Софинансирование Европейского Союза

ЦЕНТР РАЗВИТИЯ СОВРЕМЕННОЙ ЖУРНАЛИСТИКИ

LPRC ЦЕНТР ИССЛЕДОВАНИЯ ПРАВОВОЙ ПОЛИТИКИ

UDRMI O'ZBEKISTON RAQAMLI HUQUQLAR MEDIA TASHABBUSI

ЦИФРОВЫЕ ПРАВА ДЛЯ ЖУРНАЛИСТОВ, БЛОГЕРОВ И МЕДИА

Как понимать, применять и защищать на практике?

ЦИФРОВЫЕ ПРАВА ДЛЯ ЖУРНАЛИСТОВ, БЛОГЕРОВ И МЕДИА

Как понимать, применять и защищать на практике?

Ташкент
2026

Цифровые права для журналистов, блогеров и медиа. Как понимать, применять и защищать на практике? Пособие. Ташкент, 2026 — 84 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 журналистов, редакций и медиа, работающих в цифровой среде. Его задача — не только объяснить природу цифровых прав, но и помочь применять их при принятии редакционных решений, работе с информацией и управлении рисками.

Материал выстроен по принципу «от понимания к применению». Первый раздел формирует базовое представление о цифровых правах и правовой логике их регулирования. Второй — переносит эти принципы в профессиональную деятельность медиа: создание и распространение контента, доступ к информации, взаимодействие с аудиторией и платформами. Третий раздел сосредоточен на рисках и мерах безопасности, с которыми сталкиваются журналисты и редакции в цифровой среде.

Пособие можно использовать в двух режимах. С одной стороны, как последовательный материал для системного освоения темы. С другой — как рабочий справочник для решения конкретных задач: подготовки публикаций, оценки правовых рисков, реагирования на ограничения доступа к информации или взаимодействия с цифровыми платформами.

Отдельные элементы пособия — практические кейсы, рекомендации и чек-листы — предназначены для применения в повседневной редакционной работе. Они позволяют быстро соотнести конкретную ситуацию с правовыми рамками и выбрать обоснованную стратегию действий.

Важно учитывать, что цифровая среда предполагает повышенную ответственность за контент и решения редакции. Поэтому материалы пособия следует использовать не как универсальные ответы, а как основу для профессионального анализа и принятия решений с учетом конкретного контекста.

Раздел 1
Что такое цифровые права?

1.1. Введение в теорию цифровых прав

Современный мир переживает стремительную цифровую трансформацию. Развитие цифровизации затрагивает практически все аспекты жизнедеятельности человека, включая доступ к информации, получение образования, трудоустройство, ведение бизнеса и многое другое. Большинство товаров и услуг можно получить, используя предлагаемые как государством, так и бизнесом специализированные цифровые сервисы.

Более того, количество пользователей Интернета увеличивается в геометрической прогрессии. Так, в октябре 2025 года количество пользователей Интернета в мире составило более 6,4 млрд пользователей[1]. По данным DataReportal[2] количество пользователей Интернета в Узбекистане составляет 32,7 млн пользователей или 92,2 % от общего населения страны.

Принимая во внимание вышеуказанное, ключевым вопросом становится регулирование цифрового пространства через развитие феномена цифровых прав.

Цифровые права человека стали следствием информационной революции, выступающей в качестве движущей силы их развития.

Одна из наиболее распространенных теоретических позиций состоит в том, что «цифровые права» являются прямым продолжением концепции «прав человека», отраженной в множестве международных документов ООН, а также документах регионального уровня.

При этом концепция «прав человека» которую мы знаем в современном виде, через призму таких документов как Всеобщая декларация прав человека (1948), Международный пакт о гражданских и политических правах (1966), Международный пакт об экономических, социальных и культурных правах (1966), а также множества международных и региональных документов прошла огромный путь.

Таким образом, следует в общих чертах обозначить грани развития концепции прав человека в современном виде.

Итак, права человека представляют собой набор неотъемлемых прав каждого человека, независимо от его национальности, места жительства, пола, этнической принадлежности, цвета кожи, религии, языка или любых других признаков.

---

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

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

Ключевые принципы

- Универсальность: они действуют везде и для всех.
- Неотъемлемость: их нельзя отобрать (кроме редких случаев, предусмотренных законом, например, ограничение свободы за преступление).
- Неделимость: гражданские, политические, экономические и социальные права взаимосвязаны. Нельзя полноценно пользоваться одними без других.

Поколения прав человека

Концепция «поколений прав человека» была предложена в 1979 году чешско-французским юристом Карелом Вашаком[3]. Автор был вдохновлен лозунгом Великой французской революции (1789 год): «Свобода, Равенство, Братство»[4]. Каждое «поколение» соответствует одному из слов этого лозунга и отражает исторические этапы развития правовой мысли.

Первое поколение: Свобода (гражданские и политические права)

Суть поколения свободы связана с необходимостью защиты человека от произвола государства. Первое поколение прав сосредоточено вокруг так называемых **«негативных прав».** Это означает, что государство обязано воздерживаться (!) от вмешательства. От власти требуется «ничего не делать» в определенных сферах (не убивать, не сажать без суда, не пытать, не содержать в рабстве, не цензурировать). Иными словами, для реализации негативных прав государству не нужно предпринимать сверхусилий или создавать специальную инфраструктуру.

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

[3] https://bigenc.ru/c/vasak-karel-afd127

[4] https://bigenc.ru/c/kontseptsiia-pokolenii-prav-cheloveka-b16d88

Второе поколение:
Равенство (социально-экономические права)

Суть поколения равенства развивается вокруг обеспечения достойного уровня жизни и социального обеспечения человека. Второе поколение прав сосредоточено вокруг так называемых «позитивных прав». Это означает, что от государства требуются активные действия (!), для создания инфраструктуры для обеспечения максимально возможного уровня социальной поддержки человека.

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

Третье поколение:
Братство (коллективные права / права солидарности)

Суть поколения братства развивается вокруг прав, принадлежащих не отдельному человеку, а целым группам (народам, нациям) или всему человечеству, то есть это так называемые коллективные права.

Основные права:

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

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 в цифровом пространстве, в геномных исследованиях, иных инновационных сферах.

Принимая во внимание, что нас в первую очередь интересует развитие феномена цифровых прав, 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 принадлежит 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[5].

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

Тем не менее, для такого рассуждения должна быть подведена соответствующая правовая база.

К примеру, Резолюция «Поощрение защита и осуществление прав человека в Интернете»[6], 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 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 онлайновой среде имеет важное значение для реализации права свободно выражать свои мнения 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.

Подтверждает, что те же самые права, которые человек имеет в офлайновой среде, должны также защищаться в онлайновой среде.

---

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

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

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 о политических правах (свобода слова и выражения мнения), экономических (право на образование) и коллективных правах (глобальный характер Интернета).

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

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.

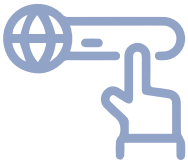
Доступ человека в Интернет сопряжен с различного рода вызовами, рисками и угрозами, транслируемыми государствами, технологическими компаниями и иными третьими лицами.

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 формирования перечня цифровых прав в большей степени применимых в случаях пользования цифровыми платформами и шире Интернетом.

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

Перечень цифровых прав

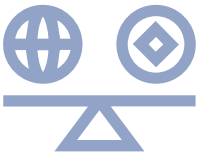


Право на доступ в Интернет

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 обусловила необходимость фундаментальной реинтерпретации классической доктрины прав человека, а именно, их переноса в виртуальное пространство на основе базового принципа ООН о тождественности защиты прав в офлайн- и онлайн-средах. По состоянию на 2026 год регулирование цифровой сферы перестало быть вопросом исключительного национального усмотрения и подчиняется сложной архитектуре международных обязательств, варьирующихся от универсальных пактов ООН до специализированных конвенций в области кибербезопасности и защиты данных. Данный нормативный каркас функционирует как многоуровневая система, где глобальные стандарты дополняются и конкретизируются региональными инструментами Совета Европы, ЕС, ОБСЕ, ШОС и СНГ, формируя единый правовой контур цифрового статуса личности. Центральное место в этой системе занимают гарантии ключевых цифровых прав, включая право на универсальный доступ к Интернету, свободу выражения мнений без алгоритмической цензуры, неприкосновенность частной жизни в условиях экономики больших данных. Особое значение международные нормы приобретают в вопросах допустимых ограничений прав, устанавливая жесткий **«трехсоставный тест»** законности и пропорциональности для предотвращения трансформации государственного регулирования в инструменты цифрового авторитаризма. При этом эволюция стандартов продолжается непрерывно, охватывая новые вызовы четвертой промышленной революции, такие как этика искусственного интеллекта, алгоритмическая дискриминация и ответственность транснациональных цифровых платформ. Таким образом, анализ международно-правового фундамента является необходимым условием для понимания границ государственного суверенитета и механизмов защиты человека, его прав и в эпоху глобальной цифровизации.

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

[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

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. Тем не менее, позиция и доклады Специальных докладчиков задают стиль и вектор правовой мысли для правовых систем отдельных государств.

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, 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:* Специальный 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 при этом, 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

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).

А именно, 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.

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):

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

   1.1. уведомление с точной причиной;

   1.2. 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:

1. **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).

2. **Легитимная цель:** защита нацбезопасности, порядка, здоровья, нравственности, прав других лиц.

3. **Необходимость и пропорциональность:** по принципу 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 в ряде случаев допускает 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 лишить диктаторские режимы возможности использовать их как предлог для репрессий.

Сиракузские принципы также представляют собой толкования ограничений и отступлений от положений Международного пакта о гражданских и политических правах (далее по тексту — Сиракузские принципы) и 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.

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

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.

Примеры

Cengiz and Others v. Turkey (2015)[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)[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 безопасность пользователей. Важно отметить, что Digital Services Act упоминается в паре с Digital Markets Act (2022)[20]. Цель принятия — ограничить власть крупнейших технологических компаний, которых закон называет «гейткиперами» (gatekeepers — «вратари» или «контролеры доступа»).

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.

---

[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

[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

№	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

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[21], принятая в 1981 году.

