а системный характер и прослеживается на всем массиве проанализированных публикаций.

Здесь и далее необходимо различать два разных явления. Под сексуализированным ИИ-контентом в узком смысле понимается эротизирующий материал: интимные и эротические изображения, угрозы публикацией порнографических материалов, помещение реального человека в сексуализированные нарративы. От него следует отличать сексуальные мотивы, применяемые не для эротизации, а как маркер униженности, – гомофобные и тюремно-сексуальные аллюзии, «феминизацию» объекта. Первый тип в проанализированном массиве применяется только в отношении женщин, второй – преимущественно в отношении мужчин; далее эти два типа не смешиваются. Дополнительным инструментом воздействия выступает запугивание, в том числе посредством угроз создания или распространения таких компрометирующих материалов. Внешняя реалистичность таких публикаций способствует распространению дезинформации и затрудняет их распознавание аудиторией. Одновременно подобный контент может использоваться для провоцирования травли со стороны подписчиков и усиления общественного давления на объект атаки.

Среди женщин, ставших объектами ИИ-атак канала:

- Евгения Сугак – наиболее частая цель: несколько десятков публикаций (сексуализированный контент, дипфейки, угрозы);
- Светлана Тихановская (1, 2) – систематический объект «Нейрокомикса» и отдельных дипфейков;
- Марина Ментусова – объект систематических угроз сексуализированным контентом и включения в «Полыханку»;
- Анастасия Ровда – прямые угрозы порнографическим контентом, созданным с помощью ИИ;
- Ольга Токарчук – создание ИИ-изображения в «покаянном видео» после ее критики государственной символики;

- Екатерина Водоносова – создание ИИ-изображения, сопровождающего нарратив о «реабилитации нацизма», в сочетании с угрозами уголовным преследованием и экстрадицией;
- Кристина Станкевич («Чабор») – создание ИИ-изображения, параллельные обещания опубликовать слив личной переписки;
- Елена Живоглод – включение в выпуск «Нейрокомикса» о «сексуальных девиациях» с сексуализированным ИИ-изображением;
- Кристина Тимановская – создание уничижительного ИИ-образа;
- Дарья Лосик – использование образа в ИИ-контенте, направленном против Игоря Лосика (случай учитывается отдельно: здесь женщина выступает не объектом атаки, а средством давления на мужчину);
- Янина Сазанович (1, 2 – создание сексуализированного контента и привлечение аудитории к выбору сюжета, и другие.

Данные анализа подтверждают следующие закономерности. Во-первых, действительно, женщины подвергаются сексуализированным атакам непропорционально чаще мужчин: из всех выявленных случаев применения ИИ для создания эротизирующего сексуализированного контента в определенном выше узком смысле объектами во всех случаях выступают женщины. Это утверждение относится именно к эротизирующему типу материалов и не означает отсутствия сексуальных мотивов в контенте о мужчинах: они присутствуют, но выполняют другую функцию (см. ниже).

Во-вторых, стратегии дискредитации различаются. В отношении женщин внешность и сексуальность используются как самостоятельные инструменты унижения (сексуализированные образы, угрозы «раздеть» нейросетью, помещение в порнографические нарративы); автор открыто признает, что с женщинами «работать приятнее». В отношении мужчин преобладают обвинения в предательстве, некомпетентности, алкоголизме, психических отклонениях и уголовных преступлениях; эротизирующая сексуализация не применяется, а сексуальные мотивы возникают исключительно в неэротизирующей функции унижения.

В-третьих, гендерная избирательность носит системный характер: применение эротизирующего ИИ-контента исключительно в отношении женщин не объясняется составом публичных деятелей, о которых пишет канал, – мужчины-политики упоминаются не реже, а персонализированные ИИ-модели обучаются и на мужчин, и на женщин. Различие проходит не по тому, кто попадает в поле зрения канала, а по тому, какой прием к нему применяется, что и указывает на целенаправленную гендерную стратегию. Наконец, угроза создания ИИ-контента используется как инструмент принуждения к прекращению законной деятельности – подачи жалоб, журналистской работы.

При этом мужчины остаются постоянными объектами ИИ-генерации канала – с иным набором образов, визуальных приемов и форм дискредитации. Если женский образ редуцируется к телесности, то мужской последовательно лишается атрибутов дееспособности: трезвости, рациональности, психической нормы и правопослушности.

