Софинансирование
Европейского Союза

ЦЕНТР
РАЗВИТИЯ
СОВРЕМЕННОЙ
ЖУРНАЛИСТИКИ

LPRC
ЦЕНТР ИССЛЕДОВАНИЯ
ПРАВОВОЙ ПОЛИТИКИ

UDRMI
O'ZBEKISTON RAQAMLI HUQUQLAR MEDIA TASHABBUSI

ЦИФРОВЫЕ ПРАВА ДЛЯ ЮРИСТОВ

Как понимать, применять и защищать на практике?

ЦИФРОВЫЕ ПРАВА ДЛЯ ЮРИСТОВ

Как понимать, применять и защищать на практике?

Ташкент
2026

Цифровые права для юристов. Как понимать, применять и защищать на практике? Пособие. Ташкент, 2026 — 93 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:
Артём Горяйнов (Кыргызстан)
Лола Махмудова (Узбекистан)
Мадина Турсунова (Узбекистан)
Ольга Диденко (Казахстан)
Роман Реймер (Казахстан)

Редактор:
Лола Исламова

Содержание

Как использовать это пособие?

Современное общество переживает масштабную цифровую трансформацию. Цифровые технологии стали неотъемлемой частью государственного управления, экономики и повседневной жизни. Сегодня получение государственных услуг, ведение бизнеса, обучение, профессиональная деятельность и коммуникация все чаще осуществляются с использованием цифровых сервисов и информационных технологий.

Настоящее пособие подготовлено как практическое руководство для юристов, работающих в государственных органах, коммерческих организациях, юридических фирмах, некоммерческом секторе и иных сферах, где вопросы цифровых прав становятся частью повседневной практики.

В отличие от традиционного учебника, пособие не ставит целью подробно изложить всю теорию цифровых прав. Его задача — помочь быстро разобраться в ключевых вопросах, понять их правовую природу и научиться применять полученные знания в профессиональной деятельности.

Структура пособия построена по принципу «от общего к частному». В первой части рассматриваются понятие цифровых прав, их место в системе прав человека, международные стандарты и национальное законодательство Республики Узбекистан. Во второй части внимание уделяется наиболее распространенным ситуациям, с которыми сталкиваются юристы на практике: защите персональных данных, конфиденциальной информации, доступу к информации, ответственности за цифровой контент, защите интеллектуальной собственности и разработке внутренних корпоративных политик. Третий раздел посвящен цифровым угрозам, информационной безопасности и практическим мерам защиты.

Для удобства читателя в пособии используются различные форматы представления информации:

- краткие теоретические пояснения, раскрывающие основные понятия;
- практические рекомендации по применению законодательства;
- примеры из судебной и правоприменительной практики;
- ссылки на международные документы и нормативные акты;
- чек-листы, позволяющие быстро проверить соблюдение основных требований;
- схемы, таблицы и сравнительные материалы, облегчающие восприятие сложной информации.

Пособие можно читать последовательно или использовать как справочник, обращаясь только к тем разделам, которые необходимы для решения конкретной профессиональной задачи.

Следует учитывать, что цифровые технологии и соответствующее законодательство развиваются очень быстро. Поэтому настоящее пособие следует рассматривать как практическую основу, которую рекомендуется дополнять изучением актуальных нормативных актов, судебной практики и международных документов.

Надеемся, что это пособие поможет юристам увереннее ориентироваться в вопросах цифровых прав, эффективнее защищать интересы своих клиентов и организаций, а также применять современные правовые подходы в условиях стремительной цифровой трансформации общества.

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.

Число пользователей Интернета во всем мире продолжает устойчиво расти. 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.

В связи с этим, 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, отраженных во многих международных документах ООН, а также документах регионального уровня, состоит в том, что «цифровые права» являются прямым продолжением прав человека.

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 множество международных и региональных документов, прошла огромный путь.

Для понимания природы цифровых прав необходимо кратко рассмотреть эволюцию прав человека.

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: они не могут быть произвольно ограничены или отняты, за исключением случаев, предусмотренных законом.
- Неделимость: гражданские, политические, экономические и социальные права взаимосвязаны. Нельзя полноценно пользоваться одними без других.

Поколения прав человека

Одним из наиболее известных подходов к классификации прав человека является концепция поколений прав человека, предложенная чешско-французским юристом Карелом Вашаком в 1979 году[3]. Автор был вдохновлен лозунгом «Свобода, Равенство, Братство»[4] Великой французской революции 1789 года. 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». В отличие от негативных прав, реализация позитивных прав предполагает активные действия государства по созданию соответствующих правовых, организационных и социальных механизмов, 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.

Поскольку предметом настоящего пособия являются цифровые права, далее внимание будет сосредоточено именно на их развитии и содержании.

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.

Отличительной особенностью цифровых прав является их непосредственная связь с информацией и данными, существующими в цифровой форме.

Цифровые права реализуются посредством цифровых технологий и возникают в процессе использования человеком цифровой среды и цифровых сервисов.

Обязательства в области цифровых прав человека включают как позитивные, так и негативные обязательства государств и частных субъектов. Таким образом, цифровые права человека в большей степени привязаны к новому отдельному поколению (или системе) прав[5].

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[7], закрепляет, в частности, следующие положения:

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 со своими международными обязательствами в области прав человека.

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

Неприкосновенность частной жизни в онлайн-среде имеет важное значение для реализации права свободно выражать 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 офлайн-среде, должны также защищаться в онлайн-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

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

Совет по правам человека ООН исходит из того, что права человека, реализуемые в цифровой среде, подлежат такой же защите, как и права, осуществляемые офлайн.

Из приведенных положений следует, что речь идет о политических правах (свобода слова и выражения мнения), экономических (право на образование) и коллективных (глобальный характер Интернета) правах.

Резолюция «Поощрение и защита прав человека в контексте цифровых технологий»[8], 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.

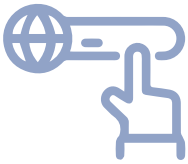
Доступ человека в Интернет сопряжен с различного рода вызовами, рисками и угрозами, транслируемыми государствами, технологическими компаниями и иными третьими лицами.

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.

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

Перечень цифровых прав

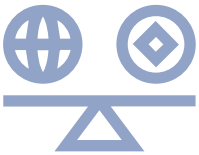


Право на доступ в Интернет

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. 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.)[9]: «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)[10], 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)[11]
Статья 17 (Неприкосновенность частной жизни)	Защищает от произвольного вмешательства в личную жизнь. Комитет по правам человека ООН в Замечании общего порядка № 16[12] интерпретирует это как обязательство государств законодательно регулировать сбор и хранение персональных данных в компьютерах и банках данных

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

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

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

[12] 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[13]	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[14]	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:* 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**[15]	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.

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

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

[15] 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).

То есть 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):

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

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

Ограничения цифровых прав т. н. «трехсоставный тест»

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

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

Законность:

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

Легитимная цель:

Защита национальной безопасности, порядка, здоровья, нравственности, прав других лиц.

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»[16]. (B.i.15 Сиракузские принципы).
- Более того, «Бремя обоснования ограничения права, гарантируемого Пактом, лежит на государстве» (A.12.Сиракузские принципы).

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

Региональные стандарты

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

В данном руководстве мы сосредоточимся на европейской системе цифрового регулирования.

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

Европейская система, включает Совет Европы и Европейский Союз

Европа в настоящее время, является глобальным лидером в кодификации цифровых прав, формируя так называемый «Эффект Брюсселя»[17], 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)[18]	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)[19]	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)[20]. 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 безопасностью пользователей. Важно отметить, что Digital Services Act упоминается в паре с Digital Markets Act (2022)[21] 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.

---

[17] 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

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

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

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

[21] 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[22], принятая в 1981 году.

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

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

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

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

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

В каждом из «поколений» принципов конфиденциальности данных можно условно (!) выделить по 10 стандартов:

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

Защита частной жизни и персональных данных

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, касающуюся защиты данных и частной жизни. Эта статья подчеркивает важность баланса между правом на доступ к информации и необходимостью защиты частной жизни и персональных данных.

Согласно разъяснения Верховного суда Республики Узбекистан по искам о защите личных неимущественных прав и иных нематериальных благ, вне зависимости от способа распространения соответствующей информации (в том числе в печатных изданиях, по радио, телевидению, на веб-сайтах, страницах веб-сайтов, в блогах, профилях в социальных сетях, мессенджерах и других информационно-коммуникационных средствах) ответчиками являются авторы не соответствующих действительности порочащих сведений, а также лица их распространившие.

Запись или распространение изображения без согласия лица, искажение изображения или размещение его в унижающем, дискредитирующем или вводящем в заблуждение контексте, несанкционированное использование изображения в коммерческих целях, цифровая обработка изображения, приводящая к искажению первоначального облика лица (включая дипфейк, внедрение в видеоматериалы, создание поддельных скриншотов и т. д.), распространение в Интернете без уведомления или получения согласия с правом неограниченного доступа считается нарушением права на изображение.

Защита права лица на изображение осуществляется путем признания действий незаконными, удаления или блокирования изображения в цифровом пространстве, возложения обязанности по удалению, блокированию или техническому ограничению доступа к визуальному материалу (в том числе путем обращения к администраторам цифровых платформ), запрета на дальнейшее использование изображения, возмещения материального ущерба и морального вреда, восстановления положения, существовавшего до нарушения права.

В случаях, когда использование изображения связано с негативным контекстом (например, в оскорбительной публикации, пародии, при добавлении фальсифицированного текста или использовании с искаженной информацией), может быть защищено не только право на изображение, но и честь, достоинство, деловая репутация лица, а также право на неприкосновенность частной жизни.

Действия, связанные с присвоением, изменением, умышленным искажением имени, использованием его в цифровом пространстве без согласия лица при обстоятельствах, которые могут повлиять на его репутацию, достоинство или правосубъектность, признаются нарушением неимущественного права.

Законодательство о свободе информации

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 органов государственной власти и управления» 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.

Законодательство об информатизации

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 Постановлением 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».

Установленный 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 строя, форма политической дезинформации
Пропаганда терроризма и религиозного экстремизма	Часто осуществляется через искажение фактов — опасная форма дезинформации
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	Борьба со спекулятивной или фейковой информацией до решения суда
Информация, порочащая честь и достоинство или деловую репутацию граждан	Запрет на публикацию заведомо ложных, позорящих лицо сведений и фактов.

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.

Практическое значение ограничений в деятельности СМИ определяется в следующем:

- превентивная функция через ответственность и обязательства СМИ проверять достоверность информации перед публикацией и создание правового барьера для распространения ложной информации, фейков, пропаганды, и манипуляций;

- защитная функция посредством механизмов по охране интересов личности, общественного порядка и государственной безопасности;

- этическая функция посредством установления ориентиров и рамок для редакционных политик СМИ и журналистов.

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 исключают 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, материалов гражданской журналистики, зарубежных изданий), 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.

Дополнительные поддерживающие механизмы содержит статья 6 Закона Республики Узбекистан «О гарантиях профессиональной деятельности журналистов», устанавливающей 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
Презумпция невиновности	Соблюдение принципа презумпции невиновности при публикации материалов о подозреваемых, обвиняемых, подсудимых и осужденных лицах
Соблюдение профессиональной этики	Установление внутренних этических правил
Запрет использования информации о частной жизни в личных целях	Запрет на распространение информации о частной жизни, являющейся конфиденциальной, за исключением сведений, опубликованных в общедоступных источниках

При этом, обязательства по проверке достоверности журналистов могут толковаться в расширенном формате и распространяться на мнение и суждения лиц. Закон не закрепляет понятия «добросовестное расследование», «журналистская проверка источника», что затрудняет защиту СМИ даже при соблюдении профессиональных стандартов. СМИ и журналисты могут нести ответственность не только за прямую дезинформацию, но и 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 журналистского сообщества должны быть оставлены на усмотрение механизмов саморегулирования.

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 СМИ от иных медиа ресурсов.

Лицо, считающее, что оценочное мнение или суждение, распространенное в средствах массовой информации, затрагивает его права и законные интересы, вправе в соответствии с ч. 6 ст. 100 ГК и ст. 34 Закона «О средствах массовой информации», пользуясь предоставленным ему правом на ответ, комментарий, реплику, может потребовать иной оценки мнений, распространенных в данном средстве массовой информации, для доказательства их необоснованности.