К принципам второго «поколения» конфиденциальности данных в большей степени относится Директива 95/46/EC[22] о защите физических лиц при обработке персональных данных и о свободном обращении таких данных.

Наконец, к третьему «поколению» стандартов конфиденциальности данных относятся GDPR[23], 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:

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

[22] 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

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

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	Подотчетный — 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
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», а также обязательством государства обеспечить доступ к информации в цифровой форме: «Государство создает 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.

Другая конституционная норма 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».

Кроме того, 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».

Данные положения составляют важнейшую часть правовой базы страны, касающейся защиты данных и частной жизни. Эта статья подчеркивает важность баланса между правом на доступ к информации и необходимостью защиты частной жизни и персональных данных.

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 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. Однако, чтобы соответствовать международным стандартам, исключения должны соответствовать конституционным обязательствам и включать трехкомпонентный тест, чтобы не допустить ограничения объема права на доступ к информации. Законы о доступе к информации не содержат правил о приоритете общественного интереса, позволяющих использовать исключения в пользу раскрытия информации. В то время как для соответствия международным стандартам максимального раскрытия информация, имеющая ключевое общественное значение, должна быть опубликована проактивно или автоматически.

1.3.1. Законодательство о средствах массовой информации

В Узбекистане деятельность средств массовой информации (СМИ) и журналистов регулируется следующими основными нормативно-правовыми актами: Конституция Республики Узбекистан, Законы Республики Узбекистан «О средствах массовой информации», «О защите профессиональной деятельности журналиста», «О принципах и гарантиях свободы информации», «Об информатизации», «Об открытости деятельности органов государственной власти и управления», а также Ппостановлением Кабинета министров «Об утверждении основных правил, регулирующих профессиональную деятельность корреспондентов средств массовой

информации иностранных государств на территории Республики Узбекистан» и Административным регламентом об оказании государственной услуги по государственной регистрации СМИ.

Свобода СМИ искать, получать, исследовать, распространять, использовать, хранить информацию гарантируется статьей 81 Конституции при условии ответственности за объективность и достоверность распространяемой информации:

> Средства массовой информации свободны и действуют в соответствии с законом. Государство гарантирует свободу деятельности средств массовой информации, реализацию ими права на поиск, получение, использование и распространение информации. Средства массовой информации несут ответственность за достоверность предоставляемой ими информации».

Установлен запрет цензуры и воспрепятствование деятельности или вмешательство в деятельность средств массовой информации влечет ответственность в соответствии с законом.

Законодательство Узбекистана о средствах массовой информации создает правовые рамки, направленные на обеспечение достоверности информации, создаваемой и распространяемой в информационном пространстве различными акторами, включая СМИ.

Закон о СМИ запрещает распространение следующих видов информации:

Категория информации	Соотношение с дезинформацией
Призывы к насильственному изменению конституционного строя и сепаратизму	Прямой запрет на публикации, направленные на подрыв государственного или конституционного строя, форма политической дезинформации
Пропаганда терроризма и религиозного экстремизма	Часто осуществляется через искажение фактов
Разглашение государственной тайны или иной конфиденциальной информации	Является нарушением, если передается как «сенсационная правда», вводя в заблуждение
Информация, возбуждающая национальную, расовую, этническую или религиозную вражду	Дезинформация может использоваться для манипуляции общественным мнением и эскалации конфликтов
Запрет публикации материалов дознания, следствия или суда	Защита конфиденциальности сведений дознания и предварительного следствия, не распространяется на освещение открытых судебных заседаний
Информация, порочащая честь и достоинство или деловую репутацию граждан	Запрет на публикацию заведомо ложных, позорящих лицо сведений и фактов (диффамация)

Кроме того, СМИ могут нести ответственность за публикацию ложной информации, повлекшей угрозу общественному порядку, манипулирование фактами в целях пропаганды запрещенных идей, публикацию без проверки фактов, повлекшую ущерб репутации, правам и частной жизни граждан.

СМИ в лице главного редактора или журналиста не несут ответственность за распространение материалов, не соответствующих действительности, в случаях, когда эти сведения:

взяты из официальных сообщений, нормативно-правовых актов или данных официальной статистической отчетности либо получены через информационные агентства или пресс-службы, а также с официальных веб-сайтов органов государственной власти и управления;

содержались в авторских выступлениях, передаваемых в эфир без предварительной записи, или являются дословным воспроизведением (стенографической, аудио-, видеозаписью) выступлений.

Данные нормы исключает ответственность, которая отражает принцип защиты журналистов и редакций от ответственности за информацию, полученную из официальных или достоверных источников, что само по себе соответствует международным стандартам свободы выражения. Однако ограниченный объем освобождения от ответственности вызывает вопросы с точки зрения реализации реальных гарантий свободы СМИ.

В случаях, когда информация получена из открытых, но неофициальных источников (например, интервью очевидцев, материалы гражданской журналистики, зарубежные издания), редакция может быть привлечена к ответственности, даже если в момент публикации не было оснований сомневаться в достоверности сведений. Такая правовая неопределенность вынуждает редакции прибегать к самоцензуре, особенно в чувствительных темах (коррупция, государственная безопасность, выборы и т. д.).

Закон о СМИ предоставляет каждому право выступать в средствах массовой информации, открыто высказывать свое мнение и убеждения. При этом отсутствует четкое разграничение между фактологическим сообщением и оценочным суждением, что создает поле для избирательного применения санкций. Мнения, даже если они спорные или неприятные, не подлежат проверке на «достоверность» и не могут быть основанием для ответственности, так как это противоречить ст. 19 МПГПП.

Дополнительные поддерживающие механизмы содержит статья 6 Закона Республики Узбекистан «О гарантиях профессиональной деятельности журналистов», устанавливающая обязанностью журналистов проверять достоверность подготавливаемых материалов и предоставлять объективную информацию.

Ключевые ограничительные меры в отношении СМИ и журналистов включают в себя:

Обязанности журналиста	Обязанности редакции
Проверка достоверности материалов и предоставление объективной информации	Проверка источников информации, фактчекинг.
Соблюдение законодательства и международных договоров	Соблюдение законодательства о деятельности СМИ и распространении информации.
Презумпция невиновности	Данный принцип обязателен для судей, народных заседателей и участников уголовного процесса, который обязывает толковать все сомнения в виновности лица в пользу обвиняемого. Журналисты и граждане не обязаны применять данный принцип при формировании мнения. Заключается в необходимости отличать лицо подозреваемое, обвиняемое или осужденное в совершении правонарушения при публикации материалов СМИ.
Соблюдение профессиональной этики	Установление внутренних этических правил, которое должно разрабатываться и применятся журналистским сообществом на основе принципа саморегулирования.
Запрет использования информации о частной жизни в личных целях	Запрет на распространение информации о частной жизни, являющейся конфиденциальной без достаточного уровня общественного интереса, за исключением сведений, опубликованных в общедоступных источниках. Не распространятся на лиц, занимающих политические должности в системе государственной власти и управления в целях осуществления общественного контроля и подотчетности.

При этом, обязательства по проверке достоверности журналистов могут толковаться в расширительном формате и распространяться на мнение и суждения лиц. Закон не закрепляет понятия «добросовестное расследование», «журналистская проверка источника», «общественный интерес», что затрудняет защиту СМИ даже при соблюдении профессиональных стандартов. СМИ и журналисты могут нести ответственность не за прямую дезинформацию, а за невозможность верифицировать сведения, полученные от третьих лиц.

В законодательстве отсутствует презумпция добросовестности СМИ, что ставит медиа-журналистов в уязвимое положение. При возникновении споров СМИ приходиться доказывать достоверность опубликованной информации. Более того, правовое регулирование этических вопросов деятельности журналистов часто ведет к их притеснению. Государство не должно определять профессиональные обязанности журналистов. Этические принципы деятельности должны быть оставлены на усмотрение журналистского сообщества.

Требования по распространению достоверной информации применяются также к Интернет СМИ, которые приравниваются к информационным ресурсам в сети Интернет, содержащих документы и сведения в электронной форме, прошедшие редакционно-издательскую обработку, предназначенные для распространения в неизменном виде. Интернет СМИ обязаны размещать на своем веб-сайте дату и номер свидетельства о государственной регистрации, позволяющие отличать зарегистрированные СМИ от иных медиаресурсов.

Законодательство о СМИ также предоставляет альтернативный способ досудебного урегулирования споров, связанные с публикацией недостоверной информации. Согласно ст. 34 Закона о СМИ предоставляет заинтересованным лицам возможность опровергнуть сведения или ответить на них без вмешательства государства. Юридические и физические лица, чьи права и законные интересы нарушены в результате публикации, вправе опубликовать в данном средстве массовой

информации опровержение или ответ. Опровержение или ответ должны быть опубликованы под специальной рубрикой на той же полосе, на которой размещался материал, послуживший причиной появления ответа. Опровержение или ответ, полученные редакцией теле-, радио-, видео-, кинохроникальных программ и иных электронных видов периодического распространения массовой информации, передаются в эфир в той же программе либо цикле передач не позднее одного месяца со дня поступления.

Если объем и время передачи опровержения или ответа могут причинить ущерб деятельности средства массовой информации, то допускается обоснованная правка текста по согласованию с источником информации или автором. Юридическое или физическое лицо вправе обратиться с исковым заявлением в суд в случае уклонения средства массовой информации от публикации опровержения, ответа или нарушения установленного срока публикации. Данные меры соответствуют международным подходам к пропорциональному реагированию на дезинформацию. Несмотря на это, действующий механизм ограничен и не охватывает опровержение общественно значимой дезинформацией, не касающейся конкретных лиц.

Требования по регистрации средств массовой информации по упрощенной процедуре создает правовые основания для осуществления надзора за законностью деятельности медиа и контроля за распространением массовой информации в сети Интернет.

Законодательство об информатизации

В целом законодательство Узбекистана в сфере информатизации и информационной безопасности направлено на защиту информационного пространства страны. Несмотря на это, отсутствует комплексное регулирование, отражающее международные принципы прозрачности и подотчетности модерации цифрового контента. Существующая система ограничения распространения информации в сети Интернет предполагает широкие полномочия административного органа по мониторингу, оценке информации и выдаче уведомлений об удалении информации.

