Софинансирование Европейского Союза

ЦЕНТР РАЗВИТИЯ СОВРЕМЕННОЙ ЖУРНАЛИСТИКИ

LPRC ЦЕНТР ИССЛЕДОВАНИЯ ПРАВОВОЙ ПОЛИТИКИ

UDRMI O'ZBEKISTON RAQAMLI HUQUQLAR MEDIA TASHABBUSI

ЦИФРОВЫЕ ПРАВА ДЛЯ ГРАЖДАНСКИХ АКТИВИСТОВ И НКО

Как понимать, применять и защищать на практике?

ЦИФРОВЫЕ ПРАВА ДЛЯ ГРАЖДАНСКИХ АКТИВИСТОВ И НКО

Как понимать, применять и защищать на практике?

Ташкент
2026

Цифровые права для гражданских активистов и ННО. Как понимать, применять и защищать на практике? Пособие. Ташкент, 2026 — 86 стр.

Данное Пособие подготовлено при финансовой поддержке Европейского Союза. Ответственность за его содержание несет исключительно Центр развития современной журналистики, и оно не обязательно отражает точку зрения Европейского Союза.

Коллектив авторов:
Лола Махмудова (Узбекистан)
Мадина Турсунова (Узбекистан)
Ольга Диденко (Казахстан)
Роман Реймер (Казахстан)
Артём Горяйнов (Кыргызстан)

Редактор:
Лола Исламова

Содержание

Как использовать это пособие?

Пособие разработано как практический инструмент для представителей некоммерческих организаций и гражданских активистов, работающих в цифровой среде. Оно объединяет теоретические основы цифровых прав, обзор законодательства и прикладные рекомендации, которые можно использовать в повседневной деятельности. Текст построен таким образом, чтобы читатель мог не только понять ключевые принципы, но и применять их в конкретных рабочих ситуациях.

Пособие можно использовать как последовательно, проходя материал от базовых понятий к практическим вопросам, так и выборочно — обращаясь к отдельным разделам в зависимости от текущей задачи. Первый раздел дает общее понимание цифровых прав и их правовой природы, второй — сосредоточен на практическом применении, т. е. коммуникациях, работе с информацией и контентом, а третий раздел посвящен рискам и мерам безопасности. Такое разделение позволяет быстро ориентироваться в тексте и находить нужную информацию без необходимости читать документ целиком.

В повседневной работе пособие удобно использовать как справочник, например, при подготовке информационной кампании, работе с запросами в государственные органы, публикации контента или оценке рисков. В этих случаях можно сразу обращаться к соответствующим подразделам и использовать предложенные подходы как основу для принятия решений. При этом важно учитывать, что рекомендации в пособии носят общий характер и требуют адаптации с учетом задач конкретной организации и контекста ее деятельности.

Материал также может служить основой для обучения сотрудников и партнеров. Его можно использовать при проведении тренингов, внутренних обсуждений и разработке рабочих процедур. Отдельные разделы могут быть включены в программы повышения квалификации или использоваться как методические материалы для новых сотрудников. Практическая ценность пособия усиливается за счет примеров, структурированных объяснений и типовых ситуаций, с которыми сталкиваются НКО в цифровой среде.

Особое внимание при работе с пособием следует уделять оценке рисков. Цифровая среда предполагает не только возможности для расширения коммуникаций и доступа к информации, но и повышенную ответственность за действия и контент. В тексте неоднократно подчеркивается, что многие решения требуют взвешенного подхода и понимания возможных правовых и репутационных последствий. Поэтому важно использовать материал не как набор готовых ответов, а как основу для анализа и принятия обоснованных решений.

Таким образом, пособие можно рассматривать как рабочий инструмент, который помогает выстраивать более устойчивые, безопасные и эффективные практики в цифровой среде. Его ценность заключается не только в изложении норм и принципов, но и в возможности применять их на практике — в ежедневной работе, проектах и коммуникациях.

Раздел 1
Что такое цифровые права?

1.1. Введение в теорию цифровых прав

Современный мир переживает стремительную цифровую трансформацию, которая охватывает практически все сферы жизни. Доступ к информации, образование, трудоустройство, ведение бизнеса и получение услуг все чаще происходят в цифровой среде. Значительная часть сервисов сегодня предоставляется через онлайн-платформы, разрабатываемые как государством, так и частным сектором. В результате цифровая инфраструктура становится неотъемлемой частью повседневной жизни.

Одновременно с этим быстро растет число пользователей Интернета. По состоянию на октябрь общее количество пользователей в мире превысило 6,4 млрд человек[1]. В Узбекистане, по данным DataReportal, Интернетом пользуются около 32,7 млн человек, что составляет 92,2% населения[2]. Эти показатели наглядно демонстрируют масштаб цифрового проникновения и его значение для общества.

В таких условиях особую важность приобретает регулирование цифрового пространства. Это связано с необходимостью обеспечения и защиты прав человека в новой среде, где традиционные правовые механизмы не всегда оказываются достаточными. Именно в этом контексте формируется и развивается концепция цифровых прав.

Цифровые права человека являются результатом технологической и информационной трансформации общества. По сути, они представляют собой адаптацию классических прав человека, закрепленных в международных документах, к условиям цифровой среды и становятся важной частью современной правовой системы.

Современное понимание прав человека сформировалось на основе таких ключевых документов, как Всеобщая декларация прав человека (1948), Международный пакт о гражданских и политических правах (1966) и Международный пакт об экономических, социальных и культурных правах (1966), а также ряда других международных и региональных актов. В этом виде права человека рассматриваются как совокупность неотъемлемых прав, принадлежащих каждому независимо от национальности, места жительства, пола, этнической принадлежности, языка, религии и других признаков.

Эти права базируются на нескольких фундаментальных принципах.

Во-первых,

универсальность означает, что они применимы ко всем людям без исключения.

Во-вторых,

неотъемлемость предполагает, что права не могут быть произвольно отобраны, за исключением строго ограниченных случаев, предусмотренных законом.

В-третьих,

неделимость подчеркивает, что гражданские, политические, экономические и социальные права взаимосвязаны и не могут полноценно реализовываться по отдельности.

[1] https://www.statista.com/statistics/617136/digital-population-worldwide/?srsltid=AfmBOopuoIjbxLwhRpgdDEsIhkuTmSJ-jYKK6UPJ25PPsIw826z9BPwD

[2] https://datareportal.com/reports/digital-2025-uzbekistan

Для понимания развития прав человека используется концепция «поколений прав человека», предложенная в 1979 году юристом Карелом Вашаком. Она опирается на идею, выраженную лозунгом Великой французской революции (1789 год): «Свобода, Равенство, Братство» и отражает историческую эволюцию правовой мысли.

Первое поколение прав связано с идеей свободы и включает гражданские и политические права. Их основная задача — защита человека от вмешательства государства. Речь идет о так называемых «негативных правах», которые предполагают обязанность государства воздерживаться от определенных действий. Это означает, что для их реализации государство должно не вмешиваться в частную сферу, не ограничивать свободу без законных оснований и не нарушать базовые гарантии личности. В отличие от других категорий прав, такие права не требуют создания сложной инфраструктуры или активных действий со стороны государства, а основаны прежде всего на принципе невмешательства. От власти требуется «ничего не делать» в определенных сферах (не убивать, не сажать без суда, не пытать, не содержать в рабстве, не цензурировать).

Основные права:

- Право на жизнь и физическую неприкосновенность
- Свобода от пыток
- Свобода от рабства
- Свобода слова, совести и религии
- Право на справедливый суд (habeas corpus)
- Избирательные права (активное и пассивное)
- Право собственности

Второе поколение прав связано с идеей равенства и включает социально-экономические права, направленные на обеспечение достойного уровня жизни и социальной защищенности человека. В центре внимания здесь находятся условия, необходимые для полноценного участия человека в обществе — доступ к труду, образованию, медицинской помощи и социальной поддержке.

Основные права:

- Право на труд и справедливую оплату
- Право на отдых (нормированный рабочий день)
- Право на социальное обеспечение (пенсии, пособия)
- Право на охрану здоровья и медицинскую помощь
- Право на образование

В отличие от прав первого поколения, эти права относятся к категории «позитивных». Их реализация требует от государства не только воздержания от вмешательства, но и активных действий. Речь идет о создании соответствующей инфраструктуры, разработке социальных программ и обеспечении механизмов, позволяющих человеку реализовать свои права на практике. Таким образом, государство выступает не просто как гарант невмешательства, а как активный участник, обеспечивающий условия для достойной жизни.

Третье поколение прав связано с идеей братства и включает так называемые коллективные права, или права солидарности. В отличие от предыдущих поколений, они принадлежат не отдельному человеку, а группам людей — народам, нациям или даже всему человечеству в целом.

Основные права:

- Право на развитие
- Право на мир и безопасность
- Экологические права, право на здоровую и чистую окружающую среду
- Право на общее наследие человечества

Эти права отражают понимание того, что ряд глобальных процессов и вызовов невозможно рассматривать исключительно на уровне индивидуальных свобод. Речь идет о таких сферах, как устойчивое развитие, мир и безопасность, благоприятная окружающая среда и общее наследие человечества. Их реализация требует не только действий отдельных государств, но и международного сотрудничества, поскольку многие из этих прав выходят за рамки национальных границ и затрагивают интересы всего мирового сообщества.

Концепция Карела Вашака, была в большей степени благосклонно принята представителями международных организаций, общественных движений, научного сообщества, правозащитниками и активистами.

Помимо благосклонного взгляда были осуществлены попытки обоснования и формирования **четвертого поколения прав человека**[3] в цифровом пространстве, в геномных исследованиях, иных инновационных сферах.

Нас в первую очередь интересует развитие феномена цифровых прав, и мы сосредоточимся исключительно на них.

Информационная революция привела не только к расширению и распространению существующих способов производства и образцов жизни, но и к глобальной замене традиционного промышленно-коммерческого общества новым, «умным» обществом, в результате чего возникло четвертое поколение прав человека — так называемые «цифровые права человека».

Одной из отличительных черт цифровых прав человека является конкретный объект — это информация (данные), представленная в специальном цифровом виде.

Цифровые права человека реализуются с помощью цифровых технологий (цифровая реализация прав) и принадлежат только «цифровым людям» (людям с цифровыми атрибутами).

Обязательства в области цифровых прав человека включают как позитивные, так и негативные обязательства государств и частных субъектов. Таким образом, цифровые права человека лучше привязаны к новому отдельному поколению (или системе) прав[4].

---

[3] https://bigenc.ru/c/prava-cheloveka-i-grazhdanina-chetviortogo-pokoleniia-9a58d6

[4] Гун Нань. 2024. «Четвертое поколение прав человека в умном обществе и трансформация основных конституционных прав»

Логично предположить, что цифровые права суть права человека в Интернет-пространстве.

Тем не менее, для такого рассуждения должна быть подведена соответствующая в том числе и правовая база.

Резолюция «Поощрение защита и осуществление прав человека в Интернете»[5], **принятая Советом по правам человека,** тезисно устанавливает следующее:

Доступ к информации в Интернете способствует широким возможностям для доступного и инклюзивного образования во всем мире, тем самым являясь важным инструментом содействия поощрению права на образование, подчеркивая при этом необходимость обеспечения цифровой грамотности и устранения цифрового разрыва, поскольку он затрагивает осуществление права на образование.

Осуществление прав человека в Интернете, в частности права на свободу выражения мнений, является вопросом, представляющим все больший интерес и важность.

Для сохранения глобального, открытого и интероперабельного[6] характера Интернета крайне важно, чтобы государства решали проблемы в сфере безопасности в соответствии с их международными обязательствами в области прав человека.

Важность применения всеобъемлющего правозащитного подхода к обеспечению и расширению доступа к Интернету.

Неприкосновенность частной жизни в онлайн-среде имеет важное значение для реализации права свободно выражать свое мнение и беспрепятственно придерживаться тех или иных взглядов и права на свободу мирных собраний и ассоциаций.

Важность расширения прав и возможностей всех женщин и девочек путем расширения их доступа к информационно-коммуникационным технологиям.

Резолюция подтверждает, что те же самые права, которые человек имеет в офлайновой среде, должны также защищаться в онлайн-среде.

Таким образом, Совет по правам человека указывает, что права человека, которые можно реализовать в онлайн-среде (становятся цифровыми правами) должны быть защищены.

Обратите внимание, что речь идет как о политических правах (свобода слова и выражения мнения), экономических (право на образование), коллективных (глобальный характер Интернета).

---

[5] https://www.refworld.org/ru/legal/resolution/unhrc/2016/ru/112398

[6] Термин «интероперабельный» (от англ. interoperable) означает способность разных систем, сервисов или технологий работать совместно и обмениваться данными друг с другом без проблем.

Резолюция «Поощрение и защита прав человека в контексте цифровых технологий»[7], **принятая Генеральной Ассамблеей ООН,** дополняет ранее принятую резолюцию:

Все права человека являются универсальными, неделимыми, взаимосвязанными, взаимозависимыми и взаимодополняющими, и подтверждая, что права, которыми люди обладают вне Интернета, должны быть также защищены и в Интернете.

Отмечая, что все более широкое использование цифровых технологий оказывает влияние на осуществление широкого спектра прав человека, и признавая, что цифровые технологии могут способствовать реализации прав человека, но без соответствующих гарантий они могут быть использованы для создания серьезной угрозы защите и полному осуществлению прав человека.

Таким образом, на уровне Организации Объединенных Наций признается, что цифровые права, во-первых, существуют и во-вторых являются прямым продолжением прав человека и в-третьих являются универсальными, неделимыми, взаимосвязанными, взаимозависимыми и взаимодополняющими.

Несмотря на универсальность, неделимость и правозащитный подход цифровые права невозможно представить без доступа к Интернету и различного рода цифровым технологиям, платформам и сервисам.

В этой связи ключевым цифровым правом является право на доступ в Интернет

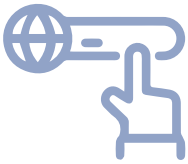
Доступ человека в Интернет сопряжен с различного рода вызовами, рисками и угрозами транслируемыми государствами, технологическими компаниями и иными третьими лицами.

К примеру, цифровой разрыв, ограничение выражения мнения в сети, блокировка доступа в Интернет, нарушение конфиденциальности частной жизни и многое другое.

Отсюда следует, что «вызовы», сопряженные с использованием Интернета, сформировали «ответ» в виде перечня цифровых прав, в большей степени применимых в случаях пользования цифровых платформ и шире Интернета.

[7] https://docs.un.org/ru/a/res/78/213

Перечень цифровых прав

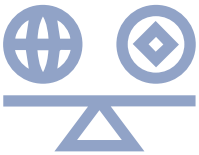


Право на доступ в Интернет

Право человека на техническую и экономическую возможность подключения к глобальной сети, необходимую для реализации свободы слова, получения образования и участия в современной общественной и экономической жизни.

Свобода выражения мнений в Интернете

Право человека искать, получать и распространять информацию и идеи любого рода через цифровые технологии и онлайн-платформы, независимо от государственных границ и без необоснованного вмешательства (цензуры) со стороны властей или корпораций.



Сетевой нейтралитет

Принцип работы Интернета, согласно которому Интернет-провайдеры должны обрабатывать все передаваемые данные одинаково, не блокируя, не замедляя и не отдавая приоритет определенному контенту, приложениям или веб-сайтам в коммерческих или политических целях.

Право быть забытым

Юридический механизм, позволяющий субъекту персональных данных требовать удаления касающихся его сведений из общедоступных источников или прекращения их распространения, при наличии определенных оснований.

Защита от слежки

Специфическая гарантия права на приватность, направленная на предотвращение произвольного вмешательства в личную жизнь через технические средства.

Конфиденциальность данных и защита

Право человека контролировать любую информацию о себе в цифровой среде (сбор, хранение, обработка), а также совокупность правовых и технических мер, гарантирующих защиту этой информации от несанкционированного доступа, утечек и злоупотреблений со стороны третьих лиц (корпораций или государства).

Право на шифрование

Право человека беспрепятственно использовать криптографические технологии и средства защиты информации для обеспечения конфиденциальности, целостности и подлинности своих цифровых коммуникаций и хранимых данных, без обязанности предоставлять ключи дешифрования третьим лицам (включая государство).

1.2. Международные и региональные стандарты в сфере цифровых прав

Цифровая трансформация общества привела к необходимости переосмысления классической доктрины прав человека и их переноса в виртуальное пространство. В основе этого процесса лежит закрепленный на уровне ООН принцип: права человека должны одинаково защищаться как в офлайн-, так и в онлайн-среде.

По состоянию на 2026 год регулирование цифровой сферы уже не является исключительно вопросом национального усмотрения. Оно формируется в рамках сложной системы международных обязательств — от универсальных пактов ООН до специализированных конвенций в области кибербезопасности и защиты данных. Этот нормативный каркас представляет собой многоуровневую систему, в которой глобальные стандарты дополняются и конкретизируются региональными инструментами Совета Европы, Европейского союза, ОБСЕ, ШОС и СНГ, формируя единый правовой контур цифрового статуса личности.

Центральное место в этой системе занимают гарантии ключевых цифровых прав. К ним относятся право на доступ к Интернету, свобода выражения мнений без алгоритмических ограничений и защита частной жизни в условиях экономики данных. Особое значение международные нормы приобретают при определении допустимых ограничений прав. Именно здесь применяется так называемый «трехсоставный тест», который устанавливает требования законности, легитимной цели и пропорциональности, предотвращая превращение государственного регулирования в инструмент цифрового авторитаризма.

При этом развитие стандартов продолжается. Они адаптируются к новым вызовам, связанным с четвертой промышленной революцией, включая вопросы этики искусственного интеллекта, алгоритмической дискриминации и ответственности транснациональных цифровых платформ.

Таким образом, анализ международно-правового фундамента необходим для понимания границ государственного суверенитета и механизмов защиты прав человека в условиях глобальной цифровизации.

Следует учитывать, что представленные ниже стандарты и подходы изложены в обобщенном виде. Их задача — дать читателю представление о логике правовой мысли и одновременно сохранить доступность и читаемость материала.

Международные стандарты

Фундаментом глобального регулирования является принцип эквивалентности прав, закрепленный в резолюции Совета по правам человека ООН (A/HRC/20/L.13, 2012 г.)[8]: «Те же права, которые человек имеет в офлайн-среде, должны быть защищены и в онлайн-среде».

Ядром нормативной базы является **Международный пакт о гражданских и политических правах (МПГПП)[9],** который содержит следующие статьи:

Статья 19 (Свобода выражения мнений, а также получение информации)	Гарантирует право распространять информацию «независимо от государственных границ» и «любыми способами» (включая Интернет, о чем Комитет по права человека прямо указывает в Замечании общего порядка № 34[10]).
Статья 17 (Неприкосновенность частной жизни)	Защищает от произвольного вмешательства в личную жизнь. Комитет по правам человека ООН в Замечании общего порядка № 16[11] интерпретирует это как обязательство государств законодательно регулировать сбор и хранение персональных данных в компьютерах и банках данных.

Помимо МПГПП и Замечаний общего порядка, стоит отдельно выделить роль Специальных докладчиков.

Специальные докладчики ООН через свои тематические доклады играют ключевую роль в развитии стандартов в области защиты и поощрения права на свободу мнений и их свободное выражение.

Несмотря на то, что позиция специальных докладчиков де-факто является «мягким правом» и по существу не обязательна к применению и имплементации отдельными государствами, они задают стиль и вектор правовой мысли для правовых систем отдельных государств.

Таким образом, благодаря работе Специальных докладчиков международные стандарты были дополнены крайне важными элементами, регулирующими подход к реализации и защите некоторых цифровых прав.

Так, опираясь на доклад Франка Ла Рю (A/HRC/17/27), международное право выработало жесткую позицию по Интернет-шатдаунам (право на доступ в Интернет).

Полное отключение доступа к Интернету или мобильной связи считается непропорциональной мерой при любых обстоятельствах (даже в режиме чрезвычайного положения), так как оно парализует работу экстренных служб и наносит несоразмерный ущерб населению, прямо не вовлеченному в предмет чрезвычайного положения.

---

[8] Поощрение, защита и осуществление прав человека в Интернете

[9] https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

[10] https://hrlibrary.umn.edu/russian/gencomm/Rhrcom34.html

[11] https://hrlibrary.umn.edu/russian/gencomm/Rhrcom16.html

Основные доклады

Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Франка Ла Рю 2011 г., A/HRC/17/27[12]

В настоящем докладе рассмотрены ключевые тенденции и проблемы, связанные с правом всех лиц искать, получать и распространять всякого рода информацию и идеи через Интернет. Специальный докладчик подчеркивает уникальный и изменчивый характер Интернета, который позволяет лицам осуществлять не только их право на свободу мнений и их свободное выражение, но и целый ряд других прав человека, а также содействовать развитию общества в целом.
В докладе описаны некоторые способы ужесточения государствами цензуры в отношении информации в Интернете, а именно:

- произвольное блокирование или произвольная фильтрация контента;
- криминализация законного выражения мнений;
- возложение ответственности на посредников;
- лишение пользователей доступа к Интернету, в том числе на основании нарушений закона о правах интеллектуальной собственности;
- кибератаки и отсутствие надлежащей защиты права на неприкосновенность частной жизни и защиту данных.

Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Дэвида Кея 2015 г., A/HRC/29/32[13]

В настоящем докладе Специальный докладчик рассматривает вопрос об использовании средств шифрования и анонимности при передаче цифровых сообщений.
В докладе сделан вывод о том, что шифрование и анонимность позволяют людям осуществлять свои права на свободу мнений и их свободное выражение в цифровой век и ввиду этого должны заслуженно пользоваться надежной защитой.
Ключевой тезис: Докладчик определил шифрование и анонимность как **«зону приватности»,** необходимую для свободного выражения мнений. Он подчеркнул, что «запрет на анонимность оказывает значительный “охлаждающий эффект” (chilling effect) на жертв насилия и репрессий», заставляя их молчать из страха быть опознанными.

Дезинформация и свобода мнений и их свободное выражение

Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Айрин Хан Доклад 2021 г., A/HRC/47/25[14]

В настоящем докладе Специальный докладчик по вопросу о поощрении и защите права на свободу мнений и их свободное выражение рассматривает угрозы, которые возникают для прав человека, демократических институтов и процессов развития в результате дезинформации.
Признавая сложности и проблемы, порождаемые дезинформацией в цифровую эпоху, Специальный докладчик считает, что меры реагирования со стороны государств и компаний являются проблематичными, неадекватными и пагубными для прав человека.
Ключевой тезис: Хан раскритиковала законы о борьбе с «фейк-ньюс», указав, что расплывчатые формулировки дают государствам «политический карт-бланш» на цензуру. Она утвердила стандарт: бороться с ложью нужно не блокировками, а продвижением достоверной информации и цифровой грамотности.

[12] https://docs.un.org/ru/A/HRC/17/27

[13] https://docs.un.org/ru/a/hrc/29/32

[14] https://docs.un.org/ru/a/hrc/47/25

Далее в докладе A/HRC/29/32 Дэвид Кей сформулировал конкретные требования к государствам в вопросах криптографии (право на приватность и шифрование):

1. Государства не должны требовать от платформ внедрения «бэкдоров» (уязвимостей для спецслужб).
2. Государства не должны требовать депонирования ключей шифрования (передачи их на хранение третьей стороне).
3. Ограничение шифрования допустимо только на индивидуальной основе (по решению суда для конкретного устройства), а не массово для всего сервиса.

Наконец в своем докладе Дэвид Кей (A/HRC/38/35). представил доклад о регулировании пользовательского контента (Искусственный интеллект и модерация):

Компании должны обеспечивать «процессуальную справедливость» при модерации. Это означает, что если алгоритм (ИИ) удаляет пост пользователя, человек должен получить:

- уведомление с точной причиной;
- возможность оспорить решение перед реальным сотрудником, а не ботом.