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, передается 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. Однако, несмотря на это, действующий механизм ограничен и не охватывает опровержение общественно значимой дезинформации, не касающейся конкретных лиц.

Требования к 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 и 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») и Экспертная комиссия в сфере информации и массовых коммуникаций.

Ограничение 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.

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.

В целях выявления информационных ресурсов сети Интернет, содержащих запрещенную информацию, Узкомназорат осуществляется мониторинг информационных ресурсов сети Интернет в порядке, установленном законодательством. Ограничение доступа к веб-сайту или информации осуществляется по результатам мониторинга Узкомназората или на основании решения Экспертной комиссия в сфере информации и массовых коммуникаций.

Узкомназорат направляет уведомление владельцу веб-сайта или страницы веб-сайта с требованием об удалении незаконного контента в течении 24 часов. Владелец 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 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 запроса о принадлежащих им информационных ресурсах сети Интернет, что противоречит международным стандартам.

Механизмы обжалования, предусмотренные законодательством, предоставляют общее право обжалования в суде действий Узкомназората по признанию информации незаконной. Тогда как международные стандарты основаны на создании независимого досудебного апелляционного механизма обжалования ограничения доступа к информационным ресурсам.

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 контента. Нет обязательств Узкомназората по опубликованию отчетов об ограничении контента, ограничен доступ к Реестру
Процедуры	Ограничение 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 Узкомназората 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 решения об ограничении контента

Раздел 2
Цифровые права для юристов

2.1. Защита персональных данных сотрудников, клиентов, контрагентов

В Республике Узбекистан действует законодательство о персональных данных, защите частной жизни и неимущественных прав граждан. Предусмотрены административная и уголовная ответственность за незаконный сбор и обработку персональных данных, разглашение сведений о частной жизни.

Согласно Закону Республики Узбекистан «О персональных данных» от 02.07.2019 г. № ЗРУ-547 (далее «Закон о ПДн») персональные данные — это любая информация или сведения, позволяющие идентифицировать человека. Законом не установлен исчерпывающий перечень персональных данных — общие требования применяются к широкому кругу данных, связанных с частной жизнью, профессиональной деятельностью и перемещениями человека.

Основным критерием является связь данных с конкретным физическим лицом или его имуществом, а также сбор и использование таких данных другим лицом или организацией с учетом цели использования и хранения персональных данных.

Закон о персональных данных устанавливает четыре вида персональных данных, которые обрабатываются в базах данных:

Специальные персональные данные — сведения о расовом или социальном происхождении, политических, религиозных или идеологических убеждениях, членстве в политических партиях и профессиональных союзах, а также сведения о состоянии физического или психического здоровья, частной жизни и судимости.

Биометрические персональные данные — персональные данные, характеризующие анатомические и физиологические особенности субъекта.

Генетические персональные данные — персональные данные, относящиеся к наследственным или приобретенным характеристикам субъекта, которые являются результатом анализа биологического образца субъекта либо анализа другого элемента, позволяющего получить эквивалентную информацию.

Общедоступные персональные данные — персональные данные, доступ к которым является свободным с согласия субъекта либо которые не подпадают под требования конфиденциальности.

При обработке персональных данных, собственник и (или) оператор обязаны внедрять организационные и технические меры по защите персональных данных с учетом угроз их безопасности.

Персональные данные работников собственника (оператора) и персональные данные субъектов, которые не являются работниками собственника (оператора), должны обрабатываться в отдельных базах данных.

ВАЖНО!

Обработка персональных данных может осуществляться только с ведома и добровольного, конкретного согласия субъекта данных или на ином законном основании.

Основные условия обработки персональных данных включают в себя:

Согласие субъекта персональных данных	Правовое основание требования	Разъяснения
Законные цели обработки персональных	Ст. 19 Закона о ПДн: Цели обработки персональных данных определяются нормативно-правовыми актами, положениями, учредительными или иными документами, регламентирующими деятельность собственника и (или) оператора, и должны соответствовать настоящему Закону. Цели обработки персональных данных должны соответствовать целям, ранее заявленным при их сборе, а также правам и обязанностям собственника и (или) оператора.	Утвердить цели и способы обработки **ПДн в локальном нормативном акте.**
Категории персональных данных	Ст. 25 Закона о ПДн: Специальными персональными данными являются данные о расовом или социальном происхождении, политических, религиозных или мировоззренческих убеждениях, членстве в политических партиях и профессиональных союзах, а также данные, касающиеся физического или душевного (психического) здоровья, сведения о частной жизни и судимости. Ст. 26 Закона о ПДн: Биометрическими данными являются персональные данные, характеризующие анатомические и физиологические особенности субъекта. Генетическими данными являются персональные данные, относящиеся к унаследованным или приобретенным характеристикам субъекта, которые являются результатом анализа биологического образца субъекта или анализа другого элемента, позволяющего получить эквивалентную информацию.	**Утвердить состав ПДн, необходимый и достаточный для целей их обработки.** Получить согласие на использование биометрических данных при использовании биометрических данных в Системах контроля и управления доступом на предприятии (СКУД). Зарегистрировать базы персональных данных, включающих специальные, биометрические и генетические данные. Провести оценку типов угроз и внедрить организационные и технические меры по защите баз ПДн.
Сроки обработки персональных данных	Ст. 10 Закона о ПДн: Срок хранения персональных данных определяется датой достижения целей их сбора и обработки. Ст. 19 Закона о ПДн: Срок обработки персональных данных не должен превышать срок, в течение которого действует согласие субъекта на обработку его персональных данных.	

Порядок дачи согласия и отзыв согласия на обработку персональных данных	Ст. 21 Закона о ПДн: Для обработки специальных персональных данных требуется согласие субъекта в письменной форме, в том числе в виде электронного документа. Субъект отзывает согласие на обработку персональных данных в той форме, в какой данное согласие было дано, либо в письменной форме, в том числе в виде электронного документа.	Разработать и утвердить форму согласия на обработку персональных данных. Утвердить порядок рассмотрения обращений по отзыву согласия на обработку персональных данных.
Право на уничтожение персональных данных (право забвения)	Ст. 17 Закона о ПДн: Персональные данные подлежат уничтожению собственником и (или) оператором, а также третьим лицом: при достижении цели обработки персональных данных; при наличии отзыва согласия субъекта на обработку персональных данных; по истечении срока обработки персональных данных, определенного согласием субъекта; при вступлении в законную силу решения суда.	Утвердить порядок уничтожения персональных данных, разработать акты об уничтожении персональных данных.
Согласие на трансграничную передачу	Ст. 15 Закона о ПДн: Трансграничная передача персональных данных на территорию иностранных государств, не обеспечивающих адекватную защиту персональных данных, может осуществляться в случаях: наличия согласия субъекта на трансграничную передачу его персональных данных.	Включить в форму согласия на обработку персональных данных случаи трансграничной передачи с указанием целей передачи и обработки данных лиц, организаций, юрисдикции трансграничной передачи. Проверить наличие законодательства о защите персональных данных в юрисдикции трансграничной передачи. Предусмотреть обязательства по обеспечению защиты персональных данных при трансграничной передаче.
Использование технологий искусственного интеллекта при обработке ПДн	Ст. 46-2 КоАО[25] Незаконная обработка персональных данных с использованием технологий искусственного интеллекта, их распространение в средствах массовой информации, сетях телекоммуникаций или всемирной информационной сети Интернет, — влечет наложение штрафа в размере от пятидесяти до ста базовых расчетных величин, с конфискацией предметов административного правонарушения.	Ограничить способы обработки ПДн с использованием технологий искусственного интеллекта. Предусмотреть согласие субъекта на обработку персональных данных с использованием ИИ при наличии законных целей обработки и отсутствии недопустимых рисков нарушения прав субъекта ПДн.
Назначение ответственного лица за обработку ПДн	Согласно п. 6 Приказа № 3477: «Основными задачами лица, ответственного за обработку и защиту персональных данных: • обеспечить их защиту, целостность, сохранность и конфиденциальность при обработке персональных данных; • для предотвращения незаконной обработки персональных данных и для блокировки (ограничения) персональных данных по согласованию с владельцем и (или) оператором в случаях выявления нарушений требований, установленных законом;	Назначить ответственное лицо за обработку и защиту персональных данных. Утвердить должностные инструкции и круг лиц, имеющих доступ к обработке персональных данных.

[25] Закон Республики Узбекистан «О внесении дополнений и изменений в некоторые законодательные акты Республики Узбекистан в связи с регулированием отношений, возникающих при применении искусственного интеллекта» от 21.01.2026 за № ЗРУ-1115. Текст закона доступен по ссылке: https://lex.uz/ru/docs/8011377

- организация и координация политики информационной безопасности для обеспечения безопасности личной базы данных владельца и (или) оператора;
- организация обучающих семинаров для сотрудников, работающих с персональными данными.

ВАЖНО!

Отсутствие надлежащего согласия, выход за пределы установленных целей обработки или несоблюдение принципов законности и достаточности признается нарушением личных прав и влечет за собой гражданско-правовую ответственность.

При признании обработки персональных данных незаконной, суд может возложить на оператора обязанность полностью удалить данные и уничтожить также их резервные копии.

СУДЕБНАЯ ПРАКТИКА:

Административное дело
№ 3-2203-2502/2951 от 26.12.2025 г.

Обстоятельства нарушения:

Начальник центра банковских услуг одного из банков для улучшения показателей занятости населения, которые были определены для него как целевые показатели (KPI), без согласия граждан получил и использовал ИНН/ПИНФЛ 68 граждан. Персональные данные граждан были внесены на платформу yangiish.mehnat.uz и оформлены как данных самозанятых лиц.

ПИНФЛ — это персональные данные, неправомерная обработка которых является прямым нарушением прав субъекта ПДн.

В решении суда отдельно подчеркивается, что «обработка персональных данных должна осуществляться с согласия субъекта персональных данных».

Работника банка признали виновным по ст. 46.2 КоАО «Нарушение законодательства о персональных данных» и назначили штраф в размере 7 БРВ со ссылкой на ст. 33 КоАО «Применение более мягкого административного взыскания» при определении размера штрафа.

Если не назначено ответственное должностное лицо за обработку ПДн, ответственность за защиту персональных данных несет руководитель предприятия.

Государственный надзор за законностью обработки персональных данных осуществляется со стороны ряда государственных органов:

Наименование	Правовое основание	Полномочия
Кабинет Министров Республики Узбекистан	Закон «О персональных данных»	Устанавливает: • уровни защищенности персональных данных при их обработке в зависимости от угроз безопасности; • требования по обеспечению защиты персональных данных при их обработке, исполнение которых обеспечивает установленные уровни защищенности персональных данных; • требования к материальным носителям биометрических и генетических данных и технологиям хранения таких данных вне баз персональных данных
Департамент миграции и персонализации при Министерстве внутренних дел Республики Узбекистан	Постановление Кабинета Министров Республики Узбекистан, от 08.02.2020 г. № 71 «Об утверждении Административного регламента оказания государственной услуги по ведению Государственного реестра баз персональных данных»	Выдача персонального идентификационного номера физическому лицу. Выдача биометрического паспорта для выезда за границу гражданину Республики Узбекистан Внесение персональных баз данных в государственный реестр персональных баз данных
Инспекция по контролю в сфере информатизации и телекоммуникаций при Министерстве цифровых технологий Республики Узбекистан («Узкомназорат»)	Положение «О порядке проведения государственного контроля за соблюдением особых условий обработки персональных данных граждан Республики Узбекистан», утвержденное Постановлением Кабинета Министров Республики Узбекистан от 29.04.2021 г. № 255	Выявление информационных ресурсов — нарушителей особых условий обработки персональных данных Включение информационных ресурсов в Реестр нарушителей прав субъектов персональных данных («Реестр») Ограничение доступа к информационным ресурсам, включенным в Реестр

Обработка персональных данных работников

Правовые основания обработки персональных данных и правила работы с ними определяет Трудовой кодекс (далее «ТК») и Закон «О персональных данных» (№ ЗРУ-547 от 02.07.2019 г.). ТК определяет основные правила обработки, хранения и использования персональных данных

Персональные данные работника — конфиденциальная информация о фактах, событиях и обстоятельствах жизни работника и членов его семьи. Сотрудники предоставляют персональные данные работодателю в связи с трудовыми отношениями.

