РАЗВИТИЕ ЦИФРОВЫХ ПРАВ В БЕЛАРУСИ:

ЦИФРОВОЙ АВТОРИТАРИЗМ И ЦИФРОВОЕ СОПРОТИВЛЕНИЕ

Human constanta

Содержание

Вступление

Когда права человека нарушаются офлайн, цифровые права редко избегают подобного удара. Авторитарные правительства все больше заинтересованы в разработке репрессивных практик в цифровом пространстве посредством ужесточения цензуры, излишнего регулирования киберпространства, использования технологий как инструмента пропаганды и массовой слежки.

Беларусь — не исключение. Печально известная как «последняя диктатура Европы» — с ее историей *насильственных исчезновений*, *пыток*, *политического преследования* диссидентов, и удручающей *ситуацией с правами человека*, — Беларусь как цифровая, а не только «аналоговая» диктатура, как правило, обращает на себя меньше внимания. Несмотря на то, что контроль над белорусскими граждан_ками онлайн еще не достиг размаха, характерного таким «классическим» цифровым диктатурам, как Китай с его *«Великим китайским файрволом»* или Россия с ее *«фабриками троллей,»* тенденция к усилению контроля за цифровыми свободами вызывает беспокойство.

События *до, во время и после президентских выборов 2020*, широко признанных в качестве *сфальсифицированных*, положили начало крупнейшему политическому и правовому кризису в новейшей истории Беларуси. Более тысячи людей официально признаны *политическими заключенными*. По состоянию на август 2021 года более *35000* подверглись произвольным задержаниям в *унижающих человеческое достоинство условиях*. С начала президентской кампании как минимум *5500* уголовных дел было возбуждено в связи с «массовыми протестами». На 1 июля 2022 года *11000* уголовных дел было возбуждено по «экстремистским статьям». Сообщается о по меньшей мере *5000* жалобах, поданных летом-осенью 2020 года в связи предполагаемым применением пыток или жестоким обращением, однако власти не возбудили ни одного уголовного дела по расследованию заявлений. При этом Международный комитет по расследованию пыток в Беларуси *задокументировал* около 1500 дел и *признал* наличие доказательств применения пыток в каждом из 50 дел, произвольно отобранных для экспертизы.

К июлю 2022 года число ликвидированных и ликвидируемых некоммерческих организаций достигло *537*. *Все независимые правозащитные организации были ликвидированы* решением беларусских властей к 2021. Журналист_ки, правозащитни_цы, активист_ки продолжают подвергаться задержаниям или вынуждены покинуть страну под угрозой преследования. Изменения в Уголовный кодекс Республики Беларусь фактически *объявили правозащиту вне закона*, криминализировав «деятельность от имени незарегистрированных или ликвидированных организаций» и установив меру пресечения в виде лишения свободы в качестве одной из санкций за нарушение такой нормы.

Беларусские власти продолжают использовать право как инструмент репрессий. *Кодекс об административных правонарушениях* и *Уголовный кодекс* были изменены с тем, чтобы ужесточить наказание за протестную активность, в том числе, посредством *введения смертной казни за «попытки совершения актов терроризма,»* — термин, толкуемый беларусскими властями крайне широко. Изменения, внесенные в *Трудовой кодекс*, ограничили право на забастовку. Изменения в *Закон «О противодействии экстремизму»* расширили понятия экстремизма, включив в него случаи проявления любого

инакомыслия. Изменения в *Закон «О массовых мероприятиях»* усложнили правила проведения массовых публичных мероприятий. Изменения в *Закон «О средствах массовой информации»* и *Закон «Об адвокатуре и адвокатской деятельности»* поместили журналистскую и юридическую сферы деятельности под полный контроль государства. *Закон «О недопущении реабилитации нацизма»* позволяет признавать символы протеста нацистской символикой, а *Закон «О геноциде беларусского народа»* для монополизации исторической памяти и упрощения механизмов по объявлению неугодных высказываний неправдивыми.

В дополнение к *массовым политическим репрессиям*, продолжающимся и усиливающимся с 2020 года, беларусские de facto власти, *не признаваемые в качестве легитимных* многими международными акторами, не остались в стороне от *российского вторжения в Украину*, предоставив беларусскую территорию для совершения нападений. И так плачевная ситуация продолжает ухудшаться, приводя ко все большему подавлению независимых проявлений и сужению пространства для гражданского активизма.

Инструменты цифрового авторитаризма

Цифровое пространство для гражданского активизма также сужается. Несмотря на то, что Беларусь является страной с большим числом интернет-пользователей, с рейтингом 69.5/100 в *GSMA Mobile Connectivity Index 2021*, ситуация с соблюдением цифровых прав в стране оставляет желать лучшего. В рейтинге свободы интернет-пространства *Freedom of the Net Index 2021* Беларусь набирает всего 31 балла из 100, что ярко иллюстрирует ухудшающуюся ситуацию с цифровыми правами на фоне все более усиливающихся репрессий.

