

ЦИФРОВОЙ КОДЕКС :

Новые грани регулирования

Цифровой кодекс: структура и источники

Цифровой кодекс Кыргызстана представляет собой комплексную правовую систему регулирования отношений в цифровой среде. Он объединяет и систематизирует нормы, ранее разрозненно содержащиеся в различных законодательных актах, создавая единое правовое поле для цифровой трансформации государства и общества.

Закон «Об электронном
управлении» 2017 года

Правовая основа для цифровизации
государственных органов

Закон «Об электронной подписи»
2017 года

Регулирование использования ЭЦП в
правовом обороте

Закон «О биометрической
регистрации граждан» 2014 года

Основы идентификации личности по
биометрическим данным

Закон «Об информации
персонального характера» 2008
года

Защита персональных данных граждан

Закон «Об электрической и
почтовой связи» 1998 года

Регулирование телекоммуникационной
инфраструктуры

Около 100 подзаконных НПА

Нормативные акты для регулирования
«аналоговой среды»

Кодекс консолидирует эти акты в единую систему, устраняя противоречия и создавая целостную правовую основу для цифровых отношений.

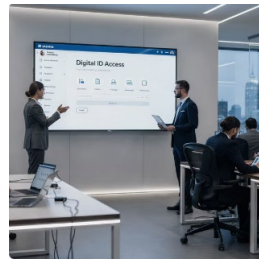
Лучшие практики международного цифрового регулирования

Цифровой кодекс Кыргызстана разработан с учётом передового мирового опыта правового регулирования цифровых отношений. При его создании были проанализированы и адаптированы наиболее эффективные модели цифрового управления ведущих юрисдикций.



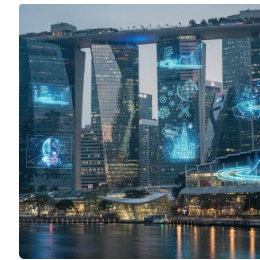
Европейский союз

Общий регламент по защите данных (GDPR) и Акт о цифровых услугах устанавливают высокие стандарты защиты прав граждан в цифровой среде



Эстония

Модель цифрового государства с электронным резидентством и комплексной системой государственных электронных услуг



Сингапур

Концепция «умной нации» с акцентом на цифровую экономику и регуляторные песочницы для инноваций

Интеграция этих подходов позволила создать современную правовую систему, отвечающую как международным стандартам, так и национальным особенностям развития цифровой среды Кыргызстана.

Приоритет и юридическая сила Цифрового кодекса

Статья 4 Цифрового кодекса устанавливает его приоритет над другими нормативными актами: при возникновении коллизии норм преимущественную силу имеют положения Кодекса. Это принципиальное решение исключает хаотичную нормотворческую самостоятельность различных ведомств и предотвращает фрагментацию правового регулирования в цифровой среде.



Прямое действие

Распространяется на все цифровые отношения независимо от организационно-правовой формы, отраслевой принадлежности и категории субъекта



Самодостаточность

Не нуждается в утверждении дополнительных подзаконных актов для вступления норм в юридическую силу



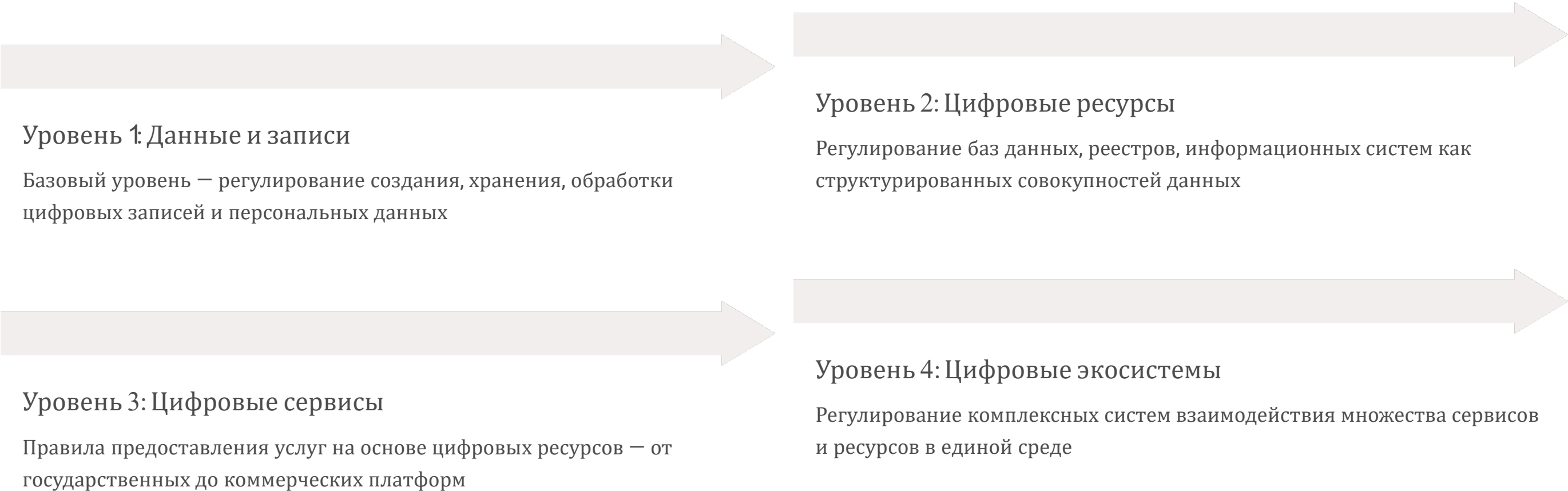
Ограничение делегирования

Органы исполнительной власти издают подзаконные акты исключительно в пределах, прямо предусмотренных Кодексом

Тем самым закрепляется фундаментальный принцип **правовой предсказуемости** в цифровой среде — все участники цифровых отношений взаимодействуют по единым, ясным и доступным правилам. Кодекс становится гарантом единообразия юридической интерпретации цифровых процессов и систем на всей территории государства.

Предмет и уровни регулирования

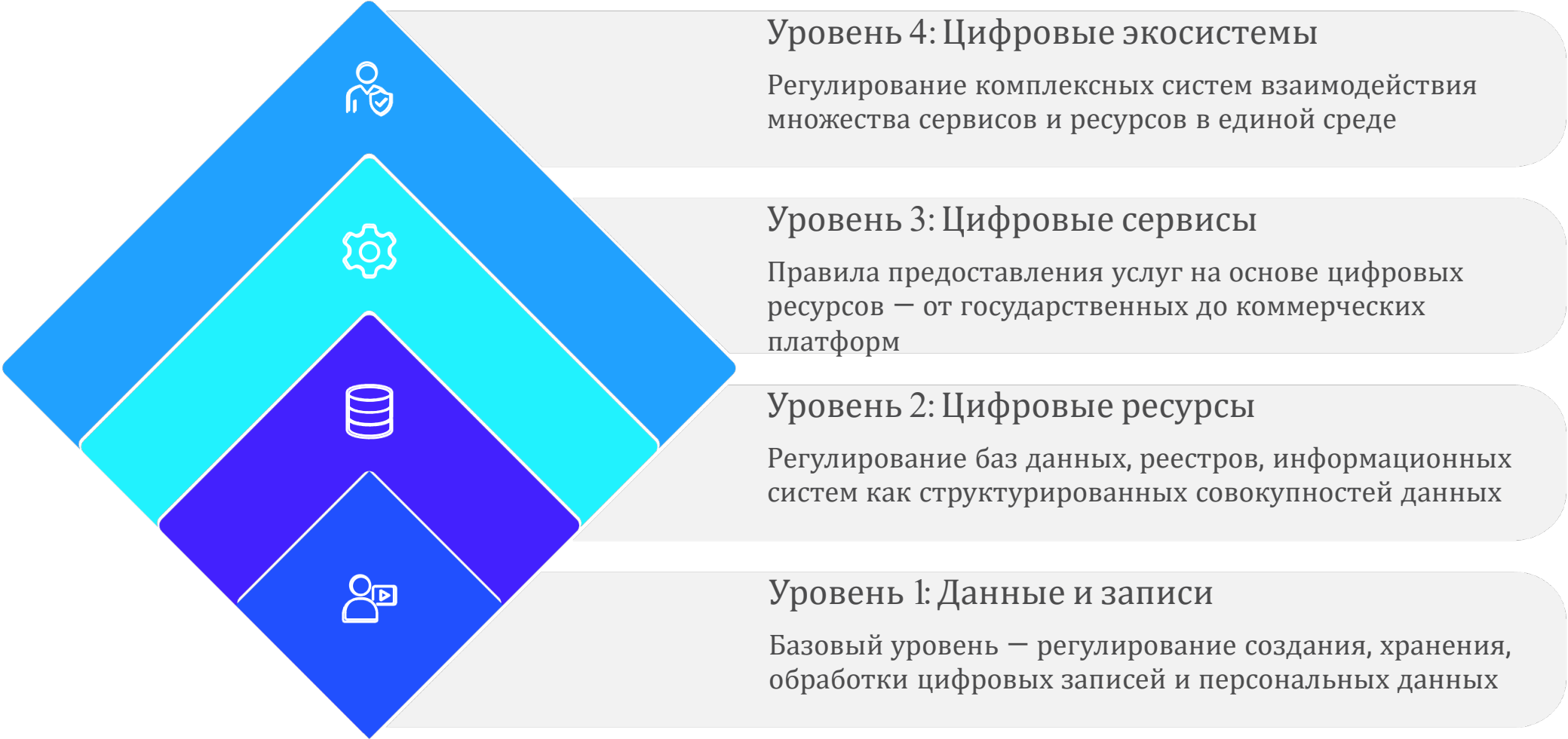
Цифровой кодекс устанавливает четырёхуровневую систему регулирования цифровых отношений. Каждый уровень характеризуется своим специфическим набором объектов правового регулирования и отношений по их созданию, использованию, изменению и прекращению.