К персональными данным относятся следующие сведения о работнике:

- Ф.И.О., дата и место рождения;
- ПИНФЛ (при наличии);
- информация и документы об образовании;
- выполняемая работа с момента начала трудовой деятельности, включая военную службу;
- адрес регистрации по месту постоянного или временного проживания;
- данные паспорта или ID-карты — серия, номер, кем и когда выдан;
- номер личного телефона, адрес электронной почты;
- отношение к воинской обязанности, сведения по воинскому учету — для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу;
- идентификационный номер налогоплательщика (при наличии);
- ИНПС;
- результаты обязательного медосмотра;
- основания прекращения с работником трудового договора;
- семейное положение, Ф.И.О. и даты рождения близких родственников;
- иные сведения о ставших известными работодателю фактах, событиях и обстоятельствах жизни работника и членов его семьи.

При обработке персональных данных работников ТК обязывает работодателя (ст. 176 ТК):

- руководствоваться положениями законодательства о персональных данных;
- получать персональные данные непосредственно у самого работника;
- получать персональные данные от третьих лиц только с письменного уведомления работника и с его согласия;
- сообщать работнику о целях, предполагаемых источниках и способах получения, а также о характере этих данных;
- сообщать работнику о последствиях, если он отказывается дать согласие на получение личных данных;
- обеспечивать защиту персональных данных работника;
- знакомить работников под подпись о порядке обработки персональных данных;
- вырабатывать меры по защите персональных данных работников;
- не допускать разглашения персональных данных, которые стали известны в процессе трудовой деятельности.

Основные положения по обработке персональных данных работников должны регулироваться внутренними локальными актами работодателя. Базы персональный данных работников не требуют регистрации.

Обработка биометрических и генетических данных

Согласно ст. 7 Закона о ПДн Кабинет Министров Республики Узбекистан уполномочен устанавливать:

- уровни защищенности персональных данных при их обработке в зависимости от угроз безопасности;
- требования по обеспечению защиты персональных данных при их обработке, соблюдение которых обеспечивает установленные уровни защищенности персональных данных;
- требования к материальным носителям биометрических и генетических данных, а также к технологиям хранения таких данных вне баз персональных данных.

Постановлением Кабинета Министров Республики Узбекистан от 05 октября 2022 года № 570 «Об утверждении некоторых нормативно-правовых актов в области обработки персональных данных» (далее «Постановление») установлены дополнительные требования к операторам персональных данных, связанные с уровнями защищенности, и утверждены:

- Положение о порядке определения уровней защищенности персональных данных при их обработке;
- Положение о требованиях к материальным носителям биометрических и генетических данных и технологиям хранения таких данных вне баз персональных данных.

Обязательные действия для соблюдения требований по оценке рисков:

- внедрение организационных и технических мер по защите персональных данных с учетом видов угроз и обеспечиваемых уровней защищенности;
- обеспечение установленного уровня защищенности материальных носителей персональных данных, а также онлайн- или цифровых баз данных в части доступа и использования базы данных;
- определение объема обязанностей руководителя собственника и (или) оператора, а также лиц, имеющих доступ к персональным данным, обрабатываемым в базах данных, в пределах, необходимых для исполнения их служебных (трудовых) обязанностей, с учетом уровней защищенности и мер по снижению угроз;
- утверждение порядка оценки соответствия уровня защищенности средств защиты информации требованиям местного законодательства об информационной безопасности;
- назначение ответственного лица за обработку персональных данных (Data Protection Officer).

Собственник или оператор при обработке биометрических и генетических данных принимает организационные и технические меры по их защите и хранению. Каждый уровень защищенности предусматривает определенные требования, которые должны быть выполнены собственником и (или) оператором персональных данных.

Первый уровень защищенности

Условия применения (уровень обязателен, если выполняется хотя бы одно условие):

1. При наличии угроз 1-го типа для баз данных и обработке в базах данных специальных и (или) биометрических и (или) генетических персональных данных.
2. При наличии угроз 2-го типа для баз данных и обработке специальных персональных данных более чем 50 000 субъектов, которые не являются работниками собственника и (или) оператора.

Требования для обеспечения уровня защищенности:

- выполнение требований, предусмотренных для второго уровня защищенности;
- автоматическая регистрация в электронном журнале безопасности изменений в полномочиях (авторизации) собственника и (или) оператора по доступу к персональным данным в базах данных;
- создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в базах данных, либо возложение функций по обеспечению такой безопасности на одно из действующих структурных подразделений.

Второй уровень защищенности

Условия применения (каждый уровень защищенности обязателен, если выполняется хотя бы одно условие):

1. При наличии угроз 1-го типа для баз данных и обработке в базах данных общедоступных персональных данных.
2. При наличии угроз 2-го типа для баз данных и обработке специальных данных работников собственника и (или) оператора либо специальных данных менее чем 50 000 субъектов, которые не являются работниками собственника и (или) оператора.
3. При наличии угроз 2-го типа для баз данных и обработке в базах данных биометрических и (или) генетических данных.
4. При наличии угроз 2-го типа для баз данных и обработке в базах данных общедоступных данных более чем 50 000 субъектов, которые не являются работниками собственника и (или) оператора.
5. При наличии угроз 3-го типа для баз данных и обработке в базах данных специальных данных более чем 50 000 субъектов, которые не являются работниками собственника и (или) оператора.

Требования для обеспечения уровня защищенности:

- выполнение требований, предусмотренных для третьего уровня защищенности;
- предоставление доступа к электронному журналу сообщений исключительно должностным лицам (работникам) либо уполномоченному лицу, которым сведения, содержащиеся в указанном журнале, необходимы для исполнения их служебных (трудовых) обязанностей.

Третий уровень защищенности

Условия применения (каждый уровень защищенности обязателен, если выполняется хотя бы одно условие):

1. При наличии угроз 2-го типа для баз данных и обработке общедоступных данных работников собственника и (или) оператора либо общедоступных данных менее чем 50 000 субъектов, которые не являются работниками собственника и (или) оператора.
2. При наличии угроз 3-го типа для баз данных и обработке специальных данных работников собственника и (или) оператора и (или) специальных данных менее чем 50 000 субъектов, которые не являются работниками собственника и (или) оператора.
3. При наличии угроз 3-го типа для баз данных и обработке биометрических и (или) генетических данных.

Требования для обеспечения уровня защищенности:

- выполнение требований, предусмотренных для четвертого уровня защищенности;
- назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в базах данных.

Четвертый уровень защищенности

Условия применения (каждый уровень защищенности обязателен, если выполняется хотя бы одно условие):

1. При наличии угроз 3-го типа для баз данных и обработке в базе данных общедоступных персональных данных.

Требования для обеспечения уровня защищенности:

- организация режима безопасности для помещений, где размещены базы данных, исключающего бесконтрольный вход или пребывание в этих помещениях лиц, не имеющих права доступа;
- обеспечение сохранности материальных носителей персональных данных;
- утверждение руководителем собственника и (или) оператора документа, определяющего перечень лиц, которым доступ к персональным данным, обрабатываемым в базах данных, необходим для исполнения их служебных (трудовых) обязанностей;

- применение средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства в области информационной безопасности, в случаях, когда использование таких средств необходимо для защиты персональных данных от актуальных угроз.

2.2. Защита конфиденциальной информации в компании

В каждой организации есть данные, которые нельзя разглашать: информация о клиентах, внутренние отчеты, коммерческие планы. Чтобы защитить такие сведения и установить единые правила, необходимо разработать Положение о конфиденциальной информации. В этом документе важно четко указать, что считается конфиденциальной информацией, кто и как должен ее хранить и какими будут последствия за нарушение этих правил.

ВАЖНО!

Положение является основанием для заключения NDA (соглашение о конфиденциальности) с сотрудниками для защиты интересов компании при раскрытии данных, утечке информации.

При разработке Положения о конфиденциальности необходимо руководствоваться реальными бизнес-процессами компании, сформировать перечень конфиденциальной информации, определить уровни доступа. Документ должен учитывать специфику компании, уровень доступа сотрудников, формы работы с данными, и риски.

Для вступления Положения в юридическую силу необходимо провести процедуру согласования, включая согласование с представительным органом работников (при наличии).

После согласования Положения работодатель вправе издать приказ, по которому локальный акт вводится в действие. С этого момента документ обязателен для исполнения, а все сотрудники, имеющие доступ к конфиденциальной информации, должны быть ознакомлены с ним под роспись.

Раздел Положения	Что включить (содержание раздела)	Примеры / примечания
I. Общие положения	Цель и задачи режима конфиденциальности. Правовая основа (НПА и внутренние документы). Термины: «конфиденциальная информация», «носитель», «доступ», «разглашение», «утечка», «инцидент». Сфера действия и круг лиц (работники, стажеры, подрядчики, консультанты, представители контрагентов). Принципы: «необходимость знать», минимизация доступа, персональная ответственность.	Формулировка: «Положение устанавливает единый режим работы с конфиденциальной информацией, определяет меры защиты и ответственность за нарушение режима».

II. Состав конфиденциальной информации и классификация	Перечень категорий (коммерческая тайна, персональные данные, финансы, клиенты/поставщики, код/технические документы, отчеты, стратегии, договоры, регламенты, базы данных). Уровни конфиденциальности. Критерии отнесения к категориям/уровням. Порядок пересмотра перечня.	Пример уровней: • «Для служебного пользования»; • «Конфиденциально»; • «Строго конфиденциально».
III. Организация учета, хранения и защиты	Места хранения (серверы, архив, облако, рабочие станции, бумага). Меры защиты: организационные / технические / физические. Порядок операций: маркировка, копирование, сканирование, фото, пересылка, печать, уничтожение, архивирование. Журналы: выдача/возврат, логи доступа, учет носителей.	Технические меры: пароли, шифрование, журналы событий, антивирус, контроль устройств, резервное копирование.
IV. Допуск сотрудников и управление доступом	Основание допуска (приказ/распоряжение, заявка руководителя, согласование ответственного). Принцип «доступ только по должностной необходимости». NDA/обязательство: момент подписания, срок действия, последствия. Уровни доступа (матрица ролей). Обучение и инструктаж при приеме и периодически.	Рекомендуется отдельная **матрица доступа** как приложение.
V. Порядок передачи третьим лицам	Когда допустима передача и на каких основаниях (договор, поручение, NDA, минимизация). Каналы передачи и запреты на несанкционированные. Требования к контрагентам: меры защиты, ограничения субподрядчиков, возврат/уничтожение по окончании. Контроль доступа представителей контрагентов (гостевой режим, учет).	Отдельный пункт о запрете передачи в мессенджер без санкционированного канала (с исключениями по приказу/регламенту).
VI. Использование информации в публичной среде	Публикации, кейсы, презентации, соцсети, мероприятия, интервью. Процедура согласования публичных материалов (кто визирует). Запрет на раскрытие/«деанонимизацию» клиентов и сотрудников без разрешения. Правила фото-, видеосъемки в офисе (если актуально).	Полезно: чек-лист «перед публикацией» (кому отправить на согласование).
VII. Контроль соблюдения режима	Ответственные подразделения (HR, IT, безопасность/комплаенс, юристы). Формы контроля: плановые/внеплановые проверки, аудит прав доступа, аудит журналов, проверка носителей. Служебное расследование: основания, сроки, оформление.	Укажите периодичность плановых проверок (например, ежеквартально/раз в полугодие).

VIII. Реагирование на инциденты	Определение инцидента. Обязанность работника немедленно сообщить. Первичные меры: блокировка доступа, изъятие носителя, фиксация следов, ограничение распространения. Расследование: комиссия, сбор доказательств, акт, корректирующие меры, обучение. Коммуникации: единый спикер, запрет несанкционированных комментариев.	Рекомендуется шаблон: «сообщение об инциденте» + форма «акт расследования».
IX. Ответственность	Дисциплинарная. Материальная. Иная ответственность по закону. Порядок оформления: объяснительная, акт, приказ, взыскание.	Формулировка: «Ответственность наступает в соответствии с законодательством и локальными актами работодателя».
X. Заключительные положения	Утверждение и введение в действие. Ознакомление работников под роспись. Порядок внесения изменений. Срок действия. Контакт ответственного лица.	Удобно: приложение «лист ознакомления» или «журнал ознакомления».
Приложения	Перечень конфиденциальной информации. Форма обязательства о неразглашении (NDA) для сотрудников. Журнал учета носителей. Журнал выдачи документов. Шаблон акта об уничтожении носителей/документов. Памятка сотруднику. Форма уведомления об инциденте.	