Беларусские de facto власти с энтузиазмом осваивают все новые технические решения, которые можно использовать для контроля за населением. Желание защищать цифровой суверенитет с помощью усиления контроля за интернет-платформами часто находит свое выражение в заявления государственных служащих и подконтрольных государству пропагандист_ок. Например, прогосударственный политолог Вадим Боровик в интервью государственному СМИ «Белта» *высказывался*:

«Формирование правильного мышления внутри общества — это возможность обеспечить безопасность нации, право на ее жизнь и существование … Население должно было увидеть, что после событий 2020-го может быть разрушена страна. К счастью, есть лидер, который не боится взять на себя ответственность, рискуя своей жизнью … Во время избирательной кампании мы понимали, что нас обыгрывают в интернете. А теперь они вообще выключают наши СМИ. Мы научились работать в интернете, у нас были конкурентные каналы, но интернет-платформы контролируем не мы. Понимаете, в чем проблема? Сегодня наши телеканалы в любой момент могут отключить. У нас могут быть хорошие "снаряды", умные эксперты, но нужно иметь и средства их доставки. У нас нет средств доставки "снарядов" для информационной войны, поэтому мы должны эффективно защищать внутреннее информационное пространство, как это делает Китай. В ближайшее время с использованием ресурсов Союзного государства мы должны создать замещающие платформы, которые позволят нам эффективно работать с массовым сознанием на нашем культурном пространстве».

Основные репрессивные тактики беларусских властей включают в себя:

- Интернет шатдауны;
- Цензура и преследование за выражение мнений онлайн;
- Государственная онлайн пропаганда;
- Массовое наблюдение.

Организация Freedom House *определяет* цифровой авторитаризм следующим образом:

«Цифровой авторитаризм позиционируется как способ правительств контролировать своих граждан с помощью технологий, в корне меняя концепцию интернета как способа свободного проявления человека».

Беларусские практики, безусловно, могут считаться проявлениями цифрового авторитаризма как способа управления страной посредством цифровых репрессивных и манипулятивных практик.

2.1. Интернет шатдауны

Интернет шатдауны, *понимаемые как* намеренное прерывание интернет-соединения или электронных коммуникаций, которое приводит к отсутствию к ним доступа или фактической невозможности их использования, для осуществления контроля за информационными потоками, особенно часто *использовались беларусскими властями* на пике мирных протестов 2020 года.

Шатдаун, связанный с мирными протестами, продлился в Беларуси всего *121 день*, повлияв на работу наиболее популярных онлайн-платформ в стране, включая YouTube, WhatsApp, Telegram, Viber. Шатдаун предполагал полное отключение интернета в период 9-12 августа 2020 года, а также *снижение* скорости интернет-соединения во время мирных собраний. Отключение интернета в Беларуси служило «механизмом предупреждения проведения мирных собраний, особенно в контексте выборов» — угроза, отмеченная Специальным докладчиком по вопросу о свободе мирных собраний и ассоциаций Организации объединенных наций Клеманом Вулем в его *докладе* «Борьба с интернет-шатдаунами: путь вперед,» а также в *докладе* Управления Верховного комиссара по правам человека 2022 года. Такие механизмы призваны усложнить координацию между протестующими онлайн, а также затруднить своевременный доступ населения к информации, включая сведения о подавлении протестов правоохранительными органами.

Несмотря на многочисленные *заявления* властей, в которых причиной шатдауна называются внешние кибератаки, правозащитни_цы и IT-специалист_ки, на основе анализа предшествующих событий и технической экспертизы, *разделяют мнение* о том, что нарушения в работе сети инициировали представитель_ницы государственной власти.

Более того, несмотря на то, что изначально *ни один из операторов мобильной связи не признал* намеренные действия государства по отключению интернета, все они впоследствии объясняли ухудшение качества сервиса распоряжением компетентных органов. Оператор мобильной связи МТС *уточнял*, что, объясняя необходимость проведения таких мер, государство ссылалось на основание существования угрозы национальной безопасности.

Для отключения интернета беларусские власти применили технологии глубокого исследования сетевых пакетов (Deep Packet Inspection или DPI), приобретенные у частной американской компании *Sandvine* в рамках *контракта* на $2.5 миллиона с российским поставщиком технологий Jet Infosystems. Приобретая оборудование DPI в 2018 году, власти объясняли его необходимость желанием бороться с киберпреступностью. В соответствии с *политикой Sandvine по недопущению нецелевого применения своих продуктов,* компания стремится гарантировать, что ее продукты не будут использованы для препятствования свободным потокам информации или нарушения прав человека. Однако, как свидетельствуют независимые эксперт_ки *Citizen Lab*, DPI-оборудование Sandvine применялось для блокировки вебсайтов и отключения интернета в Турции, Сирии, и Египте. После публичной критики в свой адрес, Sandvine *потребовал* у Национального центра обмена трафиком (НЦОТ) Беларуси возвратить оборудование и «воздержаться от отключения

интернета для целей ограничения доступа беларусов к свободным потокам информации». Тем не менее, сохраняются *опасения*, связанные с практиками компании, способствующим процветанию цифрового авторитаризма в Беларуси и мире.

