ОБСЕ Академия в Бишкеке

NUPI Norwegian Institute of International Affairs

POLICY BRIEF

#119

Цифровой кодекс Кыргызской Республики и его влияние на финансовый сектор

Джусупов Акылбек Тойчуевич

НОЯБРЬ 2026

© 2026 Академия ОБСЕ в Бишкеке. Все права защищены.

Мнения, изложенные в настоящем докладе, и сделанные в нём выводы принадлежат исключительно автору и не обязательно отражают позицию или мнение Академии ОБСЕ в Бишкеке и Норвежского института международных отношений (NUPI).

Выдержки из настоящего доклада могут цитироваться или воспроизводиться в академических целях без получения специального разрешения при условии обязательного указания стандартной ссылки на источник. Руководство Академии по подготовке публикаций доступно по ссылке: https://www.osce-academy.net/upload/file/OSCE_AiB_Publication_guidelines.pdf

Настоящий доклад подготовлен при финансовой поддержке Министерства иностранных дел Норвегии в рамках сотрудничества Академии ОБСЕ в Бишкеке с Норвежским институтом международных отношений.

ОБСЕ АКАДЕМИЯ в Бишкеке
NUPI Norwegian Institute of International Affairs
POLICY BRIEF
119, НОЯБРЬ 2026

Цифровой кодекс Кыргызской Республики и его влияние на финансовый сектор

Джусупов Акылбек Тойчуевич

Аннотация

Для страны, не имеющей выхода к морю, цифровизация финансового сектора является важным инструментом интеграции в глобальную экономику. Принятие Цифрового кодекса Кыргызской Республики формирует единую правовую основу регулирования цифровых отношений, включая цифровые данные, цифровые сервисы, национальную цифровую экосистему и системы искусственного интеллекта.

Значение Кодекса для финансового сектора связано с установлением общих правил в отношении цифровых документов, обработки данных, цифровой идентификации, киберустойчивости и взаимодействия участников цифровой среды, включая противодействие мошенничеству. Отдельные положения Кодекса сопоставляются с подходами Европейского союза в рамках проведённого сравнительно-правового анализа.

В статье рассматриваются положения Кодекса, имеющие наибольшее значение для финансового сектора, а также формулируются практические рекомендации и отмечаются потенциальные риски применения. Хотя Кодекс не регулирует финансовые институты как самостоятельную сферу, он создаёт правовую основу для более широкого использования цифровых инструментов в финансовом секторе. Вместе с тем отдельные положения требуют дополнительного отраслевого регулирования и разъяснений для обеспечения правовой определённости и надлежащего комплаенса.

Джусупов Акылбек Тойчуевич — практикующий юрист и PhD в Докторской школе права и политических наук Университета Кароли Гашпар в Венгрии (KRE). Имеет почти 20-летний опыт работы в сферах финтеха, ИТ, банковского дела и корпоративного права. Занимал руководящие юридические должности как в частных, так и в государственных банках Кыргызской Республики. Его сферы изучения включают цифровые договоры, регулирование финтеха, экономическую интеграцию и правовое сопровождение цифровой трансформации. Акылбек получил степень магистра права (LL.M.) в области международного и европейского бизнес-права в Университете ELTE. В настоящее время принимает активное участие в академических и экспертных дискуссиях, посвященных управлению цифровой экономикой и регулированию финансовых технологий.

E-mail: akyldzhusupov@gmail.com

ВВЕДЕНИЕ

31 июля 2025 года был подписан Цифровой кодекс Кыргызской Республики[1] (далее — Кодекс), который положил начало регулированию цифровых правоотношений с февраля 2026 года после вступления в полную силу. В связи с вступлением Кодекса в силу прекращают действие такие законы, как «Об информации персонального характера», «Об электрической связи», «О биометрической регистрации граждан Кыргызской Республики», «Об электронном управлении», «Об электронной подписи», а также все изменения в Законе «Об электрической и почтовой связи». Такой кодифицированный документ по цифровизации принят впервые на пространстве Центральной Азии.

Цифровые финансовые услуги и продукты уже были представлены на рынке Кыргызской Республики (КР), а регулирование этих отношений преимущественно осуществляется на уровне подзаконных актов регулятора финансового сектора — Национального банка Кыргызской Республики (НБКР). В статье рассматриваются следующие вопросы: как Кодекс может повлиять на существующий порядок предоставления финансовых услуг с использованием цифровых технологий; какие изменения могут потребоваться в действующих

[1] Цифровой кодекс Кыргызской Республики от 31 июля 2025 года № 178 // Официальный сайт Министерства юстиции Кыргызской Республики. — URL: https://cbd.minjust.gov.kg/3-48/edition/35412/ru (дата обращения: 09.07.2026).