Процедура ознакомления работников с Положением о конфиденциальности

После утверждения Положения важно правильно организовать процесс ознакомления работников с его содержанием. Это необходимо для того, чтобы сотрудники в полной мере осознавали свои обязанности по защите конфиденциальной информации и несли ответственность за возможные нарушения.

Для ознакомления работников с документом работодатель может использовать следующие способы:

1. Включить в трудовой договор пункт о необходимости соблюдать Положение о конфиденциальности и указать реквизиты документа.
2. Предусмотреть лист ознакомления с Положением, в котором расписываются все работники.
3. Вести журнал ознакомления с Положением о конфиденциальности с графами: В (Ф.И.О., должность, наименование локального акта, дата) и подпись работника.
4. Предусмотреть отдельные листы ознакомления для каждого работника с полным перечнем локальных актов. Работник ставит подпись напротив каждого локального акта.

Работодатель вправе проводить обучение ответственных сотрудников по работе с конфиденциальной информацией.

Чек-лист по внедрению Положения о конфиденциальности

- ☐ Описаны процессы: где данные создаются, кто их видит, куда уходят.
- ☐ Определены категории конфиденциальной информации и утвержден перечень.
- ☐ Назначены ответственные лица: IT/HR/юрист.
- ☐ Введены уровни доступов и порядок выдачи/отзыва доступа.
- ☐ Настроены минимальные технические меры: пароли, журналирование, резервное копирование.
- ☐ Установлен порядок работы с бумажными документами и носителями.
- ☐ Закреплены правила передачи третьим лицам (договор NDA, стандартные ограничения).
- ☐ Введен процесс реагирования на инциденты (сообщение → локализация → расследование → меры).
- ☐ Организовано ознакомление работников под роспись (журнал/лист ознакомления).
- ☐ Организовано систематическое обучение (вводное, ежегодное).

2.3. Доступ к информации для профессиональной деятельности юристов

Современная юридическая практика невозможна без оперативного доступа к достоверной информации. Юристы ежедневно работают с нормативными правовыми актами, судебной практикой, государственными реестрами, корпоративными документами, открытыми данными и цифровыми сервисами органов государственной власти.

При этом недостаточно лишь найти необходимую информацию. Важно понимать, какие источники являются официальными, каким сведениям можно доверять, какие ограничения установлены законодательством при работе с информацией ограниченного доступа и каким образом защищать права клиента при отказе в предоставлении информации.

В данном разделе рассматриваются практические инструменты поиска, проверки и законного использования информации в профессиональной деятельности юриста.

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.

Запрос информации

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

Запрос на получение информации о деятельности органов государственной власти и управления (далее «запрос») — требование пользователя информации в устной или письменной форме (в том числе в форме электронного документа), направляемое органам государственной власти и управления и (или) их должностным лицам, о предоставлении информации о деятельности этих органов. (ст. 18 Закона Республики Узбекистан «Об открытости деятельности органов государственной власти и управления»).

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

Критерий	Обращение граждан/юрлиц	Запрос на получение информации
Цель	Содействие в реализации прав, восстановление нарушенных прав, защита законных интересов, предложения по улучшению работы.	Получить конкретные сведения о деятельности госоргана (информация о деятельности органов власти и управления).
Содержание	**Заявление** — просьба о содействии. **Жалоба** — требование восстановить права. **Предложение** — рекомендации по совершенствованию деятельности.	Требование предоставить информацию. Запрос может быть устным/письменным/электронным.
Конституционное основание	Право обращаться с заявлениями, предложениями и жалобами.	Право искать, получать и распространять информацию. Также право на ознакомление с документами, затрагивающими права и интересы.
Правовое основание	Закон РУз «Об обращениях физических и юридических лиц» (виды обращений, требования, сроки).	Закон РУз «Об открытости деятельности органов государственной власти и управления» (понятие запроса, сроки).

		Закон РУз «О гарантиях и свободе доступа к информации» (право на запрос, формы и сроки). Инструкция о порядке приема, регистрации и обработки запросов на предоставление информации о деятельности государственных органов и органов управления (Рег. № 2769)
Кто подает	Физические и юридические лица.	Любой пользователь информации (физлицо или юрлицо).
Язык	Обращения подаются на государственном языке, а также на других языках.	Запросы могут быть поданы на государственном языке, а также на других языках.
Куда направляется	В госорганы/госучреждения (и в ряде случаев — иные организации по компетенции закона).	В орган власти/должностному лицу, в полномочия которого входит предоставление информации по вопросам запроса.
Срок рассмотрения	Заявление/жалоба — **до 15 дней.** При доп. изучении — **до 1 месяца.** Предложение — **до 1 месяца.**	Запрос пользователя — **до 15 дней** со дня регистрации Запрос СМИ — **до 7 дней.**
Если адресат не компетентен	Перенаправление по компетенции и уведомление заявителя (в пределах сроков закона).	Перенаправление в течение **3 рабочих дней** со дня регистрации с уведомлением пользователя.
Результаты рассмотрения	Решение по существу обращения и ответ о результатах и принятых мерах.	Предоставление информации; либо мотивированный отказ; либо ссылка на уже опубликованные источники (официальные издания/веб-сайт). В случае отказа направляется мотивированный ответ.
Требования к идентификации	Обязательны Ф.И.О./адрес (для физлица) или наименование/адрес (для юрлица) и суть обращения.	Обязательны Ф.И.О./адрес (для физлица) или наименование/адрес (для юрлица) и суть запроса.
Значение	Защита прав и интересов через действия и решения.	Реализация доступа к информации о деятельности государства и его органов.

Доступ к информации о деятельности органов государственной власти и управления ограничивается в только случае, если указанная информация отнесена в установленном законом порядке к сведениям, составляющим государственные секреты или иную охраняемую законом тайну.

Алгоритм подачи запроса на получение информации

Шаг 1. Определите компетентный государственный орган

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

Шаг 2.
Уточните полномочия органа

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

Шаг 3.
Составьте запрос правильно

Запрос — это требование пользователя информации о предоставлении сведений о деятельности органа.

Запрос может быть устным, письменным или в форме электронного документа.

Сформулируйте один или несколько конкретных вопросов. Если вы запрашиваете документ, укажите наименование и реквизиты, если они известны.

Шаг 4.
Проверьте обязательные реквизиты запроса

Для физического лица укажите Ф.И.О., сведения о месте жительства и суть запроса.

Для юридического лица укажите полное фирменное наименование, почтовый адрес и суть запроса. Письменный запрос должен быть подписан пользователем информации.

Запрос без данных для идентификации считается анонимным и не рассматривается

Шаг 5.
Выберите канал направления

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

Шаг 6.
Зафиксируйте факт подачи

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

Шаг 7.
Контролируйте сроки и переписку

Отсчет срока рассмотрения запроса информации начинается со дня регистрации запроса.

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

Доступ к правовой информации

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

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

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

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

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

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

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

Правовая пропаганда законодательных актов осуществляется следующими способами:

- проведение конференций, встреч, семинаров, круглых столов и бесед;
- через средства массовой информации, в том числе организации теле- и радиовещания, размещение статей и информационно-правовых материалов в печатных и электронных средствах массовой информации;
- распространение комментариев, брошюр, плакатов, буклетов и флаеров;
- через социальную рекламу (видеоролики, инфографики и др.) и другие виды пропаганды, не запрещенные законодательством.

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

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

2.4. Ответственность за контент в цифровой среде

2.4.1. 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, в Казахстане), 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, указанные в таблице ниже, 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 требуют максимальной осторожности, многократной проверки фактов и оценки рисков возможного давления или преследования.

Есть два способа, как обеспечить юридическую помощь и защиту в этих случаях.

1. **Предварительный анализ текста до публикации.** Если редакция планирует публикацию по «чувствительной» теме, юридическая помощь должна включаться не «в конце», а на этапе подготовки материала — до выхода и до публикации на веб-сайте и в социальных сетях. На практике это работает следующим образом: юрист получает черновик текста, заголовок, иллюстрации или видео, ссылки и ключевые цитаты, проверяет формулировки на предмет признаков противоправного контента и оценивает риск вторичной ответственности (включая комментарии, репосты, превью, теги и подписи). По результатам юрист дает короткое заключение: какие фрагменты требуется изменить, какие доказательства и подтверждения нужны (документы, ответы на запросы, скриншоты, записи), какие персональные данные необходимо удалить или обезличить, и какой формат подачи снижает риск (нейтральная констатация, баланс источников, отказ от оценочных утверждений как факта).

2. **Правовое реагирование после публикации.** В этом случае юрист фиксирует все обстоятельства (ссылки, время, скриншоты, уведомления платформ), определяет правовую квалификацию претензий, готовит позицию редакции и рекомендует стратегию правовых действия для снижения риска привлечения к ответственности.

2.4.2. 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.

Юридическая помощь заключается в представительстве в суде по гражданско-правовым искам о защите чести, достоинства и деловой репутации или защите по административным и уголовным делам (на этапе предварительного следствия

и рассмотрения дела в суде). В делах этой категории дел, как правило, проводится судебная экспертиза текста публикации или видео и используются другие методы доказывания. Наличие морального вреда для физических лиц или убытков для юридических лиц вследствие публикации должно быть подтверждено надлежащими доказательствами, которые отвечают критериям допустимости, относимости и достоверности.

Вид нарушения	Применимые процедуры	Правовые последствия
Защита чести, достоинства и деловой репутации	Гражданско-правовой порядок через подачу иска в судебном порядке в соответствии со статьей 100 Гражданского кодекса Республики Узбекистан[26].	Публикация опровержения порочащих сведений, компенсация морального вреда, прекращение распространения.
Клевета	Административное дело по статье 40 Кодекса Узбекистана об административной ответственности (КоАО)[27]. Процедура в соответствии со статьей 139 УК РУз[28] (в том числе, если деяние совершено после применения административного взыскания; отдельно выделено распространение через СМИ, Интернет)	Административный штраф 20–60 БРВ. Меры ответственности в уголовном порядке. Штраф (в т. ч. до 200 БРВ; при публикации через СМИ или Интернет штраф составит 200–400 БРВ), обязательные работы или исправительные работы, возможно ограничение свободы; при квалифицирующих признаках могут быть применены более строгие санкции (в т. ч. штраф 300–500 БРВ или ограничение свободы до 3-х лет)
Оскорбление	Административный порядок в соответствии со статьей 41 КоАО[29]. При наличии оснований могут быть применены уголовно-правовые процедуры в соответствии со статьей 140 УК РУз (в т. ч. если совершено после применения административного взыскания; отдельно при распространение через СМИ или Интернет)[30]	Административный штраф составит от 20 до 40 БРВ. Меры уголовной ответственности: штраф до 200 БРВ; при публикации через СМИ или в сети 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.

2.4.3. 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. При этом известно, что чрезмерно широкие основания и меры уголовной

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

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

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

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

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

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.

В Узбекистане предусмотрены два вида ответственности за распространение ложной информации — административная и уголовная. Ниже в таблице мы указали правовые основания возникновения нарушений и меры ответственности, которые могут быть применены в случае распространения ложной информации.

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

Юридическая помощь по делам о распространении ложной информации, как правило, включает защиту и представительство интересов автора, блогера или редакции при привлечении к административной и уголовной ответственности, на всех этапах.

В делах данной категории ключевое значение имеют доказательства достоверности опубликованных сведений. Судом или органом досудебного расследования назначается экспертиза текста публикации, заголовков, комментариев, видеоматериалов и их фрагментов (включая подписи, превью, монтаж), анализируется контекст распространения, источники сведений и добросовестность проверки информации.

Стратегия защиты по такого рода делам включает оценку заявляемым последствиям публикации (например, ущерб репутации, дискредитация, угроза общественному порядку/безопасности). Такие последствия должны быть подтверждены надлежащими доказательствами, отвечающими критериям допустимости, относимости и достоверности. Отдельно оценивается причинно-следственная связь между публикацией и наступившими последствиями, а также наличие или отсутствие умысла и повторности (в случаях, когда уголовная ответственность связывается с привлечением к административной ответственности ранее за аналогичные действия).