Ограничения прав на свободное выражение мнения и доступ к информации с помощью интернет-шатдаунов в Беларуси несовместимы с международными обязательствами Беларуси. Международный пакт о гражданских и политических правах содержит 3 условия правомерности мер по ограничению права на информацию и свободу выражения мнений: законность, необходимость и пропорциональность.[1] Такую точку зрения подтверждает и ряд авторитетных международных акторов.[2]

2.2. Цензура и преследование за выражение мнений онлайн

Арсенал инструментов, используемых белорусскими властями для подавления свободы выражения мнений в цифровом пространстве, в значительной степени, основывается на экосистеме «анти-экстремистских» законов, включая Закон «О противодействии экстремизму,» Закон «О борьбе с терроризмом,» Закон «О недопущении реабилитации нацизма,» а также соответствующие нормы Уголовного кодекса и Кодекса об административных правонарушениях, касающиеся преступлений и правонарушений экстремистской направленности.

Даже до *внесения изменений* в Закон «О противодействии экстремизму» в июне 2021 года, беларусское «анти-экстремистское» законодательство было известно размытостью своих формулировок — прежде всего, чрезмерно широким понятием «экстремистской деятельности,» распространяющимся на деяния от «участия в террористической деятельности» и вплоть до «публичных призывов к организации незаконных собраний, митингов, уличных шествий, демонстраций или пикетирования». Такие формулировки предоставляют неограниченные возможности для признания материалов, организаций, и неформальных объединений экстремистскими и вызывают сомнения в отношении истинной мотивации государства при принятии и применении таких законов.

Внесенные в Закон изменения расширяют сферу охвата понятия «экстремизм» еще более, распространяя данное понятие на, inter alia, такие действия, как:

1 *Международный пакт о гражданских и политических правах*, статья 19 (3), *Замечание общего порядка 34, Комитет по правам человека*, 12 сентября 2011, пара. 22.

2 *«Отключение доступа к интернету или сегментам интернета для населения или его части никогда не может быть оправдано, в том числе, по соображениям общественного порядка и национальной безопасности. То же самое применимо и к замедлению интернет соединения». Декларация о свободе выражения в интернете*, 1 июня 2011, пара. 6(b).

«Фильтрация контента в интернете, использование 'kill switches' (i.e. отключение целых сегментов коммуникационных систем) и физическое полное осущетсвление контроля за станциям вещания – это меры, которые никогда не могут быть оправданы по международному праву прав человека». *Совместная декларация о свободе выражения мнений и ответов на ситуации конфликтов*, 4 мая 2015, пара. 4(c).

«Решительно осуждает меры по намеренному ограничению доступа или распространию информации онлайн в нарушение международного права прав человека и призывает государства воздерживаться от таких мер». *Доклад Совета по правам человека ООН*, A/HRC/32/L.20, 27 июня 2016, пара. 10.

«Призывает все государства воздерживаться от и прекращать меры, которые, в нарушение норм права прав человека, направлены на отключение интернета и телекоммуникаций или иное препятствование доступу интернет-пользователей к получению или распространению информации онлайн или к осуществлению онлайн-собраний». Доклад Совета по правам человека, A/HRC/44/L.11, 13 июня 2020, пара. 13.

оскорбление представителя власти в связи с исполнением им служебных обязанностей, дискредитация органов государственной власти и управления;

организация и осуществление массовых беспорядков, актов вандализма, сопряженных с повреждением или уничтожением имущества, захвата зданий и сооружений;

разжигание расовой, национальной, религиозной либо иной социальной вражды или розни, политической или идеологической вражды, вражды или розни в отношении какой-либо социальной группы, в том числе совершение в указанных целях противоправных деяний против общественного порядка и общественной нравственности, порядка управления, жизни и здоровья, личной свободы, чести и достоинства личности, имущества;

содействие осуществлению экстремистской деятельности, прохождение обучения или иная подготовка для участия в такой деятельности;

распространение в этих целях заведомо ложных сведений о политическом, экономическом, социальном, военном или международном положении Республики Беларусь, правовом положении граждан в Республике Беларусь, дискредитирующих Республику Беларусь.

Новая редакция Закона вводит понятие «экстремистского формирования» как «группы граждан, осуществляющей экстремистскую деятельность, либо оказывающей иное содействие экстремистской деятельности, либо признающей возможность ее осуществления в своей деятельности, либо финансирующей экстремистскую деятельность, в отношении которой принято решение Министерства внутренних дел или Комитета государственной безопасности о признании ее экстремистской». Данный термин отличается от понятия «экстремистской организации,» поскольку для признания группы «экстремистской организацией» необходимо вступившее в законную силу решение суда, а решение о признании группы «экстремистским формированием» достаточно решения Министерства внутренних дел (МВД) или Комитета государственной безопасности (КГБ) Республики Беларусь.

Такой упрощенный механизм признания групп граждан_ок «экстремистскими формированиями» ставит под угрозу любые возможности самоорганизации и солидаризации граждан_ок, в том числе в ответ на политические репрессии и грубые нарушения прав человека, делая задачу по криминализации активизма как никогда легкой.

Вероятно, пространные формулировки Закона поспособствовали тому, что создание «экстремистских формирований» и участие в них стали одними из основных правовых оснований для привлечения к уголовной ответственности основатель_ниц, администратор_ок, и подписч_иц нежелательных онлайн-ресурсов. Еще одно популярное основание, на сей раз, для привлечения к административной ответственности, — это «распространение экстремистских материалов». Данная норма применяется как основание для привлечения к ответственности за репосты «экстремистского» контента, комментарии, реакции и даже пересылку материалов в личной переписке.