Многоуровневый характер регулирования отражает реальную архитектуру цифровой среды, где каждый последующий уровень возникает как результат отношений на предыдущем. Детальные правила для каждого уровня определяются в соответствующих разделах Особенной части Кодекса, что обеспечивает системность и логическую последовательность норм.

Уровни регулирования — жизненный цикл данных

Регулирование в Цифровом кодексе строится на понимании полного жизненного цикла данных — от создания до утилизации.



Для каждого этапа Кодекс устанавливает специфические права и обязанности субъектов, требования к безопасности и механизмы защиты, создавая целостную систему правового сопровождения данных.

Уровни регулирования – жизненный цикл данных

Цифровые данные +
метаданные = **цифровые
записи**

Систематизированные
цифровые записи = **цифровой
ресурс**

Цифровой ресурс + адрес в
Интернете = **веб-сайт**

Программа для цифровых
устройств, предназначенная
для доступа к цифровым
ресурсам = **приложение**



Возможность использования
приложений и технологических
систем для доступа к
цифровым записям или
обмена ими = **цифровой
сервис**

Сервисы и технологические
системы, доступные по
общим правилам = **цифровая
экосистема**

Технологические системы
(телекоммуникационные сети и
ЦОДы) обеспечивают
возможность обработки
цифровых данных и работу
цифровых сервисов

Размещение технологических
систем на **землях, зданиях,
строениях и сооружениях**
осуществляется по правилам
Кодекса

Принципы правового регулирования

Общественные отношения в цифровой среде развиваются чрезвычайно динамично, поэтому детальное правовое регулирование не может охватить все возможные ситуации и сценарии взаимодействия. В качестве базовых ориентиров для участников цифровых отношений и регулирующих органов Кодекс устанавливает систему фундаментальных принципов.

Нормативные принципы

Определяют основы и методы правового регулирования в цифровой среде

- Технологическая нейтральность регулирования
- Приоритет прав человека в цифровой среде
- Презумпция открытости данных публичного сектора
- Баланс интересов владельцев данных и пользователей

Целевые принципы

Описывают желаемое состояние цифровых отношений, к которому стремится законодатель

- Интероперабельность систем и сервисов
- Цифровая устойчивость инфраструктуры
- Развитие конкуренции на цифровых рынках
- Доступность цифровых услуг для всех граждан

Принципы, относящиеся к специальным сферам отношений в цифровой среде — таким как телекоммуникации, предоставление государственных услуг, электронная коммерция — детально раскрываются в соответствующих главах Особенной части Кодекса.

Метод правового регулирования

Цифровым кодексом впервые решён принципиальный вопрос о собственном, специфическом методе регулирования для формируемой им новой отрасли цифрового права. Этот метод существенно отличается от традиционных подходов гражданского или административного права.

Цифровое право на объект (Data Right)

Аналог права собственности в цифровой среде. Владелец объекта получает право управлять доступом к нему, определять условия использования, извлекать экономическую выгоду. Это создаёт правовую определённость и стимулирует инвестиции в создание и развитие цифровых ресурсов и сервисов.

Права доступа (Access Rights)

Устанавливаются в интересах общества и развития цифровой экономики в целом, подобно ограничениям права собственности. Обеспечивают интероперабельность систем, предотвращают злоупотребление доминирующим положением, гарантируют доступ к социально значимым данным и сервисам.

Метод регулирования отношений в цифровой среде представляет собой обеспечение условий для сбалансированного взаимодействия на основе этих двух конкурирующих, но взаимодополняющих прав. Законодатель стремится найти оптимальное равновесие между стимулированием частных инвестиций и обеспечением общественных интересов.

Система источников правовых норм

Цифровой кодекс учитывает реально сложившуюся структуру источников правовых норм в цифровой среде, которая значительно сложнее традиционной системы законодательства. В каждом государстве его национальное законодательство сохраняет приоритет и служит основным ориентиром как для граждан, так и для иностранных инвесторов.

01	02
Цифровой кодекс и законы	Подзаконные нормативные акты
Высший уровень — нормы Кодекса и специальных законов, имеющие прямое действие	Акты Правительства и уполномоченных органов в пределах делегированных полномочий
03	04
Технические стандарты	Правила цифровых сообществ
Национальные и международные стандарты, обеспечивающие техническую совместимость	Нормы, формируемые профессиональными и пользовательскими сообществами

Важнейшей задачей является установление понятных, стабильных и предсказуемых правил, при одновременном ограничении ведомственного нормотворчества, которое часто приводит к противоречиям и барьерам для развития.

Однако национальное законодательство не может игнорировать те правила и стандарты, по которым фактически функционирует глобальная цифровая среда. Они формируются правилами различных цифровых сообществ, международными организациями по стандартизации, а также техническими рекомендациями, определяющими, как строятся и взаимодействуют цифровые технологии. Кодекс интегрирует эти источники в национальную правовую систему.

Система регулирующих органов

В целях обеспечения долговременной стабильности правового регулирования и гибкости в условиях быстрых технологических изменений Цифровой кодекс не наделяет регулируемыми полномочиями конкретный государственный орган с указанием его названия и организационной структуры.

Функциональный подход к регулированию

Вместо привязки к конкретным ведомствам Кодекс определяет содержание полномочий по цифровому управлению и устанавливает чёткие требования к уполномоченному государственному органу, который должен эти полномочия реализовывать.

Кабинет Министров получает право определять конкретный орган или систему органов в соответствии с актуальными потребностями цифрового развития страны, изменениями в государственной структуре и эволюцией технологий.

Такой подход предотвращает необходимость внесения изменений в Кодекс при каждой административной реформе, обеспечивает преемственность регулирования и позволяет оперативно реагировать на новые вызовы без ущерба для правовой определённости.

Преимущества модели

- Адаптивность к реформам
- Избежание частых правок Кодекса
- Фокус на функциях, а не структуре

Специальное регулирование и регуляторные песочницы

Цифровой кодекс вводит инновационный механизм специального регулирования, позволяющий временно освободить субъекты от некоторых обязанностей, установленных действующим законодательством. Президент Кыргызской Республики получает право утверждать такие режимы в порядке, предусмотренном Кодексом.

Эксперименты и тестирование

Апробация цифровых инноваций в реальных условиях без риска нарушения существующих норм

Улучшение качества

Повышение качества и расширение доступности цифровых ресурсов и сервисов для граждан

Стимулирование конкуренции

Создание условий для добросовестной конкуренции и повышение эффективности управления

Привлечение инвестиций

Формирование благоприятной среды для инвестиций в развитие цифровой экономики

Механизм специального регулирования особенно важен для тестирования прорывных технологий — искусственного интеллекта, блокчейна, квантовых вычислений — когда существующее законодательство ещё не адаптировано к их особенностям. Это позволяет стране оставаться на переднем крае технологического развития, не жертвуя правовой определённостью.



Объекты и субъекты цифровых правоотношений

Цифровой кодекс устанавливает чёткую систему субъектов, участвующих в цифровых правоотношениях. Каждый субъект обладает специфическими правами и обязанностями в зависимости от своей роли в цифровой среде.



Владелец ресурсов

Лицо, обладающее правом управления доступом к цифровому ресурсу и определяющее условия его использования



Принципал данных и записей

Физическое или юридическое лицо, к которому относятся персональные данные или которое создаёт цифровые записи



Обработчик данных

Лицо, осуществляющее обработку данных по поручению владельца записей в установленных пределах



Пользователь приложений и сайтов

Конечный потребитель цифровых сервисов и услуг через веб-интерфейсы и мобильные приложения



Потребитель сервисов

Лицо, использующее цифровые сервисы для решения своих задач, включая получение государственных услуг



Поставщик техносистем и экосистем

Лицо, обеспечивающее функционирование технической инфраструктуры или комплексных цифровых экосистем

Один участник может одновременно выступать в нескольких ролях в зависимости от контекста взаимодействия. Например, гражданин является принципалом своих персональных данных, пользователем государственных сервисов и потребителем коммерческих цифровых услуг.

Взаимодействие в цифровой среде

Цифровой кодекс обеспечивает три категории взаимодействия субъектов на основе фундаментального принципа интероперабельности — технической, семантической и организационной совместимости данных, сервисов и систем.



Для каждой категории Кодекс устанавливает специфические требования к техническим стандартам, форматам данных, протоколам обмена информацией. Это гарантирует, что системы различных организаций могут эффективно взаимодействовать между собой.

Особое внимание уделяется обеспечению интероперабельности информационных систем государственных органов, что исключает необходимость многократного предоставления одних и тех же данных гражданами и организациями при обращении в различные ведомства.

Цифровая идентичность: новая парадигма

Без юридических доказательств вашего существования вы не можете голосовать, управлять автомобилем, открыть банковский счёт или получить доступ к государственным услугам. Цифровая идентичность становится новым фундаментом правосубъектности в XXI веке.

Глобальный тренд цифровизации личности

Цифровые идентификаторы необходимы для функционирования в современном цифровом мире. Они активно внедряются повсеместно — от систем контроля доступа в аэропортах до электронных медицинских карт и банковских приложений.