Положение «О порядке ограничения доступа к веб-сайтам и (или) страницам веб-сайтов всемирной информационной сети Интернет, содержащим информацию, распространение которой запрещено законодательством Республики Узбекистан» предусматривает порядок ограничения распространения информации в цифровой среде. Процедура ограничения доступа представляет собой межведомственную процедуру, в которой участвуют Инспекция по контролю в сфере информатизации и телекоммуникаций при Министерстве цифровых технологий Республики Узбекистан (далее «Узкомназорат»).

При оценке противоправного характера информации необходимо руководствоваться ст. 12^1 Закона Республики Узбекистан «Об информатизации». Узкомназорат ведет комплексный мониторинг по выявлению информации, которая признается незаконной в соответствии с действующим законодательством, распространяемую в целях:

- призыва к насильственному изменению существующего конституционного строя, территориальной целостности Республики Узбекистан;
- призыва к массовым беспорядкам, насилию над гражданами, а также к участию в собраниях, митингах, уличных шествиях и демонстрациях, проводимых

с нарушением установленного порядка, а равно координации данных противоправных действий;

- распространения заведомо ложной информации, содержащей угрозу общественному порядку или безопасности;
- пропаганды войны, насилия и терроризма, а также идей религиозного экстремизма, сепаратизма и фундаментализма;
- разглашения сведений, составляющих государственные секреты или иную охраняемую законом тайну;
- распространения информации, возбуждающей национальную, расовую, этническую или религиозную вражду, а также порочащей честь и достоинство или деловую репутацию граждан, допускающей вмешательство в их частную жизнь;
- распространения информации, в том числе выраженной в неприличной форме, демонстрирующей неуважение к обществу, государству, государственным символам;
- пропаганды наркотических средств, психотропных веществ и прекурсоров;
- пропаганды порнографии, культа насилия и жестокости, а также подстрекательства к совершению самоубийства;
- незаконного использования объектов интеллектуальной собственности, принадлежащих другим лицам;
- распространения информации, направленной на склонение или иное вовлечение граждан, в том числе несовершеннолетних, в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц.

По результатам мониторинга Узкомназорат направляет уведомление владельцу веб-сайта или страницы веб-сайта требование об удалении незаконного контента в течение 24 часов. Владелец Интернет-СМИ или веб-сайта вправе либо удалить материал, который признан незаконным, либо обжаловать в судебном порядке заключение Узкомназората и решение Экспертной комиссии о наличии на веб-сайте запрещенной законодательством информации.

Отказ в удалении информации, признанной Узкомназоратом незаконной, является основанием для комплекса организационных и программно-технических мер, направленных на прекращение доступа пользователей к соответствующему информационному ресурсу сети Интернет на территории Республики Узбекистан. Порядок ограничения доступа к информационным ресурсам сети Интернет осуществляется в следующем порядке:

Выявление информационных ресурсов сети Интернет, содержащих запрещенную информацию.

Внесение идентификационных данных информационного ресурса сети Интернет, содержащего запрещенную информацию, в Реестр.

Ограничение доступа к информационному ресурсу сети Интернет.

Несмотря на достаточно широкие полномочия по выявлению незаконной информации Узкомназорат не публикует статистику и отчеты по правоприменительной практике в сфере медиа и информационных ресурсов. Перечень веб-сайтов (Реестр информационных ресурсов всемирной информационной сети Интернет), к которым был ограничен доступ, с указанием причин и оснований ограничения доступен только уполномоченным органам государственной власти и управления, а также юридическим и физическим лицам на основании запросов о принадлежащих им информационных ресурсах в сети Интернет, что противоречит международным стандартам.

Механизмы обжалования, предусмотренные законодательством, предоставляют общее право обжалования в суде действий Узкомназорат по признанию информации незаконной. Тогда как международные стандарты требуют создания независимого досудебного апелляционного механизма обжалования ограничения доступа к информационным ресурсам в сети Интернет.

Международные стандарты	Законодательство Узбекистана	Комментарий
Прозрачность и подотчетность	Отсутствуют требования к регулятору и цифровым платформам раскрывать модерационные правила и публиковать отчеты об ограничении контента	Нет обязательств для соцсетей/платформ по разъяснению причин удаления контент. Нет обязательств Узкомназората по опубликованию отчетов об ограничении контента, Реестр ограничен в доступе
Процедуры	Ограничения контента осуществляется без судебного решения посредством единоличного административного решения	Отсутствует сбалансированный механизм принятия решений об ограничении доступа к контенту
Право на обжалование	Ограничение доступа к веб-сайтам может быть обжаловано исключительно в судебном порядке, при условии исполнения требования по удалению информации	Отсутствуют досудебные меры обжалования ограничения информации на основании мониторинга Узкомназорат или решения Экспертной комиссии
Участие гражданского общества	Не предусмотрено создание и функционирование независимого, негосударственного актора (медиа, эксперты, ННО)	Отсутствуют механизмы вовлечения гражданского общества при оценке и принятии решений об ограничении контента

В соответствии с подходом, закрепленным в Общем комментарии Комитета по правам человека ООН за № 34, свобода выражения является базовым правом, охватывающим все формы коммуникации, включая Интернет, деятельность журналистов и блогеров. Любые ограничения допустимы лишь при строгом соблюдении принципов законности, легитимной цели и необходимости.

Обязательства Интернет-СМИ и пользователей информации осуществлять постоянный мониторинг и фильтрацию информации, перекладывает на них функции цензуры. Государство создает риск чрезмерного вмешательства в свободу слова и приводит к так называемому «охлаждающему эффекту», когда пользователи и журналисты начинают воздерживаться от публикации законного, но потенциально спорного контента. Практика показывает, что подобные обязательства часто ведут к избыточному удалению контента, включая законные публикации, особенно в условиях риска санкций. В этой связи любые требования по мониторингу и фильтрации должны применяться исключительно в отношении четко определенных категорий незаконного контента, сопровождаться прозрачными процедурами и эффективными механизмами обжалования, и не подрывать фундаментальную роль СМИ и блогеров как участников свободного общественного диалога.

Раздел 2
Цифровые права медиа и журналистов

2.1. Создание и распространение контента в цифровой среде

С момента глобального распространения Интернета стало понятно, что медиасреда будет изменяться — не радикально, но значительно. Медиаконтент перестанет быть аналоговым, станет цифровым; редакции СМИ перестанут быть традиционными, станут конвергентными. Аудитория получит доступ к огромному количеству контента различной тематики, который можно «потреблять», то есть смотреть, слушать и изучать в разное время, с разных девайсов. СМИ не осталось других решений, кроме одного — стать конвергентными, производить лучший медиаконтент, перейти на другие каналы распространения контента, усилить вовлеченность аудитории.

Несмотря на то, что цифровая среда радикально ускорила производство и распространение информации: публикация может быть мгновенной, многоканальной и «живой» (обновляться по мере поступления новых данных). При этом фундаментальные права и гарантии остаются прежними: свобода выражения мнений и право искать, получать и распространять информацию гарантируются Конституцией Узбекистана, а ограничения допустимы только на основаниях и в порядке, установленных законом. Но теперь эти гарантии должны быть реализованы, а права доступны в цифровой среде, причем для всех граждан, не только для СМИ.

Так как медиабизнес адаптировался к цифровой среде, контент должен отвечать ключевым принципам цифровой среды: кликабельность, регулярность, визуализация, адаптация под различные платформы, монетизация и вовлечение аудитории. Следование этим принципам обеспечивает доходность медиабизнеса, что приводит к расширению круга производителей медиаконтента, однако правовые риски для журналистов, блогеров, производителей медиаконтента возрастают многократно. Расскажем далее об основных особенностях медиаконтента в цифровой среде и правовых рисках, а также о том, как их избежать.

2.1.1. Кликабельность заголовка

В онлайн-медиа конкуренция за внимание аудитории выше, чем в традиционных форматах. Заголовок, лид, обложка видео, карточка в социальных сетях или в мессенджерах часто «решают», откроют ли материал. Поэтому часто мы видим кричащие, шокирующие заголовки новостей и публикаций. Другая проблема для продвижения медиаконтента — это ориентация на запросы в поисковых системах. Отсюда возникает несколько правовых рисков, которые представлены в таблице ниже.

Характеристика цифрового медиаконтента	Что это значит?	Почему это — проблема?	Как снизить риски для производителей медиаконтента?
Кликабельность (кликбейт)	Яркий, кричащий заголовок	Часто такой заголовок может не соотноситься с текстом публикации. Может вызвать вопросы у аудитории и регулятора. Привести к правовым (иски, жалобы, заявления) последствиям и репутационным потерям.	Заголовок должен соответствовать тексту публикации полностью — не преувеличить и не преуменьшать его. Сверяйте заголовок с фактическим содержанием, избегайте категоричных утверждений без доказательств.
Ориентация на запросы в поисковых системах	Подгонка заголовка под поисковые запросы для того, чтобы пользователь «кликнул» на текст публикации или новости.	В этом случае тексты могут сильно отличаться от заголовка, возрастает риск обвинений в распространении ложной информации.	Исключите саму идею подгонки заголовков к публикациям, исходя из лидеров запросов в поисковых системах. Текст публикации и заголовок должны четко соответствовать друг другу. Все факты в публикации должны быть достоверными или иметь первоисточник публикации.

2.1.2. Регулярность онлайн-контента

Для онлайн-медиа регулярность обновления контента — ключевая часть стратегии выживания на медиарынке. Потребление медиаконтента смещается в стороны социальных сетей, мессенджеров и Интернет-ресурсов, увеличивается частота просмотров новостных, аналитических и развлекательных ресурсов, веб-сайтов. Туда же перенаправляются бюджеты рекламодателей. Это создает замкнутый круг: чем больше аудитория потребляет контента в социальных сетях, мессенджерах и на вебсайтах, тем сильнее редакции зависят от регулярного производства контента, чтобы удерживать внимание аудитории и не выпадать из алгоритмической выдачи. Алгоритмы онлайн-платформ (социальных сетей) и поисковых систем поощряют стабильный поток публикаций и «сигналы активности» — клики, комментарии, время просмотра, возвраты пользователей. В результате редакция вынуждена публиковать контент чаще и больше, чтобы оставаться заметной, а заметность, в свою очередь, становится условием сохранения рекламных доходов и коммерческой устойчивости.