11 августа 2022 Следственный комитет Республики Беларусь заявил, что в период с 9 августа 2020 по 1 июля 2022, было возбуждено *11 000 уголовных дел* по фактам совершения преступлений «экстремистской направленности».

Некоторые из «анти-экстремистских» дел, связанных с выражением мнения онлайн, особенно ярко иллюстрируют использование «анти-экстремистского» законодательства для подавления цифровых прав:

- В отношении *Анастасии Крупенич-Кондратьевой и Сергея Крупенича* было выдвинуто обвинение в распространении «экстремистских материалов» за пересылку в личных сообщениях постов «экстремистских» Telegram-каналов и применена мера пресечения в виде 15-ти суток административного ареста 8 раз подряд — в совокупности, срок лишения свободы для каждого из них составил 112 дней.

- *Дмитрий Подрез*, IT-специалист из Минска, был признан виновным в нарушении трех статей Уголовного кодекса и приговорен к 7-ми годам лишения свободы за передачу персональных данных сотрудников милиции, задействованных в разгоне мирных протестов, Telegram-каналу «Черная книга Беларуси,» *признанный «экстремистским».*

- *София Сапега*, задержанная беларусскими властями в рамках вынужденной посадки самолета Ryanair в Беларуси в мае 2021, была приговорена к 6 годам лишения свободы за предположительное администрирование Telegram-канала «Черная книга Беларуси».

- Нормы об ответственности за правонарушения, связанные с «экстремизмом,» часто имели обратную силу и применялись для наказания за действия по распространению материалов, совершенные до их признания в качестве «экстремистских». 22 июня 2022, *Николай Б., житель города Иваново*, был обвинен в «распространении экстремистских материалов» за репост материалов с аккаунта «Радио Свобода» от 17 марта 2017 года.

- 9 декабря 2021 года, *Артем Боярский*, бывший студент Беларусского государственного университета, был приговорен к 5 годам лишения свободы за администрирование Telegram-канала «Мая краіна Беларусь».

- Антивоенные высказывания продолжают становиться причиной для уголовного преследования в Беларуси. 28 июля 2022 года, 17-летний автор газеты «Прессобол» *Роман Качина* был задержан за комментарий в социальных сетях, где он говорил, что «беларусы всегда воевали с россиянами». После его задержания, видео с его признательными показаниями в отношении антигосударственных высказываний было опубликовано на прогосударственных Telegram-каналах. В еще одном случае, студентка *Данута Передня* была приговорена к 6.5 годам в тюрьме за репост в один из могилевских чатов текста, в котором в резкой форме критиковались действия Владимира Путина и Александра Лукашенко по развязыванию войны в Украине. Также там содержался призыв к уличным выступлениям и констатировалось отсутствие перспектив у беларусской армии в случае ее прямого вступления в войну.

Помимо репрессивного применения «анти-экстремистских» законов, практики государственной цензуры включают в себя блокировки ресурсов «нежелательных» медиа. Доступ к десяткам ресурсов *был ограничен*, даже без предварительного объявления таких ресурсов «экстремистскими» исключительно на основании решения Министерства информации Республики Беларусь, компетентного принимать подобные решения согласно *Закону «О средствах массовой информации»* и *Положению о порядке ограничения*

(возобновления) доступа к интернет-ресурсам и сетевым изданиям.

Список заблокированных онлайн-ресурсов ведется Государственной инспекцией Республики Беларусь по электросвязи Министерства связи и информатизации. Список *изъят из публичного доступа* и доступен лишь отдельным ведомствам. *Согласно данным TUT.BY (Zerkalo.io)*, уже 22 августа 2020, более 70 вебсайтов, включая belsat.eu, virtuabrest.by, babariko.vision, euroradio.fm, spring96.by, svaboda.org, honestby.org, hramada.org, by.tribuna.com, belarus2020.org, protonmai1.com, psiphon.ca, были заблокированы. Чаще всего блокировались сайты независимых медиа, гражданских инициатив и правозащитных организаций, а также сайты, предоставляющие сервисы VPN и шифрования электронной почты.

Описанные законодательные изменения и практики по расширению определений и сферы ответственности, сужающие и так ограниченное пространство для высказывания альтернативных государственным мнений, нарушают нормы международного права прав человека,[3] ставя под угрозу свободу собраний, ассоциаций и выражения мнений.[4]

2.3. Распространение пропаганды онлайн

Одновременно с проведением с самопровозглашенной *«чистки»* гражданского общества онлайн и оффлайн беларусские власти очевидно пытаются заполнить информационное пространство прогосударственными нарративами путем распространения пропаганды и дезинформации. Поскольку традиционная телевизионная пропаганда *не пользуется популярностью* в беларусском контексте, власти все чаще присматриваются к онлайн-площадкам как платформам для продвижения пропагандистской повестки.

Практика публикации *«покаяльных видео»* онлайн вызывает особые опасения. Со времен выборов 2020 года власти зачастую прибегали к принуждению диссидент_ок признать свою вину или произнести выгодные режиму слова на камеру. Одним из первых примеров такого рода пропаганды стала *запись* лидерки беларусского демократического движения Светланы Тихановской, в которой она призывает население не выходить на массовые протесты и не подвергать свои жизни опасности. Впоследствии Светлана призналась, что видео было записано и опубликовано под давлением.