Ограничения цифровых прав т. н. «трехсоставный тест»

Цифровые права не абсолютны и могут быть ограничены при соблюдении определенных условий.

К примеру, согласно п. 3. ст. 19 МПГПП, ограничения законны только при соблюдении трех условий:

Законность:

Ограничение должно быть предусмотрено законом, который доступен, ясен и сформулирован достаточно точно, чтобы гражданин мог предвидеть последствия своих действий. (Расплывчатые формулировки типа «разжигание социальной розни» без определения в законе нарушают этот принцип).

Легитимная цель:

Защита нацбезопасности, порядка, здоровья, нравственности, прав других лиц.

Необходимость и пропорциональность:

Принцип наименьшего вмешательства: Государство обязано доказать, что выбранная мера (например, блокировка) является наименее жестким способом достижения цели. Если можно удалить один комментарий, нельзя блокировать весь веб-сайт.

Бремя доказывания: Лежит на государстве, а не на пользователе.

Важным документом являются **Сиракузские принципы толкования ограничений и отступлений от положений Международного пакта о гражданских и политических правах (1984) (Сиракузские принципы).**

МПГПП при прочих равных позволяет вводить ограничения некоторых прав человека (например, свободу слова или собраний) ради определенных целей (например, общественного порядка). Однако государства часто злоупотребляют этими оговорками.

Цель **Сиракузских принципов** — дать четкое юридическое определение тому, что означают термины «национальная безопасность», «общественный порядок» и «необходимость», чтобы исключить возможность использовать их как предлог для репрессий.

Сиракузские принципы толкования ограничений и отступлений от положений Международного пакта о гражданских и политических правах (далее по тексту — «Сиракузские принципы») устанавливают:

- «Ни одно ограничение осуществления прав человека не вводится иначе, как в соответствии с национальным законом общего применения, который не противоречит Пакту и действует в момент введения ограничения»[15]. (B.i.15 Сиракузские принципы).
- Более того, «Бремя обоснования ограничения права, гарантируемого Пактом, лежит на государстве» (A.12.Сиракузские принципы).

> Сиракузские принципы (1984) являются авторитетным источником толкования допустимых ограничений прав человека. Они устанавливают, что ссылка на национальную безопасность не может использоваться для защиты правительства от критики или сокрытия правонарушений, а любые ограничения должны быть строго необходимыми и пропорциональными угрозе. В цифровую эпоху эти принципы служат главным юридическим аргументом против произвольных блокировок и тотальной слежки».

Региональные стандарты

В отличие от универсального уровня, где многие нормы носят декларативный характер, региональные системы прав человека создают обязательные правовые режимы. В мире сформировалось несколько «конкурирующих» систем цифрового регулирования. В данном руководстве мы сосредоточимся на европейской системе цифрового регулирования.

Европейская система (включает Совет Европы и Европейский Союз)

Европа в настоящее время, является глобальным лидером в кодификации цифровых прав, формируя так называемый «Эффект Брюсселя»[16], когда европейские нормы де-факто становятся мировыми.

В центре нормативной базы находится Европейская конвенция по правам человека (ЕКПЧ), **которая содержит** в себе статью 10 («Свобода выражения») и статью 8 («Частная жизнь»), которые были по существу адаптированы Европейским судом по правам человека (ЕСПЧ) к цифровой реальности.

---

[15] Сиракузские принципы толкования ограничений и отступлений от положений Международного Пакта о гражданских и политических правах http://adilet.zan.kz/rus/docs/O8500000001

[16] https://sg-sofia.com.ua/kogda-rech-zahodit-o-rinkah-evropa-vovse-ne-ugosayushaya-sila#:~:text=%C2%AB%D0%91%D1%80%D1%8E%D1%81%D1%81%D0%B5%D0%BB%D1%8C%D1%81%D0%BA%D0%B8%D0%B9%20%D1%8D%D1%84%D1%84%D0%B5%D0%BA%D1%82%C2%BB%20%D0%BF%D1%80%D0%B5%D0%B4%D0%BF%D0%BE%D0%BB%D0%B0%D0%B3%D0%B0%D0%B5%D1%82%2C%20%D1%87%D1%82%D0%BE,%D0%BD%D0%B5%D0%BC%D0%BD%D0%BE%D0%B3%D0%B8%D0%B5%20%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D0%B8%20%D0%B7%D0%B0%D1%85%D0%BE%D1%82%D0%B5%D0%BB%D0%B8%20%D0%B1%D1%8B%20%D0%BE%D1%82%D0%BA%D0%B0%D0%B7%D0%B0%D1%82%D1%8C%D1%81%D1%8F

Примеры

Cengiz and Others v. Turkey (2015 г.)[17]	Заявители обжаловали, в частности, меру, полностью лишившую их доступа к YouTube. ЕСПЧ установила стандарт, согласно которому блокировка доступа ко всей платформе (в данном случае YouTube) из-за одного видео является нарушением Конвенции, так как лишает граждан доступа к колоссальному объему легальной информации («энциклопедии видеоконтента»).
Delfi AS v. Estonia (2015 г.)[18]	Европейский Суд впервые в своей практике рассмотрел вопрос об ответственности средства массовой информации за контент, размещенный на его веб-сайте пользователями Установил ответственность новостных порталов за разжигающие ненависть комментарии пользователей, если портал получает от этого коммерческую выгоду.

В данном контексте, небезынтересным выглядит **Digital Services Act (2022)**[19]

Если Конвенция 108+ и GDPR (которые будут указаны ниже) защищают ваши данные, то Digital Services Act регулирует контент и ответственность платформ.

Цель принятия создать безопасную цифровую среду и ограничить власть технологических гигантов, через отслеживание содержания (онлайн-контента) и безопасности пользователей.

Важно отметить, что Digital Services Act упоминается в паре с **Digital Markets Act (2022 г.)**[20] Цель принятия, ограничить власть крупнейших технологических компаний, которых закон называет **«гейткиперами»**[21]**.**

Ранее антимонопольные расследования против Google или Apple длились десятилетиями; Digital Markets Act меняет подход: теперь правила установлены заранее, и компании обязаны им следовать под угрозой колоссальных штрафов.

№	Digital Services Act	Digital Markets Act
1	Устанавливает правила реагирования на нарушения	Запрещает определенные практики еще до того, как они нанесли вред
2	Запрет на «темные паттерны» (манипуляции интерфейсом) и рекламу детям	Запрет на «само предпочтение» (продвижение своих сервисов выше конкурентов)
3	Внедрение прозрачных механизмов жалоб и объяснение причин блокировок	Обеспечение «интероперабельности» (совместимости) мессенджеров и систем
4	Защита приватности. Запрет таргетинга на основе религии, здоровья, ориентации	Экономическая справедливость. Запрет гейткиперам использовать данные партнеров для конкуренции с ними
5	Борьба с фейками и юридическая процедура оспаривания блокировки аккаунта отдельного пользователя	Вы можете удалять предустановленные приложения и скачивать софт из разных источников
6	Координаторы цифровых услуг в каждой стране ЕС + Еврокомиссия (для цифровых/технологических гигантов)	Исключительно Европейская комиссия (прямой контроль из Брюсселя)
7	Штраф в случае нарушений до **6%** от годового оборота компании	Штраф в случае нарушений до **10%** от годового оборота компании

[17] https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159188%22]}

[18] https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-155105%22]}

[19] https://www.eu-digital-services-act.com/Digital_Services_Act_Articles.html

[20] https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng

[21] gatekeepers — «вратари» или «контролеры доступа»

Если Digital Services Act и Digital Markets Act регулируют контент и ответственность платформ, то Конвенция 108+, Директива 95/46/EC и GDPR защищают персональные данные.

Международные стандарты, связанные с тематикой защиты персональных данных, проходят сложный «эволюционный» путь и в настоящее время представляют три «поколения» принципов конфиденциальности данных.

К первому «поколению» принципов конфиденциальности данных относится Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных или Конвенция 108[22], принятая в 1981 году.

К принципам второго «поколения» конфиденциальности данных в большей степени относится Директива 95/46/EC[23] о защите физических лиц при обработке персональных данных и о свободном обращении таких данных.

Наконец к третьему «поколению» стандартов конфиденциальности данных относятся GDPR[24] принятые в 2016 году, а также Конвенция 108+, принятая в 2018 году, на основе Конвенции 108.

Необходимо отметить, что в каждом из «поколений» принципов конфиденциальности данных можно условно (!) выделить по 10 стандартов.

Первое «поколение» стандартов	
1	Сбор — ограниченный (не чрезмерный), законный (для законных целей) и честными средствами
2	Качество данных — релевантность, точность, актуальность
3	Определение целей по времени сбора
4	Уведомление о цели/правах
5	Использование, ограниченное (включая раскрытие) указанными или совместимыми целями
6	Безопасность с помощью разумных мер предосторожности
7	Открытость в отношении практики использования персональных данных (не только для субъектов данных)
8	Доступ — индивидуальное право на доступ
9	Исправление — индивидуальное право на исправление
10	Подотчетность — идентифицированный контроллер данных
Второе «поколение» стандартов	
1	Минимальный сбор данных, необходимый для достижения цели (минимизация данных
2	Уничтожение или обезличивание после достижения цели
3	Дополнительная защита конфиденциальных данных в определенных категориях

[22] https://rm.coe.int/1680078c46

[23] https://www.tgl.net.ru/files/infosafety/%D0%B4%D0%B8%D1%80%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D0%B0%2095-46.pdf

[24] https://gdpr-info.eu/

4	Определены законные основания для обработки данных
5	Дополнительные ограничения на некоторые чувствительные системы обработки; «предварительная проверка»
6	Ограничения на автоматизированное принятие решений (включая право знать логику обработки)
7	Возражать против обработки по веским законным основаниям
8	Ограниченный экспорт данных, требующий от страны-получателя «адекватных» или альтернативных гарантий
9	Наличие независимого органа по защите данных
10	Обращение в суд для обеспечения соблюдения прав на конфиденциальность данных
Третье «поколение» стандартов	
1	Защита данных по плану и по умолчанию
2	Демонстрируемая подотчетность
3	Уведомление о нарушении/утечки данных в независимый орган по защите данных
4	Прямая ответственность обработчиков (персональных данных)
5	Более строгие требования к получению согласия
6	Требования пропорциональности во всех аспектах обработки
7	Наличие независимого органа по защите данных для принятия решений и наложения административных санкций, включая штрафы
8	Повышенные (дополнительные) требования к защите биометрических и генетических данных
9	Усиленное право на стирание (данных), включая «право на забвение»
10	Независимый орган по защите данных должен сотрудничать в разрешении международных жалоб

1.3. Национальное законодательство Узбекистана в сфере цифровых прав

Конституция Республики Узбекистан признает верховенство общепризнанных норм международного права. Статья 15 Конституции признает принципы и нормы международного права неотъемлемой частью правовой системы Узбекистана, указывая на то, что обеспечение прав и свобод человека, а также их защита выходят за рамки исключительно внутреннего дела государства. При противоречии международных норм и национального законодательства применяются правила международного договора. Конституционные принципы создают основу для признания верховенства международных стандартов в области свободы выражения мнения, доступа к информации, доступа к Интернету и цифровым сервисам.

Право на свободу выражения мнения и доступ к информации гарантируется статьей 33 Конституции Узбекистана, которая гласит: «Каждый имеет право на свободу мысли, слова и убеждений. Каждый имеет право искать, получать и распространять любую информацию». Государство обязано обеспечить доступ к информации в цифровой форме и создавать условия для обеспечения доступа к всемирной информационной сети Интернет.

Объем прав на доступ к информации, заложенный в статье 34 Конституции предусматривает обязанность государственных органов и организаций, органов самоуправления граждан и их должностных лиц обеспечить каждому возможность ознакомления с документами, решениями и другими материалами, затрагивающими его права и законные интересы.

Статья 49 Конституции устанавливает основание для права на доступ к информации в форме общественного контроля: «Каждый имеет право на благоприятную окружающую среду, достоверную информацию о ее состоянии. Государство создает условия для осуществления общественного контроля в области градостроительной деятельности в целях обеспечения экологических прав граждан и предотвращения вредного воздействия на окружающую среду. Проекты градостроительной документации подлежат общественному обсуждению в установленном законом порядке».

Статья 31 Конституции устанавливает право на защиту частной жизни и персональных данных:

> Каждый человек имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства.
>
> Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, электронных и иных сообщений. Ограничение этого права допускается только в соответствии с законом и на основании решения суда.
>
> Каждый имеет право на защиту своих персональных данных, а также требовать исправления недостоверных данных, уничтожения данных, собранных о нем незаконным путем или более не имеющих правовых оснований».

Конституционные положения составляют основу правовой базы Узбекистан в отношении цифровых прав, свободы выражения мнения, свободы доступа к информации, защиты приватности, персональных данных и частной жизни.

Отдельное законодательство регулирует отношения, возникающие в цифровой среде. Устанавливает ограничения по распространению незаконной информации, ложной и конфиденциальной информации.

Законодательство о свободе информации: проактивный доступ

Задачи законодательства о свободе информации включают обеспечение соблюдения принципов и гарантий свободы информации; реализацию права каждого свободно и беспрепятственно искать, получать, изучать, распространять, использовать и хранить информацию; обеспечение защиты информации и информационной безопасности личности, общества и государства. Право на доступ к информации призвано обеспечить повышение ответственности органов государственной власти и управления и их должностных лиц за принимаемые решения. Каждый человек имеет право на доступ к информации об организации и функционировании

государственных органов и о процессах принятия актов, касающихся данного лица или группы лиц. Однако действующая законодательная база не подразумевает прямого права на информацию, а скорее предусматривает право на поиск информации.

Право на доступ к информации в основном обеспечивается первичными законодательными актами, такими как Закон Республики Узбекистан «О принципах и гарантиях свободы информации», Закон Республики Узбекистан «О гарантиях и свободе доступа к информации», Закон Республики Узбекистан «Об открытости деятельности органов государственной власти и управления», Закон Республики Узбекистан «О средствах массовой информации», Закон Республики Узбекистан «Об официальной статистике», Закон Республики Узбекистан «О борьбе с коррупцией», Закон Республики Узбекистан «О распространении и доступе к правовой информации».

Законодательство предусматривает общее право на доступ как к информации, так и к документам или записям. В отношении применимости правовых требований ко всем ветвям государственной власти закон дает широкое определение держателя информации как юридического или физического лица, которое владеет, пользуется и распоряжается информацией в строгом порядке и чьи права на это не ограничены правами, установленными законодательством или владельцем информации.

При этом в законодательстве отсутствует прямая обязанность подконтрольных государству предприятий, фондов, организаций, наделенных государственными функциями, по обеспечению доступа к информации о своей деятельности. В то время как международные стандарты требуют установления презумпции в пользу доступа к информации, которая должна распространяться на все органы государственной власти, а также на частные организации, получающие государственное финансирование, находящиеся под государственным контролем или выполняющие государственные функции.

В соответствии со ст. 33 Конституции «Ограничения права искать, получать и распространять информацию допускаются только в соответствии с законом и только в той мере, в какой это необходимо для защиты: конституционного строя, здоровья населения, общественной морали, прав и свобод других лиц, общественной безопасности и общественного порядка, а также для предотвращения разглашения государственной тайны или других тайн, охраняемых законом».

Статья 6 Закона Республики Узбекистан Об открытости деятельности государственных органов устанавливает, что доступ к информации о деятельности органов государственной власти и управления ограничивается, если указанная информация отнесена в установленном законом порядке к сведениям, составляющим государственную или иную охраняемую законом тайну. По общему правилу государственные органы, органы самоуправления граждан, общественные объединения, предприятия, учреждения, организации и должностные лица не вправе предоставлять информацию, содержащую государственную или иную охраняемую законом тайну.

Не может быть ограничена в доступе следующая информация:

Акты законодательства о правах и свободах граждан, порядке их реализации, а также устанавливающие правовой статус органов государственной власти и управления, органов самоуправления граждан, общественных объединений и иных негосударственных некоммерческих организаций.

Информация об экологических, метеорологических, демографических, санитарно-эпидемиологических, чрезвычайных ситуациях и другая информация, необходимая для обеспечения безопасности населения, населенных пунктов, производственных объектов и коммуникаций.

Информация, имеющаяся в открытых фондах информационно-библиотечных учреждений, архивах, ведомственных архивах, информационных системах юридических лиц, действующих на территории Республики Узбекистан.

Законодательство позволяет органам государственной власти и управления устанавливать перечень конфиденциальной информации в форме приказов или внутренних актов, в то время как согласно международным стандартам любые ограничения должны быть предусмотрены законом и должны соответствовать трехкомпонентному тесту. Граждане имеют право обжаловать в суд необоснованные решения о засекречивании сведений.

По международным стандартам свободы доступа информации, исключения должны соответствовать конституционным обязательствам государства и включать трехкомпонентный тест, чтобы не допустить необоснованного ограничения права на доступ к информации. Согласно законодательству о государственных секретах, не подлежат засекречиванию следующие сведения:

- сведения о чрезвычайных ситуациях и других случаях, угрожающих жизни, здоровью и безопасности граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и их последствиях;
- сведения о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, медицинского обслуживания, социального обеспечения и сельского хозяйства;
- сведения о состоянии преступности;
- макроэкономические показатели, параметры Государственного бюджета Республики Узбекистан, а также сводные статистические сведения о социально-экономическом развитии Республики Узбекистан;
- сведения о нарушениях прав и свобод человека;
- сведения о нарушениях законодательства государственными органами, иными организациями и их должностными лицами;
- иные сведения, использование, распространение и представление которых не ограничено законом.

Законодательство о доступе к информации не содержит конкретных норм о приоритете общественного интереса при принятии решения об ограничении доступа к информации. Международные стандарты требуют максимального проактивного раскрытия информации и законов, позволяющих использовать исключения в пользу раскрытия информации, имеющей общественное значение.

Запрос информации: реактивных доступ

Законодательство Республики Узбекистан гарантирует открытость деятельности органов государственной власти и управления. Граждане и юридические лица вправе непосредственно либо через своих представителей обращаться с запросом на получение информации о деятельности органов государственной власти и управления.

Запрос на получение информации о деятельности органов государственной власти и управления (далее — запрос) — требование пользователя информации в устной или письменной форме (в том числе в форме электронного документа), направляемое органам государственной власти и управления и (или) их должностным лицам, о предоставлении информации о деятельности этих органов.

(ст. 18 Закона Республики Узбекистан «Об открытости деятельности органов государственной власти и управления»).

Запрос на получение информации в корне отличается от обращений граждан и юридических лиц.

Критерий	Обращение граждан/ юрлиц	Запрос на получение информации
Цель	Содействие в реализации прав, восстановление нарушенных прав, защита законных интересов, предложения по улучшению работы.	Получить конкретные сведения о деятельности органов власти и управления, правоохранительных органов, судебных органов.
Содержание	**Заявление** — просьба о содействии. **Жалоба** — требование восстановить права. **Предложение** — рекомендации по совершенствованию деятельности.	Требование предоставить конкретную информацию. Запрос информации может подаваться устно/письменно и в электронной форме.
Конституционное основание	Право обращаться с заявлениями, предложениями и жалобами.	Право искать, получать и распространять информацию, право на ознакомление с документами, затрагивающими права и интересы.
Правовое основание	Закон РУз «Об обращениях физических и юридических лиц» (виды обращений, требования, сроки).	Закон РУз «Об открытости деятельности органов государственной власти и управления» (понятие запроса, сроки). Закон РУз «О гарантиях и свободе доступа к информации» (право на запрос, формы и сроки). Инструкция О порядке приема, регистрации и обработки запросов на предоставление информации о деятельности государственных органов и органов управления. (рег. № 2769).

Кто подает	Физические и юридические лица.	Любой пользователь информации (физическое лицо, организация, иностранное лицо).
Язык	Обращения подаются на государственном языке, а также на других языках.	Запросы могут быть поданы на государственном языке, а также на других языках.
Куда направляется	В любой орган власти/ должностному лицу.	В любой орган власти/должностному лицу.
Срок рассмотрения	Заявление/жалоба — **до 15 дней**. При доп. изучении — **до 1 месяца**; предложение — **до 1 месяца.**	Запрос пользователя — **до 15 дней** со дня регистрации. Запрос СМИ и журналистов — **до 7 дней.**
Если адресат не компетентен	Перенаправление по компетенции и уведомление заявителя (в пределах сроков закона).	Перенаправление в течение **3 рабочих дня** со дня регистрации с уведомлением пользователя.
Результаты рассмотрения	Решение по существу обращения и ответ о результатах и принятых мерах.	Предоставление информации либо ссылка на уже опубликованные источники (официальные издания/веб-сайт). Мотивированный отказ с обоснованием оснований для отказа в доступе к информации. Доступ к информации о деятельности органов государственной власти и управления ограничивается только в случае, если указанная информация отнесена в установленном законом порядке к сведениям, составляющим государственные секреты или иную охраняемую законом тайну.
Требования к идентификации лица	Обязательны Ф.И.О./адрес (для физлица) или наименование/ адрес (для юрлица) и суть обращения.	Обязательны Ф.И.О./адрес (для физлица) или наименование/адрес (для юрлица) и суть запроса.
Значение	Защита прав и интересов граждан через действия и решения.	Реализация права на доступ к информации о деятельности государства.

Алгоритм подачи запроса на получение информации

Шаг 1.
Определите компетентный государственный орган

Определите орган, который по полномочиям располагает запрашиваемыми сведениями. Запрос должен быть направлен органу или должностному лицу, в полномочия которого входит предоставление информации по вопросам запроса.

Шаг 2.
Уточните полномочия органа

Проверьте официальный веб-сайт органа и его положение о задачах и функциях. Это снижает риск перенаправления запроса и потери времени.

Шаг 3.
Составьте запрос правильно

Запрос — это требование пользователя информации о предоставлении сведений о деятельности органа. Запрос может быть устным, письменным или в форме электронного документа. Сформулируйте один или несколько конкретных вопросов. Если вы запрашиваете документ, укажите наименование и реквизиты, если они известны.

Шаг 4.
Проверьте обязательные реквизиты запроса

Для физического лица укажите Ф.И.О., сведения о месте жительства и суть запроса. Для юридического лица укажите полное фирменное наименование, почтовый адрес и суть запроса. Письменный запрос должен быть подписан пользователем информации. Запрос без данных для идентификации считается анонимным и не рассматривается

Шаг 5.
Выберите канал направления

Закон прямо допускает устную, письменную формы запроса и электронный документ. Электронные обращения на практике подаются через официальный веб-сайт, официальную электронную почту органа через ЕПИГУ (my.gov.uz) или

Шаг 6.
Зафиксируйте факт подачи

Сделайте копию запроса. Сохраните отметку о регистрации, входящий номер или почтовую квитанцию.

Шаг 7.
Контролируйте сроки и переписку

Отсчет срока рассмотрения запроса информации начинается со дня регистрации запроса.

Если по истечении срока ответ на запрос информации не получен, это является нарушением законодательства. Незаконный отказ в предоставлении информации может быть обжалован гражданами и юридическими лицами в органы прокуратуры или административный суд.

Доступ к правовой информации

Основным источником правовой информации является Национальная база данных законодательства Республики Узбекистан **(Lex.uz)**, где представлено текущее законодательство, включая законы, указы и постановления президента, правительственные акты, решения органов государственной власти на местах и другие нормативно-правовые документы.

На портале для всенародного обсуждения законопроектов **regulation.gov** публикуются проекты законов, указов, постановлений, приказов и решений центральных и местных органов государственной власти.

Закон Республики Узбекистан «О распространении правовой информации» (№ ЗРУ-461) закрепляет право каждого гражданина на получение достоверной, своевременной и полной правовой информации. Это включает сведения о законах, подзаконных актах, международных договорах, а также актах органов местного самоуправления.

Документ устанавливает основные принципы, которыми следует руководствоваться при предоставлении правовой информации:

- открытость и доступность;
- обеспечение полноты и достоверности;
- недопустимость вмешательства в частную жизнь при сборе и распространении информации;
- равноправие граждан в доступе к информации.

