

Осуществление прав и исполнение обязанностей в цифровой среде

Комплексный анализ правового регулирования цифровых данных, цифровой устойчивости, управления рисками и защиты прав субъектов в цифровом пространстве Кыргызской Республики

Настоящий документ представляет собой систематизированное изложение ключевых положений, регламентирующих порядок осуществления прав и исполнения обязанностей участников правоотношений в цифровой среде. Рассматриваются вопросы доступа к данным, их распространения, обеспечения цифровой устойчивости, управления рисками, а также механизмы защиты прав и разрешения споров.



Общедоступные и открытые данные

ГЛАВА I

Цифровые данные представляют собой один из ключевых объектов правоотношений в цифровой среде. Законодательство Кыргызской Республики устанавливает фундаментальный принцип: **цифровые данные могут использоваться любыми лицами по их усмотрению**, однако при обязательном соблюдении ряда условий. В первую очередь, использование данных ограничивается исключительными правами на объекты интеллектуальной собственности. Кроме того, законом могут быть установлены ограничения на распространение, предоставление, использование, иную обработку отдельных видов данных или доступ к ним.

Принципиально важным является установление **презумпции общедоступности** цифровых записей. Это означает, что цифровые записи считаются общедоступными по умолчанию, если в их метаданных не содержится прямых указаний на ограничение доступа. Такие ограничения должны быть основаны на законе, договоре или решении обладателя данных. Данная презумпция создаёт правовую основу для свободного обмена информацией в цифровом пространстве.

Права владельца цифровых записей

Владелец цифровых записей наделяется правом обусловить дальнейшее распространение записи обязанностью указывать его в качестве источника данных. Это указание должно быть зафиксировано непосредственно в метаданных цифровой записи. Таким образом, метаданные выполняют не только техническую, но и правовую функцию — они содержат информацию о режиме доступа, условиях использования и идентификации владельца.

Подобный подход обеспечивает баланс между свободой использования цифровых данных и защитой интересов их правообладателей, что является одним из фундаментальных принципов регулирования цифровой среды.

Ключевые принципы

- Свобода использования цифровых данных
- Соблюдение исключительных прав на интеллектуальную собственность
- Презумпция общедоступности записей
- Роль метаданных как правового инструмента
- Право владельца на указание источника

Распространение цифровых записей и доступ к ним

↪ ГЛАВА II

Распространение цифровых записей и доступ к ним — два взаимосвязанных, но различных по своей правовой природе процесса. **Распространение** осуществляется по инициативе владельца цифровых записей или владельца цифрового ресурса, тогда как **доступ** иницируется непосредственно пользователем. Распространение цифровых записей осуществляется свободно при соблюдении требований, установленных Цифровым кодексом, а доступ — на условиях, определённых владельцем соответствующих цифровых записей или цифрового ресурса.

Распространение	Доступ
По инициативе владельца записей или цифрового ресурса. Свободное при соблюдении требований Кодекса.	По инициативе пользователя. На условиях, определённых владельцем записей или ресурса.

Обязательные требования к метаданным

Законодатель устанавливает обязательное требование к содержанию метаданных: они должны включать **достоверные сведения о владельце** в форме и объёме, достаточных для цифровой идентификации такого лица или для возможности связаться с ним в цифровой среде. Это требование обеспечивает прозрачность и подотчётность участников цифровых правоотношений.

Право пользователя на отказ Лицо, распространяющее цифровые записи, обязано обеспечить пользователю возможность отказа от получения цифровых записей, если иное не установлено законом.	Обязательное распространение Случаи и условия обязательного распространения цифровых записей или доступа к ним устанавливаются законом, что позволяет государству обеспечивать общественные интересы.
---	---

Ограничение распространения цифровых записей и доступа к ним

 ГЛАВА III

Доступ к цифровым записям или их распространение могут быть ограничены исключительно в соответствии с метаданными таких записей и на основании закона. Кодекс устанавливает **исчерпывающий перечень оснований** для такого ограничения, что исключает возможность произвольного ограничения доступа к информации в цифровой среде.