Беларусские власти покупали рекламу в *Youtube*, на которой воспроизводились «покаяльные видео» Софии Сапеги и Романа Протасевича, задержанных после *вынужденной посадки самолета Ryanair*, следовавшего из Афин в Вильнюс, в Минском аэропорту в мае 2021. *Доказательства* наличия связи между рекламой и беларусскими властями, включают скриншоты, содержащие отсылки к прогосударственному Telegram-каналу «Беларусь — страна для жизни».

«Покаяльные видео» иногда содержали и запись аутинга представителей ЛГБТК+ сообщества. Такие видео, опубликованные на прогосударственных

3 *Доклад Специального докладчика по вопросу о положении в области прав человека в Беларуси, Анаис Марин,* A/HRC/50/5, 50-я регулярная сессия Совета по правам человека ООН, 13 июня - 8 июля 2022, пара. 23.

4 *Доклад Специального докладчика по вопросу о положении в области прав человека в Беларуси, Анаис Марин,* A/HRC/50/5, 50-я регулярная сессия Совета по правам человека ООН, 13 июня - 8 июля 2022, пара. 28.

Telegram-каналах, — еще один инструмент для маргинализации инакомыслящих. Двое из жертв аутинга — *Николай Бределев*, пресс-секретарь оператора мобильной связи A1, и *Артем Боярский*, администратор Telegram-канала.

2.4. Слежка и наблюдение

Для того, чтобы идентифицировать локальных активист_ок и мониторить их деятельность, беларусские власти прибегают к слежке. Массовое наблюдение, важное для успеха цифровой автократии, осуществляется различными способами: регулярный мониторинг публичных профилей в социальных медиа, взлом аккаунтов и девайсов, видео-слежка, сбор данных онлайн.

Несмотря на то, что точные методы наблюдения за граждан_ками и алгоритмы, находящиеся в их основе, непубличны, некоторые заявления государственных представитель_ниц позволяют пролить свет на используемые инструменты. Например, заместитель председателя Следственного комитета Республики Беларусь Анатолий Васильев *утверждал*, что «сложно представить уголовное дело, в котором следователи не изучили бы сведения о телефонных соединениях фигуранта». Он также упомянул автоматизированную информационную систему «След,» используемую с лета 2021 года для отслеживания «цифрового отпечатка» подозреваемых.

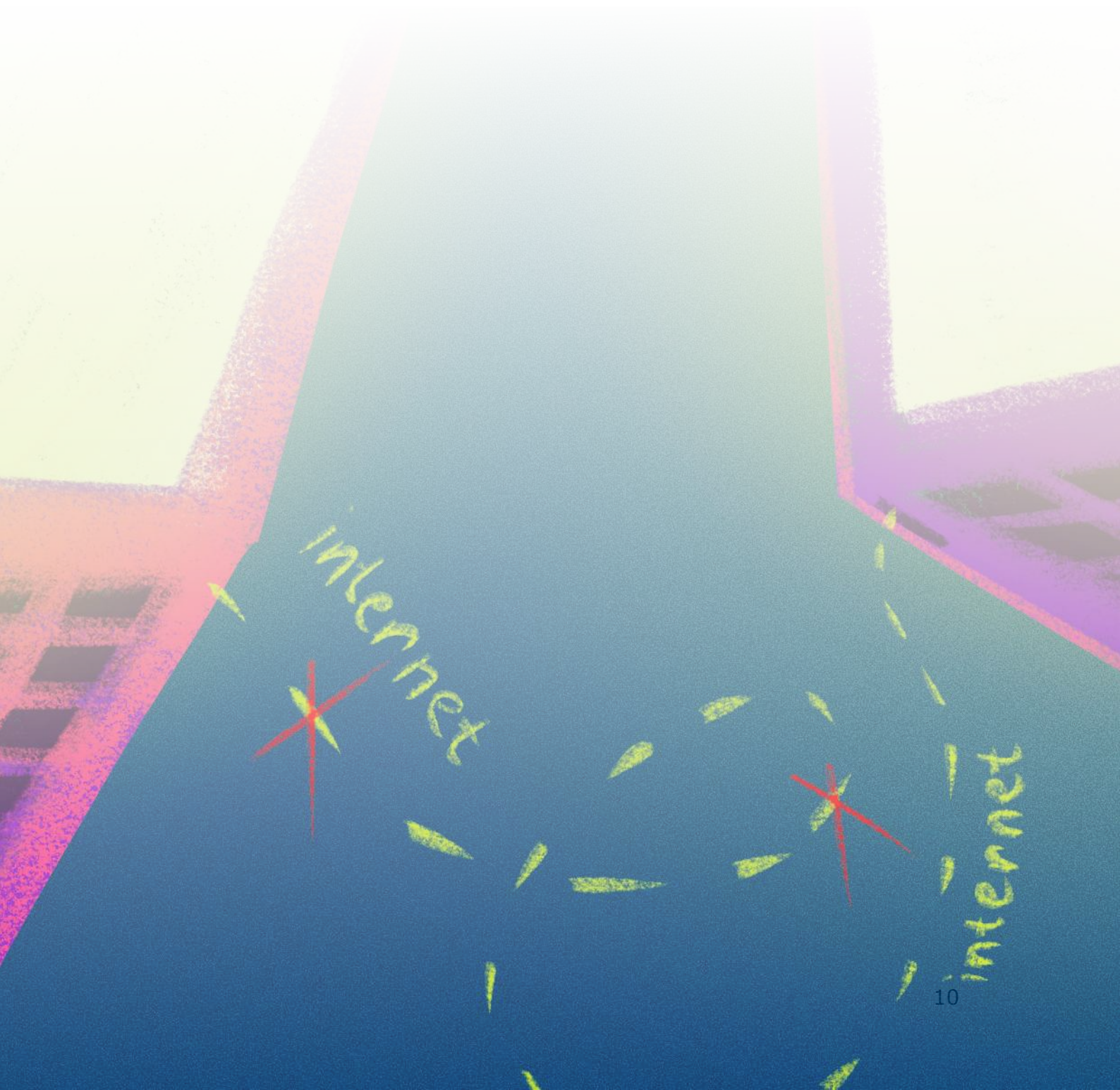
Недавний пример инструмента, используемого беларусскими властями для отслеживания диссидентов, — это система распознавания лиц и видеоаналитики *«Kipod,» разработанная компанией «24x7 Panoptes».* Последняя является дочерним предприятием Synesis — беларусской компании-разработчика, включенной в *санкционный список* Европейского союза за предоставление властям платформы видеонаблюдения и оказания содействия государству в осуществлении репрессий гражданского общества и демократической оппозиции. Synesis был также включен в санкционные списки *Великобритании* and *США*. Алгоритм был интегрирован в *республиканскую систему мониторинга общественной безопасности* по результатам национального тендера. Одним из *событий*, предположительно доказывающим использование платформы для политического преследования, является арест Николая Дедка — известного политического активиста и блогера. Правоохранительные органы установили наблюдение за знакомым Дедка и смогли вычислить стандартные пути перемещения последнего с помощью видеозаписей с камер внешнего наблюдения в Минске, интегрированных в систему Kipod.