Все было бы отлично в этой схеме, если бы не сопутствующие проблемы: требование постоянного обновления контента в большом количестве увеличивает риски публикации непроверенной информации, неточных формулировок, неверной идентификации людей, искажения цитат и контекста.

При этом любая ошибка в цифровой среде масштабируется быстрее, чем в традиционных медиа: материал мгновенно републикуется, копируется другими страницами и каналами, превращается в скриншоты и «нарезки», мемы, а исправления и уточнения распространяются значительно хуже первичного сообщения. Поэтому для онлайн-медиа регулярность обновлений становится одновременно и механизмом роста, и источником повышенных правовых и репутационных рисков. Посмотрите таблицу ниже, чтобы понять, как этого добиться.

Характеристика цифрового медиаконтента	Что это значит?	Почему это — проблема?	Как снизить риски для производителей медиаконтента?
Регулярность обновления	Необходимость частого обновления контента для присутствия в новостной выдаче, топе цитирования.	Снижается качество проверки фактов и фактических сведений. Ошибки быстро распространяются через репосты.	Не публиковать материал без минимальной перепроверки — что точно известно; какой источник; можно ли подтвердить вторым источником; есть ли позиция второй стороны (если уместно). Использовать маркировку — «обновлено», время, что именно изменилось.
Производство большого объема контента	Необходимость производства большого количества материалов в день.	Риск поверхностной проверки и публикация неверных данных. Ошибка или неточность масштабируется на несколько площадок сразу — веб-сайт, соцсети, каналы в мессенджерах.	Разные алгоритмы проверки публикуемого контента — для новостей (минимальный), собственного редакционного контента (более строгий) и для пользовательского контента, включая контент из социальных сетей (акцент на авторские права).

2.1.3. Визуализация онлайн-контента

Цифровой медиаконтент требует высокого уровня визуализации. Почему? Потому что в цифровой среде пользователи быстро просматривают ленту и лучше реагируют на визуальные элементы, которые мгновенно привлекают внимание, передают смысл и удерживают интерес. Для этого требуются фото, инфографика, скриншоты, короткие видео. Здесь два главных риска, которые представлены в таблице ниже.

Характеристика цифрового медиаконтента	Что это значит?	Почему это — проблема?	Как снизить риски для производителей медиаконтента?
Использование для визуализации чужих фото, видео, музыки, аудио, текстов, иллюстраций без разрешения автора или правообладателя	Нарушение авторского права, требований Закона Узбекистана «Об авторском праве и смежных правах».	Риск удаления контента, блокировок и ограничений аккаунтов на платформах в социальных сетях. Возможные требования о компенсации авторов и правообладателям. Административная или уголовная ответственность.	Используйте только собственный контент, фотостоки или материалы с согласием автора. Храните доказательства получения такого согласия или легального использования фото, видео, текстов и других объектов авторского права.
Переработка и создание материалов для визуализации с помощью ИИ	Использование ИИ для генерации или переработки визуальных материалов, аудио или видео, изображений.	Риск «чужих» заимствований, нарушения прав на исходные материалы, проблем с изображением реальных лиц.	Не использовать для генерации чужие фото, видео и аудио. Создавать собственные промпты. При необходимости маркировать контент, созданный с ИИ.

2.1.4. Адаптация под различные платформы

Аудитория «не привязана» к одному каналу — информационный веб-сайт, конкретная социальная сеть или мессенджер. Аудитория «мигрирует» от одного источника к другому. Это значит, что контент должен быть доступен везде.

Поэтому онлайн-медиа почти всегда распространяют один и тот же материал сразу в нескольких каналах: на веб-сайте, в социальных сетях, в мессенджерах, на видеоплатформах. Это повышает охват и помогает удерживать аудиторию, но одновременно создает риски: один и тот же смысл «переупаковывается» в разные форматы (короткое видео, карточка, сторис, пост), контекст неизбежно сокращается, а требования платформ и ожидания аудитории отличаются. Это также создает определенные риски, которые указаны в таблице ниже.

Характеристика цифрового медиаконтента	Что это значит?	Почему это — проблема?	Как снизить риски для производителей медиаконтента?
Адаптация контента под разные форматы	Чаще всего — сокращение текста, заголовка.	Возрастает риск неверного смысла, категоричных утверждений и изменение фактов.	Не изменяйте факты, смысл и суть исходной публикации. Обязательно добавляйте ссылку на полный материал.
Разные правила и алгоритмы онлайн-платформ и мессенджеров	У каждой соцсети или мессенджера свои политики по контенту, авторским правам.	Возможны блокировки аккаунтов и удаление контента в случае нарушения политик онлайн-платформ.	Изучите все политики каналов и платформ, где вы размещаете контент, и строго их придерживайтесь.

2.1.5. Монетизация контента

Монетизация онлайн-медиа обычно строится на сочетании рекламы, спонсорских материалов, партнерских спецпроектов, подписок и донатов. Ключевая юридическая линия здесь — разграничение рекламы и редакционного материала. Закон Узбекистана «О рекламе» закрепляет требование, чтобы реклама была распознаваема; отдельно регулируется спонсорство и недопустимость «скрытой рекламы» (когда рекламный характер сообщения маскируется под редакционный контент).

Однако на практике реальность другая: рекламодатели свято верят в эффективность нативной рекламы и интеграций и часто просят создать рекламный текст под видом материала журналиста или блогера. Блогеры часто под видом благотворительной деятельности собирают деньги на другие цели или не включают в налогооблагаемую базу свои доходы от рекламы и интеграций.

Рекомендуем помнить о следующих рисках:

Характеристика цифрового медиаконтента	Что это значит?	Почему это — проблема?	Как снизить риски для производителей медиаконтента?
Скрытая реклама	Рекламный материал подается как редакционный контент без явной маркировки.	Вводит аудиторию в заблуждение; риск ответственности и репутационных потерь.	Всегда маркировать рекламу и спонсорство. Принять внутренние правила и шаблоны маркировки платного контента.
Сокрытие доходов блогеров от рекламы	Рекламные доходы не фиксируются, налоги не оплачиваются.	Риск налоговых и правовых последствий; споры с рекламодателями.	Заключать договоры на любые платные размещения.

2.1.6 Вовлечение аудитории

Почему для онлайн-медиа так важно вовлечение аудитории? Комментарии, реакции, опросы, прямые эфиры и пользовательский контент напрямую влияют на распространение материалов и интерес рекламодателей. Это — фактор устойчивого роста и интереса аудитории к рекламной площадке. Однако вовлечение почти всегда повышает риски: обсуждения быстро переходят в оскорбления и травлю, пользователи публикуют персональные данные и непроверенные обвинения, оскорбления. Ошибка или неверная формулировка в таком контексте масштабируется мгновенно и может повлечь как репутационные потери, так и юридические. Посмотрите в таблице ниже, какие именно.

Характеристика цифрового медиаконтента	Что это значит?	Почему это — проблема?	Как снизить риски для производителей медиаконтента?
Комментарии и дискуссии под материалами	Пользователи активно комментируют, подогревают интерес к теме.	Анонимность комментариев. Пользователи могут распространять, hate speech, ложную информацию, оскорбления, чужие персональные данные, порочащие сведения.	Обязательная модерация комментариев. Правила для пользователей и меры реагирования — удаление явных нарушений без промедления. Для чувствительных тем — предварительная модерация и ограничение комментариев.
Прямые эфиры и live-форматы	Импровизация в реальном времени, ответы на вопросы.	Нет времени проверить факты, данные. Мнения и оценки могут быть критическими и задевать интересы третьих лиц.	Готовые тезисы и ответы на возможные вопросы. Запасной вариант, если эфир пойдет не по первоначальному сценарию. Задержка эфира и быстрое уточнение информации, если необходимо.
Пользовательский контент (UGC)	Фото, видео и аудио, небольшие тексты от читателей, очевидцев событий и т. д.	Ложная информация, постановки, нарушения прав третьих лиц, распространение персональные данные.	Принимайте такой контент только после минимальной верификации (когда и где снято, кто автор) и получения согласия автора на использование. Удаляйте персональные данные и при необходимости обезличивайте изображение (блюр на лица, номера машин и т. д.).

2.1.7. Профессиональные стандарты онлайн-медиа

Медиаконтент создает огромное количество людей: редакции онлайн-медиа, профессионалы из сферы медиа (отдельные медиапроекты — расследования и т. д.), блогеры и пользователи социальных сетей, GR и PR специалисты, рекламные агентства, студии видеопроизводства, государственные органы и частные компании.

Хорошо известно, что цифровая среда усиливает цену каждой ошибки. Контент распространяется мгновенно, копируется и пересылается, «живет» в виде мемов, скриншотов и коротких фрагментов, и аудитория часто воспринимает материал через заголовок, обложку и первый абзац. Поэтому онлайн-медиа важно не только соблюдать стандарты «внутри редакции», но и выстроить понятные правила для всех форматов — веб-сайта, социальных сетей и мессенджеров.

Профессиональные стандарты для онлайн-медиа остаются теми же, что и для традиционных медиа. Это: точность **и достоверность в изложении фактов, баланс (представление всех сторон в публикации), разделение мнений от оценочных суждений, нейтральная позиция, соблюдение этических принципов журналистики, особенно в отношении детей, жертв преступлений и уязвимых групп общества.** Посмотрите таблицу ниже, чтобы понять, как работает каждый стандарт на практике.