---

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

[32] Там же

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

2.4.4. Hate speech

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

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

Отдельный смежный риск — «пропаганда войны» (ст. 150 Уголовного Кодекса Узбекистана)[35]. 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 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 аккаунты организации не становились каналом распространения запрещенных материалов.

С учетом сложности дел этой категории, юридическую помощь обычно оказывают адвокаты, и обычно такая помощь включает защиту и представительство интересов организации, журналиста, редактора, пользователя социальных сетей или блогера по уголовным делам (на стадии доследственной проверки/предварительного следствия и в суде.

В делах этой категории всегда назначается судебная экспертиза текста, заголовков, иллюстраций, видео и комментариев для оценки наличия признаков унижения достоинства, разжигания вражды, призывов или пропаганды. При этом важно документально подтверждать контекст публикации, добросовестность редакционной проверки, отсутствие умысла на разжигание, а также своевременную модерацию и удаление запрещенных комментариев и репостов, поскольку распространение материалов может оцениваться как самостоятельная зона ответственности.

2.4.5. Распространение правовых тайн

Еще одним правовым основанием для привлечения к ответственности может стать распространение в СМИ, социальных сетях, мессенджерах информации или сведений, которые образуют **правовые тайны.**

В законодательстве Узбекистана режимы «тайн» (информации ограниченного доступа) опираются, прежде всего, на конституционные гарантии неприкосновенности частной жизни и тайны переписки, телефонных переговоров, почтовых, электронных и иных сообщений, а также на защиту персональных данных; ограничение

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

[35] Там же

этих прав допускается только в предусмотренных законом случаях и, как правило, на основании судебного решения[36]. Дополнительно Закон Узбекистана «О принципах и гарантиях свободы информации» прямо запрещает сбор, хранение, обработку, распространение и использование сведений о частной жизни и сообщений без согласия лица (кроме случаев, установленных законодательством)[37], а Закон РУз «О персональных данных» закрепляет правила обработки и защиты персональных данных[38].

Посмотрите таблицу ниже, чтобы узнать, какие еще правовые тайны установлены действующим законодательством Узбекистана, помимо тайны частной жизни. К ним относятся также некоторые профессиональные тайны — сведения о них не разглашаются определенными категориями профессионалов (например, адвокаты, банковские работники, нотариусы и т. д. Указанный перечень не является полным и может быть дополнен при практической работе по предоставлению юридической помощи.

Наименование правовой тайны	Законодательный акт, которые регулирует объем сведений	Что входит в эту правовую тайну?
Коммерческая тайна 	Закон Республики Узбекистан «О коммерческой тайне»[39]	Информация, имеющая коммерческую ценность в научно-технической, технологической, производственной, финансово-экономической и других сферах в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании, и собственник этой информации принимает меры по защите ее конфиденциальности. Закон также определяет процедурные вопросы включения сведений в коммерческую тайну и порядок предоставления и защиты таких сведений.
Банковская тайна 	Закон «О банковской тайне»[40]	Банковской тайной являются защищаемые банком сведения: • об операциях, счетах и вкладах своих клиентов (корреспондентов); • о своем клиенте (корреспонденте), полученные банком в связи с оказанием ему банковских услуг; • о наличии, характере и стоимости имущества клиента (корреспондента), находящегося на хранении в сейфах и помещениях банка; • о межбанковских операциях и сделках, совершенных по поручению клиента (корреспондента) или в его пользу; • о клиенте (корреспонденте) другого банка, ставшие известными в результате обращения сведений, составляющих банковскую тайну, между банками; • об участниках накопительной пенсионной системы, размере и движении сумм пенсионных взносов, пенсионных накоплениях на индивидуальных накопительных пенсионных счетах граждан.

[36] Статья 31 Конституции Республики Узбекистан. Текст документа доступен по ссылке: https://lex.uz/docs/6445147#6445335

[37] Статья 13 Закона Республики Узбекистан «О принципах и гарантиях свободы информации». Текст закона доступен по ссылке: https://lex.uz/docs/52709

[38] Закон Республики Узбекистан «О персональных данных». Текст закона доступен по ссылке: https://lex.uz/docs/4396428

[39] Закон Республики Узбекистан «О коммерческой тайне». Текст документа доступен по ссылке: https://lex.uz/docs/2460799

[40] Закон Республики Узбекистан «О банковской тайне». Текст документа доступен по ссылке: https://www.lex.uz/acts/41882

Налоговая тайна 	Налоговый кодекс Республики Узбекистан	Налоговую тайну составляют полученные уполномоченными органами сведения о налогоплательщике, за исключением некоторых сведений, указанных в статье 29 Налогового кодекса РУз[41].
Врачебная тайна 	Закон Республики Узбекистан «Об охране здоровья граждан»[42]	Информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении.
Адвокатская тайна 	Закон РУз «Об адвокатуре»[43], Закон РУз «О гарантиях адвокатской деятельности и социальной защите адвокатов»[44]	Предметом адвокатской тайны является сам факт обращения доверителя (подзащитного) к помощи адвоката, вопросы, по которым доверитель (подзащитный) обратился за помощью, суть консультаций, советов и разъяснений, полученных доверителем (подзащитным) от адвоката, все иные сведения, касающиеся содержания бесед адвоката с доверителем (подзащитным).
Тайна усыновления 	Семейный кодекс Республики Узбекистан[45]	Тайна усыновления охраняется законом. Воспрещается без согласия усыновителей, а в случае их смерти — без согласия органа опеки и попечительства ознакомление с содержанием книг регистрации актов гражданского состояния или иных документов, выдача из них выписок или иных сведений, из которых было бы видно, что усыновители не являются родителями усыновленного. Лица, разгласившие тайну усыновления против воли усыновителя или органа опеки и попечительства, несут установленную законом ответственность.
Тайна совещания судей 	Уголовно-процессуальный кодекс РУз[46]	Судья постановляет приговор в отдельной, а суд — в совещательной комнате. В этих комнатах могут находиться лишь судьи, входящие в состав суда по данному делу. Присутствие иных лиц не допускается.
Тайна нотариальных действий 	Закон РУз «О нотариате»[47]	Нотариусу, другим должностным лицам, совершающим нотариальные действия, а также лицам, которым о совершаемых нотариальных действиях стало известно в связи с выполнением ими служебных обязанностей, запрещается разглашать ставшие известными им сведения, в том числе и после прекращения трудового договора.

[41] Статья 29 Налогового кодекса Республики Узбекистан. Текст документа доступен по ссылке: https://buxgalter.uz/doc?id=610082_nalogovyy_kodeks_respubliki_uzbekistan_(utverjden_zakonom_ruz_ot_30_12_2019_g_n_zru-599)&prodid=1_vse_zakonodatelstvo_uzbekistana#%D1%81%D1%8229

[42] Статья 45 Закона Республики Узбекистан «Об охране здоровья граждан». Текст закона доступен по ссылке: https://lex.uz/docs/41329?ONDATE=31.05.2024%2000#41781

[43] Статья 9 Закона Республики Узбекистан «Об адвокатуре». Текст закона доступен по ссылке: https://www.lex.uz/acts/58372

[44] Закон Республики Узбекистан «О гарантиях адвокатской деятельности и социальной защите адвокатов». Текст закона доступен по ссылке: https://lex.uz/docs/1321

[45] Статья 153 Семейного кодекса Республики Узбекистан. Текст кодекса доступен по ссылке: https://lex.uz/docs/104723#161584

[46] Статья 456 Уголовно-процессуального кодекса Республики Узбекистан. Текст кодекса доступен по ссылке: https://lex.uz/docs/111463#249950

[47] Статья 6 Закона Республики Узбекистан «О нотариате». Текст закона доступен по ссылке: https://lex.uz/docs/57043#3992406

Соблюдение процедур по сохранению правовых тайн важны потому, что риски возникают не только при распространении таких сведений, но и при перепечатке документов, цитировании переписок, публикации финансовых и налоговых сведений без надлежащих правовых оснований.

Круг юридической помощи по таким делам обычно включает правовую экспертизу материалов и документов до публикации и раскрытия (правовое основание, согласие, минимизация данных) и защиту по административным и уголовным делам на стадии проверки, предварительного следствия и в суде. В делах этой категории часто назначаются судебные экспертизы, а ключевые элементы позиции строятся на надлежащих доказательствах: допустимость, относимость, достоверность, причинно-следственная связь и подтверждение вреда или убытков документально.

2.4.6. Незаконное распространение персональных данных

В Узбекистане незаконное распространение персональных данных в первую очередь регулируется Законом Республики Узбекистан «О персональных данных»[48]. Под распространением персональных данных понимается раскрытие персональных данных неопределенному кругу лиц, включая обнародование в СМИ, размещение в Интернете или предоставление доступа любым иным способом[49]. При этом собственник/оператор и любые лица, получившие доступ к персональным данным, обязаны не раскрывать и не распространять их без согласия субъекта, а работники, которые обрабатывают такие данные, обязаны не допускать разглашения доверенных или ставших им известными данных.

Ответственность за незаконные действия с персональными данными предусмотрена как административная, так и уголовная. Административная ответственность наступает за незаконный сбор, хранение, использование, предоставление, распространение и передачу, в том числе трансграничную, персональных данных. Меры ответственности — административный штраф для граждан 7 БРВ, для должностных лиц — 50 БРВ[50].

Уголовная ответственность наступает за те же деяния, совершенные после применения административного взыскания, и влечет штраф 100–150 БРВ (либо иные меры), а при квалифицирующих признаках (группа, повторность, корыстный мотив, использование служебного положения, тяжкие последствия) — более строгие санкции вплоть до ограничения свободы или лишения свободы[51].

С практической точки зрения ключевой вопрос по законности распространения персональных данных почти всегда сводится к правовому основанию обработки или публикации и доказуемости согласия. Юридическая помощь по делам о незаконном распространении персональных данных обычно включает:

- правовую оценку законного основания действия с персональными данными — было ли получено согласие, законно ли были распространены персональные данные, повлекли ли они ущерб, есть ли связь между этими событиями и т. д.;

---

[48] Закон Республики Узбекистан «О персональных данных». Текст закона доступен по ссылке: https://lex.uz/docs/4396428#4397998

[49] Статья 14. Там же

[50] Статья 46 Кодекса Республики Узбекистан об административной ответственности. Текст кодекса доступен по ссылке: https://www.lex.uz/acts/97661

[51] Статья 141 Уголовного кодекса Республики Узбекистан. Текст кодекса доступен по ссылке: https://www.lex.uz/acts/111457

- сопровождение взаимодействия с заявителями и государственными органами (подача ходатайств, объяснений, жалоб);
- защиту по административным и уголовным делам на стадии проверки, предварительного следствия и в суде.

В таких спорах ключевую роль играют доказательства, а именно:

- факт и способ распространения (скриншоты, логи, ссылки, дата и время);
- объем данных и их идентифицируемость, наличие или отсутствие согласия и его форма;
- иные допустимые, относимые и достоверные доказательства.

2.4.7. Ответственность за комментарии в аккаунтах медиа

Теперь более подробно остановимся на вопросе ответственности 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 владельцем аккаунта, под публикацией которого они были оставлены.

За содержание комментария несет ответственность сам автор комментария, однако владельцы и администраторы цифровых информационных ресурсов (веб-сайтов, страниц, каналов и аккаунтов в социальных сетях) обязаны не допускать использования веб-сайтов, блогов для размещения запрещенной информации, что прямо закреплено в Законе «Об информатизации»[52]. Поэтому отсутствие модерации и игнорирование обращений повышают риски для владельцев аккаунта.

Где проходит грань ответственности между автором комментария и владельцем аккаунта в соцсети или веб-сайта? Риски 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, можно предпринять следующие шаги:

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

---

[52] 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) владельцев и администраторов цифровых информационных ресурсов по разделению ответственности за возможные проблемные комментарии. Вот обязательный минимум, который необходимо включить в эти правила:

- правила комментирования для пользователей применяются ко всем комментариям на веб-сайте и в аккаунтах 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;
- владелец аккаунта вправе удалять комментарии, нарушающие правила, и блокировать пользователей;
- владелец аккаунта рассматривает обращения о нарушениях и принимает меры, включая удаление и ограничение доступа.