Беларусские de facto власти также *прибегали* ко взлому Telegram-каналов, в основном используя тактики давления. Такие тактики включают в себя арест и принуждение администратор_ок ресурсов предоставить доступ к последним, изменение имен и изображений в аккаунтах, изучение списка подписч_иц. Такие меры применялись, например, к каналам «Данные карателей Беларуси» и «Водители 97%».

Другие алгоритмы для идентификации активист_ок включают распространение фишинговых ссылок в Telegram-чатах и поиск мобильных номеров беларусских пользователь_ниц. С помощью таких инструментов правоохранительные органы смогли идентифицировать администраторо_к Telegram-каналов «Белые халаты,» «Мая краіна Беларусь,» «Беларусь 24,» «Баста,» «Беларусь головного мозга».

Еще один вызывающий опасение пример вмешательства государства в

деятельность медиа — взлом Telegram-канала независимого издания «Наша Ніва,» а также аккаунтов трех сотрудников издания. Доказательства, указывающие на связь взлома с деятельностью государственного аппарата, включают в себя предшествующие взлому попытки Следственного комитета получить персональные данные журналист_ок, работающих в издании на постоянной основе, и журналист_ок-фрилансер_ок, которые впоследствии подверглись кибератакам.



Инструменты цифрового сопротивления

Динамику отношений между авторитарными государствами и гражданским обществом таких государств в контексте степени контроля каждой из сторон над технологиями иногда описывают как *«игру в кошки-мышки».* В то время как беларусские власти проявляют явный интерес к использованию киберпространства как еще одного поля битвы и платформы для государственных репрессий, беларусские активист_ки используют киберпространство для продвижения прав человека. Цифровой авторитаризм в Беларуси встречает цифровое сопротивление, создавая феномен *«цифровых диссидент_ок».* Способы защиты цифровых прав от произвольного вмешательства государства разнятся и, в том числе, включают:

- Инструменты civic tech;
- Кибербезопасность и меры цифровой самопомощи;
- Хактивизм/цифровой вигилантизм.

3.1. Развитие civic tech

Мирные протесты 2020 года вывели горизонтальные связи и солидарные действия на новый уровень. Гражданское общество выработало множество технических решений для сопротивления государственным репрессиям и восстановления прав человека. *Civic tech проекты* — то есть, инициативы, использующие технологии для продвижения общественных интересов и благ, — дали граждан_кам возможность безопасно и эффективно сотрудничать для реализации прав человека, которую не может обеспечить государство.

Онлайн-инициативы позволили беларус_кам *верифицировать и считать голоса на президентских выборах*, документировать преступления, совершенные *избирательными комиссиями* и *правоохранительными органами*, *помогать политическим заключенным*, *делиться способами мониторинга и обхода шатдаунов* и *обсуждать новые формы протеста*.

Поскольку беларусские власти доказали свою неэффективность в исполнении своей функции по имплементации прав человека, инициативы civic tech зачастую стали выполнять такую функцию. В авторитарных режимах, где доверие к государственным институтам подорвано и традиционные формы организации гражданского общества немногочисленны и преследуемы, роль технических инициатив особенного важна.