Наиболее разработанный мужской ИИ-образ связан с Павлом Латушко: канал закрепил за политиком устойчивого сатирического персонажа «этилового терминатора», эксплуатирующего тему алкогольной зависимости, – от отдельных сгенерированных изображений до пародийных сюжетов об «уничтожении» персонажа, отсылающих к франшизе «Терминатор». По запросу аудитории автор сгенерировал изображение политика верхом на «белочке» – визуальной метафоре алкогольного делирия. Алкогольная тема дополняется криминализирующими и патологизирующими ярлыками («агент 0,7», «пироман-насильник»), в результате чего формируется целостный образ деградировавшего, зависимого и невменяемого деятеля.

Отдельную группу составляют политики европейских государств. В отношении них распространяются гомофобные намеки: примером служит выпуск «Нейрокомикса» «про настоящую мужскую дружбу», посвященный польским официальным лицам и построенный на тюремно-сексуальных аллюзиях. Сексуализация мужчин, в отличие от женщин, возникает не как эротизация, а как маркер униженности и «ненормальности». Наконец, мужские персонажи «Нейрокомикса» из числа европейских политиков наделяются образами психической неустойчивости и девиантности: Дональд Туск изображается покровителем «подводного

террориста», Эммануэль Макрон – носителем «детских психических травм», компенсируемых милитаризмом, Гитанас Науседа помещается в нарратив о наркоторговле.

Таким образом, целевыми мужскими группами выступают лидеры оппозиции и европейские политики. Функционально ИИ-контент с изображениями мужчин решает ту же задачу делегитимации, но иными средствами: он разрушает образ дееспособного лидера и защитника, представляя объект зависимым, невменяемым, криминальным или феминизированным. Персонализированные ИИ-модели создаются и на мужчин: автор указывал, что обучил модели более чем на пяти десятках «врагов народа», к половине из которых клонированы голоса, – то есть персонализированные ИИ-модели создаются и на мужчин.

Использование гендерных стереотипов пронизывает всю практику ИИ-генерации канала, однако тяжесть этого воздействия распределяется неравномерно. Мужские образы высмеиваются, феминизируются и приравниваются к квир-образам как способ унижения, но женщины платят несопоставимо более высокую цену: их образы сексуализируются, а сами они становятся мишенью сексуализированной формы цифрового гендерного насилия – от несогласованных интимных изображений до прямых угроз порнографическим контентом. Именно поэтому гендерное измерение этих атак следует рассматривать не как частный аспект, а как одну из наиболее тяжелых форм причиняемого вреда.

3.2. «Белорусский фронт»: дипфейк-кампании против лидеров оппозиции

Telegram-канал «Белорусский фронт» (@III_SESTRY) также функционирует как один из ключевых провластных анонимных ресурсов, направленных против беларусской диаспоры и оппозиционных структур за рубежом. Канал позиционирует себя как источник «инсайдерской информации» о деятельности беларусских эмигрантских организаций и их лидеров.

Тематическая палитра канала охватывает несколько устойчивых направлений: дискредитация лидеров беларусской оппозиции (прежде всего Светланы Тихановской, Павла Латушко, Франака Вечорко и других), дискредитация беларусских медиаструктур в эмиграции, нарративы о «грантоедстве» и коррупции диаспорных организаций, пропаганда в поддержку режима Александра Лукашенко, а также информационное сопровождение военно-политической ситуации вблизи Беларуси. Все это вписывается в концепцию транснациональных репрессий, при которых государственный контроль и психологическое давление распространяются за пределы национальных границ посредством цифровых инструментов.

Использование ИИ для создания дискредитирующего контента является одним из ключевых методов воздействия «Белорусского фронта». Анализ публикаций канала выявил устойчивую практику распространения синтетических видеоматериалов, направленных против конкретных политических деятелей беларусской оппозиции. Характерная особенность таких материалов – сексуализированный или унижающий контекст, призванный нанести репутационный ущерб объекту атаки и подорвать доверие к нему со стороны диаспоры и западных партнеров.