Стандарт онлайн-медиа	Описание профессионального стандарта	Как должен работать стандарт на практике?
Точность в изложении фактов	СМИ (онлайн-медиа) публикует только то, что можно подтвердить; цифры, имена, даты и цитаты проверяются перед публикацией.	Перед публикацией сверяем имена, даты, цифры, цитаты по первоисточнику. Сохраняем все подтверждающие документы.
Достоверность в изложении фактов	Необходимо опираться только на надежные источники и документы. Разделять при публикации факты и достоверные сведения от предположений, мнений и оценочных суждений.	Используем минимум два независимых подтверждения или документа, или комментариев. Если данных недостаточно, указываем в тексте, что это версия или предварительная информация.
Баланс (представление всех сторон в публикации)	Онлайн-медиа стремится представить позиции всех затронутых сторон, особенно если публикация затрагивает права и репутацию конкретных лиц.	Запрашиваем комментарии у ключевых сторон и отправляем запросы. Если ответ не получен к моменту публикации, то обязательно указываем это в материале и обновляем публикацию при поступлении позиции.
Разделение мнений и оценочных суждений	Факты и оценки не смешиваются — фактическая информация отделена от интерпретаций автора или экспертов.	В тексте или в видео отделяем «что произошло» от «как это оценивается». Оценочные формулировки подкрепляем источниками или прямо маркируем как мнение или комментарий.
Нейтральная позиция	Подача материала со стороны онлайн-медиа остается корректной и непредвзятой. Язык публикации не должен содержать эмоциональных обвинений, стереотипов и штампов.	Используем точные, юридически аккуратные формулировки и избегаем категоричных выводов без доказательств. В конфликтных темах — убираем эмоциональные эпитеты и оставляем только достоверные факты и сведения.
Соблюдение этических принципов журналистики	Онлайн-медиа отдает приоритет темам, имеющим общественный интерес. При этом соблюдаются не только требования законодательства, но и этические принципы журналистики.	Не публикуем шокирующие, унижающие детали, фото и видео. Не стремимся к сенсационности, обеспечиваем для аудитории получение качественного, достоверного контента.
Особая осторожность в отношении детей, жертв преступлений и уязвимых групп	Материалы о детях и уязвимых группах требуют повышенной защиты частной жизни и безопасности. Распространение персональных данных, фото допускается только при очевидной необходимости и законных основаниях.	Убираем лишние идентифицирующие данные (лица, адреса, номера, детали, по которым легко узнать человека). Оцениваем риски для безопасности и при необходимости обезличиваем материал и используем блюр на фото и видео.

2.1.8. Статус Интернет-издания в праве Узбекистана

Действующее законодательство Узбекистана прямо включает веб-сайт как возможную форму средства массовой информации[24]. Онлайн-издание как информационный ресурс с материалами в электронной форме, прошедшими редакционно-издательскую обработку и предназначенными для распространения в неизменном виде.

Если веб-сайт зарегистрирован как СМИ, на главной странице должны быть указаны как минимум: название, дата и номер свидетельства о государственной регистрации, учредитель, главный редактор, адреса редакции (почтовый и электронный). Отдельно закон регулирует ситуацию, когда у печатного издания есть электронная версия: она может распространяться без регистрации как самостоятельное СМИ при условии идентичности содержания (с рядом оговорок по рекламе и объему) и при уведомлении регистрирующего органа.

Постоянная проблема для производителей цифрового медиаконтента — это определиться, нужен или нет им статус СМИ? Ниже представлены плюсы и минусы такого решения.

Плюсы получения статуса Интернет-издания как СМИ	Минусы получения статуса Интернет-издания как СМИ
Формальная идентификация редакции и повышение доверия аудитории и партнеров.	Необходимость создания полноценной редакции.
Для рекламодателей и агентств проще работать с зарегистрированным СМИ: понятнее сторона договора, реквизиты, главный редактор как ответственное лицо, единые правила размещения.	Более строгий мониторинг за публикациями и деятельностью редакции.
В практике аккредитации и официальных коммуникаций наличие редакции, редактора и официального статуса облегчает переписку и организационные вопросы (например, подача запросов, заявок на аккредитацию от редакции).	Большой перечень санкций (ответственность) за публикацию контента (административная и гражданско-правовая). Уголовные санкции — в отношении должностных лиц редакции.

2.1.9. Аккаунты онлайн-медиа в социальных сетях и в мессенджерах

Мы уже обсуждали выше, что особенностью цифрового медиаконтента является адаптация под разные форматы и каналы распространения. Поэтому каждое Интернет-издание имеет аккаунты в социальных сетях и в мессенджерах, где количество подписчиков бывает значительным, больше, чем уникальных посетителей на веб-сайте. С официальной точки зрения, все аккаунты в социальных сетях Интернет-издания являются также СМИ, поэтому короткий пост, заголовок, подпись к видео и даже обложка материалов могут оцениваться так же, как публикация на веб-сайте. Ко всем публикациям в аккаунтах социальных сетей и в мессенджерах применимы те же риски, что и к публикациям медиаконтента на веб-сайте Интернет-издания.

[24] Закон Республики Узбекистан «О средствах массовой информации». Текст закона доступен по ссылке: https://www.lex.uz/acts/53112

Возможные проблемы

Диффамация (распространение недостоверных сведений, порочащих честь, достоинство и деловую репутацию)
Пост, заголовок или подпись к видео могут быть расценены как распространение порочащих сведений. Риск повышается при оценочных суждениях, обвинениях без доказательств и эмоциональных формулировках.

Распространение ложной информации
Быстрый репост или публикация без проверки источника может привести к распространению заведомо ложных или недостоверных данных. Особенно рискованны сообщения в периоды ЧС, техногенных и природных катастроф, пандемий, происшествий.

Распространение персональных данных
Публикация фото, видео, скриншотов переписок, номеров телефонов, адресов, ИИН и иных идентификаторов без правового основания может нарушать права человека.

Hate speech, запрещенный к распространению контент
Комментарии, цитаты и репосты могут содержать язык вражды, призывы к насилию или иные запрещенные материалы, за которые отвечает и социальная сеть, и конкретная редакция или блогер.

Нарушение авторских прав
Нельзя использовать чужие фото, видео, музыку, инфографику и мемы «по умолчанию», даже если материал найден в открытом доступе. Это создает правовую базу для претензий и исков, судебных разбирательств.

2.2. Доступ к информации и аккредитация

Реальная ситуация. В небольшом городе в нескольких школах происходят отравления детей, проводится проверка. Выбор поставщика, который обеспечивал питание для детей, проходил методом закупки из одного источника, то есть безальтернативно. Документов — договора, суммы, обязательств — нет на веб-сайте школы. После массовых отравлений редакция городского СМИ запрашивает в управлении образования и в школе документацию на поставщика питания для детей и результаты проверки санитарно-эпидемиологической службы. Но получает отказ в предоставлении документации по причине коммерческой тайны и наличия персональных данных.

Пример выше показывает, что несмотря на наличие законодательных требований и общественного интереса, журналистам и СМИ все еще непросто запросить, получить информацию от государственных органов для того, чтобы предоставить ее аудитории и объяснить суть событий.

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 журналиста это важно как минимум в двух ситуациях:
   - когда редакция проверяет законность обработки персональных данных (например, при утечках);
   - когда редакция должна корректно отделять общественный интерес от вмешательства в частную жизнь.

3. **Общественный интерес как ключ к раскрытию информации.** 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 по первому требованию, но ограничения есть, были 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?

Для журналистов и блогеров 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 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 журналистская проверка все чаще начинается не с запроса в государственные органы, а с поиска в открытых цифровых источниках. Это принципиально меняет качество фактчекинга: редакция может 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 СМИ, потому что государственный орган видит: редакция ориентируется в документах и просит не «в целом», а по существу.

Список ресурсов для получения информации:

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 РУ	https://pm.gov.uz/ru#/	Сервис для отправки обращения главе государства по широкому перечню вопросов внутренней и внешней политики.
Реестр компаний в Узбекистане	https://orginfo.uz/	Портал данных о статусе и деятельности юридических лиц.

2.2.2. Верификация и фактчекинг

Часто журналисты думают, что 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 редакции СМИ. 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, фактчекинг становится базовым принципом журналистики. 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

Часто журналисты считает, что комментарий или ответ на вопрос чиновника достаточны. Но это — не первоисточник. Ищите первоисточник — документированную информацию.

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

Шаг 3.

Поиск и изучение альтернативного источника для подтверждения

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

Результат: Снижается риски обвинений в распространении ложной информации.

Шаг 4.

Проверка фактических данных в документе

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

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

2.2.3. Аккредитация

Аккредитация как процедура более оперативного доступа к информации для журналистов практически не используется сейчас на практике, за исключением временной аккредитации журналистов на мероприятия с участием главы государства, министров и т. д. С одной стороны, цифровизация и внедрение искусственного интеллекта в деятельность государственных органов позволяет внедрить новые механизмы более оперативного доступа к информации — видеотрансляция открытых заседаний коллегиальных органов, доступ к протоколам и принятым решениям, документам в режиме онлайн, на веб-сайтах государственных органов и других обладателей информации.

В Узбекистане аккредитация формально закреплена в законодательстве как способ «регулярного доступа» журналиста к деятельности конкретного государственного органа или организации. Закон «О защите профессиональной деятельности журналиста»[25] прямо предусматривает, что журналист может быть аккредитован при государственном органе, общественном объединении и организации, а аккредитованный журналист получает понятный набор прав:

- Заранее получать информацию об открытых коллегиальных заседаниях и публичных мероприятиях.
- Посещать здания аккредитующего органа по установленному им порядку, присутствовать на открытых заседаниях.
- Запрашивать и получать документы и материалы.
- Знакомиться с записями публичных мероприятий.
- Снимать копии и использовать записи при подготовке материалов.

[25] Больше информации доступно по ссылке: https://lex.uz/docs/2024

Дополнительно действует Закон Узбекистана «О прозрачности деятельности органов государственной власти и управления»[26], который устанавливает общий принцип — открытые коллегиальные заседания должны проводиться открыто, а государственный орган обязан создать условия для присутствия пользователей информации, но конкретный порядок (правила входа, регистрация, квоты, требования безопасности) определяется внутренними документами самого органа[27].

И вот здесь начинается практическая проблема: даже при наличии обязательств, закрепленных на уровне закона, аккредитация не всегда обеспечивает гарантированный доступ. На практике в Узбекистане все большую роль играют публичная видеофиксация и онлайн-освещение открытых заседаний: в официальных коммуникациях отмечается, что пленарные заседания Сената транслируются онлайн, а также развивается практика онлайн-трансляций парламентских обсуждений.