Некоторые из наиболее значимых примеров civic tech инициатив, запущенных беларусскими активист_ками во время и после протестов 2020 года, включают:

- Платформу *ZUBR*, которая собирала и публиковала информацию о составе избирательных комиссий на каждом из избирательных участков, позволяющих избиратель_ницам и наблюдатель_ницам делиться информацией о нарушениях, свидетельни_цами которых они стали. В поствыборный период, функции платформы изменились — вместо мониторинга нарушений она стала использоваться для осуществления гражданского контроля за судебной системой, собирая и систематизируя информацию о судьях и

назначенных мирным протестующим наказаниях.

- Платформу *Голос*, которая, в контексте запрета проведения экзит-полов в Беларуси, собирала и верифицировала информацию о действительном числе голосов, сравнивая данные с официальными. В послевыборный период «Голос» трансформировался в платформу для проведения опросов общественного мнения, включая *опрос* о необходимости проведения переговоров между Офисом Светланы Тихановской и властями, de facto контролирующими беларусское государство.

- Платформу *Skarga.help*, которая в контексте непрекращающегося *преследования и лишения лицензий независимых адвокат_ок* помогает составлять обращения в государственные органы через автоматизированную систему шаблонов.

- Инициативы *Politzek.me* и *Письма в клеточку* представляют собой онлайн-площадки для написания и отправки писем в тюрьма и изоляторы и таким образом помогают коммуницировать с политическими заключенными онлайн.

- Платформу *Avocado.help*, которая помогает нуждающимся в адвокатской помощи связаться с адвокат_кой, а, а жертвам — покрыть сопряженные с такой помощью расходы.

- Плаформу *Legal.Hub*, которая предоставляет безопасную онлайн-площадку для предоставления бесплатных юридических консультаций анонимно и без сбора данных пользователь_ниц.

- Платформу *Цифровая солидарность*, которая систематизирует, структурирует и распределяет ресурсы, а также направляет запросы на оказание финансовой помощи людям, которые находятся под преследованием, в проверенные и прозрачные инициативы помощи.

- Платформа Cyber Beaver, которая существует в форме *Telegram-канала* и *Telegram-чат бота* и предоставляет онлайн консультации по вопросам кибербезопасности, которые помогают представитель_ницам гражданского общества поддерживать кибер-гигиену и минимизировать угрозы и уязвимости.

- Платформа *ICanHelpHost*, которая помогает людям, бегущим от войны в Украине, связаться с теми, кто готов предоставить бесплатное жилье в Европе и за ее пределами.

В Беларуси civic tech решения доказали свою состоятельность в качестве эффективных инструментов для сохранения стойкости гражданского общества перед лицом репрессий. Со временем вызовами для многих платформ становится сохранение их устойчивости, создание экосистем и цифровых инфраструктур, на которые могли бы положиться активные граждан_ки в Беларуси и за ее пределами. Такие устойчивые экосистемы — важный элемент цифрового сопротивления, поскольку они помогают сохранять солидарность и горизонтальные связи, таким образом выдерживая растущее давление со стороны государства.

3.2. Кибербезопасность и кибер-гигиена

Еще один урок, усвоенный многими беларус_ками, живущими в период массовых репрессий, касается важности защиты себя в цифровом пространстве. *Массовые обыски и конфискация оборудования*, *попытки властей взломать аккаунты активист_ок* и *заблокировать «нежелательные» вебсайты*, *проверки устройств на предмет наличия в них «экстремистских» материалов* сделали вопросы кибербезопасности и кибергигиены особенно актуальными для беларус_ок.

Во время интернет-шатдаунов по всей стране использование VPN для многих стало необходимостью, а не просто дополнительной мерой безопасности. Регулярное удаление данных в пограничных пунктах для многих стало привычным действием, необходимым для минимизации рисков преследования за подписки на «неправильные» каналы. Необходимость двухфакторной аутентификации стала более очевидной в локальном контексте — беларусские мобильные номера не могут служить надежным вторым фактором из-за легкости, с которой беларусские правоохранительные органы могут получить доступ к SMS-кодам, высланным на такие номера.

Несмотря на меры самопомощи, принимаемые гражданским обществом для защиты от вмешательства со стороны беларусских властей, некоторые вызовы остаются актуальными. Например, *ключевая роль*, которую продолжает играть Telegram для беларусского общества, делает платформу практически незаменимой, несмотря на ее критику с точки зрения стандартов шифрования данных и защиты личных данных пользователей в целом. Такой Telegram-центризм объясним и понятен — как минимум, потому что очень немногие мессенджеры выполняют также и функцию полноценных агрегаторов новостей. В контексте блокировок многих независимых медиа, сохранение онлайн-присутствия и доступа к аудитории через функционал Telegram-каналов — это практичное решение. Беларус_ки часто используют Telegram не просто как мессенджер для обмена сообщениями, но и как площадку для получения новостей. Однако, каким бы удобным ни было такое решение, риски, связанные с платформой, сохраняются и должны отслеживаться.

3.3. Цифровой вигилантизм и хактивизм

Цифровой вигилантизм часто понимается как совокупность практик самостоятельного отправления цифрового правосудия. Такие практики могут проявляться в различных формах — от деанонимизации представитель_ниц государства, подозреваемых в грубых нарушениях прав человека, до взлома правительственных вебсайтов.