Наиболее частым объектом дипфейк-атак со стороны канала является Светлана Тихановская. Публикации носят систематический характер и преследуют две взаимосвязанные цели: создание сексуализированного образа политика и формирование нарратива о ее «роскошной» жизни на фоне усилий рядовых оппозиционных активистов. Так, 27 января 2025 года канал опубликовал видеоматериал, в котором Тихановская якобы целуется с главой МИД Польши Радославом Сикорским; пост сопровождался характерным подзаголовком – «обиженный фотограф главы польского МИД Радослава "шампура" Сикорского слил в сеть полное видео со Сьветой» – и ироничным комментарием «кажется, что ее уже не остановить». 23 сентября 2025 года, в период работы Генеральной Ассамблеи ООН, когда Тихановская участвовала в официальных мероприятиях, канал распространил видео с аналогичным нарративом: «литовская капустница снова попала на камеры недалеко от туалета в здании ООН. Опять потянулась к женатому главе

польского МИД Сиськорскому». Публиковались также сгенерированные сцены поцелуев Тихановской с премьер-министром Польши Дональдом Туском и политиками из Норвегии, а еще одним примером служат фото и видео о том, как якобы проходит празднование Нового года – в роскоши и с большим количеством алкоголя. Весь перечисленный контент был сгенерирован с помощью инструментов ИИ и отличался разным уровнем качества.

Перечисленные публикации используют характерную риторическую технику: нарратив выстраивается как «слив от инсайдера», что имитирует достоверность и журналистский стиль. Подобная подача снижает критический порог восприятия у аудитории и повышает вероятность органического распространения.

Объектом атак выступает и Павел Латушко. 7 февраля 2024 года канал опубликовал видео, преподнесенное как свидетельство резкого сокращения западного финансирования оппозиции: «Госдеп сильно обрезал финансирование змагарским помойкам, теперь "агенту 0,7" пришлось податься в народные целители». Материал представлял Латушко в образе «народного целителя», эксплуатируя интернет-мем о лечении геморроя, и описан в исследовательских материалах как пример сгенерированного ИИ дипфейк-видео – использования лица конкретного политика в дискредитирующем контексте.

Сопоставление двух рассмотренных каналов показывает, что при разном статусе, аудитории и характере публикаций они решают схожие задачи, располагая при этом разным техническим арсеналом: «Людажоры» подробно описывают в своих публикациях используемый инструментарий (обучение моделей под конкретные лица, клонирование голосов, видеогенерация), тогда как о технической стороне материалов «Белорусского фронта» можно судить лишь по самому контенту, качество которого заметно неоднородно. Главная цель у обоих одна – дискредитация конкретных лиц, формирование устойчивых унижающих образов и придание сгенерированному контенту видимости достоверности. Совпадает и динамика: переход от отдельных экспериментов к регулярному производству синтетического контента, что свидетельствует о растущей роли генеративных инструментов в арсенале провластной пропаганды.

Заключение

Собранные нами материалы показывают, что цифровое преследование беларусской диаспоры функционирует как устойчивая система со своей воспроизводимой практикой и логикой. Каждый из описанных случаев показателен тем, что жертвы и цели таких атак почти никогда не находятся в физической досягаемости беларусских государственных органов. Цель же таких атак – демонстрация того, что участие в какой-либо гражданской или публичной деятельности фиксируется и несет неизбежные последствия. Формирование чувства неопределенности, страха и опасения любой публичности и является ключевой целью всех таких операций.

Три части этого исследования демонстрируют эту практику с разных точек зрения. Инфраструктурный анализ фиксирует, как провластные Telegram-каналы образуют связанную сеть: их соединяет общий доступ к материалам силовиков и плотный обмен репостами, а совпадающий ритм публикаций указывает на штатный, а не волонтерский характер их ведения. Типология кейсов показывает, что за разнообразием тактик стоит один и тот же набор приемов, который применяется к любой возможной точке уязвимости (будь то персональные данные, репутация, родственники в Беларуси, имущество, и так далее). Наконец, анализ применения инструментов ИИ фиксирует и переход таких практик в обновленное состояние, где производство синтетических материалов приобретает все более систематический и институциализированный характер и поддерживает пропагандистские нарративы.

Несколько факторов делают эту систему особо устойчивой. Первый – это распределенность ее частей: публикация персональных данных на нескольких каналах, существование различных

государственных реестров, государственных СМИ, и анонимные каналы, авторство которых сложно проследить. Все эти части системы рассредоточивают и ответственность: даже более глубокий количественный анализ различных ресурсов не может установить единый административный центр. Второй фактор – это общая дешевизна такой системы. Например, данные для кампаний преследования чаще всего поступают не из сложных кибератак, а из устройств задержанных, публичных реестров, финансовой отчетности организаций и переписки, оказавшейся в чужих руках. Такую практику легко воспроизводить и намного сложнее остановить. При этом темпы таких атак продолжают расти, а набор инструментов – расширяться.