Государственные органы обязаны бесплатно предоставлять доступ к правовой информации через официальные веб-сайты и другие официальные источники. Электронные версии текстов нормативно-правовых актов подлежат обязательному размещению на официальных веб-сайтах принявших их органов в установленном порядке. Закон также определяет их обязанность информировать население об изменениях в законодательстве и консультировать граждан по правовым вопросам. Формы распространения правовой информации включают официальные публикации в СМИ, размещение на государственных информационных ресурсах и предоставление в печатном виде в государственных учреждениях.

В каждом государственном органе созданы информационные службы в задачи которых входит предоставление правовую информации, регулирующей деятельности государственного органа. По запросу физических и юридических лиц государственные органы и организации разъясняют порядок применения нормативно-правовых актов по вопросам, связанным с их деятельностью. Разъяснения о порядке применения нормативно-правовых актов, подготовленные государственными органами и организациями, имеют обязательную силу для структурных и территориальных подразделений этих органов и организаций.

Правовая пропаганда законодательных актов осуществляется следующими способами:

- проведение конференций, встреч, семинаров, круглых столов и бесед;
- посредством средств массовой информации, в том числе организаций теле- и радиопередач, размещений статей и информационно-правовых материалов в печатных и электронных средствах массовой информации;
- распространение комментариев, брошюр, плакатов, буклетов и флаеров;
- через социальную рекламу (видеоролики, инфографики и др.) и другими видами пропаганды, не запрещенной законодательством.

Физические и юридические лица имеют право обращаться с запросом в государственные органы и организации о предоставлении правовой информации, касающейся их деятельности. Запрос о предоставлении правовой информации подлежит рассмотрению в срок не более **пятнадцати дней** со дня его поступления.

Предоставление правовой информации в электронном виде осуществляется бесплатно. За предоставление правовой информации на бумажном носителе может взиматься плата по соглашению сторон. Отказ в удовлетворении запроса о предоставлении правовой информации должен быть мотивированным. Граждане имеют право обжаловать незаконные действия или бездействие должностных лиц, если они нарушают их право на доступ к правовой информации. Закон также устанавливает ответственность за препятствование получению правовой информации.

Раздел 2
Цифровые права для гражданских активистов и ННО

2.1. Коммуникации в цифровой среде для ННО

Для ННО в Узбекистане коммуникации в цифровой среде — это с одной стороны, возможность расширить свою целевую аудиторию, привлечь потенциальных спонсоров и благотворителей для реализации социально-значимых проектов и инициатив, нужных для общества, с другой стороны — правовые риски ответственности за контент, комментарии, распространение персональных данных и другие нарушения, типичные для цифровой среды.

Коммуникации могут проходить как через внешние каналы — пресс-службы, СМИ, так и через внутренние каналы — собственные веб-сайты, сообщество в социальных сетях, Telegram-каналы, медиапроекты, например, канал подкастов или видео на YouTube.

На веб-сайтах, в социальных сетях и на онлайн-платформах, в мессенджерах контент ННО контролируется на нескольких уровнях: модерацией самих онлайн-платформ, жалобами аудитории и реакцией уполномоченных структур. Поэтому устойчивость коммуникаций зависит не только от качества текста, но и от процесса: кто отвечает за коммуникации, как организация реагирует на кризисы, как модерируются комментарии, осуществляется ли проверка контента перед публикацией? Эта глава будет полезна представителям ННО, отвечающим за коммуникации и информационную поддержку проектов и инициатив.

2.1.1. Стратегия эффективных коммуникаций ННО

Несмотря на огромные возможности и простоту создания и распространения медиаконтента, СМИ остаются одним из главных каналов коммуникаций. Почему? По трем причинам.

Во-первых, СМИ обеспечивают аудиторию и охват контенту ННО. Редакции СМИ уже позаботились о доверии и расширении своей аудитории. Постоянно работают стратегии расширения охвата — улучшение контента, соцсети и вовлеченность аудитории.

Во вторых, бесплатное продвижение кампаний. В большинстве своем СМИ готовы бесплатно продвигать проекты и кампании ННО, привлекать в качестве экспертов представителей гражданского общества.

В-третьих, СМИ оказывают ННО неоценимую помощь при благотворительных акциях. Различные сборы средств и благотворительные акции значительно усиливают своей воздействие при помощи СМИ. Доверие аудитории к СМИ сильнее, чем к социальным медиа.

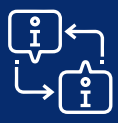
Поэтому эффективная стратегия коммуникаций ННО в цифровой среде должна состоять из нескольких этапов, реализация каждого этапа обеспечивает отличный результат всей стратегии.

Этап 1
Разработайте и реализуйте вместо хаотичных и нерегулярных коммуникаций.

Ваша роль в информационном поле? Ключевые даты, кто спикеры, ключевые сообщения. Основные форматы (пресс-релиз, пост в соцсетях, подкаст, видеоинтервью и т. д.) и каналы распространения.

Этап 2
Определите целевую аудиторию.

Какие каналы информации потребляет ваша аудитория? Работайте только с теми СМИ, которые целенаправленно доставляют ваши сообщения вашей аудитории.



Этап 3
Конвертируйте свою экспертизу в информационную поддержку.

СМИ часто запрашивают комментарии у представителей ННО по всем вопросам информационной повестки дня. Соглашайтесь при условии поддержки ваших проектов и кампаний.

Этап 4
Определите ответственного сотрудника (представителя вашей организации) для коммуникаций.

Ответственный сотрудник, который отвечает за реализацию медиаплана, осуществляет контроль и мониторинг. Не отдельный сотрудник, но ответственный и с хорошими связями в медиа-среде.

Этап 5
Что делать в кризисных ситуациях? Антикризисный план действий.

Ключевые сообщения и действия со СМИ и в социальных сетях. Осторожнее с комментариями в этот период и вовлеченностью аудитории. Должны быть подготовлены точные и ясные сообщения для вашей целевой группы.

Этап 6
Мониторинг публикаций.

Редакции СМИ не будут предоставлять вам ссылки на публикации и сюжеты, но могут представить аналитику по просмотрам и охвату аудитории. Мониторинг публикаций должен быть обеспечен с вашей стороны.

2.1.2. Собственные медиапроекты ННО vs коммуникации с медиа

Многие ННО, чувствуя недостаток или вовсе отсутствие возможностей для публикации информации о своих проектах, целевых группах в СМИ, задумываются (и часто реализуют) собственные медиапроекты.

Выбор между собственным медиапроектом и коммуникациями со СМИ — это вопрос ресурсов и ответственности. Собственный медиапроект дает контроль над темами, темпом и качеством подачи, помогает работать «в своем ритме», формировать доверие к организации и поддерживать долгие кампании. Но минусы тоже очевидны: постоянный поиск финансирования, затраты времени и человеческих ресурсов, необходимость обучения, необходимость в технике для производства качественного аудиовизуального контента, дополнительная правовая ответственность.

Ниже в таблице — вы можете ознакомиться с плюсами и минусами двух подходов для ННО — коммуникации со СМИ или запуск собственного медиапроекта.

	Плюсы	Минусы
Коммуникации со СМИ 	Быстрый доступ к широкой аудитории и доверие к редакции; редакционная проверка и выбор правильного формата для темы; меньше затрат на производство контента и продвижение.	Зависимость от редакционной повестки и формата; ограниченный контроль над заголовками, визуалами; возможны задержки, сокращения или отказ в публикации.
Запуск собственного медиапроекта 	Полный контроль над темами, темпом и качеством; прямой контакт с аудиторией и развитие лояльности. Удобно вести долгие кампании и сохранять архив материалов.	Постоянные расходы на команду, обучение, технику, расходы на веб-сайты и производство контента. Дополнительная ответственность за контент и комментарии. Зависимость от политик платформ и алгоритмов (жалобы, ограничения охвата, блокировки) и необходимость регулярной модерации.

На практике некоммерческие организации часто используют смешанную модель — комбинируют развитие и продвижение собственных медиаканалов для регулярной повестки и архива материалов и работают со СМИ для усиления ключевых тем и проведения информационных кампаний. Это требует значительных ресурсов, но дает максимальную устойчивость: организация сохраняет контроль над базовым контентом и «своим голосом», а через СМИ получает дополнительный охват и доверие аудитории.

2.1.3. Информационные кампании в деятельности ННО

Информационные кампании ННО часто выглядят как серия ситуативных и хаотичных постов на разных онлайн-платформах, без цели повысить осведомленность, изменить поведение, собрать поддержку, привлечь партнеров или повлиять на решение. Но когда мы планируем информационную кампанию именно в цифровой среде, мы особенно сильно зависим от контента и онлайн-платформы. Одинаковое сообщение по-разному «работает» на разных онлайн-платформах, а ошибки быстро масштабируются через репосты и комментарии. Поэтому кампанию разумно строить как проект, определяя цель, аудиторию, ключевые сообщения, даты публикаций, спикеров и заранее выбранные показатели успеха.

При планировании важно помнить, что контент контролируется параллельно на нескольких уровнях: платформами (модерация, ограничения охвата, блокировки), аудиторией (жалобы, проблемные комментарии) и уполномоченными государственными структурами. Это означает, что коммуникационной команде нужны не только идеи для контента, но и понятные правила комментирования и алгоритмы действий в сложных ситуациях.

Ниже в таблице — сокращенный набор KPI (key performance indicators, ключевые индикаторы), достаточный для оценки медиаконтента и кампании в цифровой среде.

KPI кампании	Что показывает?	Где смотреть?
Охваты и показы	Сколько людей увидели контент?	Аналитика онлайн-платформ
Вовлеченность аудитории (реакции, комментарии, репосты)	Насколько контент интересен аудитории?	Аналитика онлайн-платформ
Переходы по ссылкам	Интерес к материалу или действию за пределами поста	Статистика действий, переходов
Действие аудитории (регистрация, заявка и т. д.)	Реальный результат кампании	Формы заявки, анкеты и т. д.
Качество обратной связи	Понимание и доверие (вопросы по сути, обращения)	Статистика обращений

Этих показателей достаточно, чтобы видеть картину — эффективна информационная кампания или нет — без лишней детализации. Охват и вовлеченность показывают, насколько заметна ваша кампания в информационном пространстве, переходы и конверсии — насколько вы эффективно достигаете поставленных целей, а качество обратной связи — насколько вас понимают и доверяют.

2.1.4. Экспертная роль в коммуникациях

Представители ННО в Узбекистане часто становятся экспертами для СМИ не только по «своей» теме, но и по широкому кругу общественных вопросов — от социальной политики и прав уязвимых групп до образования, здравоохранения, трудовых споров, цифровых рисков и благотворительности. Чтобы удерживать такую роль, помните про три важных аспекта:

- СМИ всегда просят комментарий как можно быстрее. Скорость предоставления комментария — существенный плюс к вашей экспертности.
- СМИ любят комментарии по делу, без «воды». Комментарии по существу — признак высокой квалификации эксперта.
- СМИ знают, как много чувствительного контента и это диктует определенную осторожность в формулировках, выборе тем и спикеров. Если вы предоставляете комментарий быстро, по существу и не затрагивая чувствительные темы, то вы идеальный эксперт для СМИ.

Другими словами, СМИ выбирают эксперта, который может быстро дать понятный комментарий, опираясь на проверяемые источники и собственную практику, без эмоциональных оценок и категоричных заявлений.

Ниже — краткий список правил поведения эксперта в формате «**To Do / To Do Not»** (можно использовать как внутренний стандарт для спикеров ННО).

TO DO (делайте)	TO DO NOT (не делайте)
Уточняйте запрос — тема, формат, дедлайн, в какой форме нужен комментарий — текст, аудио или видео?	Не отвечайте «на ходу» по теме без фактов или контекста.
Давайте комментарий для СМИ как можно короче, но при этом как можно более понятно. Буквально, один тезис и к нему два поддерживающих аргумента, пара рекомендаций.	Не уходите в длинные лекции и не начинайте рассказать о себе и своих достижениях.
Ссылайтесь на проверяемые источники (документы, статистика, исследования). Насколько возможно это по дедлайну.	Не ссылайтесь на источники, которые нельзя публиковать или вы в них не уверены.
Используйте нейтральные формулировки, особенно в чувствительных темах; говорите аккуратно про спорные факты.	Не делайте публичных обвинений, громких заявлений и спорных высказываний. Все это будет вирусится в сети, станет мемами и не пойдет на пользу вашей экспертности.

Быть экспертом для СМИ — интересно, но не всегда легко: нужно быть всегда готовыми дать комментарий, быстро ориентироваться в повестке, отвечать коротко и аккуратно. Но плюсов больше, чем минусов: экспертные комментарии усиливают доверие к ННО, расширяют круг партнеров и сторонников, помогают продвигать важные темы в общественной дискуссии. СМИ доверяют ННО как надежным источникам информации, к которым журналисты возвращаются снова и снова.

2.2. Получение информации для проектов и деятельности ННО

Доступ к информации нельзя рассматривать как просьбу к государству поделиться информацией, это — элемент свободы выражения мнений и профессиональный инструмент журналиста. Он включает право искать, получать и распространять информацию и идеи любого рода, независимо от государственных границ. В практическом смысле это означает: редакция и автор имеют право запрашивать и получать данные, документы и записи, которыми располагают государственные органы и организации, а также обосновывать общественную значимость такой информации.

При этом региональная практика показывает, что право формально признается, но реализуется сложно: в рейтинге Global Right to Information Rating Узбекистан занимает 129-е место среди 140 стран. Согласитесь, низкий показатель. Он отражает устойчивые проблемы с открытостью, несоблюдением сроков предоставления ответов на запросы, низким качеством ответов и почти неработающими механизмами обжалования.

2.2.1. Доступ к открытым базам данных, реестрам и информационным системам для поиска информации и документов

В международном праве доступ к информации рассматривается как часть свободы выражения мнений: право не ограничивается публикацией — оно начинается с получения информации.

1. Доступ к информации государственных органов

В первую очередь должны быть доступны материалы, данные и документы, относящиеся к публичным вопросам: решения, отчеты, реестры, протоколы, статистика, закупки, бюджеты, результаты проверок. Это включает как право СМИ получать информацию по общественно значимым темам, так и право общества получать качественный медиаконтент на основе проверенных документов.

2. Доступ к персональным данным о себе

Каждый человек имеет право понять, есть ли о нем сведения в автоматизированных базах, какие именно, кем и с какой целью они собираются и хранятся.

Для некоммерческих организаций это особенно важно в практической работе с данными. ННО регулярно собирают и обрабатывают персональные данные — например, при регистрации участников мероприятий, работе с бенефициарами, донорами, волонтерами или при проведении исследований. В этих условиях организация должна понимать, какие данные она собирает, на каком основании и как обеспечивает их защиту.

Это право также имеет значение при оценке рисков. В случае утечек данных или неправомерного доступа ННО должна быть готова проверить законность обработки информации, оценить последствия и корректно отреагировать. Кроме того, при коммуникациях и публикации материалов важно четко разграничивать общественный интерес и вмешательство в частную жизнь, чтобы не нарушать права людей и не создавать правовые риски для организации.

3. Общественный интерес как ключ к раскрытию

Запросы должны рассматриваться своевременно, по понятной процедуре, а плата за обработку не должна создавать необоснованные барьеры. Любой отказ обязан быть мотивирован: государственный орган должен объяснить, почему именно доступ ограничен, на каком правовом основании и почему ограничение необходимо.

Конечно, мы бы хотели, чтобы информация была доступна СМИ и журналистам, организациям гражданского общества и отдельным гражданам по первому требованию, но ограничения есть, бывают и будут. Будем реалистами. Ограничения могут быть допустимы, но только при строгом обосновании. Это — вопросы, связанные с безопасностью и обороной, международными отношениями, общественной безопасностью, расследованием преступлений, защитой частной жизни, коммерческими интересами, экономической и валютной политикой, интересами правосудия, охраной окружающей среды, конфиденциальностью внутренних обсуждений.

Важно помнить, что сам по себе вопрос еще не доказывает законность ограничения. В профессиональной работе всегда задавайте три вопроса по попытке ограничить доступ к информации:

1. Есть ли прямое основание в законе?
2. Необходима ли закрытость именно этой части информации?
3. Можно ли раскрыть документ частично (с изъятием чувствительных фрагментов), а не закрывать все целиком?

Полезно различать несколько крупных категорий информации (документов, сведений), доступ к которым может быть полностью закрыт или ограничен на время.

Категории информации

Государственные секреты
Наиболее «тяжелая» и закрытая категория документов, но даже здесь действует принцип временности и строгой законности ограничения. Ограниченный круг людей, кто имеет доступ к госсекретам. Журналисты к ним не относятся.

Информация, доступ к которой может быть временно ограничен
Это широкий блок, где чаще всего возникают споры: ограничения должны быть точными, пропорциональными и мотивированными. Однако на практике временное ограничение чаще становится постоянным. Ограничивается доступ ко всему документу, а не к необходимой части.

Информация, которая не подлежит засекречиванию или ограничению
Это сведения, которые по закону должны быть открытыми, потому что напрямую связаны с прозрачностью работы государственных органов и расходованием публичных средств (бюджеты, закупки, решения, отчеты, результаты проверок и статистика по общественно значимым вопросам).

Правовые тайны (частная жизнь, коммерческая тайна и др.)
Эти режимы не отменяют право на общественно значимую информацию, но требуют более аккуратной редакционной проверки и минимизации вмешательства в частную жизнь.

Узбекистан, как и все страны Центральной Азии, успешно внедряет цифровизацию в государственное управление. Это значит, что общественная проверка все чаще начинается не с запроса в государственные органы, а с поиска в открытых цифровых источниках. Это принципиально меняет качество фактчекинга: можно быстро зафиксировать базовые факты (нормативную основу, решения местных властей, сведения о закупках, статистику), а затем уже направлять конкретные запросы, требуя предоставить тот документ, который необходим. Такой подход снижает риск получить «общий ответ ни о чем» и усиливает позицию запрашивающего, потому что государственный орган видит: редакция ориентируется в документах и просит не «в целом», а по существу.

Список ресурсов для получения информации онлайн-

Название ресурса	Ссылка	Описание
Нормативная база законодательства Lex.UZ	https://lex.uz/en/	Национальная база законодательства LexUZ (LEX.UZ), где можно быстро найти действующую редакцию закона, подзаконные акты и официальные тексты.
E-Qaror	https://cabinet-eqaror.gov.uz/ru/auth/login	Единая электронная система разработки, согласования и регистрации постановлений, принимаемых органами государственной власти на местах.
Open Data Portal of the Republic of Uzbekistan	https://data.egov.uz/eng?utm_source=chatgpt.com	Портал открытых данных государственных органов Узбекистана. Обилие данных, включая машиночитаемый формат.
Портал государственных закупок	https://xarid.uzex.uz/home	Электронная система государственных закупок на площадке UzEx (xarid.uzex.uz и связанные сервисы), которая позволяет найти объявления, процедуры и базовые сведения о закупках.
База судебных актов	https://publication.sud.uz/#!/sign/view	Вступившие в законную силу судебные акты по делам различных категорий, вынесенных судами Республики Узбекистан.
Портал национальной статистики	https://stat.uz/ru/47-ofitsialnaya-statistika	Данные об экономике, населении и показателях в других сферах Узбекистана.
Виртуальная приемная Президента РУз	https://pm.gov.uz/ru#/	Сервис для отправки обращения главе государства по широкому перечную вопросов внутренней и внешней политики.
Реестр компаний в Узбекистане	https://orginfo.uz/	Портал данных о статусе и деятельности юридических лиц.

Это не исчерпывающий список, но здесь представлены основные онлайн-площадки для получения важной информации.

2.2.2. Верификация и фактчекинг

Если получен ответ от государственного органа на их запрос, его не нужно подтверждать или верифицировать? Действительно, когда мы сообщаем о каком-то событии или мероприятии, нам чаще всего достаточно процитировать ответ государственного органа на запрос. Так достигается баланс — в публикации будут представлены все точки зрения заинтересованных сторон.

Но если речь идет о расследованиях, государственных закупках, проектах, которые осуществляются за счет бюджетных средств и т. д., ответы от государственных органов и любая другая фактическая информация подлежит **проверке, верификации, или фактчекингу.**

С учетом того, что в Узбекистане предусмотрена как административная, так и уголовная ответственность за распространение ложной информации, верификация и фактчекинг становятся действительно важными. Посмотрите в таблице ниже основные шаги по верификации данных, документов, в том числе полученных от государственных органов.

Действия (шаги) по верификации документов, ответов, данных

Шаг 1.

Зафиксировать утверждение и нужный документ

Сформулируйте один проверяемый факт (сумма, дата, поставщик, «из одного источника», результат проверки) и определите, каким документом или реестром он подтверждается.

Результат: Понятно, что именно проверять и что искать.

Шаг 2.

Найти первоисточник и документ

Комментарий или ответ на вопрос чиновника недостаточны. Это не первоисточник. Ищите первоисточник — документированную информацию.

Результат: Есть опора на документ, а не на мнения или суждение.

Шаг 3.

Найти и ознакомиться с альтернативным источником для подтверждения

Каждый факт лучше подтверждать в трех не связанных между собой источниках информации.

Результат: Снижается риски обвинений в распространении ложной информации.

Шаг 4.

Проверить фактические данные в документе

Сверьте реквизиты документа: номер, дату, наименование органа/организации, предмет, сумму, сроки, Ф.И.О. и должность человека, кто подписал документ.

Результат: Исключаются ошибки и «неполные» документы. Снижается риск жалоб и обвинений.

2.2.3. Аккредитация

Аккредитация как процедура более оперативного доступа к информации традиционно рассматривалась как инструмент для журналистов, однако на практике в Узбекистане она используется ограниченно. В большинстве случаев речь идет о временной аккредитации на отдельные мероприятия с участием главы государства, министров и других должностных лиц. В повседневной деятельности доступ к информации все чаще обеспечивается другими механизмами.

С развитием цифровизации государственные органы постепенно внедряют альтернативные способы открытого доступа к информации. К ним относятся онлайн-трансляции открытых заседаний, публикация протоколов, решений и других документов на официальных веб-сайтах, а также размещение информации в режиме реального времени. Эти инструменты становятся все более значимыми и частично заменяют традиционные процедуры аккредитации.

Формально аккредитация закреплена в законодательстве как способ регулярного взаимодействия с государственными органами. Законы предусматривают возможность получения информации о деятельности органов власти, присутствия на открытых мероприятиях и работы с документами. Однако порядок реализации этих прав во многом определяется внутренними регламентами самих органов — включая правила доступа, регистрацию, квоты и требования безопасности.

Для некоммерческих организаций это означает, что наличие формальных прав не всегда гарантирует фактический доступ к информации. На практике ННО чаще взаимодействуют с открытыми источниками и цифровыми каналами, чем используют процедуру аккредитации.

В этой связи особую роль приобретают онлайн-трансляции и публикации материалов государственных органов. Они позволяют оперативно отслеживать обсуждения, позиции должностных лиц и принимаемые решения без необходимости физического присутствия. Для ННО это удобный инструмент мониторинга, который помогает экономить ресурсы и быстрее ориентироваться в повестке.

Кроме того, такие материалы могут служить отправной точкой для дальнейшей работы. На основе просмотренных заседаний и опубликованных данных организация может более точно формулировать запросы, обращаться за дополнительной информацией и выстраивать аргументацию в своей деятельности. Таким образом, даже при ограниченном использовании аккредитации доступ к информации остается возможным за счет цифровых инструментов и открытых источников.

2.2.4. Защищенность и сохранение в тайне источников информации

Сохранение конфиденциальности источников информации — важный принцип не только для журналистики, но и для деятельности некоммерческих организаций. ННО часто работают с чувствительной информацией, взаимодействуют с бенефициарами, заявителями, экспертами, партнерами и информаторами, которые могут передавать сведения при условии анонимности. Без гарантий конфиденциальности такие люди могут отказаться делиться информацией, особенно если она касается нарушений, злоупотреблений или других вопросов общественного интереса.