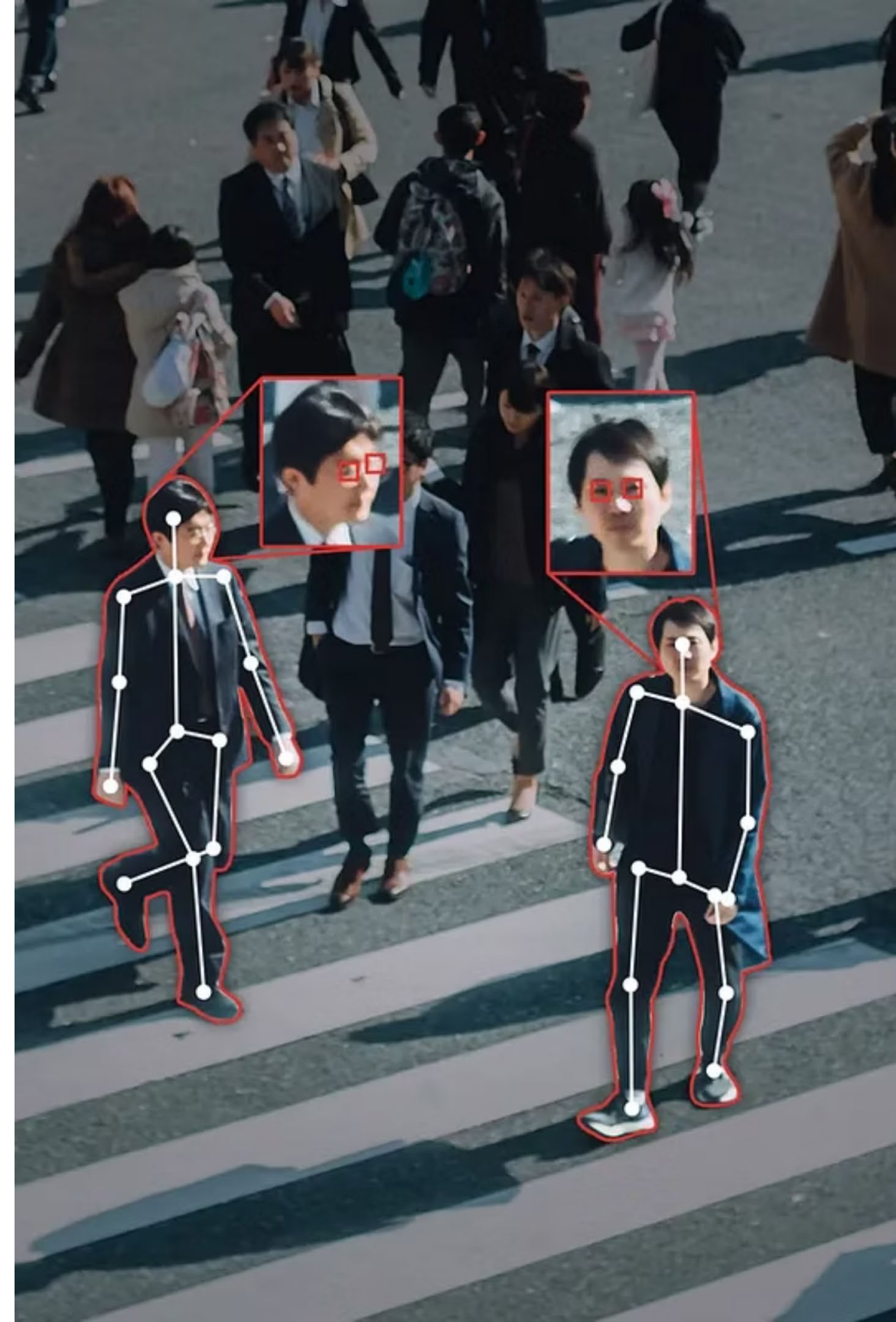
Государства стремятся «оцифровать» своих граждан в первую очередь для повышения эффективности предоставления государственных услуг, борьбы с мошенничеством и упрощения административных процедур.

Цифровой кодекс закладывает правовую основу для безопасного, защищённого и уважающего права человека развития систем цифровой идентичности в Кыргызстане.

Коммерческая мотивация

Банковские, туристические, страховые и технологические компании внедряют системы цифровой идентификации для создания бесшовных экосистем предоставления своих продуктов и услуг.

Единая цифровая идентичность позволяет клиентам мгновенно получать доступ ко всему спектру сервисов без многократного прохождения процедур идентификации и верификации.



Цифровые идентификаторы и аутентификация

Одной из ключевых правовых новелл Цифрового кодекса является введение понятия **цифрового идентификатора** — уникального набора данных, обеспечивающего юридически значимую идентификацию лица в цифровой среде.



Персональные данные

ПИН, ИНН и другие традиционные идентификаторы личности



Биометрия

Биометрические признаки для надёжной и однозначной идентификации



Облачная идентификация

Подтверждение личности через централизованный цифровой сервис



Ключи электронной подписи

Криптографические ключи для создания юридически значимых цифровых подписей

Кодекс вводит три **уровня доверия идентификатора** — низкий, средний и высокий, — что позволяет гибко регулировать требования к идентификации в зависимости от рисков операции.

Обезличивание персональных данных

Обезличивание персональных данных — процесс изъятия из данных той части, которая позволяет прямо или косвенно отождествить их с конкретным физическим лицом.

Правовой режим обезличенных данных

После обезличивания правовой режим данных существенно трансформируется:

- Обработка возможна без согласия субъекта данных .1
- Режим конфиденциальности не применяется .2
- Для заявления прав субъект должен доказать принадлежность данных .3

Цели использования

- Статистические исследования •
- Социологические опросы •
- Медицинские исследования •
- Научные разработки •



Кодекс заимствует опыт Японии: баланс между защитой прав субъектов и потребностями общества в использовании данных для общественно полезных целей.

Кибербезопасность и цифровая устойчивость

Цифровой кодекс закрепляет комплексный подход к обеспечению цифровой устойчивости, охватывающий все аспекты управления цифровыми рисками.

900K

Кибератак ежегодно

Количество зафиксированных кибератак на критическую инфраструктуру в мире

\$9,5T

Финансовый ущерб

Прогнозируемый глобальный ущерб от киберпреступности к 2024 году

Мы должны совершить парадигмальный переход: от технических специалистов, которые реагируют на взломы, к стратегам, которые системно управляют рисками цифровой среды на уровне всей организации.



Кибербезопасность

Защита от несанкционированного доступа, вредоносного ПО и кибератак



Цифровая устойчивость

Способность продолжать функционирование и быстро восстанавливаться после инцидентов



Управление рисками

Систематическая идентификация, оценка и снижение киберрисков

Цифровая устойчивость

Государственное регулирование цифровой устойчивости направлено на обеспечение **непрерывности деятельности** объектов и субъектов цифровой среды, а также их способности к быстрому восстановлению после инцидентов — с учётом практической невозможности абсолютной защиты от всех угроз.

Целостность и конфиденциальность

Обеспечение целостности, постоянной доступности цифровых объектов и конфиденциальности обрабатываемых данных

Мониторинг инцидентов

Непрерывный мониторинг, активное предупреждение инцидентов и оперативный обмен данными о них

Управление рисками

Системное управление рисками на основе утверждённой и документированной системы

Управление ресурсами

Обеспечение достаточных технических, человеческих и финансовых ресурсов для непрерывности деятельности

Отраслевые регуляторы обеспечивают координацию обмена данными об инцидентах безопасности и принятие превентивных мер по их предупреждению.

- ❏ **Владелец записей или поставщик цифрового сервиса** обязан уведомить уполномоченный регулирующий орган **не позднее 72 часов** после обнаружения инцидента. **Обработчик данных** обязан уведомить владельца записей **не позднее 48 часов** с момента обнаружения.

Уведомление об инцидентах в цифровой среде

Уведомление об инциденте, негативно влияющем на цифровую устойчивость или права субъектов данных, является обязательным и должно содержать исчерпывающую информацию для оценки масштаба происшествия и координации ответных действий.

1	2	3	4
Описание и охват инцидента Характер инцидента, затронутые системы, предполагаемое количество пострадавших субъектов	Принятые меры реагирования Действия по локализации инцидента, восстановлению систем и защите данных	Контактные данные ответственного Контакты лица, ответственного за взаимодействие с регулятором и координацию	Описание последствий Оценка фактических и возможных негативных последствий для субъектов и систем

Владелец записей или поставщик цифрового сервиса обязан **регулярно обновлять данные** в уведомлении по мере обнаружения новых сведений об инциденте, его причинах или последствиях. Это обеспечивает актуальность информации для принятия управленческих решений.

❏ Если уведомление не было направлено в течение установленного 72-часового срока, его необходимо сопроводить мотивированным объяснением причин задержки. Несвоевременное уведомление может повлечь административную ответственность.

Система управления рисками и управление ресурсами

Цифровой кодекс устанавливает требования к созданию и поддержанию систем управления рисками и обеспечению достаточных ресурсов для цифровой устойчивости.

Система управления рисками

Система управления рисками должна определять для каждого объекта правоотношений в цифровой среде:

01

Перечень рисков

Включает оценку вероятности возникновения и потенциального масштаба негативных последствий

02

Меры управления

Конкретные действия по снижению вероятности реализации и масштаба последствий для каждого выявленного риска

03

Оценка эффективности

Порядок периодической оценки и внесения изменений на основе собранных данных и инцидентов

Управление ресурсами

Субъекты самостоятельно определяют необходимые ресурсы с учётом следующих факторов:

- **Уровень развития науки и техники** — современные методы защиты
- **Характер и объём обработки данных** — масштаб операций
- **Жизненный цикл объектов** — этапы от создания до утилизации
- **Знания и навыки участников** — компетенции персонала
- **Права и интересы субъектов** — чувствительность данных



Кодекс категорически запрещает устанавливать требования, выполнение которых само по себе создаёт угрозу для цифровой устойчивости субъектов. Данные о системе управления рисками и результаты испытаний искусственного интеллекта повышенной опасности должны быть **опубликованы** в виде общедоступных цифровых записей.