Для стран, принимающих беларусские диаспоры, из этого следует важный вывод. Цифровое давление почти никогда не дотягивает до порога, за которым включаются обычные механизмы защиты: нет физического вреда, нет исполнителя в пределах юрисдикции, нет события, которое можно квалифицировать как нападение. Однако, именно на это и рассчитана такая система цифрового преследования. Пока же такое давление не признается как серьезный вид транснациональных репрессий наравне с физическими атаками, жизнь в изгнании будет означать не прекращение репрессий, а лишь смену их форм.

Рекомендации

Для беларусских НКО:

- Собирать и хранить персональные данные сотрудников, волонтеров и благополучателей только в объеме, строго необходимом для выполнения функций организации; там, где идентификация не требуется, использовать псевдонимы или идентификаторы вместо имен.
- Ввести политику минимально необходимого доступа: волонтеры и временные сотрудники не должны иметь доступа к полным базам данных получателей помощи, спискам участников или финансовой информации сверх того, что необходимо для выполнения их конкретной функции.
- При структурировании юридических лиц и публичной отчетности в принимающих странах минимизировать публичное упоминание имен физических лиц в реестрах там, где это допускает законодательство.
- Верифицировать любой входящий запрос на интервью, съемку, партнерство напрямую через официальные контакты организации или издания, которое представляет запрашивающий (независимо от убедительности предоставленных документов).
- Информировать новых сотрудников и волонтеров до начала работы о возможных рисках: угрозы в мессенджерах, вербовочные контакты, возможное давление через родственников, остающихся в Беларуси.
- Разработать и распространить среди всех сотрудников и волонтеров инструкцию с описанием признаков вербовочных контактов, предложений псевдоработодателей и операций под прикрытием – с конкретным алгоритмом действий при подозрении и контактом для эскалации внутри организации.
- Заготовить шаблонные протоколы реагирования для типовых сценариев: при обнаружении фейкового бота, клон-канала или рассылки от имени организации публиковать предупреждение для своей аудитории по заранее подготовленному шаблону, не требующему длительного согласования.
- Проводить аудит безопасности публичной инфраструктуры не реже одного раза в квартал, а также внепланово – после любого публичного инцидента или смены ключевых сотрудников.
- Поддерживать регулярный обмен информацией между организациями об актуальных угрозах и выявленных операциях.

Для принимающих государств:

- Содействовать правовой квалификации систематических транснациональных репрессий против диаспор, включая организованный доксинг и целевые кибератаки, одновременно как

уголовно наказуемых деяний, так и формы иностранного вмешательства на территории принимающего государства, затрагивающего его национальную безопасность.
- Рассмотреть возможность введения исключений из требований публичной финансовой отчетности и раскрытия персональных данных руководителей для организаций, работающих в условиях активного противодействия со стороны иностранных государственных акторов (сохраняя необходимый уровень подотчетности перед регулятором в непубличном формате).
- Интегрировать оценку цифровых угроз в процедуры предоставления международной защиты: доксинг, попытки фишинга и целевые кибератаки должны признаваться доказательством индивидуального преследования наравне с физическими угрозами.
- Обеспечить эффективное уголовное преследование операций по сбору разведывательных данных через псевдоработодателей, псевдожурналистов и подставных исполнителей на своей территории.

Для технологических платформ:

- Вести проактивное обнаружение каналов и ботов, систематически публикующих персональные данные физических лиц с призывами к их преследованию, не дожидаясь жалоб от пострадавших, в том числе отслеживать воссоздание ранее удаленных каналов с аналогичным контентом.
- Обеспечить верификацию ботов, собирающих персональные данные пользователей, с прозрачным раскрытием оператора – в первую очередь для ботов, использующих названия и идентичность известных организаций.
- Создать специализированные каналы ускоренного реагирования для правозащитных организаций, документирующих скоординированные операции государственных акторов, с оперативным временем реагирования для случаев раскрытия персональных данных с явной угрозой физической безопасности.
- Разработать политику в отношении синтетического контента, используемого в политических операциях дискредитации, включая обязательную маркировку и ускоренные процедуры приоритетного удаления по заявлению пострадавшего лица или уполномоченной организации.