1	2	3
Осуществление цифровых прав Ограничение доступа является реализацией цифровых прав обладателя данных, например, при защите персональных данных или коммерческой информации.	Охраняемая законом тайна Метаданные цифровых записей указывают на их отнесение к охраняемой законом тайне (государственной, коммерческой, банковской и др.).	Запрет в силу закона или решения суда Распространение цифровых записей или доступ к ним запрещены в соответствии с законом или решением суда.

Гарантии и исключения

Запрет произвольного ограничения

Вводимые ограничения должны соответствовать принципам регулирования отношений в цифровой среде. **Не допускается произвольное ограничение** доступа к цифровым записям и их распространения. Это является важнейшей гарантией информационных прав граждан.

Право исследователей

Исследователи и научные организации имеют право осуществлять доступ к цифровым записям, содержащим персональные данные или отнесённым к охраняемой законом тайне, **в научных, статистических или иных исследовательских целях** при условии обеспечения конфиденциальности.

 Уполномоченные лица, осуществляющие доступ к цифровым записям с ограниченным доступом, обязаны соблюдать порядок такого доступа, установленный Кабинетом Министров Кыргызской Республики. Нарушение установленных ограничений влечёт ответственность в соответствии с законом.

Доступ к данным государственных и муниципальных ресурсов

ГЛАВА IV

Бесплатность

Цифровые записи из государственных и муниципальных цифровых ресурсов предоставляются пользователям бесплатно

Отсутствие ограничений

Доступ осуществляется без ограничений, если иное не установлено законом

Без обоснования

Пользователь не обязан обосновывать необходимость получения запрашиваемых записей

Данная норма закрепляет один из фундаментальных принципов открытого государственного управления — **принцип открытости государственных данных**. Государственные и муниципальные цифровые ресурсы содержат обширные массивы информации, необходимой гражданам, организациям и исследователям для осуществления своих прав, ведения хозяйственной деятельности, научных исследований и общественного контроля.

Освобождение пользователя от обязанности обосновывать необходимость получения записей устраняет административные барьеры и обеспечивает реальную доступность государственной информации. Это положение корреспондирует с международными стандартами в области права на информацию и принципами открытых данных, принятыми в рамках Партнёрства «Открытое правительство».

Вместе с тем законодатель оставляет возможность установления исключений из общего правила о бесплатности и неограниченности доступа. Такие исключения могут быть установлены только на уровне закона, что обеспечивает надлежащий уровень правовой защиты граждан от произвольного ограничения доступа к государственной информации.