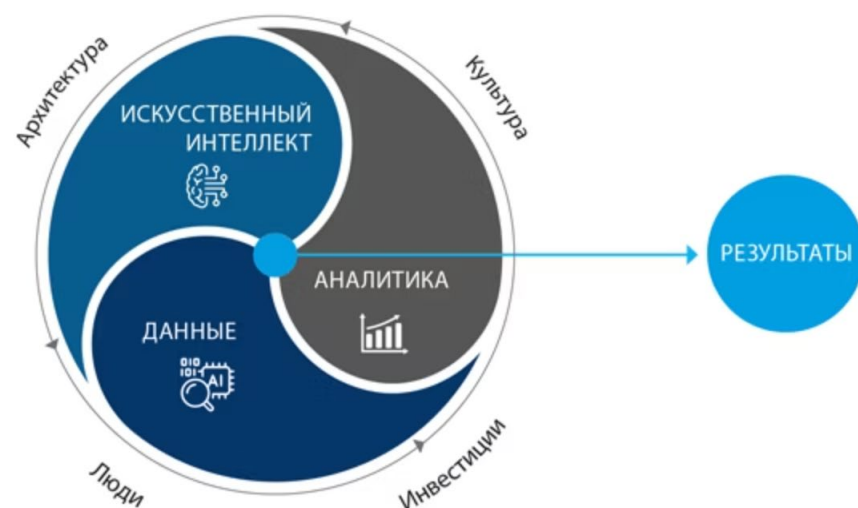


Рис. В1.
Основные драйверы цифровой трансформации (Gartner)

ДАННЫЕ СЕЙЧАС — САМЫЙ ЦЕННЫЙ РЕСУРС

Раньше вкладывались миллиарды в фабрики и оборудование — материальные активы определяли стоимость компаний и их конкурентное преимущество. Сегодня мир изменился. Лидеры инвестируют в цифровые платформы, данные и специалистов, способных анализировать эти данные и превращать их в действенные инсайты.

Данные стали новой нефтью цифровой экономики. Компании, которые умеют собирать, обрабатывать и монетизировать информацию, получают беспрецедентное конкурентное преимущество. Государства, создающие правовую основу для оборота данных, обеспечивают технологический суверенитет и экономический рост.

Технологии обработки данных

Современная цифровая экосистема представляет собой сложную взаимосвязанную сеть технологий, которые непрерывно генерируют, обрабатывают и обмениваются данными. Каждая технология играет свою уникальную роль в этом процессе.



Мобильные устройства

Предопределяют значимость сведений о местоположении объектов: от дорог до автомобилей. Каждое устройство генерирует потоки геоданных в реальном времени.



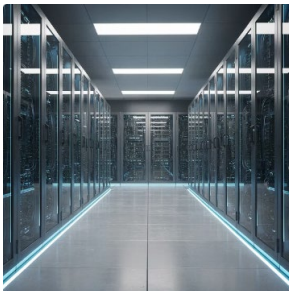
Интернет вещей

Устройства IoT всё время генерируют данные об окружающем мире — от температуры и влажности до производственных показателей и энергопотребления.



Big Data

Анализ массивов данных ведется с использованием технологии Big Data, позволяющей обрабатывать петабайты информации и находить скрытые закономерности.



Облачные решения

Хранение накопленных знаний и доступ к ним из любого места возможен с использованием облачных решений, обеспечивающих масштабируемость и надежность.



Мессенджеры и соцсети

Делиться этими знаниями и вести совместную работу над ними удобно в мессенджерах и соцсетях, создающих новые формы взаимодействия.



Цикл инноваций

Все эти данные анализируются с использованием технологий Big Data, что приводит к появлению всё новых, более удобных и эффективных мобильных устройств и облачных решений.

Большие данные, IoT и облачные вычисления

Кодекс впервые устанавливает правовой режим Big Data, Интернета вещей (IoT) и облачных вычислений. Теперь создание и использование массивов данных в Кыргызской Республике возможно без законодательных барьеров, с сохранением прав принципалов даже после обезличивания. Права на данные, генерируемые IoT-устройствами, четко закреплены за их владельцами. Владелец облачной платформы обязан учитывать международные стандарты при формировании цифровых записей.

Big Data

Технологии больших данных могут создаваться и использоваться в КР **без ограничений**, при этом принципалы данных сохраняют все права даже при обезличивании.

Интернет вещей

Цифровые права на записи от IoT-устройств принадлежат **владельцам устройств**, если иное не установлено соглашением, с обязательной защитой и сертификацией.

Облачные вычисления

Получили правовой статус как форма цифрового сервиса и учета **международной практики** при выборе форматов записей.



Автоматические решения и смарт-контракты

Когда «решает машина», а спор разрешает человек

Нормы формируют баланс: автоматизация допустима, но не устраняет процессуальные гарантии адресата решения. Поставщикам техносистем следует документировать логи и основания для обеспечения трассируемости и объяснимости при оспаривании.

Цифровой кодекс создает правовую основу для использования алгоритмических решений в юридически значимых ситуациях, одновременно защищая права граждан на прозрачность и справедливость.

Автоматические решения

Цифровой кодекс допускает автоматизацию принятия решений, если результаты обработки данных **порождают, изменяют или прекращают** правоотношения без участия человека.

Ключевая гарантия: принципал данных может потребовать остановить автоматические решения и пересмотреть их с участием человека.

Смарт-контракты

Смарт-контракт — договор, условия которого выражены в программном коде и исполняются автоматически при наступлении согласованных событий.

Обязательное требование: договор должен предусматривать процедуру разрешения споров с участием человека.



Открытые и общедоступные данные

Публичность по умолчанию и законные границы доступа

01— Презумпция открытости Цифровые записи считаются общедоступными, если в метаданных не указаны ограничения. Это стимулирует прозрачность и инновации.	02 — Контроль распространения Владельцы могут обусловить дальнейшее распространение указанием источника, сохраняя контроль над использованием.	03 — Режим доступа Распространение — по инициативе владельца; доступ — по инициативе пользователя на условиях владельца.	04 — Законные ограничения Допускаются законом и метаданными (защита прав, тайны, судебные запреты); произвол исключен.
---	--	--	--



Государственные и муниципальные записи

Предоставляются **бесплатно и без ограничений**, если иное не установлено законом. Нормы о цифровой устойчивости и способах защиты прав создают процессуальную основу для претензий к поставщикам и владельцам, включая возмещение убытков.

Правовой режим обеспечивает баланс между открытостью данных и защитой законных интересов участников цифровых правоотношений, создавая основу для развития экосистемы открытых данных.

Метод правового регулирования — баланс цифровых прав и прав доступа

Цифровой кодекс заменил классический административный метод регулирования **методом баланса интересов** — между правом личности на защиту данных и правом государства на их использование для общественных целей.



Принцип однократного предоставления

Если данные уже имеются в госсервисе, их нельзя запрашивать повторно. Это снижает административную нагрузку на граждан и бизнес.



Принцип минимизации и пропорциональности

Запрещён сбор данных сверх целей обработки. Каждый запрос должен быть обоснован и пропорционален поставленной задаче.

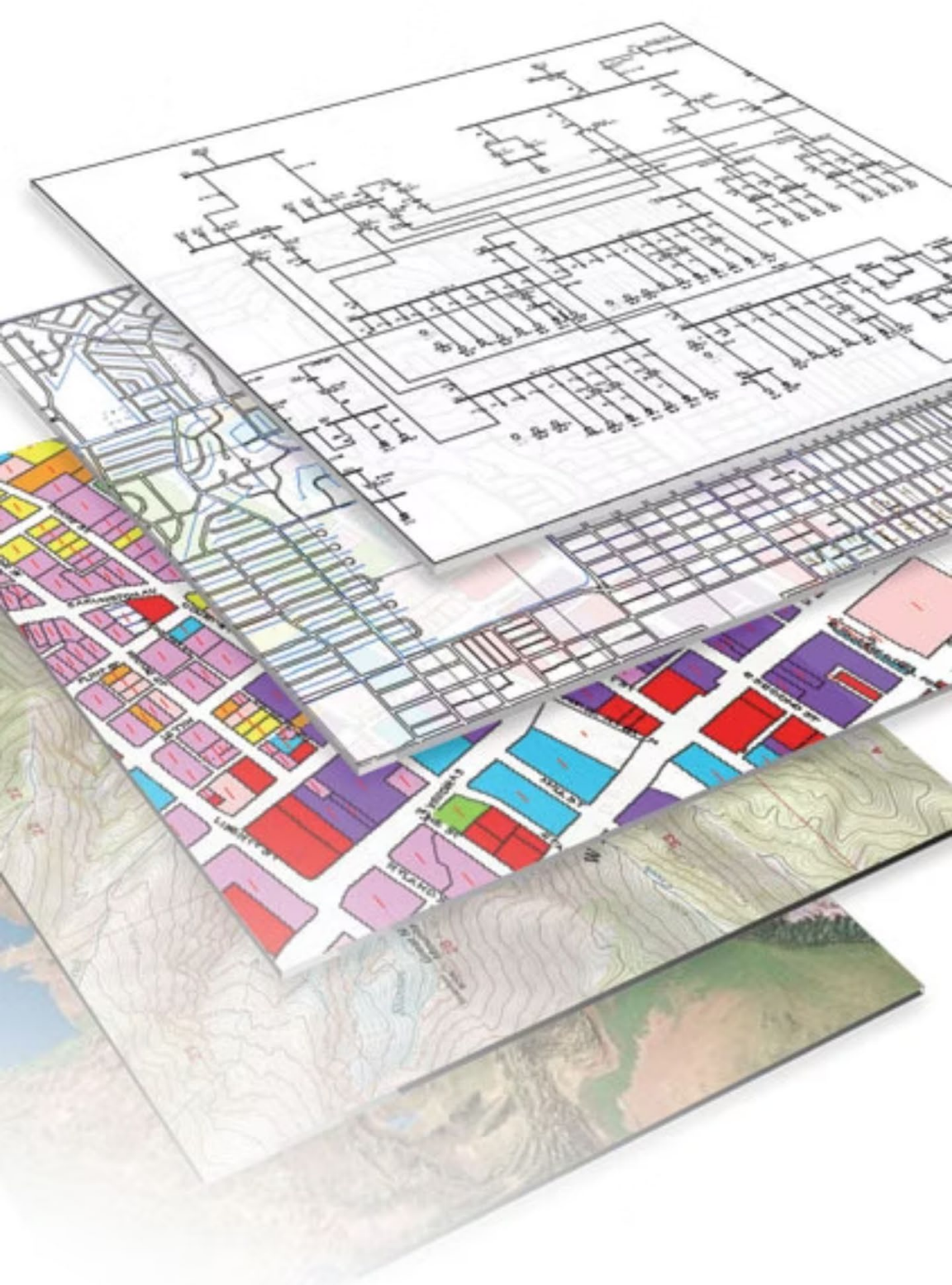


Принцип подотчётности

Каждый владелец техносистемы обязан фиксировать цифровые действия и доказывать законность обработки при любых проверках.