Для СМИ это важный рабочий инструмент, так как видеотрансляции открытых заседаний экономят время журналистов, дают первичный источник цитат и позиции должностных лиц, позволяют затем точечно запрашивать документы (повестки, проекты решений, протокол, результаты проверок), уже понимая, что именно нужно подтвердить документально.

2.2.4. Защищенность и сохранение в тайне источников информации

Сохранение источников информации журналиста в тайне — это один из базовых профессиональных принципов журналистики, зафиксированный на уровне законов, а также во Всемирной хартии журналистов[28]. Он напрямую связан со свободой выражения мнений и правом общества получать информацию: без гарантий конфиденциальности источники могут отказаться сообщать сведения по вопросам общественного интереса.

В законодательстве Узбекистана защита источников закреплена как обязанность и как гарантия. Закон Узбекистана «О средствах массовой информации» прямо устанавливает, что СМИ не вправе раскрывать имя источника, предоставившего информацию, сведение, факт или доказательство, а также имя автора, подписавшегося под псевдонимом, без их письменного согласия[29].

Кроме того, СМИ не вправе раскрывать имя источника (а также автора под псевдонимом) без письменного согласия. Закон Узбекистана «О защите профессиональной деятельности журналиста»[30] вводит понятие **журналистской тайны** (то есть, конфиденциальная информация и сведения, сообщенные с условием не раскрывать

---

[26] Закон Республики Узбекистан «Об открытости деятельности органов государственной власти и управления». Принят Законодательной палатой 11 марта 2014 года. Одобрен Сенатом 10 апреля 2014 года. Доступен по ссылке: https://lex.uz/mact/2381138

[27] Там же, статья 16

[28] Глобальная хартия этики журналистов МФЖ была принята на XXX Всемирном Конгрессе МФЖ в Тунисе 12 июня 2019 года. Она дополняет Декларацию принципов поведения журналистов (1954 г.), известную как «Декларация Бордо». Текст хартии доступен по ссылке: https://presscouncil.ru/images/docs/doc_2020/global_hartiya_etiki.pdf

[29] Статья 10. Закон Республики Узбекистан «О средствах массовой информации». Текст закона доступен по ссылке: https://www.lex.uz/acts/53112

[30] Закон Республики Узбекистан «О защите профессиональной деятельности журналиста». Текст закона доступен по ссылке: https://www.lex.uz/acts/2024

имя), запрещает ее разглашение без разрешения источника и использование в корыстных интересах, а также запрещает вмешательство в профессиональную деятельность журналиста и требование от него сведений, полученных при исполнении профессиональных обязанностей[31].

Однако, несмотря на законодательные гарантии, все чаще и чаще редакции СМИ сталкиваются с требованиями раскрыть источник информации, предоставить его данные и контакты.

Хотим поделиться практическими рекомендациями, которые помогут вам и вашему источнику информации соблюсти все требования к сохранению конфиденциальности.

Заранее фиксируйте условие конфиденциальности. Это можно сделать в переписке с источником и минимизируйте данные, по которым можно идентифицировать его.

Если поступают требования «раскрыть источник информации», сразу сообщайте редактору и юристу.

Помните, что по законодательству, защита источника — это правовая обязанность журналиста и элемент гарантий профессиональной деятельности. Не раскрывайте свои источнику по первому требованию и не подвергайте их риску быть идентифицированными и подвергнутыми давлению или преследованию.

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 редакций и аудитории, прикладывать фото, видео и документы. Такие коммуникации обеспечивают обратную связь, что тоже крайне эффективно для редакции онлайн-издания.

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 и в таких случаях присылают информацию, официальные документы, пресс-релизы через электронные адреса редакций. В таких случаях редакции онлайн-медиа безопаснее запросить дополнительно информацию через официальные источники и не полагаться на достоверность фактов или документов, полученных через Telegram-канал.

---

[31] Закон Республики Узбекистан «О защите профессиональной деятельности журналиста». Статья 7. Текст закона доступен по ссылке: https://www.lex.uz/acts/2024

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

Практика работы редакций СМИ, включая онлайн-издания, не только в Узбекистане, но и во всем регионе Центральной Азии показывают одни и те же тенденции — **доступ к информации все больше ограничивается,** несмотря на законодательные гарантии. Культура секретности и закрытости преобладает над культурой открытости и прозрачности. Государственные органы часто действуют по инерции: проще закрыть, чем раскрыть информацию и довести ее до общества. Информационные ресурсы государственных органов все еще недостаточно информативны, обновляются нерегулярно, документы публикуются выборочно. Журналиста или редакцию СМИ, которые запрашивают информацию, могут расспрашивать «Зачем вам это?» и «Что вы будете делать дальше?», интересоваться целью получения информации.

На практике часто возникают следующие нарушения в сфере доступа к информации, с которыми сталкиваются редакции СМИ и журналисты. Они изложены в таблице ниже.

Нарушение 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 редакции СМИ, 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

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

В странах Центральной Азии существует перечень тем для редакций СМИ и контент-мейкеров, 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, НКО, 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 вследствие возможных и реальных правовых проблем, которые могут наступить, если редакция СМИ будет освещать вопросы из этого списка. При этом прямого запрета на публикацию на эти темы нет, но все редакции СМИ, журналисты и редакторы хорошо осведомлены о чувствительности этих тем.

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

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[32]	Публикация опровержения порочащих сведений, компенсация морального вреда, прекращение распространения
Клевета	Административное дело по статье 40 Кодекса Узбекистана об административной ответственности (КоАО)[33]. Процедура в соответствии со ст. 139 УК РУ[34] (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)
Оскорбление	Административный порядок в соответствии со статьей 41 КоАО[35]. 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)[36]	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 отношении журналистов и блогеров.

---

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

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

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

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

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

При этом известно, что чрезмерно широкие основания и меры уголовной ответственности в отношении журналистов и СМИ 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.

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, Интернете, приводящее к унижению достоинства личности или дискредитации личности[37]. 2. Распространение ложной информации, в том числе в СМИ, в Интернете, содержащей угрозу общественному порядку или безопасности[38]	Административный штраф 50 БРВ или 50–100 БРВ (в зависимости от части статьи)
Уголовная ответственность 	Распространение ложной информации, в том числе в СМИ, Интернете, приводящее к унижению достоинства личности или дискредитации личности, совершенное после применения административного взыскания за такие же действия[39]	Штраф до 150–200 БРВ; обязательные работы до 240–300 часов или исправительные работы до 2 лет или ограничение свободы до 2–3 лет

2.3.4. Hate speech

В странах Центральной Азии, включая Узбекистан, тема hate speech (язык вражды) для редакций 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»[40].

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 как у распространителя контента.

---

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

[38] Там же

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

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

Отдельный смежный риск — это нормы по запрету «пропаганды войны» (ст. 150 Уголовного Кодекса Узбекистана)[41]. Под нее подпадает распространение идей или призывов с целью вызвать агрессию одного государства против другого; санкция предусматривает лишение свободы от 5 до 10 лет. Практический вывод для онлайн-редакции 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 редакция СМИ не становилась каналом распространения запрещенных материалов.

2.3.5. Ответственность за комментарии в аккаунтах медиа

Теперь более подробно остановимся на вопросе ответственности редакции СМИ, блогеров 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 обязаны не допускать использования веб-сайтов, блогов для размещения запрещенной информации, что прямо закреплено в Законе «Об информатизации»[42]. Поэтому отсутствие модерации и игнорирование обращений повышают риски для самой редакции.

Где проходит грань ответственности между автором комментария и редакцией СМИ? Риски для редакции СМИ быть привлеченными 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, редакция СМИ или блогер могут разработать и внедрить:

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

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

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

Правила комментирования для пользователей — это публичная политика (позиция) редакции СМИ или блогера 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 редакции 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, скриншоты, нецензурная лексика;
- редакция вправе удалять комментарии, нарушающие правила, и блокировать пользователей;
- редакция рассматривает обращения о нарушениях и принимает меры, включая удаление и ограничение доступа.

Кроме Правил комментирования, редакция СМИ 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 редакция реагирует 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 редактору 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 редакцией рассматривается как дополнительный фактор ответственности.

2.3.6. Правила онлайн-платформ по контенту

Отдельно затронем вопрос с правилами онлайн-платформ по контенту. Выше мы разбирали проблемные ситуации, когда ответственность за контент в цифровой среде может наступать в соответствии с национальным законодательством Узбекистана. Но онлайн-платформы действуют также по своим правилам. Для редакции 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 для редакции — ориентируйтесь в своей редакционной политике 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 медиа

Журналисты и медиа постоянно создают контент, а также работают с чужим контентом: текстами, фото, видео, музыкой, инфографикой, дизайном. Большинство медиаматериалов создаваемых журналистами и редакциями является объектом авторского права.

Основные критерии для признания медиаконтента объектом авторского права включают:

- творческую деятельность — индивидуальную или совместную;
- выражение в конкретной доступной для восприятия форме (текст, изображение, аудио/видео, цифровая запись и т. д.).

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

В цифровой среде публикация в сети Интернете 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	Право 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) произведение 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

Авторское право на интервью принадлежит лицу, давшему интервью, и лицу, проводившему интервью как соавторам, если иное не предусмотрено соглашением между ними. Использование интервью допускается лишь с согласия лица, давшего интервью. Для получения авторских прав на интервью необходимо заключать соглашения с лицом, давшим интервью с указанием условия о передаче исключительных прав и выплате авторского вознаграждения.

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

2.4.3. 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, и нельзя воспроизводить все 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 републикации для всех и везде.

Новости не являются объектами авторского права. Статья 8 закона РУз «Об авторском праве и смежных правах» определяет, что к произведениям, охраняемым законом, не относятся «сообщения о новостях дня или сообщения о текущих событиях, имеющие характер обычной пресс-информации».

Таким образом, только материалы, представляющие результат творческой деятельности (фото и видеорепортажи, аналитические или обзорные статьи, журналистские расследования, интервью) являться произведениями с авторско-правовой охраной. Журналисты выступают авторами медиаконтента, а редакции средств массовой информации — правообладателями материалов, опубликованных в периодическом издании в печатной форме или онлайн.