Кроме Правил комментирования рекомендуется 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 ре-публиковать проблемные комментарии как «позицию аудитории». Любое выделение комментария редакцией рассматривается как дополнительный фактор ответственности.

Юридическая помощь по вопросам ответственности за комментарии, как правило, включает защиту и представительство владельцев и администраторов паблика по гражданским спорам, в том числе о защите чести, достоинства и деловой репутации, и по административным или уголовным делам, если претензии связаны с противоправным контентом в комментариях, — оскорблением, клеветой или распространением ложной информации.

В таких делах в качестве доказательства фиксируется ссылка на комментарий, дата и время, данные аккаунта (если доступны), поступившие жалобы и действия модерации (скрытие, удаление или блокировка). При необходимости проводится экспертиза текста комментария и контекста публикации.

2.4.8. Правила онлайн-платформ по контенту

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

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

- hate speech (язык ненависти): дегуманизация, унижение, призывы к дискриминации или насилию), как указано выше;
- опасный контент и призывы к насилию, экстремистский и террористический контент;
- дезинформация в чувствительных темах (здоровье, безопасность, кризисы);
- травля, домогательства или угрозы;
- персональные данные и публикации, которые нарушают приватность.

Политики онлайн-платформ:

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

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

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

Telegram
https://telegram.org/moderation

Практический вывод — ориентируйтесь в своей 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.

2.4.9. Как осуществляется контроль за контентом в цифровой среде?

Для юристов будет полезно знать, как осуществляется контроль за контентом в цифровой среде не только в Узбекистане, но в других странах Центральной Азии. Такой контроль осуществляют (1) сами онлайн-платформы, (2) аудитория и (3) государственные органы/уполномоченные структуры.

Обратите внимание на то, что эти каналы действуют параллельно. Это значит, что один и тот же пост или комментарий может одновременно нарушать правила платформы, затрагивать права конкретного лица и подпадать под ограничения национального законодательства.

Во-первых, онлайн-платформы применяют собственные стандарты и процедуры выявления запрещенного контента (язык вражды, призывы к насилию, порнография, незаконная торговля и т. п.) — через автоматические фильтры и модерацию. Последствия чаще всего — это удаление, ограничение охвата, предупреждения («страйки»), временные блокировки, отключение монетизации. Для редакций и авторов это означает необходимость заранее оценивать риски по правилам площадки, сохранять доказательства добросовестности (источники, фактчекинг) и использовать процедуры обжалования решений платформы.

Во-вторых, аудитория может отправлять жалобы в администрацию онлайн-платформ и в госорганы, полицию, прокуратуру. На практике поток жалоб становится самостоятельным механизмом давления, поэтому юридически грамотная модель — иметь понятные правила комментирования, канал приема обращений и фиксацию реакции (что именно удалено или скрыто, когда и на каком основании).

В-третьих, государственные органы или уполномоченные организации могут проводить мониторинг публичного контента в социальных сетях и на веб-сайтах на предмет материалов, запрещенных национальным законодательством, и инициировать меры реагирования в пределах своих полномочий (включая требование удалить контент, ограничение доступа, процессуальные проверки).

Такая трехуровневая система контроля и мониторинга контента в цифровой среде означает, что правовой риск для редакции или автора складывается сразу из трех источников: (1) действий, политики и решения платформы, (2) жалоб аудитории и (3) действий и решений уполномоченных государственных органов. Поэтому юристу важно оценивать материал одновременно по правилам площадки, по рискам частных претензий (диффамация, персональные данные, оскорбления, авторские права) и по ограничениям национального законодательства Республики Узбекистан.

2.5. Защита авторских прав в цифровой среде

Пользователи Интернета, журналисты и медиа постоянно создают контент, а также работают с чужим контентом (тексты, фото, видео, музыка, инфографика, дизайн). 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 Интернет является «доведением до всеобщего сведения» — когда пользователи могут получить доступ «из любого места и в любое время по собственному выбору». Данное действие относится к исключительным правам автора или правообладателя (то есть требует разрешения/лицензии), наряду с воспроизведением и распространением.

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

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

В соответствие со статьей 5 Закона РУз «Об авторском праве и смежных правах», «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) произведений 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.

2.5.1. Правила использования чужих произведений

Широкое распространение контента в сети Интернет, социальных сетях, мессенджерах и на веб-сайтах позволяет получать доступ к чужому контенту, который может 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 ре-публикации 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».

Только материалы, представляющие результат творческой деятельности (фото- и видеорепортажи, аналитические или обзорные статьи, журналистские расследования, интервью) являются 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.

Смежные права, которые предоставляются исполнителям, производителям фонограмм и организациям эфирного или кабельного вещания, также охраняются в Интернете. Например, фонограммы, записи музыкальных произведений, трансляции и записи концертов и живых исполнений.

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

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.

2.5.2. Способы защиты авторских прав

Если автор или правообладатель считает, что нарушены его авторские права, для их защиты он вправе обратиться (желательно письменно) к нарушителю с требованием 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, правообладатель вправе требовать возмещения наряду с другими убытками упущенной выгоды в размере не меньшем, чем эти доходы;
- выплаты компенсации в размере от 20 до 1 000 базовых расчетных величин вместо возмещения убытков, выплачиваемой независимо от факта причинения убытка, исходя из характера нарушения и степени вины нарушителя, с учетом обычаев делового оборота.

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

Виды ответственности	Когда применяется	Меры ответственности
Статья 177[1] 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** либо 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[1]. 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

2.5.3. Механизмы ограничения использования объектов авторских прав в цифровой среде

Закон Республики Узбекистан «Об информатизации» запрещает использование объектов интеллектуальной собственности, принадлежащих другим лицам. Владельцы веб-сайта и (или) страницы веб-сайта либо иного информационного ресурса, в том числе блогеры, обязаны не допускать использования на своих веб-сайтах и (или) страницах веб-сайтов либо ином информационном ресурсе 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 г. (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 течении 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.

Механизмы защиты авторских прав в социальных сетях и на 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 нарушение 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.

2.6. Важные документы и политики для компаний

Политика использования конфиденциальных материалов — это внутренний документ компании, который устанавливает понятные правила обращения с информацией, не предназначенной для свободного распространения. Такая политика защищает интересы компании, клиентов, партнеров и сотрудников, а также снижает риски утечек, злоупотреблений и конфликтов. С точки зрения цифровых прав важно, чтобы защита конфиденциальности не превращалась в чрезмерный контроль и не нарушала право на частную жизнь, свободу выражения и справедливую процедуру рассмотрения спорных ситуаций.

Политика должна ясно объяснять, что считается конфиденциальными материалами и какие категории информации существуют. Обычно выделяют:

- персональные данные (клиентов, сотрудников, кандидатов);
- коммерческую тайну и внутреннюю стратегическую информацию;
- техническую информацию (исходный код, архитектура систем, модели, алгоритмы);
- материалы партнеров и подрядчиков, переданные по договору;
- служебные документы, которые ограничены для внутреннего использования.

Практически важно вводить классификацию по уровням доступа (например: публичная, внутренняя, конфиденциальная, строго ограниченная) и приводить примеры. Это снижает произвольность и помогает сотрудникам понимать, как действовать в повседневной работе. С точки зрения цифровых прав важно разграничить корпоративные и личные данные: меры защиты должны быть направлены на безопасность рабочих материалов и не превращаться в неконтролируемый доступ к личной информации сотрудника.

Политика должна опираться на базовые принципы, которые одновременно усиливают безопасность и защищают права человека:

- **Минимизация доступа:** доступ получают только те, кому информация необходима для выполнения рабочих задач.
- **Прозрачность:** сотрудники заранее информируются о правилах доступа, хранения и контроля.
- **Пропорциональность:** меры безопасности и мониторинга должны соответствовать реальным рискам и не быть чрезмерными.
- **Подотчетность:** должно быть понятно, кто отвечает за решение, доступ и контроль (ответственные лица и подразделения);
- **Справедливая процедура:** при подозрении на нарушение компания обязана соблюдать понятный порядок проверки и рассмотрения обстоятельств, без произвольных решений.

Современные риски связаны с использованием публичных ИИ-сервисов и чат-ботов. Политика должна отдельно закреплять:

- запрет на ввод конфиденциальной информации и персональных данных в публичные ИИ-инструменты без разрешения и оценки рисков;
- использование только тех сервисов, с которыми у компании есть договорные гарантии конфиденциальности и защиты данных;
- необходимость обезличивания информации при подготовке запросов и примеров.

Политика по комментированию в социальных сетях — это внутренние правила компании (или организации), которые определяют, как администраторы страниц и модераторы реагируют на комментарии пользователей, какие материалы допускаются, а какие могут быть ограничены. Такая политика особенно важна с точки зрения цифровых прав, потому что затрагивает свободу выражения, доступ к информации, защиту персональных данных и справедливую процедуру модерации.

Политика должна прямо обозначать, зачем она нужна. Обычно цели включают:

- обеспечение безопасного и уважительного общения;
- предотвращение языка вражды и насилия;
- защита пользователей от травли и дискриминации;
- соблюдение законодательства и правил платформ;
- сохранение пространства для критики и общественной дискуссии.

Важно подчеркнуть, что модерация не должна использоваться для подавления неудобных мнений или удаления критики о деятельности организации.

Политика должна устанавливать этические стандарты:

- недопустимы унижающие формулировки, «шок-контент», давление на эмоции через стигматизацию;
- использование фото/видео получателей помощи — только при их согласии и с пониманием последствий публикации;
- корректное обращение к темам инвалидности, насилия, бедности и освещение других чувствительных вопросов;
- уважение к различным языкам аудитории и недискриминационные формулировки.

Политика по проведению благотворительных акций онлайн или в социальных медиа

Онлайн-благотворительность — это сбор средств или ресурсов через Интернет и социальные сети. Такие кампании повышают доверие к организации, но при неправильной организации создают риски мошенничества, нарушения прав доноров и получателей помощи, а также утечки персональных данных. Политика нужна, чтобы обеспечить прозрачность, безопасность и уважение прав всех участников.

В политике следует определить:

- какие форматы поддерживаются (донаты, краудфандинг, сбор вещей, сбор услуг, волонтерство);
- какие площадки используются (официальный веб-сайт, соцсети, платежные сервисы);
- кто может инициировать кампанию (только организация/уполномоченные лица).

Рекомендуемые принципы:

- Прозрачность: ясная цель, сроки, сумма/потребность, способ расходования.
- Подотчетность: отчетность по итогам, подтверждение платежей и расходов.
- Безопасность: защита платежей, предотвращение фишинга и подмены реквизитов.
- Минимизация данных: сбор только тех персональных данных, которые действительно нужны.
- Уважение достоинства: этичная коммуникация о получателях помощи без унижения и сенсационности.

Перед стартом кампании рекомендуется публиковать:

- организатора и ответственных лиц;
- цель сбора и критерии, как будет оказана помощь;
- сроки кампании и механизм остановки (если сумма достигнута);

- официальные реквизиты/ссылки на платежный сервис;
- порядок отчетности (когда и где будет опубликована);
- контакты для вопросов и жалоб.

Это снижает риск злоупотреблений и повышает доверие аудитории.

Политика должна закреплять меры защиты:

- использовать только официальные платежные каналы;
- запрет на публикацию «частных карт сотрудников», если это не предусмотрено и не контролируется;
- двухфакторная защита аккаунтов, где размещаются объявления;
- правила реагирования на попытки подмены реквизитов;
- предупреждение подписчиков о типовых схемах мошенничества (поддельные аккаунты, похожие ссылки).

Персональные данные доноров и получателей помощи

С точки зрения цифровых прав, ключевой блок — защита данных и достоинства:

- доноры должны понимать, какие данные собираются (например, имя, контакт для подтверждения), и зачем;
- публикация списка доноров возможна только при согласии (опция «анонимно» должна быть доступна);
- данные получателей помощи (особенно детей и уязвимых групп) нельзя раскрывать без необходимости и без законного основания/согласия;
- запрещается публиковать документы, диагнозы, адреса, точную геолокацию и иные сведения, которые создают риск для человека.

При работе с чувствительными случаями лучше использовать обезличивание: общие описания, закрытые лица, исключение деталей, позволяющих прямо или косвенно идентифицировать человека.