Такой метод ориентирован не на ограничение технологий, а на **их ответственное использование**. Он создаёт новую модель взаимодействия гражданина и государства — основанную на прозрачности, а не на недоверии.

Это переход от парадигмы «электронного управления» к **цифровому правовому государству**, где данные рассматриваются как юридически охраняемая форма общественного ресурса, требующая баланса публичных и частных интересов.



Пространственные данные в цифровой экономике

Виды данных

Пространственные данные включают географическую информацию, координаты объектов, картографические материалы и данные дистанционного зондирования Земли.

Они критически важны для транспорта, логистики, градостроительства, сельского хозяйства и множества других отраслей цифровой экономики.

Доступ к данным

Кодекс устанавливает специальный режим доступа к пространственным данным, обеспечивая баланс между открытостью информации и защитой стратегических интересов государства.

Государственные пространственные данные предоставляются в открытом доступе, за исключением сведений, составляющих государственную тайну.

Цифровые записи о юридических фактах

Цифровые записи становятся полноценным основанием возникновения, изменения и прекращения правоотношений в цифровой среде. Это революционное изменение в правовой системе, признающее цифровую форму равной традиционной бумажной.

1 Юридические факты в цифровой форме

Основаниями возникновения, изменения, прекращения правоотношений в цифровой среде являются юридические факты, выраженные в цифровых записях, в том числе представленные в виде цифровых документов или в составе цифровых ресурсов.

2 Баланс интересов при использовании инструментов

Кодекс закрепляет правила, позволяющие поддержать баланс интересов сторон отношений при использовании современных цифровых инструментов, таких как смарт-контракт, цифровые подписи, печати и иные доверенные сервисы, а также при автоматическом принятии решений.

3 Признание иностранных сервисов

Кодекс предлагает механизм, аналогичный Регламенту eIDAS в Евросоюзе или Модельному закону IdM ЮНСИТРАЛ, позволяющий использовать в качестве оснований для возникновения, изменения, прекращения правоотношений в цифровой среде результаты использования иностранных сервисов.



Юридическая основа цифровых правоотношений

Цифровые записи, цифровые права, доверенные сервисы

Права принципала данных возникают по факту связи данных с лицом и прекращаются при уничтожении или обезличивании. Эта правовая архитектура обеспечивает **доказуемость** и **переносимость** прав в цифровом пространстве.

Она также создает основу для признания иностранных доверенных сервисов при соблюдении критериев соответствия, открывая путь к международной интеграции цифровых экосистем.



Цифровые записи

Юридические факты в цифровой среде выражаются в цифровых записях — в виде документов или в составе ресурсов. Удостоверение через доверенные сервисы.



Доверенные сервисы

Включают аутентификацию, электронные подписи, архивы, гарантированную доставку, аутентификацию сайтов. Международная совместимость через реестр.



Цифровые права

Возникают с момента создания/получения объекта, не требуют регистрации. При отчуждении права переходят к новому владельцу.

Цифровая подпись: от электронного документа к юридическому действию

Цифровой кодекс вводит новый правовой институт — **доверенные сервисы**, обеспечивающие юридическую достоверность действий, совершаемых в цифровой среде (глава 17).



Облачные подписи

Формируются удалённо, без токена или флеш-носителя, криптографическая база хранится в доверенном сервисе. Это упрощает использование и повышает доступность цифровой подписи для широкого круга пользователей.



Метки времени

Обеспечивают юридическую фиксацию момента совершения цифрового действия. Критически важны для доказывания последовательности событий и соблюдения сроков в правоотношениях.



Архивирование

Долгосрочное хранение цифровых записей с сохранением юридической силы. Гарантирует возможность проверки подлинности документов даже через десятилетия после их создания.

Владельцы таких сервисов обязаны обеспечивать непрерывность, безопасность и сохранность записей; нарушение этих обязанностей влечёт административную и гражданско-правовую ответственность. Это создаёт основу для безбумажного взаимодействия и электронных сделок с полноценной юридической силой.

цифровые документы

Обеспечение юридической силы цифровых документов

С криптографией (ЦП)

Без
криптографии

Неквалифицированная подпись
или печать

Квалифицированная подпись или
печать

Использование идентификатора в
цифровой записи в соответствии
с правилами системы
идентификации

Юридическая значимость
признается в случаях, когда есть
НПА или соглашение сторон,
предусматривающие порядок
проверки цифровой подписи

Юридическая значимость
признается **во всех случаях** (кроме
законодательного запрета
составления документа в цифровой
форме)

Юридическая значимость
признается, если **идентификатор
указан в самой цифровой записи**
или использован при её создании,
на что указано в метаданных

Доверенные сервисы

Доверенные сервисы образуют технологическую инфраструктуру цифрового правового государства. Они обеспечивают идентификацию, аутентификацию, подтверждение целостности данных и юридическую значимость цифровых действий.

Система доверенных сервисов включает аккредитацию поставщиков, технические стандарты, процедуры аудита и механизмы ответственности. Это создает надежную основу для цифровой трансформации государственных услуг и коммерческих сделок.



Государственные сервисы: участники, рамки и виды

Государственные сервисы предоставляются внутри национальной цифровой экосистемы (НЦЭ), за исключением сервисов специального органа по национальной безопасности.



Потребители

Физические и юридические лица, которым предоставляются пользовательские госсервисы — государственные услуги в электронной форме.



Пользователи

Государственные органы и юридические лица, использующие госсервисы для межведомственного взаимодействия и обработки данных.



Поставщики

Государственные органы, органы местного самоуправления и юридические лица — участники НЦЭ. Обязаны обеспечивать цифровую устойчивость госсервисов.

Виды госсервисов

- **Сервисы взаимодействия** — для межведомственной обработки данных и координации
- **Пользовательские сервисы** — для предоставления государственных услуг гражданам и организациям

Принципы

Пропорциональность, совместимость, учет интересов потребителя, доступность, уверенность в надежности, упрощение процедур, обратная связь.



Важная гарантия: основанием обработки персональных данных является исполнение публичных полномочий, согласие не требуется; запрещена избыточная обработка. Потребитель вправе не дублировать данные, уже имеющиеся в государственных ресурсах.

Особые требования для государственных сервисов

Для обращения в государственные органы и органы местного самоуправления Кыргызской Республики, включая получение государственных услуг, применяются специальные правила использования идентификаторов в рамках **Единой системы идентификации**, утверждаемые Кабинетом Министров Кыргызской Республики.

Юридическая равнозначность

Обращение и приложенные к нему материалы, образующие цифровой документ, признаются равнозначными обращению и материалам, подписанным собственноручной подписью и представленным на бумажном носителе.

Это фундаментальный принцип, устраняющий дискриминацию цифровой формы и стимулирующий переход к безбумажному документообороту.

Исключения из правила

Равнозначность не применяется в случаях, когда законодательством Кыргызской Республики установлен прямой запрет на обращение в государственные органы и органы местного самоуправления в форме цифровой записи.

Такие исключения должны быть минимальными и обоснованными особой важностью или чувствительностью процедур.



Правовое значение

Данные положения устанавливают правовую основу для цифрового взаимодействия граждан с государственными органами, обеспечивая юридическую защиту электронных обращений и документов при соблюдении установленных требований к использованию идентификаторов.

Роли в создании госсервисов и «фабрика госсервисов»