В законодательстве Узбекистана защита источников напрямую закреплена применительно к СМИ, однако сами принципы конфиденциальности применимы и к деятельности ННО. Это касается, в частности, работы с персональными данными, а также с информацией, переданной на условиях неразглашения. Организация должна понимать, что в ряде случаев она несет ответственность за сохранность таких сведений и за недопущение раскрытия личности источника без его согласия.

На практике ННО могут сталкиваться с ситуациями, когда от них требуют раскрыть источник информации, предоставить контактные данные или подтвердить происхождение сведений. Такие требования могут исходить как от государственных органов, так и от других заинтересованных сторон. В этих условиях важно выстраивать внутренние процедуры работы с конфиденциальной информацией и заранее учитывать возможные риски.

Рекомендуется с самого начала фиксировать условия конфиденциальности при взаимодействии с источником, например в переписке или в рамках соглашений. При этом важно минимизировать сбор и хранение данных, которые позволяют идентифицировать человека, если в этом нет необходимости для работы. Это снижает риски утечки и повышает уровень защиты.

В случае поступления требований о раскрытии источника информацию не следует передавать автоматически. Необходимо оценить правовые основания такого запроса, привлечь юриста и принять решение с учетом возможных последствий для организации и самого источника. Важно помнить, что защита конфиденциальности — это не только вопрос этики, но и элемент управления рисками, включая репутационные и правовые.

Таким образом, для ННО защита источников информации означает выстраивание ответственного подхода к работе с данными и людьми. Это позволяет сохранять доверие, обеспечивать безопасность информаторов и снижать вероятность давления или негативных последствий для всех участников процесса.

2.2.5. Получение официальной информации через мессенджеры и Telegram-каналы

Коммуникации государственных органов все больше переходят в более оперативный и полностью цифровой формат. Пресс-службы имеют свои аккаунты в социальных сетях и используют каналы и чаты в мессенджерах не только для оперативной связи с журналистами, но и для экстренных и кризисных коммуникаций. Пресс-службы могут сразу публиковать заявления, цифры и разъяснения, быстро реагировать на резонанс и ошибки, доносить позицию напрямую до аудитории, прикладывать фото, видео и документы. Такие коммуникации обеспечивают обратную связь.

Однако, коммуницируя с государственными органами через Telegram-каналы, нужно разделять два уровня — (1) оперативная коммуникация — ответы на вопросы, обратная связь, уточнение или дополнение предыдущей информации, запрос фото или видео, корректировки должностей и других данных и (2) получение официальной информации, на которую безопасно опираться в публикации, при обязательном указании государственного органа, ссылки на веб-сайт.

В некоторых случаях пресс-службы государственных органов сразу уточняют, что Telegram-канал не является источником официальной информации. В таких случаях безопаснее запросить дополнительно информацию через официальные источники и не полагаться на достоверность фактов или документов, полученных через Telegram-канал.

2.2.6. Как действовать в случае проблем? Категории информации «Для служебного пользования», государственные секреты и другие категории информации, доступ к которым может быть ограничен

Практика работы некоммерческих организаций в Узбекистане и в странах Центральной Азии показывает схожие тенденции: доступ к информации нередко оказывается ограниченным, несмотря на формальные законодательные гарантии. ННО, работающие с общественно значимыми темами, регулярно сталкиваются с трудностями при получении данных, необходимых для реализации проектов, мониторинга и подготовки аналитики.

Во многих случаях культура закрытости продолжает преобладать над принципами прозрачности. Государственные органы могут действовать по инерции, предпочитая ограничивать доступ к информации вместо ее раскрытия. Официальные вебсайты и информационные ресурсы не всегда содержат актуальные и полные данные, обновляются нерегулярно, а документы публикуются выборочно.

При обращении за информацией представители ННО также могут сталкиваться с дополнительными барьерами. Запросы сопровождаются уточняющими вопросами о целях получения информации, предполагаемом использовании данных

и дальнейших действиях организации. Хотя такие вопросы не всегда имеют правовое основание, на практике они могут использоваться как способ затянуть процесс или ограничить доступ.

В результате в деятельности ННО возникают типичные проблемы, связанные с доступом к информации.

Нарушения в сфере доступа к информации	Описание нарушения и как действовать
Нарушение сроков ответа	Ответ не предоставляется в установленный законом срок либо направляется с опозданием без объяснений. Иногда заявителю не сообщают о регистрации запроса и не дают промежуточную информацию (кто рассматривает, когда будет готов ответ). Редакционный подход может быть следующим. Фиксируйте дату отправки и регистрации, направляйте короткое напоминание со ссылкой на исходный запрос и просьбой подтвердить статус рассмотрения. Если срок истек направляйте повторный запрос с требованием указать причину задержки и дату предоставления ответа. При необходимости, сразу же отправляйте жалобу в органы прокуратуры.
Неполный ответ на запрос редакции СМИ	В ответе приводят общие формулировки, но не отвечают на конкретные вопросы, не дают запрошенные документы или данные, выбирают для ответов только удобные пункты, либо перенаправляют на веб-сайт без предоставления данных. Часто отсутствуют реквизиты документа (номер, дата), источники данных и ответственное должностное лицо. Как действовать редакции? Сверяйте ответ с пунктами запроса и направляйте уточнение списком — что именно не предоставлено. Просите предоставить копии документов или выписки из них, реквизиты и источник данных. Если часть сведений не может быть раскрыта — можно запросить правовое основание отказа и направить требование о предоставлении остальной части информации.
Отказ предоставить информацию со ссылкой на то, что запрашиваемая информация предназначается только для служебного использования	Не соблюдается процедура отнесения к информации для служебного использования, слишком много документов получают маркировку ДСП, не учитывается срок ограничения, закрывают весь документ вместо частичного ограничения. Редакционный подход здесь должен быть следующим — если документ закрыт целиком, требуйте объяснить, какие именно фрагменты защищаются и почему нельзя предоставить остальную часть.
Отказ предоставить информацию со ссылкой на то, что запрашиваемая информация является тайной, например, коммерческой тайной	Коммерческая тайна часто используется частными организациями и госорганами как аргумент против раскрытия данных. Всегда подчеркивайте, что ваш запрос имеет общественную значимость (например, когда речь о расходовании публичных средств или программах, проектах для социальных сфер). Раскрытие общественно-значимой информации всегда должно быть приоритетом.

Несмотря на различные ограничения в предоставлении государственными органам частными компаниями и организациями информации по запросам, если несколько общих рекомендаций, которые основаны на практическом опыте правовой помощи редакциям СМИ:

- Желательно формулировать запросы ясно и конкретно. Чем точнее сформулирован запрос или обозначены требуемые документы, тем больше вероятность, что вы получите требуемую информацию.

- Не полагайтесь только на запросы. Активно используйте альтернативные источники информации — открытые данные, реестры, базы, в качестве информационного повода — блоги, социальные сети.

Запрашивайте в государственных органах документы, а не комментарии. Комментарии вам могут предоставить эксперты. В таком случае вы меньше зависите от интерпретации и субъективного мнения.

2.3. Ответственность за контент в цифровой среде

В цифровой среде некоммерческие организации выступают не только как получатели информации, но и как ее активные распространители. Публикации на веб-сайтах, в социальных сетях, мессенджерах и других онлайн-платформах формируют публичную позицию организации и напрямую влияют на ее репутацию.

При этом любая размещенная информация — тексты, изображения, комментарии пользователей — может повлечь правовую ответственность. Это касается как собственных материалов ННО, так и контента, распространяемого от имени организации или размещаемого на ее площадках.

Поэтому важно понимать, какие виды контента могут считаться нарушением законодательства, где проходит граница допустимого высказывания и какие риски возникают при работе в цифровой среде.

2.3.1. Что относится к противоправному (запрещенному) и чувствительному контенту

В странах Центральной Азии существует перечень тем для контент-мейкеров, включая ННО, которые в некоторых странах на уровне законодательства являются противоправными (например, Казахстан), в других странах — публикации на эти темы нежелательны, так как могут повлечь существенные проблемы для авторов публикаций, ННО, редакций СМИ, их собственников.

Международные обязательства Узбекистана диктуют, что наиболее явные запретительные меры должны быть приняты в случае, если информация связана:

- с пропагандой экстремизма и терроризма и материалами запрещенных организаций (в том числе, запрет распространения материалов или символики, различных призывов);
- с пропагандой наркотиков;
- с разглашением государственных секретов и вопросами национальной безопасности;
- с разжиганием национальной, этнической или религиозной вражды, hate speech;
- с защитой детей от порнографии и непристойного контента;
- с частной жизнью, персональными данными, если нет явного общественного интереса.

Однако большой перечень тем является чувствительным для журналистов и СМИ, а также для ННО вследствие возможных и реальных правовых проблем, которые могут наступить, если редакция СМИ или ННО в рамках своего медиапроекта или деятельности информационного ресурса будет освещать вопросы из этого списка.

При этом прямого запрета на публикацию на эти темы нет, но все контент-мейкеры хорошо осведомлены о чувствительности этих тем.

Чувствительность этих тем также определяется правоприменительной практикой, возросшим количеством дел в отношении всех, кто производит и распространяет медиаконтент в цифровой среде.

Темы, указанные в ней, не являются табуированными или закрытыми для СМИ, но требует максимальной осторожности, многократной проверки фактов и оценки рисков возможного давления или преследования.

Тема для публикации	Что охватывает тема
Деятельность запрещенных партий	Упоминание или описание деятельности организаций, признанных запрещенными; их заявления и материалы; символика, лозунги, атрибутика; ссылки на их ресурсы; призывы к поддержке, участию или финансированию.
Суициды	Сообщения о суициде или попытке суицида с детализацией причин и обстоятельств. Детальное описание случаев среди несовершеннолетних; публикации, которые могут содержать «инструктивные» детали (способы, места, последовательность действий), что может вызвать эффект Вертера[25].
Частная жизнь высших публичных лиц	Семья и личные отношения; здоровье; место проживания и бытовые детали; личная переписка и фото (за исключением случаев, когда члены семей сами выкладывают фото и информацию в социальные сети); данные о детях и близких; сведения, не связанные напрямую с публичной функцией и исполнением полномочий.
Исторические события	Оценки и интерпретации исторических периодов и событий; темы репрессий, конфликтов, границ, идентичности; спорные памятные даты; исторические сравнения, которые могут провоцировать общественные споры.
Межэтнические конфликты	Инциденты и споры «между группами»; бытовые конфликты, получившие межэтнический оттенок; дискриминация по этническому признаку; язык вражды; обвинения в адрес этнических групп.
Внешняя политика	Международные отношения и заявления должностных лиц; дипломатические конфликты; позиции по войнам/кризисам; международные соглашения; визиты, переговоры, ноты; оценки других государств и их лидеров.
Санкции	Санкционные списки и ограничения (в отношении лиц, компаний, отраслей); заморозка активов, запреты на сделки, поставки, въезд; вторичные последствия для бизнеса.
Коррупция	Антикоррупционные расследования. Обвинения в адрес должностных лиц; конфликты интересов; госзакупки и распределение бюджетных средств.
Социальные конфликты	Конфликты вокруг тарифов, цен, коммунальных услуг, земли и жилья; конфликты между жителями и властями и бизнесом; массовые жалобы; резонансные инциденты.
Дискриминация	Неравное обращение и ограничения по признаку пола, возраста, инвалидности, происхождения, языка, религии и др., а также язык вражды; унижение достоинства; стереотипизация групп.
Митинги и протесты	Массовые собрания, акции, пикеты; призывы к участию; освещение требований участников; задержания и административные меры; публикация фото и видео участников и организаторов.

[25] Эффе́кт Ве́ртера; синдро́м Ве́ртера — массовая волна подражающих самоубийств, которые совершаются после самоубийства, широко освещенного телевидением или другими СМИ, либо описанного в популярном произведении литературы или кинематографа

Забастовки	Коллективные трудовые споры; остановка работы; требования работников; переговоры с работодателем; увольнения/давление; публикация персональных данных работников и профсоюзных активистов.
Вопросы ЛГБТ сообщества	Публикации о правах, дискриминации и безопасности; кейсы насилия и травли; медицинские и правозащитные темы; контент, связанный с сексуальностью.
Языковой вопрос	Статус языков, языковая политика; конфликты вокруг языка обучения и обслуживания; требования «говорить на...»; дискриминация по языковому признаку; резонансные заявления и споры.
Религия	Деятельность религиозных организаций; религиозные обряды и символы; религиозные конфликты; обвинения в экстремизме; чувствительные публикации, которые могут восприниматься как оскорбительны.
Гендерные вопросы	Равные права и возможности; домашнее/гендерное насилие; участие женщин в политике и экономике; репродуктивные права; дискриминация по полу; уязвимые группы женщин, девочек и девушек, которые подвергаются перекрестной дискриминации.

Еще раз подчеркнем, что указанные выше темы не являются табуированными или закрытыми, но требует максимальной осторожности, многократной проверки фактов и оценки рисков.

2.3.2. Ответственность за диффамацию, клевету и оскорбление

Защита чести, достоинства и репутации физических и юридических лиц может быть реализована как через гражданский иск в судебном порядке, так и через административные и уголовные процедуры в случае клеветы и оскорбления.

Вид нарушения	Применимые процедуры	Правовые последствия
Защита чести, достоинства и деловой репутации	Гражданско-правовой порядок через подачу иска в судебном порядке в соответствии со статьей 100 Гражданского кодекса Республики Узбекистан[26].	Публикация опровержения порочащих сведений, компенсация морального вреда, прекращение распространения.
Клевета	Административное дело по ст. 40 Кодекса Узбекистана об административной ответственности (КоАО)[27]. Процедура в соответствии со ст. 139 УК РУ[28] (в том числе, если деяние совершено после применения административного взыскания; отдельно выделено распространение через СМИ, Интернет).	Административный штраф 20–60 БРВ. Меры ответственности в уголовном порядке. Штраф (в т. ч. до 200 БРВ; при публикации через СМИ или Интернет штраф составит 200–400 БРВ), обязательные работы или исправительные работы, возможно ограничение свободы; при квалифицирующих признаках могут быть применены более строгие санкции (в т. ч. штраф 300–500 БРВ или ограничение свободы до 3-х лет).

[26] Статья 100. Гражданский кодекс Республики Узбекистан. Текст кодекса доступен по ссылке: https://lex.uz/docs/111181#159215

[27] Статья 40 Кодекса Республики Узбекистан об административной ответственности. Текст кодекса доступен по ссылке: https://www.lex.uz/acts/97661

[28] Статья 139 Уголовного Кодекса Республики Узбекистан. Текст кодекса доступен по ссылке: https://www.lex.uz/acts/111457

Оскорбление	Административный порядок в соответствии со статьей 41 КоАО[29]. При наличии оснований может быть применены уголовно-правовые процедуры в соответствии со статьей 140 УК РУ (в т. ч. если совершено после применения административного взыскания; отдельно при распространение через СМИ или Интернет[30]).	Административный штраф составит от 20 до 40 БРВ. Меры уголовной ответственности: штраф до 200 БРВ; при публикации через СМИ/Интернет — 200–400 БРВ), обязательные работы или исправительные работы; при квалифицирующих признаках штраф составит от 400 до 600 БРВ или ограничение свободы от 1 года до 2-х лет.

2.3.3. Ответственность за распространение ложной информации

Ответственность за распространение ложной информации была внедрена как мера реагирования на волну фейков в период пандемии, которые были связаны, в основном, с рисками и последствиями вакцинации, лечения, последствий пандемии и т. д. Пандемия давно завершилась, однако ответственность за распространение ложной информации широко применяется сейчас в основном в отношении журналистов и блогеров. При этом, известно, что чрезмерно широкие основания и меры уголовной ответственности в отношении контент-мейкеров имеют охлаждающий эффект — то есть, журналисты, редакции СМИ, блогеры начинают избегать острых тем, смягчать формулировки, отказываться от расследований и критических материалов, быстрее удалять публикации и закрывать обсуждения из-за риска привлечения к ответственности; повышается уровень самоцензуры. Такой же эффект возможен и в отношении представителей ННО.

Ответственность за распространение ложной информации в Узбекистане предусмотрена двух видов — административная и уголовная. Ниже в таблице мы указали правовые основания возникновения нарушений и меры ответственности, которые могут быть применены в случае распространения ложной информации.

Виды ответственности	Когда применяется?	Меры ответственности
Административная ответственность 	1. Распространение ложной информации, в том числе в СМИ, Интернет, приводящее к унижению достоинства личности или дискредитации личности[31]. 2. Распространение ложной информации, в том числе в СМИ, в Интернет, содержащей угрозу общественному порядку или безопасности[32].	Административный штраф 50 БРВ или 50–100 БРВ (в зависимости от части статьи).
Уголовная ответственность 	Распространение ложной информации, в том числе в СМИ, Интернет, приводящее к унижению достоинства личности или дискредитации личности, совершенное после применения административного взыскания за такие же действия[33].	Штраф до 150–200 БРВ; обязательные работы до 240–300 часов или исправительные работы до 2-х лет или ограничение свободы до 2–3 лет.

[29] Статья 41 Кодекса Республики Узбекистан об административной ответственности. Текст кодекса доступен по ссылке: https://www.lex.uz/acts/97661

[30] Статья 140 Уголовного Кодекса Республики Узбекистан. Текст кодекса доступен по ссылке: https://www.lex.uz/acts/111457

[31] Статья 202 Кодекса Республики Узбекистан об административной ответственности. Текст кодекса доступен по ссылке: https://www.lex.uz/acts/97661

[32] Там же

[33] Статья 244 Уголовного Кодекса Республики Узбекистан. Текст кодекса доступен по ссылке: https://www.lex.uz/acts/111457

2.3.4. Язык вражды (hate speech)

В странах Центральной Азии, включая Узбекистан, тема hate speech (языка вражды) прежде всего связана с уголовно-правовым запретом возбуждения национальной, расовой, этнической или религиозной вражды. В Узбекистане такой запрет реализован в Уголовном кодекса, статья 156 «Возбуждение национальной, расовой, этнической или религиозной вражды»[34].

Статья охватывает умышленные действия, направленные на разжигание вражды и унижение достоинства по указанным признакам, а также изготовление, хранение с целью распространения и распространение материалов, которые пропагандируют такую вражду. Это означает, что зона риска возникает не только в авторском тексте, но и при републикации чужих материалов, в заголовках и иллюстрациях, а также в комментариях аудитории на площадках редакции СМИ или информационных ресурсах ННО как у распространителя контента.

Отдельный смежный риск — «пропаганда войны» (ст. 150 Уголовного Кодекса Узбекистана)[35]. Под действие статьи подпадает распространение идей или призывов с целью вызвать агрессию одного государства против другого; санкция предусматривает лишение свободы от 5 до 10 лет. Практический вывод простой: в темах, где возможен язык вражды или призывы к насилию, нужна максимально нейтральная подача, отказ от обобщений и стереотипов, аккуратное цитирование (без тиражирования оскорбительной лексики) и быстрая модерация комментариев для того, чтобы ваш ресурс не становился каналом распространения запрещенных материалов.

2.3.5. Ответственность за комментарии

Теперь более подробно остановимся на вопросе ответственности ННО за контент, который оставляют пользователи под публикациями. Комментарии могут и не касаться обсуждаемой статьи, но есть риск того, что тексты комментариев могут содержать противоправный контент, оскорбление, hate speech, чужие персональные данные, порочащие сведения, ложную информацию. Комментарии могут быть проблемными с точки зрения разделения ответственности между автором комментария и редакцией СМИ или блогером.

За содержание комментария несет ответственность сам автор комментария, однако редакции СМИ, блогеры, представители ННО обязаны не допускать использования веб-сайтов, блогов для размещения запрещенной информации, что прямо закреплено в Законе «Об информатизации»[36]. Поэтому отсутствие модерации[37] и игнорирование обращений повышают риски.

Где проходит грань ответственности между автором комментария и владельцами онлайн-ресурса? Риски для редакции СМИ и ННО быть привлеченными

---

[34] Статья 156 Уголовного Кодекса Республики Узбекистан. Текст кодекса доступен по ссылке: https://www.lex.uz/acts/111457

[35] Там же

[36] Статья 12 Закона Республики Узбекистан «Об информатизации». Текст закона доступен по ссылке: https://lex.uz/acts/82956

[37] Модерация — это процесс контроля контента, публикуемого пользователями, на соответствие правилам сайта, соцсети или форума. Основная цель — обеспечить безопасность, удалить спам, оскорбления и запрещенные материалы, тем самым защищая репутацию площадки. Она может быть ручной (модератором) или автоматической (алгоритмами)

к ответственности за проблемный комментарий резко повышаются, если есть хотя бы один из трех факторов:

Одобрение проблемного комментария (закрепили, выделили, сослались как на «позицию аудитории»)

Отсутствие модерации (нет ответственного, нет правил, нет удаления)

Игнорирование обращений на комментарии (не удаляете явное нарушение, не фиксируете реакцию)

Чтобы избежать ответственности за проблемные комментарии, можно разработать и внедрить:

- правила комментирования для пользователей;
- внутренний порядок премодерации и модерации.

Правила комментирования для пользователей — это публичная политика (позиция) контент мейкера по разделению ответственности за возможные проблемные комментарии. Вот обязательный минимум, которые необходимо включить в эти правила:

- Правила комментирования для пользователей применяются ко всем комментариям на веб-сайте и в аккаунтах ННО в социальных сетях и в мессенджерах.
- Оставляя комментарий, пользователь подтверждает согласие с правилами и несет личную ответственность за содержание.
- Запрещены в комментариях оскорбления и унижение достоинства, дискриминация, разжигание розни и призывы к насилию, экстремизм, пропаганда войны, порнография и наркотики, ложная информация, а также фишинг, спам, навязчивая реклама, публикация персональных данных и личной переписки, скринщоты, нецензурная лексика.

ННО вправе удалять комментарии, нарушающие правила, и блокировать пользователей.

ННО рассматривает обращения о нарушениях и принимает меры, включая удаление и ограничение доступа.

Кроме Правил комментирования, редакция СМИ или ННО может разработать и принять **внутренний порядок модерации комментариев.** Вот какие положения должны быть включены в этот документ (минимальный перечень):

- Определяется модель — это будет премодерация или постмодерация? Для тем повышенного риска (рознь, насилие, война, фейки, персональные данные) устанавливается усиленный режим (например, премодерация или ограничение комментариев).
- Устанавливаются сроки — как быстро проверяются новые комментарии и как быстро вы реагируете на жалобы (например, в течение рабочего дня или в течение нескольких часов для тем высокого риска).
- Закрепляется, что комментарии, содержащие запрещенный контент и нарушения Правил комментирования, удаляются (или скрываются), а пользователи при повторных нарушениях блокируются. Решения принимаются по единым критериям.

- Для спорных или потенциально рискованных случаев предусмотрена фиксация проблемных комментариев. Это означает, что необходимо сохранить ссылку на комментарий, дату и время. Скриншоты проблемных комментариев делаются только для внутреннего досье и не распространяются.

- Определяется, какие случаи обязательно передаются руководству или юристу. Это комментарии, где есть признаки возбуждения розни, призывы к насилию, экстремизм, публикация персональных данных, ложная информация, пропаганда наркотиков и другой запрещенный контент.

- Запрещается закреплять, цитировать или републиковать проблемные комментарии как «позицию аудитории». Любое выделение комментария рассматривается как дополнительный фактор ответственности.

2.3.6. Правила онлайн-платформ (социальных сетей) по контенту

Отдельно затронем вопрос с правилами онлайн-платформ по контенту. Выше мы разбирали проблемные ситуации, когда ответственность за контент в цифровой среде может наступить в соответствии с национальным законодательством Узбекистана. Но онлайн-платформы действуют также по своим правилам. Это отдельный риск, так как контент могут заблокировать, вынести предупреждение, отключить монетизацию или заблокировать аккаунт. Каждая онлайн-платформа имеют собственную политику, которая является публичной и обязательной для выполнения.