Итоговый отчет по онлайн-благотворительной кампании должен содержать сведения о собранной сумме (или объеме помощи), ключевых расходах и подтверждающих документах с соблюдением требований по защите персональных данных, описании достигнутого результата (кому и как оказана помощь без излишней идентификации), а также заранее определенное правило обращения с остатком средств — перенос, возврат или иное целевое использование.

Раздел 3
Угрозы для юристов и адвокатов 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 юридического сообщества. 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 деятельности помешать.

Для юристов и адвокатов понимание ландшафта цифровых угроз перестало быть просто вопросом «для информации». Теперь это вопрос сохранения адвокатской тайны, репутации и свободы клиентов. 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, затрагивающими 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** (путей, посредством которых могут быть реализованы угрозы) и четкого представления своих цифровых ресурсов и их уязвимостей. Именно на фундаменте этих знаний формируется устойчивый **профиль безопасности** (security posture) организации — состояние, при котором обеспечение безопасности становится не разовым действием, а непрерывным процессом.

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

К примеру:

Психологическое давление

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

Выгоревший сотрудник

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

Взлом цифровых ресурсов

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

Утечка данных

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

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

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

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

- **Сбор данных и разведка (OSINT) — не является прямой угрозой,** но часто бывает начальным этапом для целенаправленной атаки, включающий анализ публично доступной информации для выявления разного рода уязвимостей, от технических до психосоциальных.
- **Заражение вредоносным ПО (шпионское ПО, вирусы-шифровальщики) — наиболее распространенная киберугроза,** которая включает в себя как массовые вирусы, которые, к примеру, шифруют данные и требуют выкуп, так

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

- **Взлом цифровых аккаунтов — объединяет все виды несанкционированного доступа** (к почте, соцсетям, мессенджерам, финансовым аккаунтам). В основном происходит за счет **фишинга, приемов** социальной инженерии, утечки 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 угроза при работе из публичных мест** (кафе, аэропорты) Wi-Fi точкой, которую вы не контролируете. При этом злоумышленник может перехватывать незашифрованный трафик, включая логины и пароли. Эта же угроза применима к посещению веб-сайтов не использующих шифрование (http протокол), о чем обычно предупреждает браузер и некоторые антивирусы.

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

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

2. Психосоциальные угрозы — угрозы, направленные на личность юриста, 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 юриста или его клиентов.

- **Сексторшн, порноместь, секспионаж — шантаж интимными материалами** (как реальными, так и сфабрикованными с помощью ИИ) угроза, применяемая как против адвокатов, так и направленная на компрометацию их клиентов.

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 биометрии, 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 вебсайтов-клонов, перехват пожертвований, так и косвенное как искусственное создание конкурирующих проектов (GONGO), 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 юридической практики 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. Уголовное преследование или дисциплинарные взыскания часто становятся возможными при отсутствии выверенной политики коммуникаций и несоблюдении норм профессиональной этики.

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

3.2. Меры по безопасности юристов и адвокатов

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 юридических организаций и отдельных адвокатов.

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, Google-уведомления), а в некоторых ее нужно включать вручную. Тем не менее, необходимо убедиться не только в том, что во всех сервисах она включена, но и 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: в WhatsApp — двухшаговая проверка, в Telegram — облачный пароль, в Signal — блокировка регистрации. Эти настройки предотвращают возможность взлома мессенджера путем перехвата регистрационного SMS-сообщения или подмены SIM-карты.

- **Настройка резервного копирование (бэкапы)** — критически важный компонент безопасности данных, хранящихся на локальных устройствах, от таких угроз, как аппаратные сбои, атаки вредоносного ПО (в частности, программ-шифровальщиков) и физическая утеря или изъятие оборудования. Ключевым принципом эффективного резервного копирования является его автоматизация. Системы, полагающиеся на ручное копирование файлов пользователем, обладают низкой надежностью из-за наличия человеческого фактора. Существуют два основных подхода к реализации автоматизированного резервного копирования: локальное резервное копирование с использованием внешних носителей и облачное резервное копирование и синхронизация. Для локального резервного копирования используются внешние носители информации (жесткие диски, SSD-накопители...). Для автоматизации этого процесса можно использовать встроенные средства операционной системы. В Microsoft Windows эту функцию выполняет инструмент «История файлов» (File History), который позволяет настроить периодическое копирование файлов из пользовательских папок на указанный внешний диск. В Apple Mac OS аналогичную функциональность предоставляет система Time Machine, которая создает инкрементальные снимки всей системы, позволяя восстановить как отдельные файлы, так и операционную систему целиком на определенный момент времени. Для облачного резервного копирования используются облачные сервисы, такие как Google Drive, Microsoft OneDrive, Dropbox и другие. Большинство современных облачных сервисов работают по принципу автоматической синхронизации, когда устанавливается локальное приложение, которое создает на локальном диске специальную папку, и любые файлы, помещенные в эту папку, автоматически копируются в облачное хранилище и синхронизируются между всеми подключенными устройствами. Для организаций, работающих с особо чувствительной информацией, рекомендуется рассмотреть специализированные облачные сервисы, предлагающие сквозное (end-to-end) шифрование. В таких системах (например, Proton Drive, Sync.com, Tresorit, Mega.io) данные шифруются на устройстве пользователя перед отправкой на сервер, что делает их недоступными даже для сотрудников самого сервиса, обеспечивая максимальный уровень конфиденциальности. В мобильных данных синхронизация идет, как правило, на привязанных аккаунтах (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 этого необходимо ввести два понятия 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. Предназначен для отдельных адвокатов и небольших команд, цель которого превратить единичные индивидуальные практики в общую дисциплину и культуру безопасности.

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

Постараться по максимуму использовать только лицензионное программное обеспечение. Для адвокатских практик доступны стандартные коммерческие продукты: Microsoft 365 Business и Google Workspace Business, которые предоставляют весь необходимый набор инструментов, включая корпоративную почту, облачное хранение и офисные приложения. Для адвокатов, работающих в составе НКО или занимающихся правозащитой, могут быть доступны льготные программы — в частности, Techsoup и программы Microsoft и Google для некоммерческих организаций.

Необходимо обеспечить полнодисковое шифрование: для Windows — Bitlocker, для MacOS — 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.

Провести внутренний инструктаж о ключевых «красных линиях» в законодательстве, касающихся цифровой деятельности адвоката: требования к хранению адвокатской тайны в электронном виде, законодательство о персональных данных, риски уголовного преследования за публикации в Интернете.

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 Wi-Fi-точек. Наконец, это постоянная мотивация развития критического мышления: проверка подозрительных запросов и открытое обсуждение в команде любых подозрительных сообщений, угроз, создавая благоприятную атмосферу взаимодействия. Также важно постоянно отслеживать новости об изменениях в законодательстве, касающиеся деятельности адвокатских образований и адвокатской тайны.

Уровень 2:
Внедрение формализованных организационных процессов. Предназначен для адвокатских бюро, коллегий и юридических фирм, 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. Предназначен 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 для мест проживания ключевых сотрудников. Так же должна быть определена формальная роль ответственного за безопасность и установлены контакты с внешними экспертами (юристы, IT-специалисты) 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 онлайн-ресурсов адвокатских образований

В эпоху цифровой трансформации веб-сайты и онлайн-платформы адвокатских образований стали важной частью их публичного присутствия и коммуникации с клиентами. Это делает их уязвимыми перед кибератаками. Особенно уязвимы адвокаты, занимающиеся резонансными делами, правозащитники и юристы, представляющие интересы активистов или оппозиции, — они могут являться целями как для преступников, так и для государственных субъектов.

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

Компрометация ресурса (взлом)

Эта категория включает все инциденты, когда посторонние лица получают несанкционированный доступ к «внутренностям» вашего веб-сайта — его системе управления, серверу или аккаунтам администраторов. Последствия такого проникновения могут быть разными, в зависимости от целей злоумышленника. Иногда это публичный вандализм (дефейс), когда на главной странице размещается чужое сообщение. В более сложных случаях — это скрытая подмена информации, когда на веб-сайте незаметно меняют цифры или факты, чтобы подорвать 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. Так же 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, 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, блокировки ресурса в стране или отзыва доменного имени. Так же это может делаться через юридическое преследование, когда публикации на веб-сайте или комментарии становятся основанием для возбуждения дел против организации.

Атаки на идентичность и доверие

Эта категория объединяет угрозы, направленные не на ваш ресурс как таковой, а на 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 клиентов и других организаций.

Для адвокатских образований оптимальным выбором являются коммерческие хостинг-провайдеры с юрисдикцией вне страны деятельности, строгой политикой конфиденциальности и поддержкой 2FA. Для адвокатов, занимающихся правозащитой или представляющих активистов и гражданское общество, могут быть доступны специализированные сервисы защищенного хостинга: VirtualRoad.org (https://www.qurium.org/) и eQualitie (https://deflect.ca/), предоставляющие защиту организациям из группы риска, а Project Galileo от Cloudflare (https://www.cloudflare.com/galileo/) — бесплатную защиту от DDoS. Использование Azure (Microsoft) возможно, но потребует технического специалиста для настройки.

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

Своевременное обновление программного обеспечения — большое количество взломов веб-ресурсов происходит из-за необновленного программного обеспечения — как правило, это система управления контентом (CMS), дополнительные модули (плагины) и платформа, на которой написан веб-сайт. Часто разработчики веб-сайтов подходят к своей задаче «спустя рукава» и не ориентируются на безопасность, в результате клиент получает необновляемые или уязвимые темы, плагины или, в случае «самописных» систем, полностью уязвимую и неподдерживаемую систему. В самых популярных системах, таких как WordPress, Drupal, Joomla существуют встроенные системы автообновления, которые автоматически обновляют компоненты системы. Это хорошо и правильно с точки зрения безопасности, но нужно иметь 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 восстановление из резервной копии. Если точно не известно, когда был произведен взлом, то, возможно, необходимо будет восстановление из более ранней версии. Удостоверьтесь, что хостинг-провайдер делает регулярные копии и хранит их версии. Если в организации есть технический специалист, частью его обязанностей должно быть резервное копирование и хранение их версий. Частота резервного копирования зависит от частоты обновления ресурса, как правило, вы должны задать себе вопрос — как часто должна делаться копия, чтобы восстановление заняло минимально возможные время и усилия?

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

Меры противодействия DDoS-атакам

В настоящее время DDoS-атаки могут достигать огромных величин, сравнимых с потреблением Интернета небольшой страны. Одна из наиболее значимых зафиксированных атак произошла в 2025 и составила 29,7 Тбит/с. Это примерно, как в секунду скачать с веб-сайта примерно 7 000 фильмов в HD-качестве. В атаке, предположительно, участвовало более 1 млн зараженных устройств. Справиться с подобными атаками, даже меньшей мощности, не имея огромных ресурсов, практически невозможно, поэтому наиболее эффективный способ — использование специализированных сервисов-посредников, которые принимают удар на себя. Для адвокатских образований наиболее практичным решением является подключение к Cloudflare (платный тариф) или Project Galileo — для тех, кто занимается правозащитой. VirtualRoad.org и eQualitie также доступны для организаций гражданского общества и их юридических партнеров.

Меры противодействия юридическому и административному давлению

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

В первую очередь к этому относится минимизация наличия ресурсов внутри страны, таких как хостинг ресурса внутри страны и доменное имя в страновой зоне. При использовании административного давления на хостинг-провайдера

или администратора доменной зоны ваш ресурс может быть выключен или удален, а доменное имя разделегировано (изъято). Чтобы этого не произошло, позаботьтесь о надежном хостинге за пределами страны и используйте общее доменное имя (к примеру, .org, .info, .ngo). Так же предусмотрите наличие веб-сайтов-зеркал и использование сетей распределения контента (CDN), таких как Cloudflare или Akamai. И не забывайте про резервное копирование.

Меры противодействия атакам на идентичность и доверие

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

Расследование инцидентов и реагирование на угрозы

Когда происходит инцидент безопасности, будь то взлом веб-сайта, угроза 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 в будущем минимизировать или вероятность инцидента, или его последствия, и восстановиться быстрее.

Обнаружение, первая реакция и документирование

Необходимо без промедления обратиться за внешней экспертной помощью к специалистам по цифровой безопасности. Адвокатам, занимающимся правозащитой или представляющим активистов и гражданское общество, доступна помощь Access Now Digital Security Helpline (help@accessnow.org, https://www.accessnow.org/). Эта организация специализируется на поддержке группы риска и взаимодействии

с платформами. Коммерческим адвокатским практикам следует заблаговременно установить контракт с профессиональным IT-партнером или MSSP (Managed Security Service Provider), который сможет оперативно подключиться в случае инцидента.