Координация, учет, тестирование, KPI

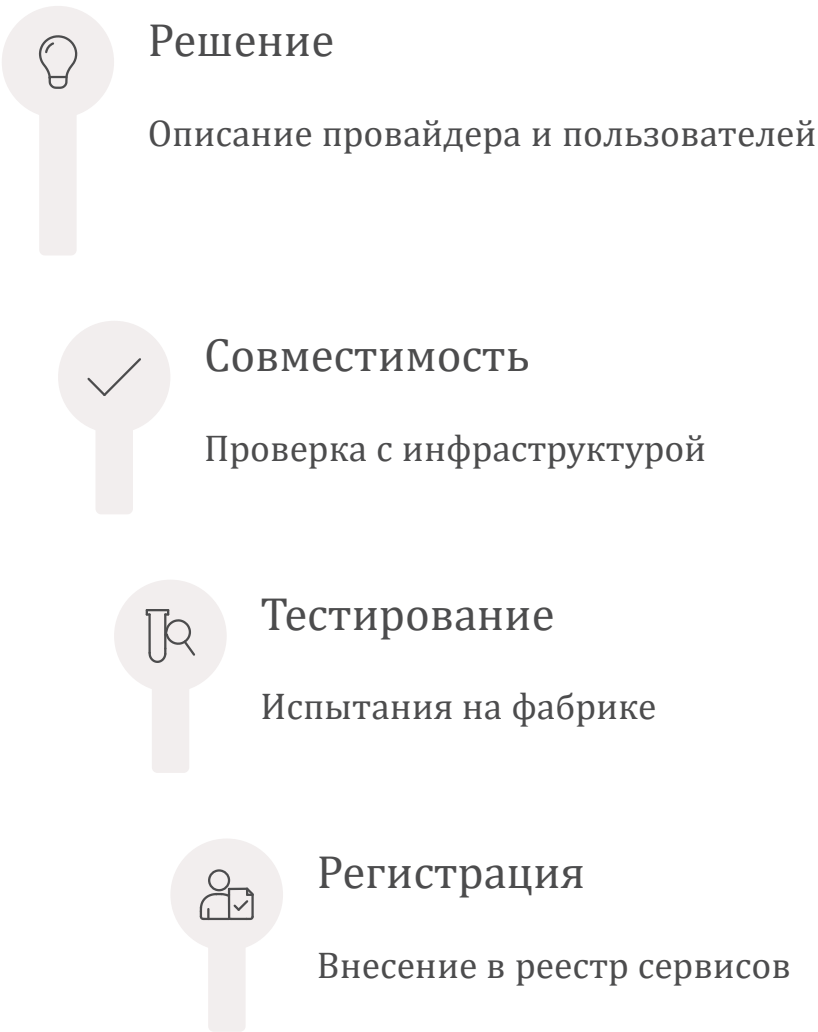
Отраслевой регулятор НЦЭ

- Создание и учет государственных сервисов
- Эксплуатация фабрики госсервисов
- Ведение приложений и сайта госсервисов
- Установление технических требований и KPI
- Проведение оценки цифровой устойчивости
- Выдача обязательных к исполнению предписаний

Фабрика госсервисов

- Доступ к общему пространству данных НЦЭ
- Тестирование сервисов перед запуском
- Мониторинг работы сервисов
- Развитие и совершенствование сервисов

Этапы создания сервиса



Споры по государственным сервисам

Административная процедура внутри НЦЭ

Процедура создает оперативный и обязательный к исполнению контур исправления нарушений качества и сроков предоставления услуг, усиливая подотчетность государственных органов в сфере цифровых публичных услуг.



Использование идентификаторов в цифровых записях

В соответствии с законодательством Кыргызской Республики, цифровая запись, содержащая идентификатор, используемый согласно правилам системы цифровой идентификации, приобретает юридическую силу цифрового документа, эквивалентного бумажному документу с собственноручной подписью.



Условие 1: Идентификатор в составе записи

Идентификатор содержится непосредственно в цифровой записи и в соответствии с правилами системы цифровой идентификации однозначно указывает на согласие лица, к которому относится идентификатор, с содержанием цифровой записи или подтверждает ознакомление данного лица с её содержанием.



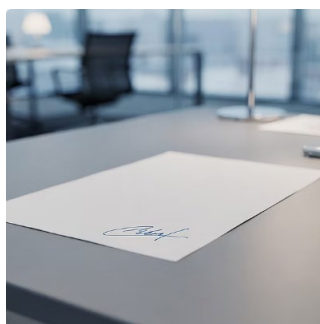
Условие 2: Идентификатор в метаданных

Указание идентификатора согласно правилам системы являлось необходимым условием создания цифровой записи, при этом метаданные записи содержат однозначное указание на лицо, от имени которого была создана данная цифровая запись.

Эти условия обеспечивают юридическую определенность и доказательственную силу цифровых записей, создавая надежную основу для электронного документооборота и цифровых сделок.

Цифровые документы

Цифровой документ — это цифровая запись, удостоверенная в установленном порядке и обладающая юридической силой. Кодекс устанавливает, что цифровые документы равнозначны традиционным бумажным документам при соблюдении определенных условий.



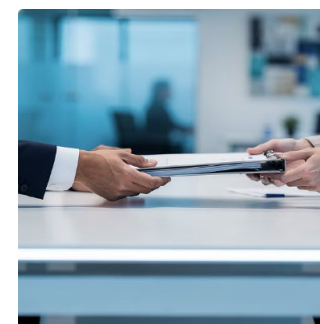
Требования к цифровому документу

Цифровой документ должен содержать реквизиты, позволяющие его идентифицировать, определить автора и дату создания. Обязательно использование средств электронной подписи или иных доверенных сервисов для удостоверения.



Хранение и архивирование

Владельцы цифровых документов обязаны обеспечивать их сохранность и возможность проверки подлинности в течение установленных сроков. Доверенные сервисы архивирования гарантируют долгосрочное сохранение юридической силы.



Обмен документами

Цифровые документы могут свободно передаваться между участниками цифровых правоотношений. Кодекс обеспечивает правовую определенность при электронном документообороте между гражданами, бизнесом и государством.

Сервисы цифрового благополучия

Сервисы цифрового благополучия — новый институт, направленный на защиту прав пользователей в цифровой среде и обеспечение здорового взаимодействия с технологиями. Эти сервисы помогают гражданам контролировать свое цифровое присутствие и защищать личные данные.



Защита персональных данных

Сервисы обеспечивают прозрачный контроль над тем, кто и как использует персональные данные пользователя. Включают инструменты для отзыва согласий и удаления данных.



Управление цифровым опытом

Инструменты для настройки алгоритмов рекомендаций, ограничения времени использования приложений, блокировки нежелательного контента. Поддержка осознанного потребления цифровых услуг.

Концепция цифрового благополучия признает, что технологии должны служить человеку, а не наоборот. Государство берет на себя роль защитника прав граждан в цифровом пространстве, создавая инфраструктуру для осознанного и безопасного использования цифровых сервисов.



Контроль цифрового следа

Пользователи получают возможность видеть свой цифровой след — кто собирал их данные, для каких целей, с кем они были переданы. Обеспечивается право на информацию.



Цифровая грамотность

Образовательные материалы и рекомендации по безопасному и эффективному использованию цифровых технологий. Помощь в развитии навыков критического мышления в цифровой среде.

Пользователь сервисов цифрового благополучия

Каждый гражданин Кыргызской Республики имеет право на использование сервисов цифрового благополучия. Эти права неотчуждаемы и гарантируются государством.

Права пользователя

Право на информацию о сборе и обработке персональных данных

Право на доступ к своим данным и их исправление

Право на удаление данных и забвение

Право на переносимость данных между сервисами

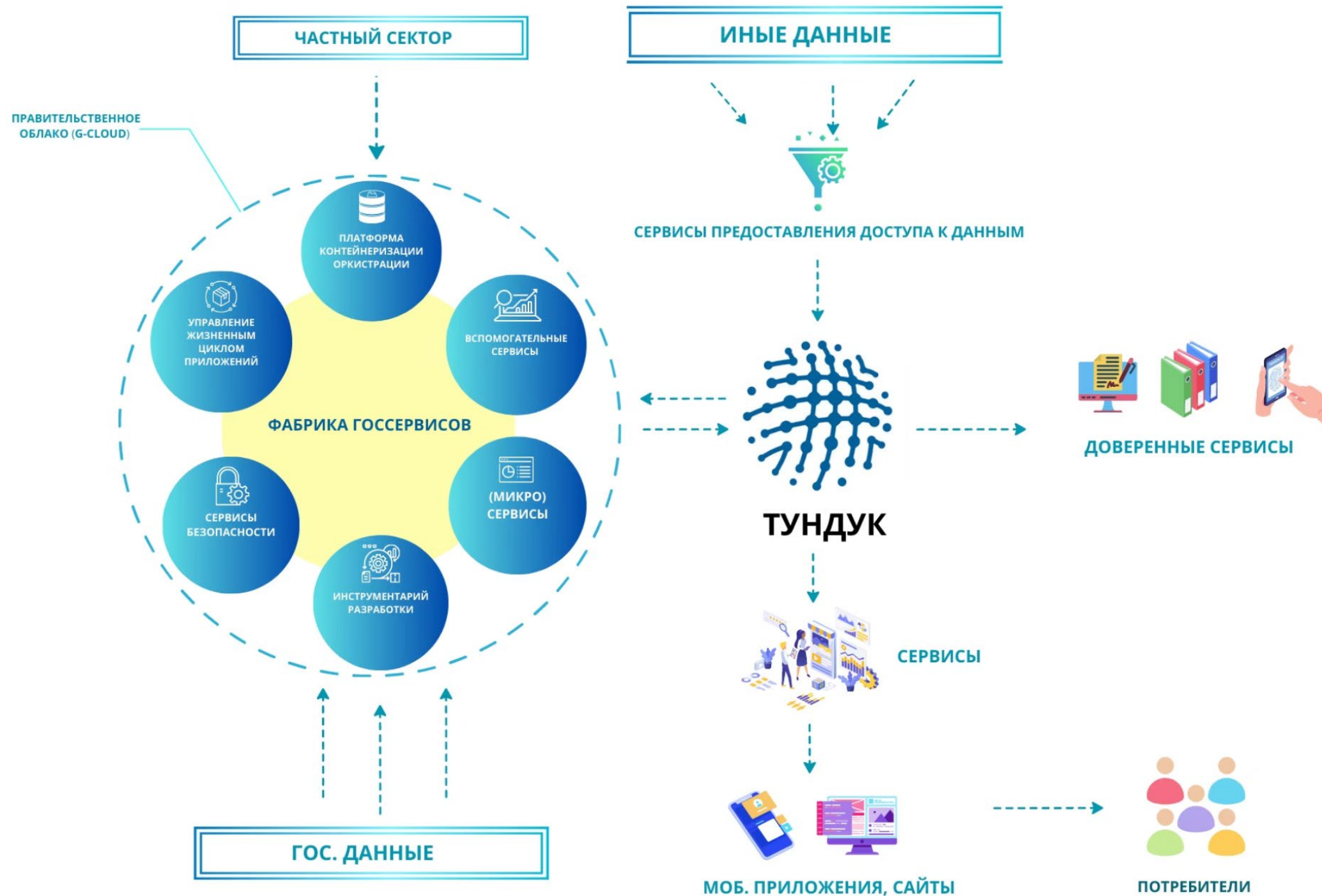
Право на отказ от автоматизированных решений

Право на защиту от манипулятивных практик

Цифровое благополучие — это не просто защита данных. Это концепция, при которой технологии обогащают жизнь человека, не причиняя вреда его психическому и физическому здоровью, социальным связям и личному развитию.