Какой контент является проблемным с точки зрения политик онлайн-платформ?

- hate speech или язык ненависти (дегуманизация, унижение, призывы к дискриминации или насилию), как указано выше;

- опасный контент и призывы к насилию, экстремистский и террористический контент;

- дезинформация в чувствительных темах (здоровье, безопасность, кризисы);

- травля, домогательства или угрозы;

- персональные данные и публикации, которые нарушают приватность.

Политики онлайн-платформ:

Meta (Facebook, Instagram) Hateful Conduct
https://transparency.meta.com/policies/community-standards/hateful-conduct/?utm_source=chatgpt.com

YouTube Hate Speech Policy
https://support.google.com/youtube/answer/2801939?hl=en&utm_source=chatgpt.com

TikTok
https://ads.tiktok.com/help/category?id=535nt8Z20sG4lW62MZPJvL

Telegram
https://telegram.org/moderation

Практический вывод: ориентируйтесь в политике публикаций не только на действующее законодательство Узбекистана, но и на четко очерченные запрещенные зоны онлайн-платформ, особенно в темах, которые затрагивают вопросы дискриминации, насилия, фейков и персональных данных. В спорных случаях безопаснее снижать риски, публиковать контент, который не вызовет проблем, но при этом не обходит стороной общественно-значимые темы.

2.4. Авторские права и ННО

Закон Республики Узбекистан «Об авторском праве и смежных правах» (ЗРУ-42 от 20.07.2006) устанавливает, что авторское право возникает «в силу факта создания» и не требует регистрации или иных формальностей.

В цифровой среде публикация в сети Интернет является «доведением до всеобщего сведения» — когда пользователи могут получить доступ «из любого места и в любое время по собственному выбору». Данное действие относится к исключительным правам автора или правообладателя (то есть требует разрешения/лицензии), наряду с воспроизведением и распространением.

Узбекистан включен в международную систему охраны авторских прав. Страна участвует в Бернской конвенции по охране литературных и художественных произведений (Бернская конвенция) с 19 апреля 2005, а также в так называемых «Интернет-договорах» Всемирной организации интеллектуальной собственности с 17 июля 2019 года — Договор ВОИС об авторском праве (WCT) и Договор ВОИС по исполнениям и фонограмма (WPPT).

Бернская конвенция закрепляет принцип национального режима охраны для авторов и произведений из стран-участниц, автоматическую охрану авторских прав по факту создания и минимальный срок охраны авторских прав в течение 50 лет. Договоры ВОИС адаптируют охрану авторских прав к цифровой среде: включая защиту технических мер (например, обход защиты/шифрования) и информации об управлении правами (rights management information).

В соответствие со статьей 5 Закона, «Авторское право распространяется на произведения науки, литературы и искусства, являющиеся результатом творческой деятельности, независимо от назначения и достоинства произведения, а также от способа его выражения». Авторское право распространяется как на обнародованные (опубликованные, распространенные каким-либо способом, в том числе в сети Интернет), так и на необнародованные произведения, находящиеся в какой-либо объективной форме.

Авторское право состоит из личных неимущественных и имущественных прав автора. Личные неимущественные права неотчуждаемы, тогда как имущественные права действуют всю жизнь автора (соавторов) и 70 лет после смерти автора (соавторов). Имущественные права включают широкий список прав и способ использования авторского произведения в любом формате, включая перевод и переработку произведения в другие форматы.

Вид прав	Категория	Объем защиты	Способы нарушения
Личные неимущественные	Право авторства	Признаваться автором произведения	Копирование и распространение произведения без указания имени автора или присвоение авторства (плагиат)
	Право на авторское имя	При использовании произведения обязательно указание автора, его псевдонима	Публикация и распространение произведения без согласия авторам или под чужим именем, либо с искажением имени, раскрытие псевдонима авторам
	Право на обнародование	Право обнародовать или разрешать обнародовать произведение в любой форме, включая право на отзыв от обнародования произведения	Публикация экземпляров произведения, не обнародованного авторов без его согласия
	Право на защиту репутации автора	Право на защиту произведения, включая его название, от всякого искажения или любого иного посягательства, способного нанести ущерб чести и достоинству автора	Искажение и редактирование произведения без согласия автора
Имущественные права	Право на воспроизведение	Создание цифровых ил физических экземпляров (копий) произведения	Создание, копирование без разрешения автора (пиратство)
	Право на распространение	Распространение и продажа цифровых или физических экземпляров произведения, включая право на прокат	Продажа, сдача в прокат без разрешения автора. (нелегальная продажа книг, музыки или фильмов)
	Право на публичный показ и исполнение	Публичное исполнение и показ на публике	Показ или публичное исполнение произведения в общественных местах без разрешения авторам
	Право на переработку	Создание новых (производных) произведенийй на основе оригинала	Переработка произведения в другие форматы, перевод на иностранные языки, адаптация в сценарий, пьесу, постановку, кавер-версии музыкальных произведений, ремиксов без разрешения автора
	Доведение до всеобщего сведения	Распространение цифровых экземпляров в Интернете	Загрузка и распространение цифровых экземпляров произведений в цифровой среде без разрешения автора

Автору (правообладателю) гарантируется право на авторское вознаграждение. Законодательство устанавливает минимальные ставки авторского вознаграждения за конкретные виды произведений и способы использования.

ВАЖНО ЗНАТЬ

Основным способом возникновения и передачи авторских прав является заключение авторского договора с указание объекта авторского права, способов использования и размеров авторского вознаграждения.

Правила использования чужих произведений

Широкое распространение контента в сети Интернет, социальных сетях, мессенджерах и веб-сайтах позволяет получать доступ к чужому контенту, которые могут использоваться без разрешения правообладателей. Материалы из Интернета не свободны для использования, их нельзя воспроизводить без согласия авторов и (или) правообладателей и выплаты вознаграждения. У каждого текста или фотографии, аудио или видеоконтента есть автор или правообладатель. Необходимо внимательно прочитать политику использования материалов на веб-сайтах и в социальных сетях. **Публикация текста или фотографии в открытом аккаунте не означают возможность их использования и публикации для третьих лиц.**

По общему правилу лицо, желающее использовать произведения, исключительные авторские права на которые принадлежат другим физическим лицам или компаниям, обязаны получить разрешение обладателя исключительных прав (ст. 19 закона «Об авторском праве и смежных правах»). Разрешение должно быть выражено в письменной форме посредством заключения авторского договора (ст. 38 закона) и выплачено авторское вознаграждение.

Примеры свободного использования чужого контента в Интернете

Допускается использование объектов авторского права в ограниченном объеме без отдельного разрешения правообладателя, при соблюдении обязательных условий:

- **указание автора и источника (и/или правообладателя, если применимо);**
- **использование в объеме, оправданном целью;**
- **использование не должно наносить ущерб нормальному использованию произведения и ущемлять законные интересы автора.**

В следующих случаях:

- цитирование фрагментов обнародованных произведений для научных, исследовательских, полемических, критических и не связанных с рекламой информационных целей;

- воспроизведение опубликованных материалов по текущим политическим, экономическим, социальным и религиозным вопросам при отсутствии специального запрета автора/правообладателя;

- воспроизведение публично произнесенных политических речей, обращений, докладов и подобных выступлений в объеме, оправданном информационной целью;

- использование произведений, которые становятся увиденными или услышанными в ходе текущих событий, в объеме, оправданном информационной целью.

Красные флаги при использовании чужого контента

Если присутствует хотя бы один признак, свободное использование требует дополнительной проверки и/или получения разрешения автора или правообладателя:

Рекламная цель или продвижение

Если материал используется в рекламе, нативной рекламе, спонсорском контенте, PR-публикациях или для стимулирования продаж/подписок.

Чрезмерный объем заимствования

Копирование больших фрагментов текста, публикация полного фоторепортажа/полного видео/полной аудиозаписи выходит за пределы «объема, оправданного целью» и создает риск нарушения авторских прав.

Отсутствие корректной атрибуции (указания источника)

Не указан автор, источник, нет ссылки или указаны неполные сведения является основанием для претензий даже в случаях, когда само использование могло быть допустимо.

Автор + источник + дата + ссылка (при наличии)

Золотое правило атрибуции.

Наличие специального запрета автора/правообладателя

Если первоисточник прямо запрещает перепечатку/публикацию (на веб-сайте, в конце материала, в условиях использования), полагаться на свободное использование по пункту о перепечатке текущих статей нельзя.

Переработка вместо цитирования в ограниченном объеме

Перевод, адаптация, монтаж, наложение музыки, создание «производного» контента могут требовать отдельного разрешения, даже если исходный материал использован в ограниченном объеме для информационных целей.

ВАЖНО!

Указание знака копирайта «©», указание источника заимствования (например, другое СМИ или веб-сайт) или ссылка на него, некоммерческое использование авторского произведения не освобождает от претензий авторов или правообладателей по поводу незаконного использования.

Способы защиты авторских прав

Если автор или правообладатель считают, что нарушены их авторские права, для их защиты они вправе обратиться (желательно письменно) к нарушителю с требованиями прекратить незаконное использование. Если нарушитель отказывается выполнить требования, автор (правообладатель) вправе обратиться в гражданский (если одна из сторон физическое лицо) или экономический суд (если обе стороны — юридические лица) с иском о:

- признании прав;
- восстановлении положения, существовавшего до нарушения права, и прекращения действий, нарушающих право или создающих угрозу его нарушения;
- возмещении убытков в размере неполученных доходов, которые правообладатель получил бы при обычных условиях гражданского оборота, если бы его право не было нарушено. Если нарушитель получил вследствие нарушения авторского права или смежных прав доходы, правообладатели вправе требовать возмещения наряду с другими убытками упущенной выгоды в размере не меньшем, чем эти доходы;
- выплаты компенсации в размере от двадцати до тысячи базовых расчетных величин вместо возмещения убытков, выплачиваемой независимо от факта причинения убытков, исходя из характера нарушения и степени вины нарушителя с учетом обычаев делового оборот.

Автор (или правообладатель) в случае нарушения их прав вправе требовать от нарушителя компенсацию морального вреда. Законодательством предусмотрена административная и уголовная ответственность за нарушение авторских прав.

Виды ответственности	Когда применяется	Меры ответственности
Статья 177[7] КоАО. Нарушение авторского права и смежных прав	Незаконное использование произведений или объектов смежных прав, а равно и воспроизведение, распространение, доведение до всеобщего сведения контрафактных экземпляров произведений или объектов смежных прав **Имущественные права** Указание ложной информации на экземплярах произведений или объектов смежных прав об их изготовителях, о местах их производства, а также об обладателях авторского права и смежных прав **Неимущественные права**	Первичное нарушение Граждане — штраф от 1 до 5 БРВ Должностные лица — штраф от 5 до 10 БРВ Повторное нарушение в течение года Граждане — штраф от 5 до 10 БРВ Должностные лица — штраф от 10 до 20 БРВ с конфискацией контрафакта, материалов, оборудования.
Статья 149. Нарушение авторских или изобретательских прав	Присвоение авторства, принуждение к соавторству на объекты интеллектуальной собственности, а равно разглашение без согласия автора сведений об этих объектах до их официальной регистрации или публикации **Неимущественные права**	Штраф от 50 до 70 БРВ Лишение определенного права до 5 лет Обязательные работы до 360 часов Ограничение свободы до 2-х лет

Статья 149. Нарушение авторского права и смежных прав	Незаконное использование произведений или объектов смежных прав, а также воспроизведение, распространение, доведение до всеобщего сведения контрафактных копий произведений или объектов смежных прав, изготовление копий с ложной информацией об их производителях, месте изготовления, а также об обладателях авторских и смежных прав, если это причинило ущерб в значительном размере **Имущественные права**	Штраф от 50 до 100 БРВ Исправительные работы до 2-х лет Ограничение свободы до 2-х лет Лишение свободы до 2-х лет

Механизмы ограничения использования объектов авторских прав в цифровой среде

Закон Республики Узбекистан «Об информатизации» запрещает использование объектов интеллектуальной собственности, принадлежащих другим лицам. Владельцам веб-сайта и (или) страницы веб-сайта либо иного информационного ресурса, в том числе блогеры, обязаны не допускать использование своих веб-сайтов и (или) страницы веб-сайтов либо иного информационного ресурса во всемирной информационной сети Интернет чужих авторских произведений без согласия правообладателя.

Постановление Кабинета Министров Республики Узбекистан «О мерах по совершенствованию информационной безопасности во всемирной информационной сети Интернет» № 707 от 5 сентября 2018 года (Постановление № 707) предусматривает механизм удаления онлайн-контента, нарушающего авторские права ограниченного в распространении. Постановление № 707 уполномочивает Инспекцию по контролю в сфере информатизации и телекоммуникаций при Министерстве цифровых технологий Узкомназорат выдавать предписания об удалении информации на веб-сайтах и в социальных сетях.

Правообладатель (автор) вправе обратиться в Узкомназорат с заявлением о фактах незаконного использования объектов авторских прав. Узкомназорат направляет уведомление владельцу веб-сайта, страницы веб-сайта или информационного ресурсы уведомление о необходимости удаления незаконных материалов в течение 24 часов.

Если информация не будет удалена в указанный срок, Узкоманзорат имеет право предпринять следующие меры:

Обратиться напрямую к администрации соответствующей социальной сети или мессенджера с требованием удалить информацию.

Ограничить доступ к веб-сайту или странице веб-сайта, где размещены незаконные материалы.

Обратиться в суд с иском к администрации платформы с требованием удалить запрещенный контент.

Заявление о нарушение авторских прав в цифровой среде может направляться в уполномоченный орган по досудебного рассмотрения споров в сфере интеллектуальной собственности — Департамент по интеллектуальной собственности Министерства юстиции Республики Узбекистан.

Механизмы защиты авторских прав в социальных сетях и цифровых платформах

В Интернете нарушения происходят массово и не требуют больших затрат в отличие от офлайн-среды. Самые частые нарушения — незаконное копирование и распространение чужого авторского контента, плагиат, переработка произведений и использование их в коммерческих целях.

Большинство цифровых платформ и социальных сетей предоставляют механизм подачи жалобы о нарушении авторских прав. Правообладатели могут оформить претензию и направить уведомление о нарушении авторских прав владельцу веб-сайта или платформы, на которой был размещен контент.

Жалоба направляется по форме, предоставляемой платформой и требует указания следующих сведений:

- ссылки где размещены чужие авторских произведения;
- документ, доказывающий права автора или правообладателя на объект авторских прав (авторский договор, свидетельство о регистрации авторских прав;
- контактные данные автора и правообладателя;
- доверенность, если жалоба подается представителем правообладателя.

Поиск по тексту или изображению в поисковых системах, мониторинг социальных сетей, проверку ссылок и упоминаний или просмотр веб-сайтов с похожей тематикой позволяют выявить нарушения авторских прав;

Некоторые специальные автоматические инструменты, которые помогают в обнаружении нарушения;

Google Image Search	Copyscape	Pixsy
бесплатный инструмент, позволяет искать копии изображений в Интернете	международный сервис для поиска плагиата в текстовых материалах. Доступны как бесплатная, так и платная версии с расширенными возможностями	платформа для фотографий с функцией поиска по изображению

2.5. Благотворительные акции и сборы онлайн

2.5.1. Общая характеристика онлайн-благотворительности и правовой подход государства

Благотворительные акции и сборы средств, осуществляемые в онлайн-среде, включая социальные сети, мессенджеры, веб-сайты и цифровые платформы, в Республике Узбекистан не образуют самостоятельного вида правового регулирования. Законодательство исходит из принципа технологической нейтральности,

согласно которому способ распространения информации и привлечения пожертвований не изменяет правовой природы возникающих правоотношений. Онлайн-формат рассматривается исключительно как технический канал реализации благотворительной деятельности, к которому в полном объеме применяются общие нормы действующего законодательства.

Отсутствие специального закона, прямо регулирующего онлайн-сборы средств, не означает наличия правового вакуума. Напротив, благотворительные онлайн-акции подпадают под комплексное регулирование, включающее законодательство о благотворительности, негосударственных некоммерческих организациях, гражданское право, нормы финансового контроля и положения об административной ответственности. Именно совокупное применение этих актов формирует правовой режим онлайн-благотворительности и определяет пределы допустимого поведения для ННО.

2.5.2. Нормативно-правовая база проведения благотворительных онлайн-акций

Правовое регулирование благотворительных онлайн-сборов основывается на совокупности следующих нормативных правовых актов.

Системообразующим актом в данной сфере является **Закон Республики Узбекистан «О благотворительности»**. Он закрепляет базовые принципы благотворительной деятельности, которые в равной степени распространяются как на офлайн-, так и на онлайн-форматы. Благотворительность определяется как добровольная деятельность, что исключает любые формы принуждения, скрытого давления или манипуляции при сборе средств. Для онлайн-сборов это означает недопустимость создания у аудитории ощущения обязательности участия либо маскировки пожертвований под иные платежи.

В соответствии со статьями 3 и 4 благотворительность осуществляется на добровольной основе, а ее субъектами, в том числе, выступают негосударственные некоммерческие организации. Статьи 6–7 устанавливают формы и порядок осуществления благотворительной деятельности, включая сбор пожертвований, а статья 21 закрепляет ответственность за нарушение установленного порядка, в том числе за нецелевое использование средств и нарушение принципов прозрачности.

Закон Республики Узбекистан «О негосударственных некоммерческих организациях» дополняет правовой режим онлайн-благотворительности, устанавливая институциональные рамки деятельности ННО. Ключевым является принцип уставной обусловленности. ННО вправе проводить благотворительные акции и сборы средств исключительно в пределах целей и задач, закрепленных в ее уставе. Онлайн-сбор, не связанный с уставной деятельностью, может быть квалифицирован как нарушение законодательства, независимо от его социально полезного характера.

Закон о ННО также закрепляет обязанность вести финансовый учет, обеспечивать прозрачность источников финансирования и представлять отчетность в уполномоченные государственные органы. Эти требования распространяются на все пожертвования, включая полученные через социальные сети и цифровые платформы, независимо от их объема и продолжительности сбора. Таким образом, даже краткосрочные или разовые онлайн-акции подпадают под режим финансовой подотчетности.

Закон Республики Узбекистан «О противодействии легализации доходов, полученных преступным путем» распространяется на ННО как на субъектов, осуществляющих финансовые операции. В контексте онлайн-сборов это означает обязательность использования официальных банковских счетов, соблюдение процедур финансового мониторинга и недопустимость привлечения анонимных или сомнительных источников средств.

Кодекс Республики Узбекистан об административной ответственности устанавливает меры ответственности за незаконный сбор денежных средств, использование пожертвований не по целевому назначению, отсутствие обязательной отчетности и введение жертвователей в заблуждение.

Дополнительно следует учитывать изменения, внесенные **Законом Республики Узбекистан № ЗРУ-1083 от 21 августа 2025 года,** которыми:

- физическим лицам разрешено собирать пожертвования исключительно для себя или близких родственников;
- сбор средств в пользу третьих лиц допускается только через организации, обладающие официальным правовым статусом;
- при сборе пожертвований наличными допускается использование исключительно прозрачных, опломбированных ящиков либо перечисление средств на банковские счета.

В совокупности анализ действующего законодательства позволяет сделать вывод, что благотворительные акции и сборы средств в онлайн-среде не находятся вне правового поля. Напротив, они подпадают под комплексное регулирование, требующее от ННО высокого уровня правовой осознанности, финансовой дисциплины и публичной ответственности. Именно системное понимание законодательной базы позволяет негосударственным некоммерческим организациям не только минимизировать юридические риски, но и выстраивать устойчивые, доверительные отношения с донорами, государством и обществом в целом.

2.5.3. Налоговые последствия благотворительных онлайн-акций и сборов средств

При организации благотворительных акций и онлайн-сборов средств негосударственным некоммерческим организациям необходимо учитывать налоговые последствия для всех участников благотворительной деятельности: благотворителя, благотворительной организации и получателя помощи.

Для благотворительного фонда (ННО). Денежные средства, поступающие в благотворительный фонд в виде пожертвований, относятся к целевым поступлениям и не подлежат налогообложению, при условии их использования строго по заявленной цели и ведения раздельного учета (ст. 48, 58 и ч. 1 п. 1 ст. 318 НК Республики Узбекистан). Сам факт получения пожертвований, в том числе через онлайн-платформы, не образует налогового обязательства у ННО.

Для юридических лиц — благотворителей. Суммы благотворительной помощи, перечисляемые предприятиями в благотворительные фонды, признаются невычитаемыми расходами при исчислении налога на прибыль, независимо от формы

помощи (п. 7 ст. 317 НК). Исключения предусмотрены для меценатской поддержки, а также отдельных социально значимых направлений, установленных законодательством.

Для физических лиц — получателей помощи через фонд. Средства, полученные физическим лицом от благотворительного фонда, квалифицируются как прочий доход, однако не облагаются налогом на доходы физических лиц, если их сумма не превышает 15 млн сумов в течение налогового периода (п. 1 ст. 377 и п. 20 ст. 378 НК). При превышении указанного лимита налог удерживается только с суммы превышения.

При прямом перечислении средств физическому лицу. Если благотворительная помощь перечисляется напрямую физическому лицу, минуя благотворительный фонд (например, на личную банковскую карту), полученные средства подлежат обложению налогом у источника выплаты как прочий доход (п. 15 ст. 377 и п. 4 ч. 1 ст. 387 НК).

С точки зрения налогового законодательства наиболее безопасной и прозрачной формой благотворительности является сбор и распределение средств через зарегистрированные благотворительные фонды и ННО с использованием официальных банковских счетов и последующей отчетностью. Это минимизирует налоговые риски как для доноров, так и для получателей помощи.

2.5.4. Ключевые требования безопасности при проведении онлайн-сборов

С точки зрения действующего законодательства и правоприменительной практики безопасное проведение благотворительных онлайн-акций предполагает соблюдение комплекса взаимосвязанных требований.

Прежде всего, идентифицируемость организатора сбора. ННО обязана обеспечить, чтобы в каждом публичном объявлении о сборе средств были указаны полное наименование организации, ее регистрационные данные и официальные контакты. Проведение сборов от имени физических лиц, использование личных банковских карт или неофициальных реквизитов создает риск признания такой деятельности незаконной.

Вторым обязательным элементом является четкая определенность цели сбора. Цель должна быть конкретной, проверяемой и заранее объявленной. Недопустимы формулировки общего характера без указания получателей помощи, направлений расходования средств и ожидаемых результатов. Принцип целевого использования пожертвований является базовым как для благотворительного, так и для гражданского законодательства.

Третьим требованием выступает ограниченность по времени. Благотворительная акция должна иметь заранее установленный срок проведения. Отсутствие временных рамок снижает уровень доверия и может рассматриваться как нарушение принципов прозрачности и добросовестности.

Четвертым элементом являются прозрачные финансовые механизмы. Онлайн-сборы должны осуществляться исключительно через официальные банковские счета ННО или законные платежные инструменты. Это позволяет обеспечить финансовый контроль, соблюдение требований финансового мониторинга и возможность последующей проверки использования средств.

Наконец, публичная отчетность является обязательным завершающим этапом благотворительной акции. По итогам онлайн-сбора ННО обязана раскрыть информацию о сумме поступивших пожертвований, направлениях их использования и достигнутых результатах. Отчетность служит не только юридической обязанностью, но и ключевым инструментом формирования доверия.

2.5.5. Защита прав благотворителей и персональных данных

При проведении благотворительных акций и онлайн-сборов негосударственные некоммерческие организации обязаны обеспечивать защиту прав благотворителей и соблюдать требования законодательства Республики Узбекистан о персональных данных. В соответствии с Законом Республики Узбекистан «О персональных данных» обработка любой информации, позволяющей идентифицировать благотворителя (включая имя, контактные данные, платежные реквизиты, никнеймы и комментарии в социальных сетях), допускается исключительно с согласия соответствующего лица и в пределах заявленной цели сбора средств.