Цифровая устойчивость: концепция и меры обеспечения

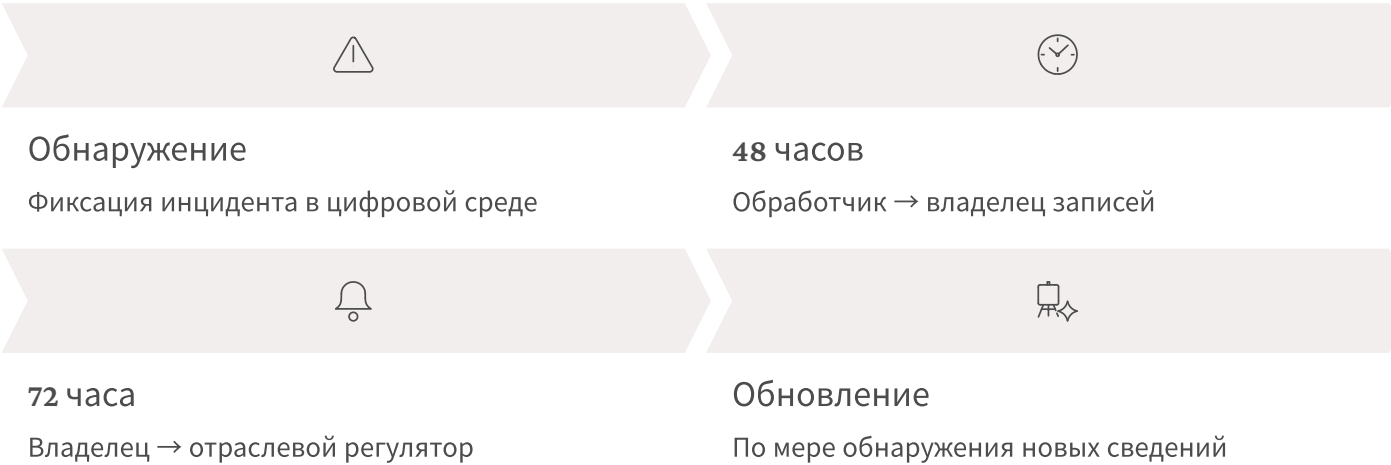
ГЛАВА V – ЦИФРОВАЯ УСТОЙЧИВОСТЬ

Государственное регулирование цифровой устойчивости осуществляется в целях обеспечения **непрерывности деятельности** объектов и субъектов и их **восстановления после инцидентов** в цифровой среде. При этом законодатель исходит из практической невозможности полной защиты от инцидентов, что свидетельствует о реалистичном подходе к вопросам кибербезопасности.



Уведомление об инцидентах

Кодекс устанавливает строгие временные рамки для уведомления об инцидентах в цифровой среде. Владелец записей или поставщик цифрового сервиса обязан уведомить отраслевого регулятора **не позднее чем через 72 часа** после обнаружения инцидента. Обработчик обязан уведомить владельца записей **не позднее чем через 48 часов**.



Уведомление должно содержать: описание инцидента и оценку числа затронутых пользователей; контактную информацию ответственного лица; описание последствий; описание принятых мер по устранению и минимизации негативных последствий.

Система управления рисками в цифровой среде

 ГЛАВА VI

Система управления рисками в цифровой среде является обязательным элементом обеспечения цифровой устойчивости. Для каждого объекта правоотношений в цифровой среде, на который она распространяется, система должна определять три ключевых компонента.

Перечень рисков

Включает оценку вероятности и масштаба негативных последствий для каждого выявленного риска. Формирует основу для принятия управленческих решений.

Меры по управлению рисками

Определяют конкретные действия по снижению вероятности и масштаба негативных последствий в отношении каждого из выявленных рисков.

Оценка эффективности и корректировка

Устанавливает порядок оценки эффективности существующей системы управления рисками и внесения изменений на основе собранных данных.

Методика и ответственность

Если иное не установлено законом, система управления рисками разрабатывается и реализуется **владельцем (поставщиком) объекта правоотношений** самостоятельно, с учётом общепризнанной мировой практики. Такой подход предоставляет участникам рынка гибкость в выборе методологии, одновременно устанавливая стандарт качества на уровне международных норм.

В случаях, установленных Кодексом и законодательством в сфере кибербезопасности, владельцы обязаны провести **испытания** для определения наиболее подходящих мер по управлению рисками. Испытания признаются успешными, если объект может использоваться по назначению и соответствует предъявляемым требованиям.

Прозрачность данных об ИИ

Все данные о системе управления рисками, методике внедрения и результаты испытаний **систем искусственного интеллекта повышенной опасности** должны быть представлены в виде цифровых записей и опубликованы на сайте владельца (в части, не отнесённой к государственным секретам).

Управление ресурсами для обеспечения цифровой устойчивости

ГЛАВА VII

Субъекты правоотношений в цифровой среде наделены правом **самостоятельно определять ресурсы** — человеческие, финансовые, технические и другие, — необходимые для обеспечения цифровой устойчивости. При этом законодатель устанавливает важную гарантию: запрещается устанавливать требования, выполнение которых создаёт угрозу для цифровой устойчивости самих субъектов.