АРХИТЕКТУРА НАЦЭКОСИСТЕМЫ



Национальная цифровая экосистема представляет собой интегрированную архитектуру взаимосвязанных элементов, обеспечивающих цифровое взаимодействие участников. Система построена на принципах модульности и распределенности, что гарантирует высокую отказоустойчивость и масштабируемость инфраструктуры.

Принципы и развитие НЦЭ

Фундаментальные основы построения экосистемы

Общедоступность

Каждый может стать участником при соблюдении правил НЦЭ без дискриминации. Отсутствуют барьеры для входа, за исключением базовых требований безопасности и соответствия стандартам.

Модульность

Локальные инциденты не выводят из строя всю систему благодаря архитектуре независимых модулей. Каждый компонент функционирует автономно.

Облачный принцип

Независимость от конкретных устройств и географического местоположения пользователей обеспечивает гибкость и доступность сервисов.

Вариативность

Участник самостоятельно определяет состав используемых элементов экосистемы в зависимости от своих потребностей и задач.

Параллельность

Функции одного элемента могут дублироваться другими для обеспечения отказоустойчивости и непрерывности работы системы.

Независимость от поставщика

Открытые форматы данных и интерфейсы, отсутствие технологической привязки (vendor lock-in) гарантируют свободу выбора решений.



Управление развитием экосистемы

Развитие НЦЭ осуществляется по программам и планам, утверждаемым Кабинетом Министров. Допускается **инициативное создание** элементов с обязательным последующим внесением в реестр. На практике это требует архитектурного управления: единых форматов данных, открытых API, регламентов миграции и обратной совместимости для обеспечения бесшовной интеграции новых компонентов.

Ключевые механизмы функционирования НЦЭ

Регистрация и управление данными в экосистеме

01	02
Регистрация метаданных Метаданные подлежат обязательной регистрации в общедоступном для участников Каталоге метаданных, который ведет отраслевой регулятор Нацэкосистемы.	Принцип однократного сбора Цифровые ресурсы функционируют на принципах однократного сбора и многократного использования данных. Потребитель вправе не предоставлять данные, которые уже содержатся в государственных цифровых ресурсах.
03	04
Источники мастер-данных Определены официальные источники эталонных данных для обеспечения их достоверности и актуальности во всей экосистеме.	Подключение к системе Түндүк Каждый участник НЦЭ, зарегистрированный в цифровом реестре, может присоединиться к системе Түндүк, зарегистрировав заявку в Каталоге и выполнив технические требования.
05	
Фабрика сервисов Тестирование и запуск государственных сервисов осуществляется исключительно посредством Фабрики сервисов для обеспечения единых стандартов качества.	

1



Упрощенный доступ и обработка данных

2



R&D песочницы для исследования больших данных

3



Системные меры по развитию больших данных в традиционных отраслях

4



Обеспечение возможности обмена / обогащения данных

5



Финансирование инноваций и ресурсная экосистема

6



Стимулы для инновационных отраслей

Данные в НЦЭ и государственные цифровые технические средства

Общее пространство данных и требования к системам

Общее пространство данных

Цифровые ресурсы участников образуют **общее пространство данных НЦЭ**, обеспечивающее единую информационную среду для всех участников экосистемы.

Режим открытости

По общему правилу данные в общем пространстве являются **открытыми данными**. Право обработки данных может ограничиваться только законом; участники обязаны предоставлять доступ к ресурсам в случаях, установленных законом или соглашениями между участниками.

Обработка с учетом метаданных

- Владельцы и принципалы данных четко идентифицируются
- Цели и способы обработки документируются и контролируются
- Форматы данных стандартизированы для совместимости
- Интерфейсы доступа регламентированы и открыты

Обработка допускается независимо от формата данных, если иное не установлено нормативными актами. Для персональных данных и сведений, составляющих охраняемую законом тайну, предусмотрены специальные гарантии защиты.

1

Соблюдать требования

Выполнять требования, установленные Кабинетом Министров для государственных цифровых технических средств

2

Внести в реестр

Передать полные сведения о системе в централизованный реестр НЦЭ

3

Утвердить правила

Обеспечить их соответствие требованиям Цифрового кодекса

Техносистемы в составе НЦЭ

Цифровые технические средства представляют собой разнообразные системы обработки информации, от современных облачных платформ до традиционных решений.



Облачные платформы

Современные облачные сервисы и инфраструктура для хранения и обработки данных



Информационные системы

Автоматизированные системы управления данными и бизнес-процессами



Программное обеспечение

Прикладные и системные программные решения для участников экосистемы



Традиционные решения

Включая аналоговые системы; даже картотека на бумажных карточках является информационной системой

 **Широкое определение информационной системы:** Картотека на бумажных карточках – тоже информационная система. Это подчеркивает технологическую нейтральность подхода к регулированию и включение в экосистему различных форм организации данных.

Регулирование применения искусственного интеллекта

Нигде в мире ещё не существует проверенного временем подхода к регулированию применения ИИ. Все страны сейчас экспериментируют с различными моделями и методами. Чей подход окажется наиболее эффективным и чем именно он будет лучше – покажет только время и практика применения.



Два уровня регулирования

Важно различать **техническое регулирование ИИ** (в строгом смысле это вопрос технических регламентов и стандартов, определяющих параметры работы систем) и **регулирование применения ИИ** – это вопрос государственной политики: какое поведение в отрасли мы хотим стимулировать, какие риски минимизировать, и чего хотим добиться в долгосрочной перспективе развития технологий.



Основные международные подходы к регулированию применения ИИ

Четыре модели регулирования в мировой практике



Рекомендации по саморегулированию

- AI Bill of Rights (США)
- Рекомендации ОЭСР, ЮНЕСКО
- Добровольные этические принципы

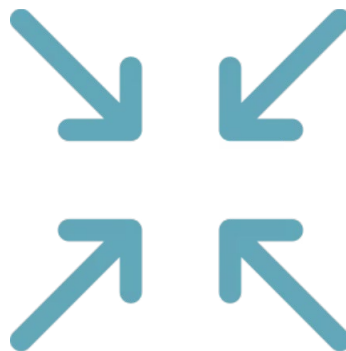
Мягкий подход, ориентированный на самостоятельную ответственность компаний



Тематическое и секторальное регулирование

- Ethical Norms for New Generation AI (КНР)
- Illinois Artificial Video Interview Act (США)
- Internet Information Service Algorithmic Recommendation Management Provisions (КНР)

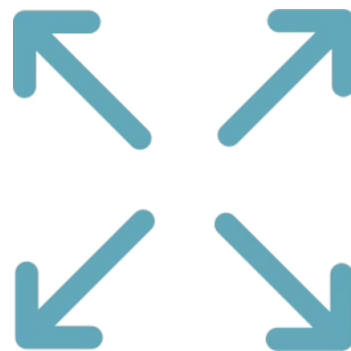
Регулирование конкретных применений и отраслей



Закон, детализируемый подзаконными актами

- Artificial Intelligence and Data Act (Канада)
- Establishing a pro-innovation approach to regulating AI (Великобритания)

Гибкая рамочная система с возможностью адаптации



Детальный общий закон

- EU AI Act (Европейский Союз)
- Комплексное горизонтальное регулирование с детальными требованиями и классификацией рисков

Принципы проектирования систем искусственного интеллекта

Базовые требования к разработке и применению ИИ

Разработчики сами определяют способы проектирования, разработки и применения систем ИИ. Вместе с тем, они обязаны следовать установленным принципам проектирования и учитывать широко применяемые документы по стандартизации, а также общепринятую мировую практику.



Снижение рисков

Минимизация потенциальных негативных последствий применения ИИ



Открытость

Прозрачность работы систем и доступность информации о них



Цифровая устойчивость

Обеспечение кибербезопасности и защиты от угроз

Подконтрольность

Возможность управления и контроля за работой системы

Объяснимость

Способность разъяснить принятые решения

Надёжность

Стабильность и предсказуемость работы (робастность)

Точность

Минимизация ошибок и высокое качество результатов



Презумпция соответствия: Предполагается, что эти принципы соблюдены, если выполнены конкретные требования Цифрового кодекса. Это создает правовую определенность для разработчиков.



Свобода разработки и применения систем ИИ

Общее правило: системы ИИ можно проектировать, разрабатывать и применять в Кыргызской Республике без каких-либо ограничений

Это фундаментальный принцип регулирования, направленный на стимулирование инноваций и технологического развития. Государство не устанавливает предварительных барьеров для создания и внедрения систем искусственного интеллекта.



Но есть исключения

Определенные категории систем ИИ подлежат специальному регулированию в случаях, когда их применение может создать повышенные риски для прав и законных интересов граждан, безопасности общества или государства.

Ограничения применения техносистем ИИ

Категории запрещенных и ограниченных систем

Цифровой кодекс устанавливает четкие границы допустимого использования искусственного интеллекта, основываясь на оценке рисков для фундаментальных прав человека и общественной безопасности.