Публикация информации о благотворителях, размещение списков доноров, благодарственных сообщений, скриншотов переводов и иных материалов возможны только при наличии согласия благотворителя и с соблюдением принципа минимизации данных. ННО обязана принимать организационные и технические меры по ограничению доступа к персональным данным и предотвращению их несанкционированного распространения.

Одновременно с этим ННО обязана обеспечивать реализацию прав благотворителей на получение достоверной информации об организаторе сбора, его целях, сроках и результатах, что вытекает из законодательства о благотворительности и общих принципов добросовестности. Баланс между прозрачностью благотворительной деятельности и защитой частной жизни благотворителей является обязательным элементом законного и устойчивого функционирования ННО в цифровой среде.

2.5.6. Репутационные аспекты и устойчивость благотворительной деятельности

Безопасность онлайн-благотворительности имеет не только правовое, но и стратегическое значение для сектора ННО. Нарушения при проведении отдельных сборов способны подорвать доверие к конкретной организации и негативно отразиться на общественном восприятии благотворительности в целом. В условиях цифровой среды, где информация распространяется мгновенно, именно соблюдение правовых и этических стандартов становится основой устойчивости и легитимности благотворительной деятельности.

Онлайн-благотворительность является законной и эффективной формой деятельности негосударственных некоммерческих организаций при условии строгого соблюдения законодательства Республики Узбекистан, принципов целевого использования средств, прозрачности и подотчетности. Для ННО соблюдение этих требований выступает не формальной обязанностью, а необходимым условием правовой защищенности, доверия доноров и устойчивого развития.

2.6. Важные документы и политики для ННО

Как сказано выше, для ННО правовые риски связаны как с созданием цифрового медиаконтента, так и с каналами, через которые этот медиаконтент распространяется. Чаще все риски и меры, которые необходимо предпринять для того, чтобы ваша активность в медиа развивалась успешно отражаются в письменных документах — специальных политиках, которые рекомендуется разрабатывать и принимать в письменном виде, публиковать или использовать только внутри организации.

Таблица ниже содержит минимальный перечень политик для онлайн-активностей (всего 5 политик), исходя из особенностей медиабизнеса — создание медиаконтента и распространение его в цифровой среде. В приложении можно найти также шаблоны рекомендуемых документов (политик и правил):

- правила использования материалов;
- политика по персональным данным;
- правила комментирования для пользователей (подписчиков);
- политика по проведению благотворительных акций онлайн-или в социальных медиа.

Ниже кратко описание каждой политики в контексте работы в медиа-среде в Узбекистане и зачем такую политику нужно разрабатывать и принимать.

2.6.1. Правила использования материалов (контента) онлайн-издания

Цель этой политики — публично заявить о том, что редакция онлайн-издания или ННО является правообладателем контента, который создается и распространяется через различные платформы и каналы. Эта политика также определяет позицию (разрешение) правообладателя по **использованию своего контента без разрешения правообладателя,** но выполняя определенные условия:

- В случаях цитирования — необходимо соблюдать объем цитирования, установленный онлайн-изданием (не более 30% текста, первый абзац и т. д.), а также применение гиперссылки на первоисточник и т. д.
- В случаях иллюстрирования, использования авторских фотографий — количество фотографий или других визуальных материалов, которые можно републиковать с обязательным указанием автора фото и т. д.
- В случаях использования в дайджестах и обзорах необходимо соблюдать объем цитирования, установленный редакцией онлайн-издания (не более 30% текста, первый абзац и т. д.), а также применять гиперссылки на первоисточник и т. д.

Также эта политика определяет процедуры по использованию UGC (пользовательский контент; users-generated content)[38], включая получение согласия от пользова-

[38] UGC (User-Generated Content, пользовательский контент) — это любые материалы, созданные обычными людьми (клиентами, подписчиками), а не брендами или профессионалами: отзывы, фото, видеообзоры, комментарии, посты в соцсетях

теля на публикацию, ответственность пользователя за права на присланные материалы, порядок удаления UGC по обращению третьих лиц.

Политика содержит основные принципы по использованию материалов из Интернета, социальных сетей, мессенджеров и содержит запрет на использование текстовых и аудиовизуальных материалов «из Интернета» без проверки прав.

2.6.2. Политика по персональным данным

Цель политики — законно собирать и использовать персональные данные пользователей веб-сайта, подписчиков и т. д. Политика должна содержать следующую информацию:

- какие данные собираются (регистрация, рассылки, комментарии, заявки, cookies/аналитика, продажа мерча, сбор персональных данных в период проведения благотворительных акций и т. д.);
- цели обработки, сроки хранения, категории получателей;
- контакты ответственного лица/канала для обращений;
- меры защиты и права субъекта данных.

2.6.3. Правила комментирования и модерации

Цель этой политики — заранее установить требования (red flags) для аудитории и снизить риски ответственности за распространение запрещенной, порочащей, ложной информации в комментариях на ваших страницах.

Такая политика должна содержать следующую информацию:

- запрещенный (противоправный) и чувствительный контент (язык вражды/дискриминация, призывы к насилию, экстремистские материалы, порнография, разглашение персональных данных, угрозы, травля, очевидно ложные сведения, иные нарушения закона);
- каким образом редакция проводит мониторинг комментариев (премодерация или постмодерация), правила блокировки, удаления, ограничения обсуждений;
- порядок сообщения о нарушениях (как сообщить о нарушениях, что будет считаться достаточным обоснованием);
- единые правила для веб-сайта и аккаунтов издания в социальных сетях и в мессенджерах.

Почему такая политика важна как для редакций онлайн-изданий, так и ННО? Закон Республики Узбекистан «Об информатизации» прямо устанавливает обязанности владельцев веб-сайтов и (или) страниц веб-сайтов (в том числе размещенных в социальных сетях и в мессенджерах) не допускать использования ресурса для запрещенных целей и удалять запрещенную информацию. В случае нарушений предусмотрена возможность ограничения доступа к ресурсу[39].

[39] Закон Республики Узбекистан «Об информатизации». Текст закона доступен по ссылке: https://lex.uz/acts/82956

Раздел 3
Угрозы для гражданских активистов и ННО в цифровой среде

3.1. Ключевые угрозы

В последнее десятилетие в связи с развитием цифрового пространства происходит фундаментальный сдвиг в том, какие угрозы являются превалирующими для гражданского общества. Если раньше фокус был на физических угрозах, то сегодня линия фронта стала виртуальной и проходит через наши смартфоны, ноутбуки и облачные хранилища. Мы живем в эпоху «стеклянного дома», когда цифровая прозрачность и «повсеместность», которые помогают нам распространять идеи и привлекать сторонников, одновременно делают нас уязвимыми перед теми, кто хочет этой деятельность помешать.

Для активистов и сотрудников ННО в Центральной Азии понимание ландшафта цифровых угроз перестало быть просто вопросом «для информации». Теперь это вопрос выживания, сохранения свободы и репутации. Иллюзия того, что «мне нечего скрывать» или «я слишком мелкая фигура, чтобы мной интересовались», — это очень опасное заблуждение. В современных системах массового наблюдения (DPI, распознавание лиц, аналитика больших данных) нет «неважных» целей; под прицелом могут оказаться все.

Критически важно понять, что **границы между онлайн-угрозами и офлайн-последствиями стерты**. Взлом электронной почты — это не просто технический сбой, это критическое событие безопасности с далеко идущими последствиями, затрагивающее большой круг лиц, фотография с метаданными геолокации может привести к физическому нападению на участников закрытой встречи, а кампании по кибербуллингу и дезинформации наносят вполне реальные психологические травмы, приводящие к выгоранию и прекращению деятельности организаций.

Многие организации воспринимают цифровую безопасность как покупку антивируса: установил и забыл — при этом возникает ложное чувство безопасности. Однако настоящий защитный механизм строится иначе. Он требует понимания **ландшафта угроз** (контекст, внешняя среда), знания **векторов атаки** (пути, посредством которых могут быть реализованы угрозы) и четкого представления своих цифровых ресурсов и их уязвимостей Именно на фундаменте этих знаний формируется устойчивый **профиль безопасности** (security posture) организации — состояние, при котором обеспечение безопасности становится не разовым действием, а непрерывным процессом.

Однако в современном цифровом мире недостаточно просто настроить технические компоненты защиты своих цифровых активов. В настоящее время все большую популярность набирает холистический (целостный) подход к безопасности, который исходит из того, что цифровая, физическая и психосоциальная безопасность неразделимы. Они образуют единую экосистему, где уязвимость в одной сфере неминуемо разрушает защиту в других.

К примеру:

Психологическое давление

(угрозы, шантаж) приводит к **эмоциональному выгоранию** сотрудника.

Выгоревший сотрудник

теряет бдительность и становится легкой жертвой фишинга или социальной инженерии **(цифровая уязвимость)**.

Взлом цифровых ресурсов

раскрывает сенситивные персональные данные (сексуальная ориентация, ВИЧ статус...), что создает прямую угрозу **физической безопасности** источников.

Утечка данных

приводит к правовым санкциям со стороны государства, подрыву репутации, недоверию доноров и, как итог, к **финансовой недостаточности** и **закрытию деятельности** организации.

Поэтому в данном сборнике угрозы рассматриваются не изолированно, а в их совокупности, с фокусом на то, что **человек — это главный актив и одновременно — главный вектор атаки** в любой системе безопасности.

Для удобства мы можем разбить угрозы на несколько категорий по сфере воздействия: технические, физические, правовые, психосоциальные, экономические и угрозы человеческого и организационного характера. Деление достаточно условное, так как большинство угроз являются гибридными и могут быть разложены на составляющие относящиеся к разным категориям, например законы об «иноагентах» попадают сразу в несколько категорий: правовая — это закон, который определяет условия, при которых наступает ответственность; экономическая — ставит под угрозу финансовую стабильность организаций; психосоциальная — стигматизирует попавших под определение иноагента; организационная — накладывает дополнительное административное бремя на организацию в виде дополнительных отчетов, маркировок; и техническая — несоблюдение требований может привести к блокировке аккаунтов, веб-сайтов, отзыву доменов. При этом в зависимости от того, кто рассматривает угрозу, на первое место будет выходить категория близкая рассматривающему лицу: для юриста — правовая, для финансиста — экономическая, для директора — операционная, для специалиста по цифровой безопасности — техническая. В данном пособии мы будем ориентироваться на цифровую составляющую угроз и оценивать их именно с этой точки зрения.

1. Технические угрозы — угрозы, направленные на нарушение работы, компрометацию или несанкционированный доступ к цифровой инфраструктуре, устройствам и данным)

- **Сбор данных и разведка (OSINT) — не является прямой угрозой, но часто бывает** начальным этапом для целенаправленной атаки, включающий анализ публично доступной информации для выявления разного рода уязвимостей, от технических до психосоциальных.

- **Заражение вредоносным ПО (шпионское ПО, вирусы-шифровальщики) — наиболее распространенная киберугроза,** которая включает в себя как массовые вирусы, которые, к примеру, шифруют данные и требуют выкуп, так

и целенаправленные атаки с использованием сложного шпионского ПО (например, Pegasus, Predator и др.), которое дает полный удаленный контроль над устройством.

- **Взлом цифровых аккаунтов** — объединяет все виды несанкционированного доступа (к почте, соцсетям, мессенджерам, финансовым аккаунтам). В основном происходит за счет **фишинга, приемов** социальной инженерии, утекших паролей. Результат — потеря контроля над каналами коммуникации и репутацией.

- **Атаки на веб-сайты (DDoS, взлом веб-сайтов)** — прямые атаки на публичные ресурсы организации Цель DDoS-атаки — сделать ресурс недоступным для аудитории, перегрузив его запросами с зараженных устройств. Цель взлома обычно — дефейс (замена контента), кража данных или размещение вредоносного кода.

- **Перехват данных в незащищенных сетях** — актуальная при работе из публичных мест (кафе, аэропорты) Wi-Fi точкой, которую вы не контролируете. При этом злоумышленник может перехватывать незашифрованный трафик, включая логины и пароли. Эта же угроза применима к посещению веб-сайтов не использующих шифрование (http протокол), о чем обычно предупреждает браузер и некоторые антивирусы.

- **Подброс компрометирующих данных — достаточно редкая, но опасная** угроза, при которой злоумышленник, получив доступ к устройству, не крадет данные, а наоборот, подбрасывает на него нелегальный контент (экстремистские материалы, порнографию) для последующей дискредитации или уголовного преследования.

- **Атаки на цепочку поставок (Supply Chain Attacks) — набирающая популярность угроза,** при которой атакуют не вас напрямую, а вашего доверенного партнера (например, разработчика вашего веб-сайта, поставщика ПО или компьютерный сервис), чтобы получить доступ к вашей инфраструктуре через их системы.

2. Психосоциальные угрозы — угрозы, направленные на личность активиста, его репутацию, психологическое состояние и социальные связи с целью деморализации и прекращения деятельности

- **Координированная онлайн-травля и кампании по дезинформации (кибербуллинг, «фабрики троллей»)** — массированные атаки в комментариях, соцсетях и других источниках, распространение оскорблений, угроз и лжи, в том числе с помощью дипфейков, организованная, как правило, с целью очернения репутации.

- **Доксинг** — сбор и публичное обнародование персональных данных (адреса, телефоны, данные родственников) с целью перевести цифровую угрозу в реальную физическую опасность и запугать активиста.

- **Сексторшн, порноместь, секспионаж** — шантаж интимными материалами (как реальными, так и сфабрикованными с помощью ИИ) часто применяемая угроза против женщин-активисток в консервативных обществах.

3. Правовые и регуляторные угрозы — угрозы, использующие законодательство, государственные институты и правовую систему как инструмент давления, цензуры и преследования

- **Применение репрессивного законодательства (о «фейках», «клевете», «экстремизме») — угроза** использования расплывчатых формулировок в законах для возбуждения административных и уголовных дел за публикации в Интернете.
- **Применение законов об «иностранных агентах/представителях»** — гибридная угроза, которая является правовой по своей сути, но имеет прямые экономические, психосоциальные и операционные последствия.
- **Блокировка или удаление онлайн-ресурсов по требованию госорганов — угроза блокировки веб-сайта, страницы в соцсети или удаления контента вследствие** внесудебного или судебного решения по цензурированию контента.
- **Злоупотребление юридическими механизмами платформ (DMCA-атаки) —** использование легальных инструментов платформ, таких как жалобы на авторские права, контент по официальным каналам в соцсети, мессенджеры для нелегитимных целей (вымогательство, цензурирование).
- **Государственный цифровой надзор (СОРМ, DPI, распознавание лиц) — непрямая** угроза **злоупотребления формально-легальными инструментами, такими как СОРМ, DPI, системы распознавания лиц и биометрия, создание цифровых профилей для ведения массового и нецелевого сбора данных, выходящего далеко за рамки заявленных целей** (например, борьбы с терроризмом или тяжкими преступлениями).

4. Экономические угрозы — в основном гибридные угрозы, основной целью или механизмом которых является прямое воздействие на финансовую устойчивость организации.

- **Прямое цифровое мошенничество и кража средств — несанкционированный доступ к финансовым аккаунтам путем взлома или социальной инженерии.**
- **Блокировка банковских счетов и финансовых операций** — действие, которое может быть инициировано по формальному правовому предлогу (например, в рамках обеспечения ходатайства по обеспечению иска).
- **Атаки на фандрайзинг или краудфандинг — может быть как** прямое мошенничество, такое как **создание веб-сайтов-клонов, перехват пожертвований, так и косвенное как искусственное создание конкурирующих проектов (GONGO), перехватывающих финансирование.**
- Угрозы вторичных санкций или побочного ущерба — угроза «сверхсоблюдения», когда международные банки, IT-компании, доноры и платформы из-за опасения нарушить санкционный режим могут **полностью прекратить или ограничить работу со всем регионом близким к санкционному, что может привести к блокировке банковских операций, счетов, ограничению со стороны сервисов.**

5. Человеческий фактор и организационные угрозы — угрозы, возникающие из-за недостатков во внутренних процессах, человеческого фактора, а также физической безопасности устройств

- **Непреднамеренные ошибки и уязвимости персонала** — объединяет такие угрозы, как **халатность**, **цифровая неграмотность** и **выгорание.** Уставший, необученный или немотивированный сотрудник — это уязвимость, через которую реализуются многие технические и психосоциальные угрозы (например, фишинг).

- **Преднамеренные враждебные действия изнутри (инсайдеры)** — угроза, исходящая от сотрудников или волонтеров, которые намеренно саботируют работу, сливают данные или предоставляют доступ третьим лицам.

- **Физическая утеря, кража или изъятие устройств и носителей данных** — объединяет все сценарии, при которых вы теряете физический контроль над техникой (забыли в такси, украли, конфисковали при обыске). Без шифрования это равносильно полной утечке данных а без наличия резервных копий — полной потере данных.

Переход от простого перечисления внешних угроз к выработке стратегии защиты требует дальнейшего расширения вопросов, которые необходимо себе задать. И это не только вопрос «Кто или что может представлять угрозу?», но и вопросы «Что именно мы защищаем?» и «Где наши слабые места?» Вместо того чтобы концентрироваться исключительно на внешних факторах, которые часто находятся вне нашего контроля, необходимо сфокусироваться на внутренней среде организации. В основе любой стратегии лежит точное понимание того, какие активы являются для организации критически важными. Для гражданского сектора это, в первую очередь, **информация и данные,** компрометация которых может нанести прямой вред людям; **репутация и общественное доверие,** служащие фундаментом легитимности; **команда**, чье благополучие является условием работоспособности; и **каналы коммуникации,** обеспечивающие организации возможности взаимодействия с внешним миром. Внешние угрозы становятся реальной опасностью только тогда, когда они находят и эксплуатируют соответствующие им уязвимости. Каждая успешная атака — это история о том, как внешний фактор использовал бреши во внутренней защите.

Этот анализ подводит нас к формальному определению **риска.** Риск — это не сама угроза и не сама уязвимость, а **вероятность того, что конкретная угроза успешно использует конкретную уязвимость, что приведет к определенному ущербу для активов организации.**

Так, технические угрозы, такие как внедрение шпионского ПО, напрямую нацелены на информационные активы. Однако их успех почти всегда обусловлен наличием уязвимостей: слабых парольных политик, отсутствия двухфакторной аутентификации или, что наиболее часто, уязвимостей человеческого фактора, таких как недостаточная осведомленность или снижение бдительности из-за выгорания. Незашифрованный жесткий диск с базой данных становится легкой добычей при физической потере или изъятии устройства.

В свою очередь, психосоциальные атаки, включая дезинформацию, доксинг и использование дипфейков, направлены на подрыв репутации и доверия. Они находят благодатную почву в таких уязвимостях, как избыточное раскрытие персональных

данных сотрудниками в социальных сетях или отсутствие у организации четкой коммуникационной стратегии для противодействия фейкам. Атака становится успешной там, где размыты границы между личным и публичным цифровым следом.

Аналогичным образом, правовое и экономическое давление становится особенно эффективным, когда оно нацелено на организационные уязвимости. Законы об «иностранных агентах» эксплуатируют финансовую зависимость от одного источника, а внезапные блокировки счетов выявляют отсутствие у организации диверсифицированных финансовых потоков и резервных фондов. Юридическое преследование за клевету часто становится возможным при отсутствии выверенной редакционной политики и процедур фактчекинга.

Поскольку ресурсы любой организации ограничены, невозможно устранить все уязвимости одновременно. Ключевой задачей становится **приоритезация рисков.** Этот процесс осуществляется путем оценки каждой угрозы по двум основным критериям: **вероятности** ее реализации и потенциальному **ущербу** в случае успеха. Вероятность зависит от привлекательности организации как цели и легкости эксплуатации ее уязвимостей. Ущерб определяется ценностью актива, который окажется под ударом и стоимостью его восстановления. Риски с высокой вероятностью и высоким потенциальным ущербом, такие как компрометация базы данных с чувствительной информацией из-за отсутствия двухфакторной аутентификации, требуют немедленного внимания. В то же время, риски с низкой вероятностью и незначительным ущербом могут быть временно отложены.

После того как риски оценены и приоритезированы, организация может выбрать одну из четырех ключевых **стратегий управления** для каждого из них. Во-первых, это **избегание (Avoidance)** — стратегическое решение прекратить деятельность, связанную с высоким риском. Например, организация может принять решение не собирать определенные виды чувствительных данных, если они не являются абсолютно необходимыми для ее миссии, тем самым полностью устраняя риск их утечки. Во-вторых, существует стратегия **принятия (Acceptance)**, которая применяется к рискам с низким приоритетом, когда стоимость их уменьшения превышает потенциальный ущерб. В-третьих, это делегирование рисков **(Transfer)** — перенос части риска на третью сторону. Классическим примером является использование надежного облачного провайдера для хранения данных, что передает ему риски, связанные с физической безопасностью серверов и отказами оборудования. Наконец, это снижение рисков **(Mitigation)** — наиболее распространенная стратегия, которая заключается в принятии мер для снижения вероятности или ущерба. Примерами служат внедрение шифрования, проведение тренингов для персонала или создание резервных копий. Это основная стратегия, которая будет рассматриваться в следующем разделе.

3.2. Меры по безопасности гражданских активистов и НКО

Обеспечение безопасности своих цифровых ресурсов — это сложнейший процесс, особенно, если нет отдельного IT-отдела или специалиста и ресурсов. Далеко не полный перечень угроз, который был перечислен в предыдущем разделе может ввести в уныние и заставить опустить руки, так как кажется невозможным защититься от всего. Тем не менее, данный подход не является конструктивным и в

этом разделе мы попробуем подобрать варианты для большинства организаций и отдельных активистов.