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 СМИ

Редакция СМИ может использовать объекты 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 (репортаж с концерта, открытия галереи, фотовыставки).

Красные флаги для редакции

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.

Золотое правило атрибуции: **Автор + источник + дата + ссылка (при наличии). 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.

2.4.4. 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 оборота.

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 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

2.4.5. 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 досудебного рассмотрения споров в сфере интеллектуальной собственности — Департамент по интеллектуальной собственности Министерства юстиции Республики Узбекистан.

2.4.6. 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, проверка 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

бесплатный инструмент позволяет искать копии изображений в Интернете;

Copyscape

международный сервис для поиска плагиата в текстовых материалах. Доступны как бесплатная, так и платная версии с расширенными возможностями;

Pixsy

платформа для фотографий с функцией поиска по изображению.

2.5. Этические аспекты профессиональной деятельности журналистов и медиа в цифровой среде

Цифровая среда усиливает эффект журналистских материалов. Публикации в Интернете распространяются мгновенно, доступны для неограниченной аудитории и легко копируются. Алгоритмы цифровой среды могут способствовать конфликтам, травле и распространению чувствительного контента быстрее, чем редакция СМИ успеет среагировать. Этические правила в онлайн среде это практический инструмент снижения рисков и сохранения доверия к источникам информации.

Принципы профессиональной этики журналистов включают несколько ключевых аспектов:

Журналистская этика требует от журналистов быть честными, точными и объективными.

Социальные сети и выражение личного мнения

Принцип: журналист остается журналистом и в социальных сетях. Даже личный аккаунт часто воспринимается аудиторией как позиция профессионального журналиста и/или редакции.

В Кодексе профессиональной этики журналистов Узбекистана закрепляются базовые ориентиры профессии: честность, объективность, справедливость, плюрализм мнений и уважение прав человека; также подчеркивается обязанность проверять точность информации и оперативно признавать ошибку, извиняться и исправлять ее.

Практические рекомендации:

- **Разделяйте факт и оценку.** Если вы выражаете мнение, обозначайте это как мнение/колонку/комментарий, а фактическую часть подкрепляйте источниками.
- **Избегайте языка ненависти.** Сарказм и эмоции в соцсетях «кликабельны», но могут оказывать давление и подталкивать аудиторию к травле.
- **Прозрачность конфликтов интересов.** Если вы пишете о теме, где есть личная вовлеченность (родственные связи, партнерство, участие в проекте), раскрывайте это корректно.
- **Исправляйте ошибки или неточности.** Исправляйте с пометкой, отдельным комментарием/постом с указанием на ошибки или неточности.
- **Учет интересов и уязвимости отдельных групп.** Ключевой принцип — «не навреди». Люди с низкой цифровой грамотностью (включая детей, пожилых людей, людей с инвалидностью), а также лица в уязвимом положении часто не осознают последствий публикации, репостов или вторичного распространения.

Недопустимость кибербуллинга и ответственность медиа за цифровую среду

Кибербуллинг представляет собой систематическую онлайн-травлю, часто затрагивающую журналистов, особенно женщин, в форме угроз, оскорблений и доксинга. В Узбекистане и Центральной Азии эта проблема усиливается отсутствием специального законодательства, но журналистика играет ключевую роль в ее освещении и борьбе. Журналисты сами становятся жертвами, что приводит к самоцензуре и психологическому давлению.

Кибербуллинг включает оскорбления, угрозы, распространение личных данных и фейковых аккаунтов в соцсетях, отличаясь от офлайн-травли круглосуточным характером. Журналистки сталкиваются с этим в 73% случаев по данным UNESCO, включая гендерное насилие.

Журналистам, освещающим кибербуллинг в Узбекистане, важно учитывать гендерную чувствительность, особенно при работе с жертвами, часто женщинами, чтобы избежать вторичной травматизации. Безопасность включает анонимизацию источников, юридическую защиту и технические инструменты, с учетом местных законов о СМИ. Эти меры помогают минимизировать риски для себя и жертв.

Практические рекомендации:

- **Модерация и правила комментариев**
  Публикуйте понятные правила (запрет на угрозы, оскорбления, доксинг, разжигание ненависти), отслеживайте и фиксируйте нарушения.
- **Не усиливать травлю**
  Если герой материала уже подвергается нападкам, избегайте публикации личных данных, которые помогают идентифицировать человека.
- **Защита сотрудников**
  Необходимо разрабатывать внутреннюю политику на случай кибербуллинга: оценка угроз, фиксация доказательств, обращение в правоохранительные органы.

Чувствительный контент: суициды, самоповреждения, тяжелое насилие, травматичные события

В отношении суицидов существуют доказательства, подтверждающие, что определенные способы освещения могут повышать риск подражания, тогда как истории преодоления кризиса и корректные материалы могут поддерживать профилактику. Всемирная организация здравоохранения прямо указывает на эти эффекты и рекомендует журналистам следовать «Do’s and Don’ts» при освещении суицида.

Рекомендуется:

- писать осторожно и нейтрально, без сенсационности и кликабельности;
- **не превращать событие в «историю-легенду»** и не романтизировать;
- давать полезную информацию: куда обращаться за помощью, что делать близким;
- по возможности смещать фокус на профилактику и поддержку, включая истории обращения за помощью и преодоления кризиса.

Не рекомендуется:

- описывать способ, детали, место, способы суицида;
- публиковать фото/видео с места, предсмертные записки, «последние сообщения»;
- делать кричащие заголовки, стигматизацию и драматизацию.

Практический стандарт для медиа

Если материал содержит упоминания суицида/самоповреждений — добавлять предупреждение о чувствительном контенте и **контакты служб помощи** (локальные официальные службы психологической помощи, телефоны доверия), а также избегать любых деталей, которые могут стать триггером.

2.6. Политики для онлайн-медиа

Для редакции онлайн-издания 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 медиабизнес развивался, успешно отражаются в письменных документах — специальных политиках, которые рекомендуется разрабатывать и принимать в письменном виде, публиковать или использовать только внутри редакции.

Таблица ниже содержит минимальный перечень политик для редакции онлайн-издания (всего 5 политик), исходя из особенностей медиабизнеса — создание медиаконтента и распространение его в цифровой среде.

Внешние политики (публичные документы, должны быть опубликованы на веб-сайте издания)	**Внутренние политики (не публикуются, но обязательны для выполнения сотрудниками редакции)**
1. Правила использования материалов	1. Политика по защите редакционного контента от незаконного использования
2. Политика по персональным данным	2. Внутренний регламент работы редакции
3. Правила комментирования для пользователей (подписчиков)	

Ниже кратко описание каждой политики в контексте работы онлайн-издания 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 является правообладателем контента, который создается и распространяется через различные платформы и каналы. Эта политика также определяют позицию (разрешение) правообладателя по **использованию своего контента без разрешения правообладателя (редакции),** но выполняя определенные условия:

- В случаях цитирования — необходимо соблюдать объем цитирования, установленный редакцией онлайн-издания (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 применение гиперссылки на первоисточник и т. д.

Также эта политика определяет процедуры по использованию UGC (пользовательский контент; users-generated content), включая получение согласия от пользователя 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 и на страницах издания.

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 сообщений 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 для редакций онлайн-изданий? 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[43].

2.6.4. Политика по защите редакционного контента от незаконного использования

Эта внутренняя политика, которую **не нужно публиковать на веб-сайте,** однако все сотрудники редакции должны знать положения этой политики и применять на практике. Цель этой политики — алгоритмы действий сотрудников редакции, в случае, если они обнаружили или выявили факты незаконного использования редакционного контента. Другими словами, что и как делать сотрудникам редакции в случаях, когда материалы редакции копируются и используются без разрешения.

Таких фактов всегда много — незаконно могут использоваться тексты, фото, аудиовизуальные материалы как частично, так и в полном объеме в других СМИ, блогерами, пабликами, Telegram-каналами. Если ваши материалы незаконно используются, вы теряете просмотры, уникальных посетителей, соответственно, теряете рекламные доходы.

Вот минимум положений, которые должны быть включены в такую политику:

- Какие сервисы использовать для отслеживания и выявления фактов незаконного использования вашего контента (тексты, фото, аудио и видеоматериалы)?
- Как фиксировать факты нарушений? Обязательно указывать и сохранять ссылки, скриншоты, дата и время публикации, сохранение HTML или видео, данные о том, кто незаконно использует ваш контент.
- Действия для досудебного урегулирования: отправка уведомления, запрос на удаление или легализацию использования.
- Действия для судебной защиты в ситуациях, если досудебное урегулирование не принесло положительного эффекта.

Положения этой политики и все алгоритмы действий должны быть хорошо известны всем сотрудникам.

2.6.5. Внутренний регламент работы редакции

Это также политика для внутреннего использования в редакции, не для публикации. Цель этой политики — внедрить стандарты по подготовке и распространению редакционного контента и минимальные юридические процедуры для того, чтобы снизить риски ответственности за контент до минимума.

---

[43] Закон Республики Узбекистан «Об информатизации»

Какие положения может включать такая политика?

- этапы создания редакционного контента — новостного, лонгридов, аудио и визуального контента, акций для вовлечения аудитории;
- обязательные проверки перед публикацией (фактчекинг, источники, диффамационные риски, персональные данные, авторские права, маркировка рекламы);
- порядок исправлений, обновлений, архивирования материалов;
- правила работы с официальными обращениями и запросами (кто принимает, кто отвечает, как фиксировать);
- управление доступами к веб-сайту и аккаунтам, требования к паролям и двухфакторной идентификации, другим мерам цифровой и физической безопасности журналистов и других сотрудников редакции.

Рекомендуем вам разработать, принять и внедрить эти пять политик как минимальный пакет документов, обеспечивающий работу современной редакции онлайн-медиа.

Раздел 3
Угрозы для журналистов и редакций 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 журналистов и сотрудников редакций 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 аудитории и рекламодателей 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 н**ачальным 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) с 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, перехватывающих финансирование.
- **Угрозы вторичных санкций или побочного ущерба** — угроза «сверх соблюдения», 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 медиа 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 безопасности для журналистов и редакций

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 редакций и отдельных журналистов.