Запрещенные системы

Системы, создающие недопустимый риск нарушения прав человека и основных свобод

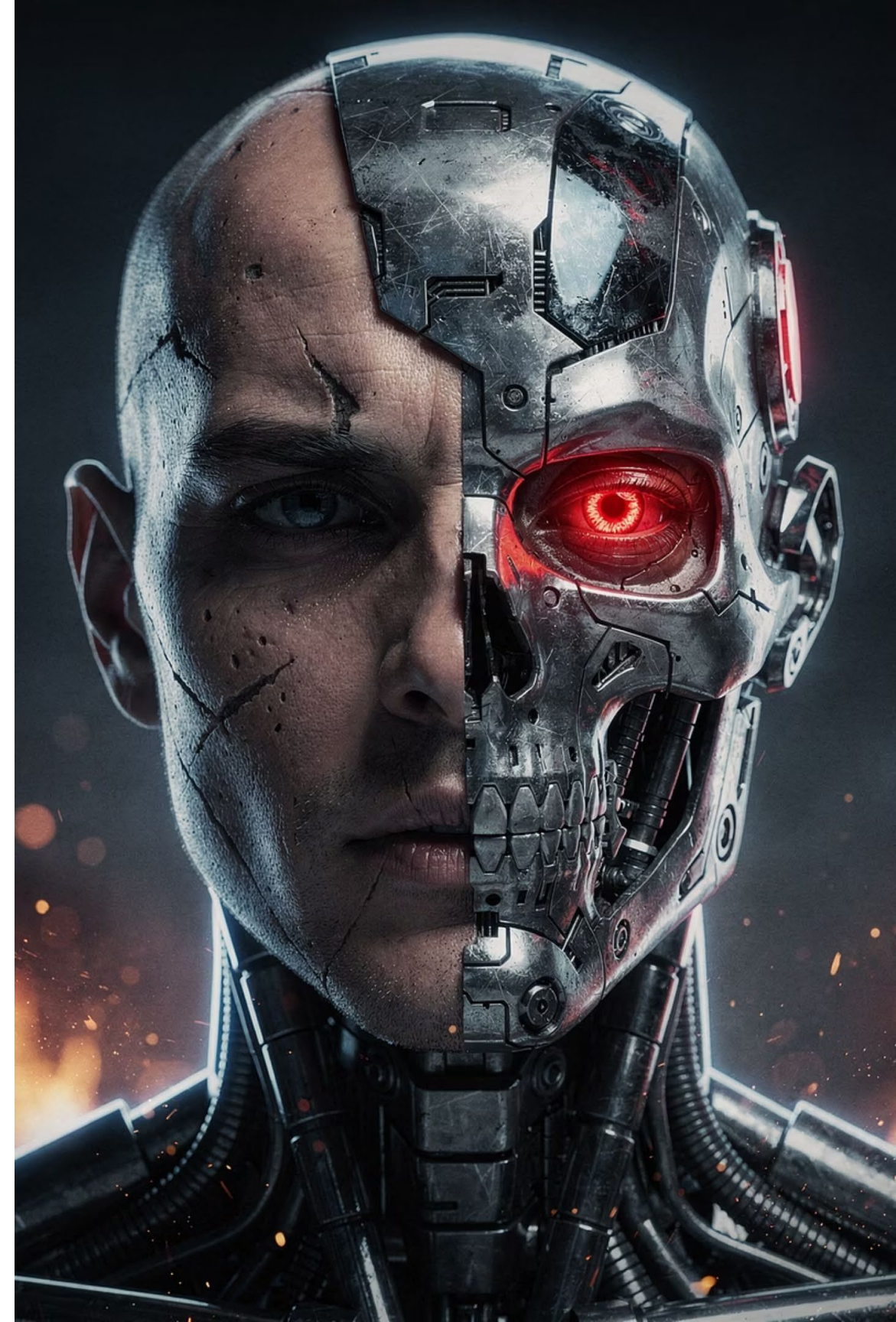
Системы повышенной опасности

Требуют специальных мер контроля и дополнительных гарантий безопасности

Системы с ограниченной прозрачностью

Должны раскрывать факт использования ИИ при взаимодействии с людьми

Классификация систем основана на риск-ориентированном подходе: чем выше потенциальный вред от системы, тем строже требования к ее разработке, внедрению и эксплуатации.



Системы ИИ повышенной опасности

Критерии классификации и дополнительные требования

Владелец сам оценивает риски

Владелец системы самостоятельно определяет, повышает ли использование ИИ риск для:

- Жизни и здоровья людей
- Конституционных прав и свобод граждан
- Общественной безопасности и правопорядка
- Экономической стабильности
- Окружающей среды

Это возлагает на владельцев систем ответственность за объективную оценку потенциальных рисков.

Дополнительные требования

Для систем ИИ с повышенной опасностью применяются усиленные стандарты:



Открытость

Документирование архитектуры и принципов работы



Объяснимость

Способность разъяснить логику принятия решений



Подконтрольность

Механизмы надзора и вмешательства человека



Точность и надёжность

Строгое тестирование и валидация



Цифровая устойчивость

Защита от кибератак и несанкционированного доступа



Принципы регулирования систем искусственного интеллекта

Регулирование искусственного интеллекта в Кыргызской Республике строится на сбалансированном подходе, который обеспечивает защиту прав граждан при одновременном стимулировании инновационного развития технологий. Система регулирования основана на принципах гибкости, пропорциональности рисков и технологической нейтральности.

Оценка рисков

Классификация систем по уровню потенциальной опасности

1

Самооценка и контроль

Владельцы систем несут ответственность за соответствие

2

3

4

Пропорциональное регулирование

Требования соответствуют уровню риска

Поддержка инноваций

Минимальные барьеры для развития технологий



Ключевые особенности подхода

Сбалансированное решение для развития экосистемы

Адаптация без копирования

Европейский подход использован как основа, но адаптирован к местным условиям. Исключены все излишне сложные процедуры и институты, которые могли бы затормозить развитие.

Без новых госорганов

Регулирование осуществляется в рамках существующих структур, что снижает административную нагрузку и обеспечивает эффективность.

Добровольная сертификация

Мы не требуем обязательной сертификации для большинства систем, что упрощает процесс внедрения инноваций.

Защита стартапов

Особое внимание уделяется защите растущих технологических компаний и создателей инновационных решений от избыточного регулирования.

Норм-принципы вместо жестких правил

Кодекс предлагает сбалансированное решение: регулирование на основе норм-принципов, без установления сложных и затратных процедур, что обеспечивает гибкость и адаптивность.

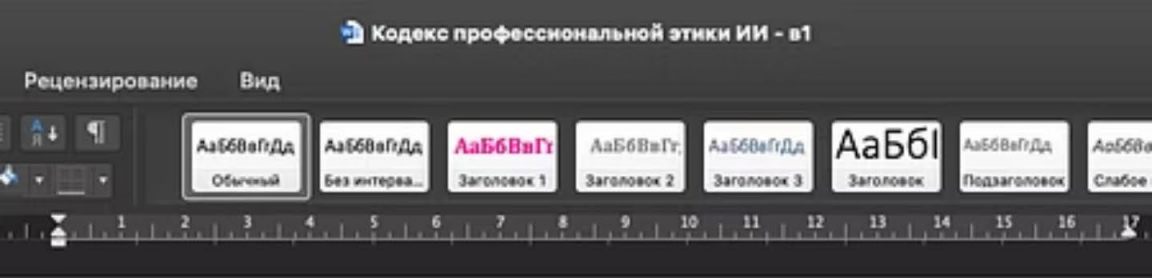
Стимулирование саморегулирования в сфере ИИ

Цифровой кодекс активно поощряет объединение владельцев систем искусственного интеллекта в профессиональные ассоциации, обеспечивающие контроль за деятельностью своих участников и их методическую поддержку.

Обязательные документы профессиональных ассоциаций

01
Кодекс профессиональной этики Этические стандарты разработки и применения ИИ
02
Методика оценки опасности систем ИИ Инструменты классификации рисков
03
Методика управления рисками Процедуры минимизации и контроля рисков
04
Методики проектирования и разработки систем ИИ Лучшие практики создания систем
05
Методика управления цифровыми данными Стандарты обработки и защиты данных
06
Требования к системе менеджмента качества Обеспечение стабильного качества разработки

Такой подход позволяет индустрии самостоятельно определять стандарты качества и безопасности, адаптируясь к быстро меняющимся технологиям, при сохранении государственного контроля за соблюдением базовых принципов.



КОДЕКС ПРОФЕССИОНАЛЬНОЙ ЭТИКИ для владельцев и разработчиков систем искусственного интеллекта в Кыргызской Республике AIDA

Преамбула

Настоящий Кодекс профессиональной этики (далее - Кодекс) устанавливает этические принципы, ценности и стандарты, которыми следует руководствоваться владельцам и разработчикам систем искусственного интеллекта (далее - ИИ) в Кыргызской Республике, а также доступные инструменты и практики по реализации указанных общих принципов и требований.

Кодекс распространяется на отношения, связанные с проектированием, конструированием, пилотированием, внедрением и использованием технологий ИИ на всех этапах их жизненного цикла, применяемых исключительно в гражданских целях, и призван обеспечить их ответственное развитие и использование, уважая при этом права человека, общественные интересы и культурные ценности Кыргызской Республики.

I. Цели и задачи Кодекса

Целями и задачами настоящего Кодекса являются:

1.1.Цели:

- Сформировать этическую основу для развития и использования ИИ в Кыргызской Республике.
- Повысить уровень доверия общества к системам ИИ.
- Минимизировать риски и негативные последствия, связанные с использованием ИИ.
- Способствовать развитию профессионального сообщества владельцев и разработчиков ИИ.

1.2.Задачи:

- Определить основные этические принципы, ценности и стандарты поведения для владельцев и разработчиков ИИ.
- Создать механизмы контроля и обеспечения соответствия систем ИИ этическим нормам.
- Повысить осведомленность общественности о этических аспектах ИИ.
- Способствовать международному сотрудничеству в области этики ИИ.

II. Ценности профессионального сообщества

Общими ценностями профессионального сообщества в сфере ИИ являются:

ьте рекомендации