В первую очередь есть абсолютно необходимый минимум — это те 20% усилий, которые решают 80% проблем:

- Инвентаризация цифровых ресурсов — это составление списка наиболее ценных цифровых ресурсов, в которые, как правило, входят в**се ваши email-адреса** (личные и рабочие), **аккаунты в социальных сетях (FB, IG, ,.,) и мессенджерах (WhatsApp, Telegram, Signal...), облачные хранилища (Google Drive, Dropbox, OneDrive...), список наиболее важных документов и мест, где они находятся. Этот этап для персоналий или небольших организаций редко занимает больше одного часа, но его значение трудно переоценить. Мы не можем защитить те цифровые ресурсы, которые мы не помним, таким образом этот этап вводит в зону видимости наиболее ценные цифровые активы.**

- **Менеджер паролей** — это программа, которая создает и запоминает за вас сверхсложные пароли для каждого веб-сайта. Вам нужно помнить только один главный пароль. **Это немедленно закрывает самую большую дыру в защите ваших аккаунтов. Одна из серьезных уязвимостей — это использование очень слабых паролей или переиспользование одного и того же пароля для нескольких ресурсов. С менеджером паролей эти проблемы решаются. Так как все пароли будут содержаться в парольном менеджере и не будет необходимости их запоминать. Помимо паролей в парольных менеджерах можно хранить разного рода секретные заметки, данные банковских карт, персональные данные и другую информацию. Важным моментом является то, что ваши пароли в парольном менеджере хранятся** в зашифрованном виде и даже, если их сервис будет взломан, доступ к вашим паролям злоумышленники не получат. Использовать нужно только проверенные, надежные парольные менеджеры, к примеру Bitwarden, который имеет бесплатную версию или 1Password. В настоящее время многие сервисы внедряют беспарольный вход, с помощью парольных ключей, что может показаться идеальной альтернативой паролям — сложный ключ сохраняется на вашем устройстве, не требует запоминания и никуда не передается. При этом данный способ тоже не застрахован от угроз. Так доступ к ключу осуществляется путем ввода PIN-кода или биометрического распознавания и, если кто-то узнает ваш PIN-код или под принуждением вынудит использовать отпечаток пальца или FaceID, то получит доступ к вашим аккаунтам. Использование менеджера паролей в отличие от беспарольных схем может быть адаптировано к различным вариантам использования при разных угрозах

- **Двухфакторная аутентификация (2FA)** — это второй рубеж обороны для ваших аккаунтов. Даже если ваш пароль украдут, без кода с вашего телефона, токена, отпечатка пальца или FaceID злоумышленник не сможет войти в аккаунт. **Это самая эффективная мера против взлома.** На многих сервисах она включается автоматически (к примеру, Google-уведомления), в некоторых нужно включать вручную. Тем не менее необходимо убедиться, не только в том что во всех сервисах она включена, но в том, что она настроена правильно. В частности аутентификация через SMS является небезопасной и легко может быть взломана путем перехвата SMS-сообщения, поэтому этот способ должен быть отключен везде, где есть альтернативные способы. Так «золотой серединой» с точки зрения удобства и безопасности является использование приложения аутентификатора

(Google Authenticator, Authy, Microsoft Authenticator, ...), автономно генерирующего коды для входа. Помимо этого необходимо убедиться, что в надежном безопасном месте сохранены резервные коды восстановления (backup codes), одноразовые коды, которые используются в том случае, если телефон недоступен. Это крайне важный этап, без которого вы можете потерять доступ к аккаунту. Отдельно проверьте, что в мессенджерах, которыми вы пользуетесь, так же стоит **двухфакторная аутентификация. В разных мессенджерах она может называться по разному: WhatsApp — двухшаговая проверка, Telegram — облачный пароль, Signal — блокировка регистрации. Эти настройки предотвращают возможность взлома мессенджера путем перехвата регистрационного SMS-сообщения или подмены SIM-карты.**

- **Настройка резервного копирование (бэкапы) — критически важный компонент безопасности данных, хранящихся на локальных устройствах, от таких угроз, как аппаратные сбои, атаки вредоносного ПО (в частности, программ-шифровальщиков) и физическая утеря или изъятие оборудования.** Ключевым принципом эффективного резервного копирования является его автоматизация. Системы, полагающиеся на ручное копирование файлов пользователем, обладают низкой надежностью из-за наличия человеческого фактора. Существуют два основных подхода к реализации автоматизированного резервного копирования: локальное резервное копирование с использованием внешних носителей и облачное резервное копирование и синхронизация. Для локального резервного копирования используются внешние носители информации (жесткие диски, SSD накопители...). Для автоматизации этого процесса можно использовать встроенные средства операционной системы. В Microsoft Windows эту функцию выполняет инструмент «История файлов» (File History), который позволяет настроить периодическое копирование файлов из пользовательских папок на указанный внешний диск. В Apple Mac OS аналогичную функциональность предоставляет система Time Machine, которая создает инкрементальные снимки всей системы, позволяя восстановить как отдельные файлы, так и операционную систему целиком на определенный момент времени. Для облачного резервного копирования используются облачные сервисы, такие как Google Drive, Microsoft OneDrive, Dropbox и другие. Большинство современных облачных сервисов, работают по принципу автоматической синхронизации, когда устанавливается локальное приложение, которое создает на локальном диске специальную папку и любые файлы, помещенные в эту папку, автоматически копируются в облачное хранилище и синхронизируются между всеми подключенными устройствами. Для организаций, работающих с особо чувствительной информацией, рекомендуется рассмотреть специализированные облачные сервисы, предлагающие сквозное (end-to-end) шифрование. В таких системах (например, Proton Drive, Sync.com, Tresorit, Mega.io) данные шифруются на устройстве пользователя перед отправкой на сервер, что делает их недоступными даже для сотрудников самого сервиса, обеспечивая максимальный уровень конфиденциальности. В мобильных данных синхронизация идет, как правило, на привязанных аккаунт (Google, iCloud), но могут использоваться и мобильные версии приложений облачных сервисов. Лучше всего сочетать оба способа по формуле «3-2-1» — 3 копии данных, две на разных физических носителях и одна — в облаке. Такой подход обеспечивает максимальную отказоустойчивость и гарантирует сохранность данных в подавляющем большинстве кризисных сценариев. При этом обеспечивается только доступность данных, защита резервных копий осуществляется защитой аккаунта в случае облачного бэкапа и полно дисковым шифрованием в случае локального хранения.

Для того, чтобы двигаться дальше и сделать положительные изменения по безопасности постоянными, мало разовых акций типа тренингов или установок необходимых для безопасности настроек. В дальнейшем важен системный подход, когда безопасность становится неотделимым компонентом всей деятельности организации. Для это необходимо ввести два понятия из корпоративной безопасности Due Diligence и Due Care. Прямого перевода нет, но можно из определить так:

- Due Diligence — это «подумать прежде чем сделать», это оценка рисков и планирование действий. Это ответ на вопрос: «Сделали ли мы все возможное, чтобы подготовиться к угрозам?»

- Due Care — это «обязательство действовать каждый день» — ежедневные усилия по поддержанию созданной системы в рабочем состоянии. Это ответ на вопрос: «Делаем ли мы все возможное, чтобы подготовиться к угрозам?»

Для этого на каждом уровне вводятся меры, которые необходимо принять для планирования и для исполнения. Соответственно на каждом уровне важно чтобы были выполнены минимальные требования и требования предыдущего уровня.

Уровень 1:
Формирование дисциплины и базовой гигиены — предназначено для отдельных активистов и небольших команд, цель которого превратить единичные индивидуальные практики в общую дисциплину и культуру безопасности.

Планирование и подготовка фундамента (Due Diligence): На этом этапе закладывается фундамент операционной безопасности. Он включает в себя необходимый минимум, представленный выше, а так же несколько ключевых дополнительных шагов.

Постараться по максимуму использовать только лицензионное программное обеспечение. Для зарегистрированных ННО многие вендоры предоставляют свои программные продукты бесплатно или с большой скидкой. У крупных производителей есть специальные программы для ННО, к примеру Google для некоммерческих организаций и Microsoft для некоммерческих организаций, в рамках которых можно получить доступ к коммерческим сервисам бесплатно или Techsoup, который является точкой входа для ННО для получения доступа ко многим продуктам, в том числе лицензиям Windows по специальным ценам.

Необходимо обеспечить полнодисковое шифрование, для Windows — Bitlocker, для Mac OS — Filevault, с сохранением ключей восстановления в надежное безопасное место (например, в парольный менеджер).

Провести первичный тренинг для команды, на котором объясняются не только технические аспекты, но и основы распознавания фишинга, социальной инженерии и основы физической безопасности.

Провести оценку и настройку приватности на личных и общих страницах в соцсетях для повышения контроля и уменьшения цифрового следа.

Выработать неформальные правила внутри команды— например, «всю рабочую переписку ведем только в Signal» или «не храним пароли в Google Docs». Это еще не политика безопасности, но уже первые шаги к ней.

Организовать базовый правовой инструктаж с юристом или экспертом о ключевых «красных линиях» в законодательстве страны (законы об экстремизме, клевете и т. д.) и их возможном влиянии на работу организации

Ежедневная практика (Due Care): Это, в первую очередь, **своевременная установка обновлений** программного обеспечения на всех устройствах, так как это основной способ защиты от известных уязвимостей. Сюда же относится практика **физической безопасности устройств** — привычка блокировать экран компьютера, уходя с рабочего места. Использование VPN при работе с публичных WiFi-точек. Наконец, это постоянная мотивация развития **критического мышления:** проверка подозрительных запросов и открытое обсуждение в команде любых подозрительных сообщений, угроз, создавая благоприятную атмосферу взаимодействия. Также важно постоянно отслеживать новости об изменениях в законодательстве, касающихся деятельности НКО и свободы слова.

Уровень 2:
Внедрение формализованных организационных процессов — предназначено для команд и зарегистрированных НКО, готовых перейти к системной работе над безопасностью.

Планирование и подготовка фундамента (Due Diligence): Основным шагом на этом этапе является разработка и утверждение единой Политики информационной безопасности. Этот документ формализует требования к паролям, использованию ПО, хранению данных, физической безопасности и становится основой для всех дальнейших действий. Вводится процедура управления доступом, основанная на принципе наименьших привилегий (предоставление сотрудникам доступа только к той информации, которая им абсолютно необходима для работы). Кроме того, проводится базовая оценка безопасности используемых сторонних сервисов. К примеру для каждого сервиса можно составить чек лист: поддерживается ли безопасная двухфакторная аутентификация, есть ли распределение доступа по ролям, как делаются резервные копии и т. д. На этом же этапе создается программа вводного инструктажа по безопасности для всех новых сотрудников и проводятся тренинги по управлению стрессом, цифровым выгоранием и базовой психологической самопомощи. Помимо этого нужно провести юридический и финансовый аудит деятельности организации, чтобы убедиться в ее соответствии всем требованиям законодательства.

Ежедневная практика (Due Care): Операционная деятельность на этом уровне должна быть более структурированной. Фактически — это ежедневное внедрение разработанной политики по безопасности. Должны проводиться регулярные проверки работоспособности резервных копий, к формуле резервного копирования «3-2-1» добавляется ноль ошибок при восстановлении и формула становится «3-2-1-0». Так же регулярно должна проводиться проверка прав доступа к ключевым сервисам. Особенно важным это становится при текучке кадров или смене позиций сотрудников. Отсутствие проверки может приводить к тому, что ушедший из организации сотрудник будет иметь доступ к сервисам организации, или у действующего

сотрудника будут оставаться излишний доступ к сервисам или документам. На этом же уровне должна быть отработана процедура безопасного вывода из эксплуатации старой техники, включающая обязательное криптографическое стирание данных. Для команды должны проводиться периодические короткие тренинги и обсуждения актуальных угроз на общих собраниях, включая правовые, психосоциальные и экономические.

Уровень 3:
Построение стратегической и проактивной защиты — предназначено для организаций, работающих в среде с высоким уровнем риска, при котором необходимо предвидеть угрозы и планировать действия в условиях кризиса.

Планирование и подготовка фундамента (Due Diligence): На этом этапе для организации основным становится стратегическое планирование. Оценка рисков становится основным фундаментом, на основе которого должен быть разработан детальный план реагирования на инциденты (Incident Response Plan) — пошаговый сценарий действий для различных типов атак (взлом, доксинг, DDoS). Этот план дополняется планом обеспечения непрерывности деятельности (Business Continuity Plan), который описывает, как организация продолжит свою миссию в случае реализации катастрофических сценариев. Должны быть разработаны протоколы на случай физических угроз не только для офиса, но и мест проживания ключевых сотрудников. Так же должна быть определена формальная роль ответственного за безопасность и установлены контакты с внешними экспертами (юристами, IT-специалистами) и разработан план коммуникаций на случай кризиса. Для противодействия экономическим угрозам необходимо сформировать резервный фонд для обеспечения работы организации на несколько месяцев.

Ежедневная практика (Due Care): На данном этапе организация не просто должна реагировать на инциденты, а предвидеть и готовиться. Для этого должен быть регулярный мониторинг своего цифрового следа и информационного поля для раннего обнаружения угроз. Должны проводиться внутренние симуляции атак и учебные тревоги для проверки и отработки плана реагирования на инциденты различного характера и плана обеспечения непрерывности деятельности. Все разработанные политики и планы должны подвергаться ежегодному пересмотру и адаптации к новой обстановке.

3.3. Меры по защите веб-сайтов и медиаресурсов ННО

В эпоху цифровой трансформации веб-сайты и онлайн-платформы НПО стали критической инфраструктурой для их миссий. Однако это же сделало их уязвимыми перед растущим числом кибератак. Особенно уязвимы правозащитные организации, независимые медиа-ресурсы и группы активистов, которые могут являться целями как для преступников и хактивистов так и для государственных субъектов, в том числе иностранных.

Для построения эффективной системы защиты онлайн-ресурсов, в частности веб-сайтов, необходимо понимать, с какими типами угроз может столкнуться организация. Все атаки можно условно разделить на четыре основные категории, каждая из которых требует своего подхода к предотвращению и реагированию.

Компрометация ресурса (взлом)

Эта категория включает все инциденты, когда посторонние лица получают несанкционированный доступ к «внутренностям» вашего веб-сайта — его системе управления, серверу или аккаунтам администраторов. Последствия такого проникновения могут быть разными, в зависимости от целей злоумышленника. Иногда это публичный вандализм (дефейс), когда на главной странице размещается чужое сообщение. В более сложных случаях это скрытая подмена информации, когда на веб-сайте незаметно меняют цифры или факты, чтобы подорвать доверие к вам. Часто главной целью является кража данных — персональных, финансовых и других. Кроме того, ваш веб-сайт могут превратить в оружие, используя его для рассылки спама или заражения устройств посетителей. Так же результатом взлома может стать полное уничтожение информации на веб-сайте.

Атака на отказ в обслуживании (DDoS-атака)

Эта категория объединяет атаки, чья главная цель — сделать ваш веб-сайт недоступным для посетителей, фактически не давая вашей аудитории воспользоваться ресурсом. Как правило это техническая атака, когда ваш ресурс искусственно перегружают огромным потоком бесполезных запросов с сети зараженных устройств (ботнета), и он перестает справляться с нагрузкой и отвечать на запросы пользователей. Часто такая атака используется во время каких либо важных событий, например, выборы, протесты, публикация каких-либо резонансных материалов, чтобы не дать аудитории возможность получить информацию.

Юридическое и административное давление

Эта категория включает использование законов и формальных процедур для оказания давления на вашу организацию через ее онлайн-ресурс. Это может проявляться в виде принудительного удаления контента (цензуры), когда власти или другие структуры требуют убрать определенные материалы под угрозой санкций, блокировки ресурса в стране или отзыва доменного имени. Так же это может делаться через юридическое преследование, когда публикации на веб-сайте или комментарии становятся основанием для возбуждения дел против организации.

Атаки на идентичность и доверие

Эта категория объединяет угрозы, направленные не на ваш ресурс как таковой, а на ваши имя, бренд и доверие аудитории. Такие атаки используют различные методы, чтобы обмануть ваших посетителей. Основные методы включают «угон» доменного имени, когда контроль над вашим веб-адресом перехватывают и направляют посетителей на поддельный веб-сайт. Другой популярный метод — создание веб-сайтов-клонов на адресах, очень похожих на ваш, или с идентичным дизайном веб-сайта, чтобы дискредитировать вас или собирать пожертвования от вашего имени. Цель таких атак — подорвать репутацию, которую вы выстраивали годами.

Как отмечалось ранее, понимание угроз является первым шагом к безопасности. Следующий, шаг — внедрение конкретных мер для их предотвращения и смягчения последствий. Ниже представлены ключевые стратегии защиты, сгруппированные в соответствии с четырьмя основными категориями угроз.

Меры противодействия компрометации (взлому) веб-ресурса

Надежный хостинг-провайдер — выбор хостинг-провайдера является фундаментальным решением, определяющим безопасность и устойчивость вашего онлайн-ресурса. При оценке следует выходить за рамки стоимости и времени бесперебойной работы, рассматривая комплекс технических, юридических и операционных факторов. Техническая надежность включает в себя наличие современной инфраструктуры, обязательную защиту от DDoS-атак, а также автоматизированную систему ежедневного резервного копирования с возможностью быстрого восстановления. Не менее важна и юридическая защищенность: необходимо оценить юрисдикцию провайдера, его политику конфиденциальности и готовность отстаивать интересы клиентов в ответ на запросы государственных органов. Идеальный провайдер должен демонстрировать прозрачность в своей деятельности и иметь безупречную репутацию, подтвержденную отзывами других организаций гражданского общества.

Операционная надежность определяется качеством и доступностью технической поддержки 24/7, а также удобством панели управления для администрирования веб-сайта. Однако для ННО критически важным является и этический аспект: провайдер должен не только предоставлять услуги, но и понимать специфические риски, с которыми сталкиваются правозащитники и независимые медиа. Предпочтение следует отдавать тем компаниям, которые разделяют ценности свободы слова, активно поддерживают гражданское общество и готовы оказать дополнительную помощь в кризисной ситуации, в том числе в расследовании попыток взлома.

Специализированные сервисы, такие как VirtualRoad.org (https://www.qurium.org/) или eQualitie в рамках проекта eQPress предоставляющие защищенный хостинг для веб-сайтов на WordPress (https://deflect.ca/solutions/hosting/), а также программы поддержки, вроде Project Galileo от Cloudflare (https://www.cloudflare.com/galileo/), являются оптимальным выбором, так как они изначально спроектированы для противодействия угрозам, с которыми сталкивается сектор и предоставляют свои услуги для организаций гражданского общества с высоким уровнем риска бесплатно.

В рамках программы Microsoft for nonprofits (https://nonprofit.microsoft.com/) Майкрософт также предоставляет годовой кредит на $2000USD на использование своей платформы Azure, которую в том числе можно использовать для хостинга, но использование ее может оказаться сложным для усредненной ННО и скорее всего потребует технического специалиста для настройки.

Обеспечение безопасного доступа к администрированию веб-сайта — необходимо обеспечить максимальную защиту доступа к административной панели как вашего веб-сайта (к управление контентом и настройками) так и панели хостинга. Как минимум, что можно сделать самостоятельно — это использовать сложные, уникальные пароли и в обязательном порядке включить двухфакторную аутентификацию (2FA). Для хороших хостингов при регистрации это будет настроено по умолчанию. Для систем управления контентом (CMS), таких как WordPress, Drupal придется использовать сторонние модули. Дополнительными методами защиты, которые могут потребовать технической помощи являются обеспечение доступа к панели администрирования только через VPN или изменение адреса входа по умолчанию на другой. Помимо этого можно настроить временную блокировку учетной записи при нескольких попытках неправильного введения пароля.

Своевременное обновление программного обеспечения — большое количество взломов веб-ресурсов происходит из-за необновленного программного обеспечения, как правило это система управления контентом (CMS), дополнительные модули (плагины) и платформа на которой написан веб-сайт. Часто разработчики веб-сайтов подходят к своей задаче «спустя рукава» и не ориентируются на безопасность, в результате клиент получает необновляемые или уязвимые темы, плагины или, в случае «самописных» систем полностью уязвимую и неподдерживаемую систему. В самых популярных системах, таких как WordPress, Drupal, Joomla существуют встроенные системы автообновления, которые автоматически обновляют компоненты системы. Это хорошо и правильно с точки зрения безопасности, но нужно иметь ввиду, что в зависимости от разработчиков, компонентов и прочих факторов, при масштабных обновлениях веб-сайт может частично или полностью прекратить работать. Поэтому прежде всего необходимо позаботиться о наличии резервных копий веб-сайта, чтобы была возможность восстановить предыдущую версию и провести обновление с помощью технической поддержки.

Резервное копирование — главный инструмент для быстрого и полного восстановления после инцидентов, включая взломы. Даже самой лучшей защиты может оказаться недостаточно, к примеру, в случае наличия так называемых уязвимостей нулевого дня, о которых еще не знают разработчики платформы. Такие уязвимости могут быть использованы даже в случае полностью обновленных систем. Лучшим способом восстановления в таком случае, для того чтобы исключить наличие зловредного кода, будет восстановления из резервной копии. Если точно не известно когда был произведен взлом, то, возможно, необходимо будет восстановление из более ранней версии. Удостоверьтесь, что хостинг-провайдер делает регулярные копии и хранит их версии. Если в организации есть технический специалист, частью его обязанностей должно быть резервное копирование и хранение их версий. Частота резервного копирования зависит от частоты обновления ресурса, как правило, вы должны задать себе вопрос — как часто должна делаться копия, чтобы восстановление заняло минимально возможные время и усилия.

Внешние защитные сервисы — для сокращения вероятности взлома, в том числе с использованием уязвимостей нулевого дня, могут применяться дополнительные сервисы, такие как WAF (Web Application Firewall), которые представляют собой защитный механизм, который отрезает большинство попыток взлома еще до достижения веб-ресурса. Как правило сервисы, которые предоставляют такую функцию, имеют возможность включить базовый набор без вникания в технический подробности одной кнопкой. К примеру Project Galileo от Cloudflare, упоминавшийся выше, включает в себя WAF корпоративного уровня с возможностью простого включения основного набора настроек. Также существуют WAF плагины для CMS, к примеру Wordfence для Wordpress и Akeeba Admin Tools для Joomla, но большая часть функционала для них платная.

Меры противодействия DDoS-атакам

В настоящее время DDoS-атаки могут достигать огромных величин, сравнимых с потреблением Интернета небольшой страны, одна из наиболее значимых зафиксированных атак произошла в 2025 и составила 29,7 Тбит/с. Это примерно как в секунду скачать с веб-сайта примерно 7 000 фильмов в HD-качестве. В атаке предположительно участвовало более 1 млн зараженных устройств. Справиться с подобными атаками, даже меньшей мощности, не имея огромных ресурсов практически невозможно, поэтому наиболее эффективный способ — использование

специализированных сервисов-посредников, которые принимают удар на себя. Уже упомянутые Cloudflare Project Galileo, VirtualRoad.org, eQualitie предоставляют защиту от DDoS-атак для гражданского общества.

Меры противодействия юридическому и административному давлению

Защита от этого типа угроз лежит в основном в юридической и процедурной плоскости, в частности — соответствие законодательству, консультации с юристами и наличие грамотной редакционной политики. При этом есть технические аспекты, позволяющие провести подготовительную работу и при выполнении таких угроз продолжать работу.

В первую очередь к этому относится минимизация наличия ресурсов внутри страны, таких как хостинг ресурса внутри страны и доменное имя в страновой зоне. При использовании административного давления на хостинг-провайдера или администратора доменной зоны ваш ресурс может быть выключен или удален, а доменное имя — разделегировано (изъято). Чтобы этого не произошло позаботьтесь о надежном хостинге за пределами страны и используйте общее доменное имя (к примеру, .org, .info, .ngo). Так же предусмотрите наличие веб-сайтов-зеркал и использование сетей распределения контента (CDN), таких как Cloudflare или Akamai. И не забывайте про резервное копирование.

Меры противодействия атакам на идентичность и доверие

Большинство угроз в этой категории плохо контролируются, так как, как правило, они находятся вне пределов зоны вашего контроля. Но, как уже упоминалось ранее, знание об угрозах дает нам возможности на них реагировать, поэтому введите себе в практику мониторинг цифрового окружения, периодически осуществляйте поиск веб-сайтов с похожими на ваш названиями. Это же относится и к страницам в соц. сетях. Проверяйте все сообщения о поддельных аккаунтах. В случае обнаружения поддельных веб-сайтов-клонов, обращайтесь с жалобами к их хостинг-провайдеру и регистратору доменов. В случае соцсетей используйте официальные каналы жалоб, а также предупреждайте свою аудиторию через все доступные каналы. Со своей стороны вам необходимо защитить доменное имя вашего веб-сайта. Необходимо убедиться, что вы знаете, где и на кого оно зарегистрировано и как получить к доступ к его настройкам. Очень часто этим занимаются разработчики веб-сайтов, оформляют его на себя и не используют существующие опции безопасности (сложный пароль, двухфакторная аутентификация, запрет переноса домена). В результате, в случае проблем с доменным именем, к примеру «угон» домена, организации может быть очень сложно или невозможно вернуть его обратно. Также важно позаботиться о том, чтобы у вашего веб-ресурса был действительный сертификат безопасности. Отсутствие такого сертификата может привести к падению доверия к вашему веб-сайту у аудитории, за счет того, что соединение будет нешифрованное и трафик может быть перехвачен или изменен, так же некоторые антивирусы на данный момент блокируют доступ к таким веб-сайтам. Большинство надежных хостингов предоставляют такую возможность по умолчанию. В случае отсутствия такой возможности можно получить бесплатный сертификат с помощью Let’s Encrypt (letsencrypt.org), что потребует некоторых технических навыков.