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 **все 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, уведомления Google), 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 копирования (резервные копии)** — 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 привязанный 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 полнодисковым 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 их 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 журналистов и небольших команд для трансформации единичных индивидуальных практик 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 также несколько ключевых дополнительных шагов.**

Постараться по максимуму использовать только лицензионное программное обеспечение. Если у медиаорганизации есть дополнительно регистрация в качестве ННО, то 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. Помимо этого, можно напрямую писать вендорам с просьбой предоставления скидки

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 атмосферу** взаимодействия. Также важно постоянно отслеживать новости об изменениях в законодательстве, касающихся деятельности редакций и свободы слова.

Уровень 2:
Внедрение формализованных организационных процессов — предназначено для команд и редакций, 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 доступами, 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 редакций

В эпоху цифровой трансформации веб-сайты и онлайн-платформы редакций и журналистских организаций 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 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 к вам доверие. 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. Также результатом взлома может стать полное уничтожение информации на веб-сайте.

Атака на отказ в обслуживании (DDoS-атаки)

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, во время выборов, протестов, публикации 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, блокировке 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 ваше 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 редакций критически важным является и этический аспект: провайдер должен не только предоставлять услуги, но и понимать специфические риски, с которыми сталкиваются журналисты и независимые редакции. 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 и медиаорганизаций с высоким уровнем риска бесплатно.

Обеспечение безопасного доступа к администрированию веб-сайта — необходимо обеспечить максимальную защиту доступов 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 оправданно с точки зрения безопасности, но нужно иметь в виду, 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 погружения в технические детали — 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.

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). Также 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 трудно поддаются контролю, поскольку, как правило, они находятся за пределами вашего прямого влияния. Но как уже упоминалось ранее, знание об угрозах дает нам возможности на них реагировать, поэтому возьмите за правило мониторинг цифрового окружения, периодически осуществляйте поиск веб-сайтов с похожими на ваши названия, это же относится и к страницам в социальных 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 социальных сетей 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 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 подорвать доверие аудитории к вашему веб-сайту: соединение будет нешифрованное и трафик может быть перехвачен или изменен, также 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 соответствующего

направления (администратор веб-сайта или соцсетей 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 примеру, 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 в виду, 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 социальными сетями и другими организациями. В части расследования атак на веб-ресурсы, кампании по дезинформации можно также 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 редакций. 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 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. Настоятельно рекомендуется получить консультацию у доверенного адвоката, специализирующегося на защите прессы и свободы слова, до любых контактов с правоохранительными органами.

Заключение

Цифровая среда стала неотъемлемой частью деятельности редакций и медиаорганизаций. 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 редакций. 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. Редакции 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 партнеров. 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 редакций 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 перед публикацией чужого контента (для редактора/журналиста)

1. Определите тип использования
   - ☐ Это цитата/обзор/репортаж о событии (ограниченный фрагмент) или фактически перепубликация/перезалив целиком?
2. Есть законное основание для использования чужого контента:
   - ☐ Есть письменное разрешение/лицензия/договор
   - ☐ Контент под открытой лицензией (Creative Commons/куплен на стоке)
   - ☐ Подпадает под свободное использование (цитирование, обзор печати, текущие вопросы без запрета, речь, обзор события)
3. Проверен запрет правообладателя (особенно для перепечатки материалов):
   - ☐ В первоисточнике нет явной пометки «перепечатка запрещена» / запрета на публикацию / ограничительных условий
   - ☐ В первоисточнике не указано обязательство по получению разрешения на использование
4. Объем минимально необходимый для целей использования
   - ☐ Использовано ровно столько, сколько нужно для информационных/обзорных целей
   - ☐ Публикация не заменяет оригинал и не отбивает у него аудиторию (нет ощущения «полный материал уже здесь»)
5. Атрибуция оформлена корректно
   - ☐ Указаны автор (и/или правообладатель) + источник + дата + ссылка
   - ☐ Для перевода отмечено: «перевод редакции» + ссылка на оригинал
   - ☐ Для фото/видео указано происхождение (автор/агентство/сток/официальный аккаунт)
6. Проверка на переработку
   - ☐ Нет монтажа/адаптации/перевода/наложения музыки/обрезки смысла, которые превращают использование в переработку без разрешения
   - ☐ Не удалены водяные знаки/логотипы/метаданные и иные сведения об управлении правами
7. Контекст публикации не рекламный
   - ☐ Это не реклама/нативная реклама/пиар материал
8. Доказательства о первоисточнике сохранены
   - ☐ Сохранены: ссылка, скрин первоисточника, условия лицензии/разрешение, дата доступа (на случай претензии)
9. Финальный тест
   - ☐ Если бы вы были автором, вы бы сочли использование законным и уважением к источнику?
   - ☐ В случае сомнений необходимо запросить разрешения или не использовать чужой контент.

Приложение 2

Редакционный регламент по обработке и публикации общедоступных персональных данных

1. Общие положения
   1.1. Настоящий Регламент устанавливает порядок сбора, обработки и публикации персональных данных журналистами и редакцией.
   1.2. Цель Регламента — обеспечить:
      - соблюдение законодательства о персональных данных;
      - защиту прав и свобод человека;
      - баланс между свободой выражения мнения и правом на частную жизнь.
   1.3. Регламент применяется ко всем сотрудникам редакции, включая:
      - штатных журналистов;
      - редакторов;
      - внештатных авторов;
      - SMM-специалистов.

2. Нормативная основа
   - законодательство Республики Узбекистан о персональных данных;
   - международные стандарты свободы выражения мнения;
   - принципы защиты данных и приватности.

3. Ключевые принципы:
   - Любая обработка персональных данных должна иметь правовое основание.
   - Персональные данные используются только для конкретной журналистской цели в общественных интересах.
   - Публикуются только те данные, которые необходимы, релевантны, соразмерны цели публикации.
   - Вмешательство в частную жизнь не должно превышать общественный интерес.
   - Редакция обязана проверять достоверность публикуемых данных.

4. Основания для публикации персональных данных:
   4.1. Добровольное, информированное, выраженное в явной форме (письменное согласие) согласие субъекта персональных данных выраженное
   4.2. Публикация персональных данных допускается в целях защиты общественной безопасности, сообщения о правонарушении, предотвращение введения общества в заблуждение.
   4.3. Допускается обработка без согласия при условии соблюдения принципов пропорциональности и минимизации вреда субъекту персональных данных.

5. Классификация субъектов данных
   5.1. Публичные лица — политики, депутаты, государственные служащие, лица занимающие высшие управленческие должности, иные лица с правом

принятия решения и наложения санкций. Допускается более широкий объем публикации персональных данных при условии их связи с публичной функцией лица.

5.2. Частные лица — пользуются повышенным уровнем защиты персональных данных, публикация которых возможна с согласия лица.

5.3. Несовершеннолетние лица — пользуются абсолютным правом на конфиденциальность. Распространение персональных данных, сведений о место жительстве, учебе, фото и видео, способных идентифицировать несовершеннолетнее лицо не допускается. Публикация персональных данных несовершеннолетних лиц до 14 лет допускается только с согласия обоих родителей, законных представителей, опекунов и попечителей. Исключение освещение спортивных соревнований, официальных церемоний, олимпиад и фестивалей с участием несовершеннолетних лиц от 14 лет.

5.4. Уязвимые категории (жертвы насилия, лица с инвалидностью, лица с редкими заболевания, лица с тяжелой жизненной ситуации) — пользуются абсолютным правом на конфиденциальность. Распространение персональных данных, сведений о место жительстве, учебе, фото и видео, способных идентифицировать уязвимое лицо не допускается.

6. Ограничение на публикацию персональных данных

6.1. Без исключительных оснований запрещается публиковать:

- точный адрес проживания;
- контактные данные (телефон, email);
- идентификационные документы;
- банковские данные;
- сведения, составляющие медицинскую тайну (см. medical confidentiality);
- данные о частной и семейной жизни.

При публикации персональных данных редакция обязана оценивать риски идентификации лица и долгосрочные последствия публикации.

7. Публикация визуальных материалов

7.1. При публикации визуальных материалов редакция обязана:

- проверять текст, фото и видео на наличие данных позволяющих прямо или косвенно идентифицировать лицо;
- размывать лица при необходимости защиты персональных данных;
- удалять метаданные (геолокацию);
- осуществлять иные меры, препятствующие распространению персональных данных.

8. Оценка риска перед публикацией материалов с персональными данными

8.1. Перед публикацией редакция, журналист обязаны осуществить оценку на основании следующих критериев:

- Есть ли в публикации персональных данных общественный интерес?
- Можно ли опубликовать материал без указания персональных данных без ущерба общественного интереса?

- Есть ли вероятность причинения вреда после публикации персональных данных?
- Есть ли вероятность наступления ответственности, возникновения спора после публикации персональных данных?
- Из каких источников получены персональные данные (веб-сайты, социальные сети, официальные пресс-релизы, биографии кандидатов в депутаты, иные документы)?
- Необходимо/возможно ли получить согласие на публикацию персональных данных?

9. Процедура согласования перед публикацией материалов с персональными данными

9.1. Материалы, содержащие персональные данные проходят обязательную проверку редактором. В спорных случаях может привлекаться юрист для получения правовой консультации.

9.2. Редакция обязана предоставить лицу право на ответ или исправление персональных данных, а также рассматривать запросы на удаление персональных данных. Окончательное решение остается за ответственным редактором.

10. Заключительные положения

10.1. Регламент является обязательным для всех штатных и внештатных сотрудников редакции. Нарушение регламента влечет дисциплинарную ответственность.

10.2. Регламент подлежит регулярному пересмотру с учетом изменений в законодательстве и развития цифровых технологий.

10.3. Все сотрудники редакции ознакамливаются с Регламентом под роспись.


Софинансирование
Европейского Союза
ЦЕНТР
РАЗВИТИЯ
СОВРЕМЕННОЙ
ЖУРНАЛИСТИКИ
LPRC
ЦЕНТР ИССЛЕДОВАНИЯ
ПРАВОВОЙ ПОЛИТИКИ
UDRMI
O'ZBEKISTON RAQAMLI HUQUQLAR MEDIA TASHABBUSI