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 неоднозначным и для адвокатов. 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, доверителях и стратегии защиты.

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

Заключение

Цифровая среда стала неотъемлемой частью деятельности юристов и адвокатов. 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 адвоката. Доступ Защита персональных данных клиентов, соблюдение адвокатской тайны в цифровой среде, 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. Адвокаты работают в среде, где одновременно действуют национальное законодательство, профессиональные стандарты адвокатуры 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 о клиентах, ведение дел, взаимодействие с доверителями и партнерами — все это связано с потенциальными угрозами, которые могут затрагивать как саму практику, так и ее доверителей. В этих условиях важно выстраивать внутренние политики, процедуры и практики, направленные на защиту данных, соблюдение адвокатской тайны 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.

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

Приложения

Приложение 1

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

Источник: https://www.itts.uz/

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

7	Как фиксируется согласие субъекта на обработку ПДн? Хранятся ли дата/время/ID устройства/ IP-адрес, с которого давалось согласие?	ст. 21 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398514
8	Если ли возможность отзыва согласия в той же форме, в которой оно давалось? Есть ли возможность направить отзыв согласия в виде электронного документа?		
9	Обрабатываются ли персональные данные умерших субъектов? Кем дано согласие на такую обработку? (согласие, данное при жизни, согласие законных наследников)		
10	Какое подразделение занимается предоставлением данных об обработке ПДн по запросам субъектов?	ст. 22 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398536
11	Определен ли порядок блокировки и уничтожения персональных данных на основании обращения субъекта персональных данных?	п. 30.13 Приказа Минюста № 3478 от 15.11.2023 г.	https://lex.uz/docs/6663967#6664487
12	Произведено ли разделение баз, если обработка ПДн в них осуществляется с несовместимыми между собой целями?	п. 5 Приказа Минюста № 3478 от 15.11.2023 г.	https://lex.uz/docs/6663967#6664304
13	Как производится уведомление субъекта о включении его ПДн в базу ПДн?	ст. 23 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398628
14	Как производится уведомление субъекта при передаче его ПДн третьим лицам?		
15	Сформирован ли перечень третьих лиц? Кто и как его актуализирует?		
16	Осуществляется ли на предприятии полностью автоматизированная обработка ПДн, например, скоринг?	ст. 24 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398652
17	Как получается согласие субъекта на полностью автоматизированную обработку его ПДн? Каковы правовые основания такой обработки?		
18	Производится ли обработка специальных (сведения о здоровье, составе семьи, национальности) ПДн?* *Обработка специальных персональных данных запрещается, за исключением ограниченного числа случаев	ст. 25 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398682

19	Производится ли на предприятии обработка биометрических ПДн (фотографии, отпечатки пальцев и др.)?	ст. 26 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398727
20	Каковы правовые основания такой обработки? Давал ли субъект/работник согласие на такую обработку?		
21	Есть ли на предприятии биометрическая СКУД (система контроля и управления доступом)? Зарегистрирована ли его база в госреестре баз ПДн? Получены ли письменные согласия всех включенных в базу СКУД?		
22	Как осуществляется учет материальных носителей, содержащих биометрические/генетические данные?	п. 5 Приложения № 2 к ПКМ РУз № 570 от 05.10.2022 г.	https://lex.uz/ru/docs/6225462#6227477
23	Как именно реализовано требование о шифровании и криптографической защите биометрических данные?	п. 4 Приложения № 2 к ПКМ РУз № 570 от 05.10.2022 г.	https://lex.uz/ru/docs/6225462#6227475
24	Проставлены ли грифы на носителях биометрических данных? Какие конкретно обязательные меры применяются для обеспечения физической безопасности носителей? Фиксируются ли IP и MAC-адреса устройств, получающих доступ к биометрическим данным?	гл. 2 Приложения № 2 к ПКМ РУз № 570 от 05.10.2022 г.	https://lex.uz/ru/docs/6225462#6227469
25	Где и как обрабатываются ПДн граждан Узбекистана? Где физически расположено оборудование, на котором осуществляется обработка?	ст. 27.1 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#5271076
26	Осуществляется ли передача ПДн на территорию других стран (трансграничная передача)? На территорию каких стран?	ст. 15 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398348
27	Утвержденный состав персональных данных, необходимый и достаточный для выполнения задач предприятия?	ст. 31 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398788
28	Определено ли структурное подразделение или должностное лицо, ответственное за работу, связанную с обработкой и защитой персональных данных?		

29	Определены ли сроки обработки персональных данных (по каждой категории, по каждой базе)? Каковы эти сроки?	ст. 10 и 19 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398106
30	Проводятся ли на предприятии исторические, статистические, социологические или научные исследования с персональными данными? Производится ли при этом обязательное обезличивание этих персональных данных?	ст. 16 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398378
31	Производится ли уничтожение персональных данных? Кем? Как? Какой документ это регулирует?	ст. 17 Закона РУз «О персональных данных»	https://lex.uz/docs/4396428#4398388
32	Определены ли типы угроз, актуальные для каждой базы ПДн? Присвоены ли каждой базе уровни защищенности?	п. 2 ПКМ РУз № 570 от 05.10.2022 г.	https://lex.uz/uz/docs/6225462#6227189
33	Выполняются ли требования ИБ для каждой из баз ПДн на основании присвоенного им уровня защищенности? Какие именно меры применимы к конкретной базе?	гл. 10 ПКМ РУз № 570 от 05.10.2022 г.	https://lex.uz/uz/docs/6225462#6227279
34	Подчиняется ли подразделение, ответственное за обеспечение защиты персональных данных, непосредственно руководителю предприятия?	п. 3 Приказа Минюста № 3477 от 15 ноября 2023 г.	https://lex.uz/docs/6663969#6668986
35	Проводятся ли периодические проверки базы персональных данных? Когда в последний раз проверялась актуальность регистрационных данных?	п. 8 Приказа Минюста № 3477 от 15 ноября 2023 г.	https://lex.uz/docs/6663969#6669029
36	Сформирован ли список работников предприятия, имеющих доступ к работе с базами персональных данных?		
37	Проводятся ли семинары или тренинги для работающих с персональными данными (журналисты, ИТ, кадры, юристы)?		
38	Обеспечена ли возможность восстановления персональных данных, уничтоженных или поврежденных в результате несанкционированного доступа к ним?		
39	Если обработка персональных данных осуществляется на основании оферты, указаны ли в ней конкретные цели обработки?	п. 9 Приказа Минюста № 3478 от 15.11.2023 г.	https://lex.uz/docs/6663967#6664327

40	Осуществляется ли на предприятии видеонаблюдение? С какой целью? Какие персональные данные обрабатываются?	п. 12 Приказа Минюста № 3478 от 15.11.2023 г.	https://lex.uz/docs/6663967#6664354
41	Утверждены ли внутренние документы, определяющие политику собственника/оператора по обработке и защите персональных данных?	п. 30.12 Приказа Минюста № 3478 от 15.11.2023 г.	https://lex.uz/docs/6663967#6664485
42	Учитываются ли в кадровом делопроизводстве требования нового Трудового кодекса РУз в части защиты персональных данных работника? Обладают ли работники кадровой службы минимальной компетенцией в сфере персональных данных?	§ 6. Защита персональных данных работника. Трудовой кодекс РУз	https://lex.uz/ru/docs/6257291#6262031
43	Если персональные данные работника получаются у третьих лиц (судимость, учет в диспансерах), то уведомляется ли работник письменно об этом заранее, и было ли от него получено письменное согласие?	ст. 176 Трудового кодекса РУз	https://lex.uz/ru/docs/6257291#6262106
44	Имеет ли работник полный доступ ко всем его персональным данным, которые хранятся у работодателя? Может ли он снимать с них копии?	ст. 179 Трудового кодекса РУз	https://lex.uz/ru/docs/6257291#6262129
45	*В формах согласия и офертах отсутствуют «темные паттерны»: • галочки и флажки с согласием на обработку ПДн не проставлены автоматически; • кнопка согласия с условиями может быть нажата только когда субъект просмотрел все страницы предлагаемого договора (оферты) полностью; • факт проставления отметок и нажатия кнопки подтверждения с условиями должен быть зафиксирован с указанием даты, времени, IP-адреса и идентификатора клиента * Требования применимы только к коммерческим банкам	п. 28 Постановления ЦБ РУз № 3030 от 2.07.2018 г.	https://lex.uz/docs/3804290#3805017
46	Внедрена ли в систему управления информационной безопасности (СМИБ/СУИБ) защита персональных данных?	п. 31 приказа Минюста № 3478 от 15.11.2023 г. A.5.34 ISO/IEC 27001:2022 A.18.1.4 O‘z DSt ISO/IEC 27001:2020	https://lex.uz/docs/6663967#6664488 https://stt2.unicon.uz/#/post/772

Приложение 2

Универсальный чек-лист процедур по обработке ПДн

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

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

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

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

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

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

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

H. Процедура распространения (публикации)
   - Любое распространение сверх заявленных целей — только с согласия субъекта. ([LEX.UZ][1]).
   - Отдельные правила для веб-сайта, соцсетей, кейсов, фото/видео, отзывов.
   - Проверка «общедоступности» данных и основания доступа.

I. Процедура трансграничной передачи
   - Определяется страна и оценивается «адекватная защита» (наличие законодательства, договора о конфиденциальности, внутренних политик, технических мер защиты).
   - Для «неадекватных» стран фиксируется основание (например, согласие).
   - Ведется реестр трансграничных передач (система, провайдер, дата, основание).
   - Процедура уведомления регулятора о трансграничной передаче.

J. Локализация и регистрация (для данных граждан РУз)
   - Сбор/систематизация/хранение обеспечены на технических средствах в РУз.
   - База зарегистрирована в госреестре.
   - Контроль облачных сервисов, резервных копий и внешних сервисов.

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

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

https://lex.uz/docs/4396428. ЗРУ-547-сон 02.07.2019. О персональных данных

Приложение 3

Структура Политики обработки и защиты персональных данных

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

7. Права субъектов и порядок их реализации
    7.1. Право получать информацию об обработке и состав предоставляемой информации.
    7.2. Право требовать временного приостановления обработки при проблемах качества/законности/необходимости данных
    7.3. Каналы подачи запросов и сроки внутреннего рассмотрения (внутренний SLA)
    7.4. Идентификация заявителя

8. Уведомления субъектов
    8.1. Уведомление при включении данных в базу (цели и права)
    8.2. Уведомление при передаче третьему лицу (3 дня, исключения)

9. Конфиденциальность и общедоступные данные
    9.1. Режим конфиденциальности
    9.2. Общедоступные персональные данные и правила работы с ними

10. Локализация и регистрация баз
    10.1. Условия обработки данных граждан РУз с использованием ИТ/Интернета (локализация + регистрация в госреестре)
    10.2. Регистрация баз и уведомление об изменениях данных для регистрации

11. Меры защиты
    11.1. Правовые, организационные и технические меры
    11.2. Управление доступом, учетные записи, журналы, носители, помещения
    11.3. Контроль подрядчиков и третьих лиц

12. Удаление, уничтожение и «право на забвение» в практическом смысле
    12.1. Основания уничтожения/удаления (цель достигнута, отзыв согласия, истечение срока, решение суда)
    12.2. Обработка требований на ограничение/приостановление
    12.3. Документирование уничтожения (акты, логи)

13. Реагирование на инциденты и утечки
    13.1. Обязанность приостанавливать обработку или уничтожать данные при наличии информации о нарушении условий обработки
    13.2. Порядок расследования, локализации, исправления и отчетности

14. Трансграничная передача
    14.1. Критерии «адекватной защиты»
    14.2. Передача в «неадекватные» страны и допустимые основания (включая согласие)
    14.3. Реестр трансграничных передач и контроль потоков

15. Заключительные положения
    15.1. Обучение персонала и ответственность
    15.2. Аудит и пересмотр Политики
    15.3. Контакты ответственного лица

Софинансирование
Европейского Союза

ЦЕНТР
РАЗВИТИЯ
СОВРЕМЕННОЙ
ЖУРНАЛИСТИКИ