Факторы принятия решений



Уровень развития науки и техники

Учёт актуального состояния технологий и научных достижений в области кибербезопасности



Знания и навыки людей

Уровень компетенций участников создания и использования соответствующего объекта



Характер и объём обработки

Цели обработки цифровых данных, предоставления цифровых сервисов или эксплуатации технологических систем



Жизненный цикл объекта

Учёт всех этапов жизненного цикла, начиная с проектирования соответствующего объекта



Права субъектов

Законные интересы владельцев, пользователей и потребителей соответствующего объекта

Защита прав и разрешение споров в цифровой среде

ГЛАВА VIII

Кодекс устанавливает комплексную систему защиты прав субъектов правоотношений в цифровой среде. Механизмы защиты включают как превентивные технические и организационные меры, так и традиционные правовые способы восстановления нарушенных прав.

Способы защиты прав

- 1

Технические, организационные и правовые меры

Защита принадлежащих субъектам объектов правоотношений в цифровой среде
- 2

Восстановление положения

Восстановление положения, существовавшего до нарушения, и пресечение действий, нарушающих право
- 3

Принуждение к исполнению

Принуждение пользователя к исполнению обязанности или законного требования обладателя
- 4

Возмещение убытков

Включая убытки от нарушения ограничений доступа, конфиденциальности и указания источника данных
- 5

Компенсация морального вреда

Независимо от возмещения имущественного вреда и понесённых убытков

Разрешение споров в цифровых сообществах

Особый интерес представляет институт разрешения споров в рамках цифровых сообществ. Правила цифровых сообществ должны предусматривать обязательные процессуальные гарантии:

01	02	03
Уведомление сторон Обязанность уведомления всех лиц, затрагиваемых спором, и предоставления им доступа к относящимся цифровым записям	Право на возражения Возможность для любого лица высказать возражения, представить аргументы и доказательства	Независимое рассмотрение Рассмотрение спора независимым арбитром либо путём голосования всех участников сообщества

Решение по спору, вынесенное в рамках цифрового сообщества в соответствии с его правилами, обязательно для всех участников данного сообщества. Сообщество участников цифровой экосистемы обеспечивает исполнение решений на базе цифровой экосистемы.

Ответственность за правонарушения в цифровой среде

⚠ ГЛАВА IX – ОТВЕТСТВЕННОСТЬ

Совершение правонарушений в цифровой среде влечёт ответственность в соответствии с применимым законодательством. Отдельными главами Кодекса устанавливаются особенности ответственности за правонарушения, совершённые в соответствующих сферах деятельности. Кодекс выделяет конкретные основания для возмещения убытков, возникающих в цифровой среде.

Основания возмещения убытков

Неправомерный отказ в доступе Отказ в доступе к объектам правоотношений в цифровой среде	Несвоевременно е предоставление Задержки в предоставлении доступа к цифровым записям	Недостоверные данные Предоставление заведомо неполных, недостоверных или неактуальных записей	Нарушение требований Нарушение доступности и надёжности цифровых сервисов и технологических систем
--	--	---	--

Исключения из ответственности

Кодекс предусматривает важные исключения для поставщиков, выполняющих исключительно функции посредников. Меры по возмещению убытков и компенсации морального вреда **не применяются** в отношении поставщиков, цифровые сервисы которых заключаются в:

Передача данных Передача цифровых данных, предоставленных другим лицом, при условии их передачи без изменений и исправлений	Хранение данных Хранение цифровых данных и обеспечение доступа к ним при условии, что поставщик не знал о незаконности обрабатываемой информации
--	---

Возмещение физическому лицу морального вреда, причинённого нарушениями в цифровой среде, осуществляется **независимо** от возмещения имущественного вреда и понесённых убытков — это важнейшая гарантия защиты прав граждан в цифровом пространстве Кыргызской Республики.