Беларусь — это одна из стран, где к доксингу (doxxing) или деанонимизации, активно прибегали активист_ки для оказания давления на политический режим. Со времен сфальсифицированных выборов 2020 года, последовавших за ними мирных протестов, их жестоких разгонов и связанных с ними длительных сроков тюремного заключения протестующих и даже смертельных исходов для последних, люди стали искать альтернативные способы восстановления справедливости и использовать инструменты гражданского сопротивления для того, чтобы разоблачить нарушитель_ниц и подвергнуть их публичному осуждению.

Такие инициативы, как *Кибер Партизаны*, занимаются взломом государствен-

ных порталов и публикацией чувствительных данных, а такие Telegram-каналы, как «Черная книга Беларуси,» регулярно предают огласке имена, контакты и фотографии сотрудн_иц правоохранительных органов, подозреваемых в нарушении прав человека. Беларусские de facto власти препятствуют деятельности подобных хактивист_ок или вигиланте. Согласно недавно измененным «анти-экстремистским» законам, инициатива Кибер Партизаны была признана *«экстремистской»*, а администраторка «Черной книги Беларуси» *София Сапега* была приговорена к 6 годам тюрьмы. Граждан_ки, передающие информацию таким каналам, часто подвергаются *преследованию за содействие экстремизму*, в то время, как представитель_ницы государства позиционируются как *жертвы* нарушений норм о защите персональных данных или защите чести и достоинства.

В то же время беларусские власти стараются анонимизировать и защитить представитель_ниц правоохранительных органов, задействованных в спонсируемом государством насилии, *позволяя им скрывать свою личность* во время дачи показаний по политически мотивированным делам (с помощью сокрытия лица, изменения голоса или использования вымышленных имен).

Растущая практика деанонимизации кажется, в некотором смысле, палкой о двух концах. С одной стороны, она позволяет сбалансировать влияние репрессивных государств с монополией на управление значительной частью интернет-пространства и влияние активист_ок, которые получают новый рычаг для достижения своих целей. С другой стороны, опасения в отношении потенциального регресса стандартов защиты частной жизни онлайн остаются актуальными.

Выводы и рекомендации

Динамика развития цифровых прав в Беларуси характеризуется попытками беларусских властей атаковать цифровые свободы и попытками активистов защитить и отстоять их. Вполне закономерно, что Беларусь, стремясь к обретению титула полноправной цифровой автократии, продолжает видеть в свободном и открытом интернете угрозу и платформу для распространения «разрушительных» или «экстремистских» идей. Следовательно, необходимо, чтобы все стейкхолдеры, на которых влияют такие авторитарные тенденции и которые могут в ответ влиять на них, предпринимали необходимые шаги для сопротивления репрессивным практикам. Следующие рекомендации сформулированы именно для этой цели:

Бизнесам и платформам:

- Уважать обязательства в сфере бизнеса и прав человека, включая *Руководящие принципы предпринимательской деятельности в аспекте прав человека ООН* и *Принципы ОБСЕ для мультинациональных предприятий*;

- Формулировать и применять подходящие стратегии для работы в обстановке цифрового авторитаризма, балансируя необходимость граждан_ок иметь доступ к ключевым цифровым инструментам и сервисам и необходимость ограничить сотрудничество с репрессивным режимом с помощью предоставления технологий двойного назначения или использования платформ для распространения пропаганды;

- Действовать с должной осмотрительностью в контексте нарушений прав человека (human rights due diligence) в ходе сотрудничества с локальными и региональными правозащитни_цами, журналист_ками, техническими специалист_ками и инициативами в сфере цифровых прав;

- Поддерживать гражданское общество посредством предоставления активист_кам инструментов и решений на основе равентсва, а также посредством поддержки активист_ок в разработке собственных civic tech решений.

Государствам:

- Уважать обязательства в сфере права прав человека онлайн и оффлайн в соответствии с договорным и обычным международным правом;

- Призывать цифровых автократов уважать обязательства в сфере права прав человека онлайн и оффлайн в соответствии с договорным и обычным международным правом;

- Продвигать цифровые права и цифровую грамотность как часть образования в сфере демократического участия и прав человека.

Представителям гражданского общества:

- Участвовать в образовательной, аналитической, и адвокационной деятельности, направленной на повышение осведомленности в вопросах цифрового авторитаризма и его последствий для гражданского общества;

- Оказывать давление на цифровых автократов, требуя привлечения их к ответственности за нарушение прав человека онлайн и оффлайн;
- Поддерживать и повышать осведомленность об инструментах цифрового сопротивления, которые помогают граждан_кам защищать свои цифровые свободы и минимизировать риски.

Human Constanta — правозащитная организация.

Мы работаем с правами человека в трех основных направлениях:

- защита прав иностранных граждан и лиц без гражданства;
- продвижение антидискриминации и образование в области прав человека;
- цифровые свободы и права.

Наша миссия

Продвижение общественных интересов и совместные действия в ответ на современные вызовы в сфере прав человека.

Что мы делаем?

- Помогаем другим защищать свои права.
- Сравниваем беларусские законы и практику с лучшими зарубежными примерами и стандартами прав человека.
- Передаем эти знания через просветительские и образовательные мероприятия.

Авторка документа: Татьяна Зинякова.

Email: info@humanconstanta.org
Website: https://humanconstanta.org