Расследование инцидентов и реагирование на угрозы

Когда происходит инцидент безопасности — будь то взлом веб-сайта, угрозы сотруднику или скоординированная атака — первая реакция — почти всегда хаос и паника, нескоординированные действия без системы, что часто приводит к ухудшению ситуации, утере следов для расследования и прочим сопутствующим потерям. Поэтому в случае любого инцидента необходимо следовать четкому, пошаговому плану действий. Эффективное реагирование не только минимизирует ущерб, но и помогает извлечь уроки, чтобы будущем минимизировать или вероятность инцидента или его последствия и восстановиться быстрее.

Обнаружение, первая реакция и документирование

Первые минуты и часы после обнаружения инцидента являются критически важными. Главная задача на этом этапе — предупредить лиц ответственных за организацию и за ресурсы которые пострадали в инциденте. В первую очередь это директор организации, IT-специалист, если он есть, руководители соответственного направления (администратор веб-сайта или соц. сетей при взломе, HR-специалист при угрозах, руководитель проекта при утечке и т. д.). Собрать команду реагирования и вести всю коммуникацию по инциденту через защищенные каналы, к пример Signal, чтобы предотвратить утечки информации. Крайне важно начать вести журнал инцидента, документируя все происходящее: время, симптомы, предпринятые действия. Эта документация станет основой для последующего анализа. Ни в коем случае нельзя немедленно удалять следы атаки; вы скорее всего не сможете так решить проблему, только удалите важные доказательства. Вместо этого следует сделать скриншоты и сохранить копии логов, так как эти данные могут быть важны для последующего расследования. Если затронутое инцидентом устройство активно эксплуатируется (рассылается спам, на нем происходят какие-то действия) нужно немедленно отключить его от сети (физически выдернуть сетевой кабель или отключить WiFi). Не нужно выключать его, так как вы можете затереть важные следы. В случае взлома веб-сайта можно перевести его в режим обслуживания. Необходимо без промедления обратиться за внешней экспертной помощью, в первую очередь в специализированные организации, такие как Access Now (https://www.accessnow.org/) в их Digital Security Helpline (help@accessnow.org), которые окажут профессиональную поддержку в оценке ситуации. Нужно иметь ввиду, что Access Now при первом запросе должны будут провести проверку вас через доверенных партнеров для подтверждения вашего статуса и это может занять некоторое время. Поэтому лучше заранее подготовьтесь к инцидентам и напишите в Access Now с электронной почты организации с просьбой проверки для последующих обращений, чтобы в случае инцидента получить помощь незамедлительно. Digital Security Helpline специализируется на широком круге вопросов, включая взаимодействие с соцсетями и другими организациями. В части расследования атак на веб-ресурсы, кампании по дезинформации можно так же обратиться в Qurium — The Media Foundation (https://www.qurium.org/rapid-response/request/).

Анализ и оценка ущерба

Далее совместно с техническими специалистами необходимо провести анализ, чтобы определить вектор атаки: был ли это взломанный пароль, уязвимость в программном обеспечении или результат фишинга. Понимание того, как именно злоумышленник проник в систему, является ключом к закрытию этой уязвимости. Параллельно проводится оценка ущерба: были ли украдены или изменены данные, использовался ли ресурс для атак на других, и насколько широко инцидент мог распространиться (на другие устройства или задеть других людей).

Устранение последствий, восстановление и коммуникация

На этом этапе происходит непосредственное устранение последствий и возвращение к нормальной работе. Для взломанного веб-сайта наиболее надежным методом является не попытка «очистить» его от вредоносного кода, а полное восстановление из заведомо чистой резервной копии. Взломы любых аккаунтов должны сопровождаться немедленной сменой всех паролей, связанных со скомпрометированной системой, и включением двухфакторной аутентификации. В случае скомпрометированных устройств, правильным является полная переустановка системы или сброс до заводских настроек. Важным шагом является коммуникация с затронутыми сторонами. Если произошла утечка персональных данных пользователей, их следует уведомить об этом, предварительно проконсультировавшись с юристами о том, как предоставить необходимую информацию.

Выводы после инцидента

После того как ситуация стабилизирована, необходимо провести внутренний разбор инцидента. Цель этого анализа — не поиск виновных, а выявление слабых мест в процессах и технологиях. На основе сделанных выводов следует обновить внутренние политики безопасности, создать или обновить процедуры реагирования на инциденты, провести дополнительное обучение для команды и внедрить новые технические средства защиты. Такой подход превращает каждый инцидент в урок, который делает организацию более устойчивой в будущем.

Обращение в правоохранительные органы

Вопрос о подаче официального заявления в полицию является достаточно сложным и рискованным для ННО. С одной стороны, официальное заявление фиксирует факт инцидента, что может служить юридической защитой, если украденные данные или скомпрометированный ресурс будут использованы для незаконной деятельности от вашего имени. С другой стороны, существует серьезная опасность «превращения жертвы в подозреваемого», когда в рамках расследования правоохранительные органы могут изъять всю вашу технику, получив легальный доступ к конфиденциальной информации о вашей деятельности, бенефициарах и партнерах.

Это решение должно приниматься только после тщательной оценки рисков, взвешивая политический контекст в стране, уровень доверия к правовой системе и чувствительность данных, которые могут быть раскрыты. Золотым правилом является получение консультации у доверенного адвоката, специализирующегося на защите активистов, до любых контактов с правоохранительными органами.

Заключение

Цифровая среда стала неотъемлемой частью деятельности некоммерческих организаций. Она открывает новые возможности для коммуникаций, доступа к информации, реализации проектов и взаимодействия с аудиторией. В то же время цифровизация усиливает требования к ответственности, правовой грамотности и управлению рисками.

Как показано в данном пособии, цифровые права — это не абстрактная категория, а практический инструмент, напрямую влияющий на повседневную работу ННО. Доступ к информации, защита персональных данных, правила публикации контента, взаимодействие с государственными органами и онлайн-платформами — все эти вопросы требуют осознанного и системного подхода.

Важно учитывать, что формальные гарантии прав не всегда означают их автоматическую реализацию на практике. ННО работают в среде, где одновременно действуют национальное законодательство, международные стандарты и правила цифровых платформ. Это требует умения ориентироваться в нескольких уровнях регулирования и принимать взвешенные решения с учетом правовых и репутационных последствий.

Отдельное значение приобретает управление рисками. Работа с чувствительной информацией, публикация контента, взаимодействие с аудиторией и партнерами — все это связано с потенциальными угрозами, которые могут затрагивать как саму организацию, так и ее бенефициаров. В этих условиях важно выстраивать внутренние политики, процедуры и практики, направленные на защиту данных, источников информации и устойчивость коммуникаций.

Пособие не ставит целью дать универсальные ответы на все возможные ситуации. Его задача — сформировать у читателя понимание логики цифровых прав, показать ключевые риски и предложить инструменты для принятия решений в конкретных условиях.

Таким образом, эффективная работа ННО в цифровой среде сегодня невозможна без сочетания правовой осведомленности, практических навыков и стратегического подхода к коммуникациям и безопасности. Именно это сочетание позволяет не только минимизировать риски, но и использовать цифровые инструменты в интересах общества максимально эффективно.

Приложения

Приложение 1

Чек-лист по выполнению базовых требований законодательства Республики Узбекистан о персональных данных

Источник: https://www.itts.uz/contacts

	Требование	Как требование реализовано на предприятии? Проще — «Есть»/«Нет» или «+»/ «-». Лучше указать имена ответственных лиц, номера приказов, названия документов и др.	Источник (нормативно-правовой акт)	URL, ссылка на пункт НПА
1	Определены ли правовые основания для обработки ПДн на предприятии? Какие? (письменное согласие, исполнение договора, требования НПА)		ст. 18 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398418
2	Разработаны ли типовые формы согласия на обработку ПДн?			
3	Включены ли в типовые формы договоров пункты об обработке ПДн?			
4	Производится ли обработка ПДн после истечения сроков договора с субъектом? Если да, то на каком основании?			
5	Удовлетворяет ли форма согласия на обработку персональных данных требованиям законодательства, включены ли в нее все обязательные поля?		п. 11 Приказа Минюста № 3478 от 15.11.2023 г.	https://lex.uz/docs/6663967#6664336
6	Зарегистрированы ли все соответствующие базы ПДн в государственном реестре?		ст. 31 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398788
7	Как фиксируется согласие субъекта на обработку ПДн? Хранятся ли дата/время/ID устройства/ IP-адрес, с которого давалось согласие?		ст. 21 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398514

8	Если ли возможность отзыва согласия в той же форме, в которой оно давалось? Есть ли возможность направить отзыв согласия в виде электронного документа?		
9	Обрабатываются ли персональные данные умерших субъектов? Кем дано согласие на такую обработку? (согласие, данное при жизни, согласие законных наследников)		
10	Какое подразделение занимается предоставлением данных об обработке ПДн по запросам субъектов?	ст. 22 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398536
11	Определен ли порядок блокировки и уничтожения персональных данных на основании обращения субъекта персональных данных?	п. 30.13 Приказа Минюста № 3478 от 15.11.2023 г.	https://lex.uz/docs/6663967#6664487
12	Произведено ли разделение баз, если обработка ПДн в них осуществляется с несовместимыми между собой целями?	п. 5 Приказа Минюста № 3478 от 15.11.2023 г.	https://lex.uz/docs/6663967#6664304
13	Как производится уведомление субъекта о включении его ПДн в базу ПДн?	ст. 23 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398628
14	Как производится уведомление субъекта при передаче его ПДн третьим лицам?		
15	Сформирован ли перечень третьих лиц? Кто и как его актуализирует?		
16	Осуществляется ли на предприятии полностью автоматизированная обработка ПДн, например, скоринг?	ст. 24 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398652
17	Как получается согласие субъекта на полностью автоматизированную обработку его ПДн? Каковы правовые основания такой обработки?		
18	Производится ли обработка специальных (сведения о здоровье, составе семьи, национальности) ПДн?* *Обработка специальных персональных данных запрещается, за исключением ограниченного числа случаев	ст. 25 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398682
19	Производится ли на предприятии обработка биометрических ПДн (фотографии, отпечатки пальцев и др.)?	ст. 26 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398727

20	Каковы правовые основания такой обработки? Давал ли субъект/работник согласие на такую обработку?		
21	Есть ли на предприятии биометрический СКУД? Зарегистрирована ли его база в госреестре баз ПДн? Получены ли письменные согласия всех включенных в базу СКУД?		
22	Как осуществляется учет материальных носителей, содержащих биометрические/генетические данные?	п. 5 Приложения № 2 к ПКМ РУз № 570 от 05.10.2022 г.	https://lex.uz/ru/docs/6225462#6227477
23	Как именно реализовано требование об шифровании и криптографической защите биометрических данные?	п. 4 Приложения № 2 к ПКМ РУз № 570 от 05.10.2022 г.	https://lex.uz/ru/docs/6225462#6227475
24	Проставлены ли грифы на носителях биометрических данных? Какие конкретно обязательные меры применяются для обеспечения физической безопасности носителей? Фиксируются ли IP и MAC адреса устройств, получающих доступ к биометрическим данным?	гл. 2 Приложения № 2 к ПКМ РУз № 570 от 05.10.2022 г.	https://lex.uz/ru/docs/6225462#6227469
25	Где и как обрабатываются ПДн граждан Узбекистана? Где физически расположено оборудование, на котором осуществляется обработка? Включена ли юрисдикция в список стран с адекватной защитой? Отвечают ли стандартные договорные условия, корпоративные правила оператора требованиям уполномоченного государственного органа? Соблюдает ли оператор международные стандарты в области управления и хранения персональных данных?	ст. 27.1 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#5271076
26	Осуществляется ли передача ПДн на территорию других стран — трансграничная передача? На территорию каких стран?	ст. 15 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398348
27	Утвержденный состав персональных данных, необходимый и достаточный для выполнения задач предприятия?	ст. 31 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398788

28	Определено ли структурное подразделение или должностное лицо, ответственное за работу, связанную с обработкой и защитой персональных данных?		
29	Определены ли сроки обработки персональных данных (по каждой категории, по каждой базе)? Каковы эти сроки?	ст. 10 и 19 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398106
30	Проводятся ли на предприятии исторические, статистические, социологические или научные исследования с персональными данными? Производится ли при этом обязательное обезличивание этих персональных данных?	ст. 16 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398378
31	Производится ли уничтожение персональных данных? Кем, как? Какой документ это регулирует?	ст. 17 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398388
32	Определены ли типы угроз, актуальные для каждой базы ПДн? Присвоены ли каждой базе уровни защищенности?	п. 2 ПКМ РУз № 570 от 05.10.2022 г.	https://lex.uz/uz/docs/6225462#6227189
33	Выполняются ли требования ИБ для каждой из баз ПДн на основании присвоенного им уровня защищенности? Какие именно меры применимы к конкретной базе?	гл. 10 ПКМ РУз № 570 от 05.10.2022 г.	https://lex.uz/uz/docs/6225462#6227279
34	Подчиняется ли подразделение, ответственное за обеспечение защиты персональных данных, непосредственно руководителю предприятия?	п. 3 Приказа Минюста № 3477 от 15 ноября 2023 г.	https://lex.uz/docs/6663969#6668986
35	Проводятся ли периодические проверки базы персональных данных? Когда в последний раз проверялась актуальность регистрационных данных?	п. 8 Приказа Минюста № 3477 от 15 ноября 2023 г.	https://lex.uz/docs/6663969#6669029
36	Сформирован ли список работников предприятия, имеющих доступ к работе с базами персональных данных?		
37	Проводятся ли семинары или тренинги для работающих с персональными данными (журналисты, ИТ, кадры, юристы)?		
38	Обеспечена ли возможность восстановления персональных данных, уничтоженных или поврежденных в результате несанкционированного доступа к ним?		

39	Если обработка персональных данных осуществляется на основании оферты, указаны ли в ней конкретные цели обработки?	п. 9 Приказа Минюста № 3478 от 15.11.2023 г.	https://lex.uz/docs/6663967#6664327
40	Осуществляется ли на предприятии видеонаблюдение? С какой целью? Какие персональные данные обрабатываются?	п. 12 Приказа Минюста № 3478 от 15.11.2023 г.	https://lex.uz/docs/6663967#6664354
41	Утверждены ли внутренние документы, определяющие политику собственника/оператора по обработке и защите персональных данных?	п. 30.12 Приказа Минюста № 3478 от 15.11.2023 г.	https://lex.uz/docs/6663967#6664485
42	Учитываются ли в кадровом делопроизводстве требования нового Трудового кодекса РУз в части защиты персональных данных работника? Обладают ли работники кадровой службы минимальной компетенцией в сфере персональных данных?	§ 6. Защита персональных данных работника Трудового кодекса РУз	https://lex.uz/ru/docs/6257291#6262031
43	Если персональные данные работника получаются у третьих лиц (судимость, учет в диспансерах), то уведомляется ли работник письменно об этом заранее и было ли от него получено письменное согласие?	ст. 176 Трудового кодекса РУз	https://lex.uz/ru/docs/6257291#6262106
44	Имеет ли работник полный доступ ко всем его персональным данным, которые хранятся у работодателя? Может ли он снимать с них копии?	ст. 179 Трудового кодекса РУз	https://lex.uz/ru/docs/6257291#6262129
45	*В формах согласия и офертах отсутствуют “темные паттерны”: • галочки и флажки с согласием на обработку ПДн не проставлены автоматически; • кнопка согласия с условиями может быть нажата только когда субъект просмотрел все страницы предлагаемого договора (оферты) полностью; • факт проставления отметок и нажатия кнопки подтверждения с условиями должен быть зафиксирован с указанием даты, времени, IP-адреса и идентификатора клиента * требования применимы только к коммерческим банкам	п. 28 Постановления ЦБ Руз № 3030 от 02.07.2018	https://lex.uz/docs/3804290#3805017
46	Внедрена ли в систему управления информационной безопасности (СМИБ/СУИБ) защита персональных данных?	п. 31 Приказа Минюста № 3478 от 15.11.2023 г. A.5.34 ISO/IEC 27001:2022 A.18.1.4 O‘z DSt ISO/IEC 27001:2020	https://lex.uz/docs/6663967#6664488 https://stt2.unicon.uz/#/post/772

Приложение 2

Универсальный чек-лист процедур по обработке персональных данных (ПДн)

A. Реестр процессов обработки ПДн и баз ПДн
- Составлен реестр процессов обработки ПДн (цели, основания, категории субъектов, состав данных, получатели, сроки хранения).
- Составлен реестр баз ПДн.
- Базы ПДн зарегистрированы.
- Назначен владелец каждого процесса.
- Проведена оценка угроз и составлен акт оценки.
- Утверждена политика обработки ПДн.

B. Процедура сбора ПДн и уведомления
- Для каждого канала сбора определены цели и основания.
- Подготовлен текст уведомления субъекту при включении в базу.
- Настроены формы/скрипты (веб-сайт, анкеты, договоры, HR-формы).
- Исключены лишние поля («на всякий случай» не считается основанием).

C. Процедура согласий
- Согласие фиксируется в форме, позволяющей подтвердить факт получения.
- Для специальных данных — письменное согласие (в т. ч. электронный документ).
- Хранится доказательство согласия (лог, подписанный документ, чек-бокс с записью).
- Отзыв принимается в той же форме или письменно (в т. ч. электронно).

D. Процедура доступа и внутреннего использования
- Введена матрица доступов (role-based).
- Доступ выдается по заявке и по принципу необходимости.
- Ведутся журналы доступа и операций.
- Регламентированы копирование, выгрузки, съемные носители.
- Регламентированы места хранения съемных носителей.

E. Процедура изменения и качества данных
- Есть канал для исправления/уточнения данных по подтверждающим документам.
- Если исправить нельзя, предусмотрено уничтожение.
- Установлены сроки обновления критичных данных (контакты, документы).

F. Процедура запросов субъектов ПДн
- Описан состав информации, выдаваемой субъекту ПДн об обработке.
- Настроена идентификация заявителя.
- Обеспечена возможность подачи документов в электронном виде на приостановление/уничтожение.
- Прописаны сроки внутреннего исполнения и шаблоны ответов на запрос ПДн.

G. Процедура передачи третьим лицам
   - Передача допускается только при наличии основания (в т. ч. согласие/договор/закон).
   - Заключен договор с обязательствами по защите и конфиденциальности.
   - Субъект уведомляется о передаче третьему лицу в течение 3-х дней, если нет исключения.
   - Ведется реестр третьих лиц и категорий передаваемых персональных данных.

H. Процедура распространения (публикации)
   - Любое распространение сверх заявленных целей — только с согласия субъекта.
   - Отдельные правила для веб-сайта, соцсетей, кейсов, фото/видео, отзывов.
   - Проверка «общедоступности» данных и основания доступа.

I. Процедура трансграничной передачи
   - Определяется страна и проверка в списке стран с адекватной защитой (наличие законодательства, договор о конфиденциальности, внутренние политики, технические меры защиты)
   - Для «неадекватных» стран фиксируется основание (например, согласие).
   - Ведется реестр трансграничных передач (система, провайдер, дата, основание).
   - Процедура уведомления регулятора о трансграничной передаче

J. Локализация и регистрация (для данных граждан РУз)
   - Сбор/систематизация/хранение обеспечены на технических средствах в РУз (только для биометрических и генетических данных).
   - Требуется ли регистрация баз персональных данных.
   - Контроль стандартов защиты облачных сервисов, резервных копий и внешних сервисов.

K. Процедура хранения, удаления и уничтожения
   - Установлены сроки хранения по целям обработки.
   - Основания уничтожения: цель достигнута, отзыв согласия, срок обработки истек, решение суда.
   - Уничтожение оформляется актом.
   - Проверяется удаление копий и резервов по регламенту.

L. Процедура реагирования на инциденты (утечки/нарушения)
   - Определены категории инцидентов и команда реагирования.
   - Предусмотрена приостановка обработки или уничтожение при наличии информации о нарушении условий обработки.
   - Обеспечены: локализация, расследование инцидентов, устранение причин, документирование.
   - Введены шаблоны уведомлений и протокол коммуникаций.

См. ЗРУ-547-сон 02.07.2019 «О персональных данных» (https://lex.uz/docs/4396428)

Приложение 3

Структура Политики обработки и защиты персональных данных

1. Общие положения
    1.1. Цель Политики
    1.2. Область применения (работники, кандидаты, клиенты, контрагенты, представители контрагентов)
    1.3. Термины и определения (субъект, оператор/собственник, третье лицо, база ПДн, распространение, трансграничная передача)
    1.4. Принципы обработки
2. Роли и ответственность
    2.1. Собственник и (или) оператор
    2.2. Ответственное подразделение/должностное лицо по ПДн (назначение и функции)
    2.3. Полномочия пользователей доступа и владельцев процессов
3. Правовые основания и цели обработки
    3.1. Условия (основания) обработки (согласие, договор, закон, законные интересы, общественно значимые цели, исследования при обезличивании, общедоступные источники)
    3.2. Определение целей обработки во внутренних документах и их соответствие ранее заявленным целям при сборе
4. Категории данных и субъектов
    4.1. Категории субъектов.
    4.2. Категории данных (обычные, специальные; при наличии — биометрические/генетические)
    4.3. Минимизация состава данных (необходимость и достаточность)
5. Жизненный цикл обработки
    5.1. Сбор, систематизация, хранение
    5.2. Использование.
    5.3. Предоставление и доступ внутри компании
    5.4. Передача третьим лицам
    5.5. Распространение (публикация, веб-сайт, СМИ)
    5.6. Трансграничная передача
    5.7. Обезличивание (если применимо)
    5.8. Уничтожение (удаление)
6. Согласие и управление согласиями
    6.1. Форма согласия и доказательства его получения
    6.2. Согласие на специальные данные (письменная форма, включая электронный документ.
    6.3. Отзыв согласия и его фиксация

7. Права субъектов и порядок их реализации
    7.1. Право получать информацию об обработке и состав предоставляемой информации
    7.2. Право требовать временного приостановления обработки при проблемах качества/законности/необходимости данных
    7.3. Каналы подачи запросов и сроки внутреннего рассмотрения (внутренний SLA)
    7.4. Идентификация заявителя
8. Уведомления субъектов
    8.1. Уведомление при включении данных в базу (цели и права)
    8.2. Уведомление при передаче третьему лицу (3 дня, исключения)
9. Конфиденциальность и общедоступные данные
    9.1. Режим конфиденциальности
    9.2. Общедоступные персональные данные и правила работы с ними
10. Локализация и регистрация баз
    10.1. Условия обработки данных граждан РУз с использованием ИТ/Интернета (локализация + регистрация в госреестре)
    10.2. Регистрация баз и уведомление об изменениях данных для регистрации
11. Меры защиты
    11.1. Правовые, организационные и технические меры
    11.2. Управление доступом, учетные записи, журналы, носители, помещения
    11.3. Контроль подрядчиков и третьих лиц
12. Удаление, уничтожение и «право на забвение» в практическом смысле
    12.1. Основания уничтожения/удаления (цель достигнута, отзыв согласия, истечение срока, решение суда)
    12.2. Обработка требований на ограничение/приостановление
    12.3. Документирование уничтожения (акты, логи)
13. Реагирование на инциденты и утечки
    13.1. Обязанность приостанавливать обработку или уничтожать данные при наличии информации о нарушении условий обработки
    13.2. Порядок расследования, локализации, исправления и отчетности
14. Трансграничная передача
    14.1. Критерии «адекватной защиты». Учет перечная стран с адекватной защитой
    14.2. Передача в «неадекватные» страны и допустимые основания (включая согласие)
    14.3. Реестр трансграничных передач и контроль потоков
15. Заключительные положения
    15.1. Обучение персонала и ответственность
    15.2. Аудит и пересмотр Политики
    15.3. Контакты ответственного лица

Софинансирование
Европейского Союза

ЦЕНТР
РАЗВИТИЯ
СОВРЕМЕННОЙ
ЖУРНАЛИСТИКИ