правоотношениях, локальных актах, договорах и публичных офертах финансовых институтов; а также какие возможности и правовые риски создают новые положения Кодекса для финансового сектора.

Поскольку отдельные нововведения Кодекса имеют сходство с законодательством Европейского союза (ЕС), в качестве сравнительной базы использовались правовые акты ЕС, в частности Закон eIDAS (2014). Исследование опирается на формально-юридический и сравнительно-правовой методы. Исследование основано на анализе Кодекса и иных нормативных правовых актов Кыргызской Республики, регулирующих цифровые правоотношения, а также на сопоставлении отдельных положений с подходами Европейского союза. Работа не оценивает сложившуюся практику правоприменения, судебные споры, фактическое соблюдение требований финансовыми институтами или результаты для потребителей. В целом Кодекс создаёт важную правовую основу для дальнейшей цифровизации финансового сектора, однако отдельные его положения могут порождать вопросы правовой определённости и комплаенса, требующие дополнительного отраслевого регулирования и разъяснений компетентных органов.

Ключевые выводы для финансового сектора

1. Кодекс создаёт общую правовую основу для цифровой идентификации, обработки персональных данных, доверенных цифровых сервисов, цифровых архивов и противодействия мошенничеству.

2. Наиболее существенные последствия для финансового сектора связаны с использованием идентификаторов, биометрических данных, обработкой персональных данных, цифровыми архивами и антифрод-взаимодействием.

3. Отдельные вопросы требуют дополнительного разъяснения или отраслевого регулирования, в том числе со стороны НБКР и иных компетентных органов.

4. Финансовым институтам следует пересмотреть договорную документацию, процедуры обработки данных, удалённой идентификации, хранения цифровых документов и противодействия мошенничеству.

ОБСУЖДЕНИЕ КАЖДОГО РАЗДЕЛА КОДЕКСА

Раздел первый

Анализ терминологического аппарата показывает переход от термина «электронный» к термину «цифровой». Это касается и базовых понятий: «электронная подпись» и «электронный документ» с вступлением Кодекса в силу именуются соответственно «цифровой подписью» и «цифровым документом».

Вызывает вопрос деление принципов регулирования цифровой среды на 3 группы: общеправовые, организационные и отраслевые принципы. Если в итоге принципы остаются принципами и ни одна из групп не обладает приоритетом, то преимущество такого группирования неочевидно. В этой связи предпочтительнее бы выглядел общий перечень принципов: так легче для восприятия.

«Принцип устойчивости», определяемый Кодексом, направлен на обеспечение стабильности правил и правоотношений. Данный принцип должен соблюдаться — в отличие от аналогичного принципа Налогового кодекса КР, в котором зафиксировали обязательство вносить изменения и дополнения только один раз в год, но с момента утверждения его уже несколько раз нарушали и вносили изменения.[2] Остается наблюдать, будет ли соблюдаться аналогичное ограничение Кодекса.

Кодекс определяет следующие сферы для регулирования (ч. 2 ст. 9 Кодекса):

1. персональные данные;
2. национальная цифровая экосистема[3] (далее — нацэкосистема);
3. телекоммуникации.

Отдельная сфера регулирования «финансы» в Кодексе не выделена; возможно, финансовый сектор будет регулироваться в

---

[2] Налоговый кодекс Кыргызской Республики // Официальный сайт Министерства юстиции КР. — URL: https://cbd.minjust.gov.kg/3-39/edition/1286442/ru (дата обращения: 09.07.2026).

[3] Цифровая экосистема — совокупность общедоступных цифровых технологических систем, цифровых ресурсов и цифровых сервисов, используемых для обеспечения взаимодействия субъектов правоотношений в цифровой среде по единым правилам (Кодекс, ч. 2 ст. 9).

рамках цифровой экосистемы. Вероятно, Национальный банк КР (НБКР) сохранит роль основного регулятора, что следует оценить положительно, т.к. единый надзорный орган обеспечивает большую определенность для финансовых организаций.

Кодекс предусматривает возможность проведения проверок субъектов регулирования аккредитованными лицами. Данный механизм следует анализировать с учётом положений Кодекса и соответствующего подзаконного регулирования. Если проведение таких проверок допускается при согласии субъекта регулирования, данный механизм целесообразно рассматривать как форму частного комплаенс-аудита, способную дополнять государственный контроль. Практическое значение механизма будет зависеть от порядка аккредитации, объёма полномочий проверяющих лиц, правового статуса результатов проверки и гарантий защиты прав субъектов регулирования.

Положительным сигналом для цифровых игроков является разрешение специального регулирования, или «песочницы», хотя и с исключением для банковского и платежного секторов. Правда, не совсем понятно, почему такое решение отнесено к компетенции Президента (ч. 1 ст. 16). При чтении Кодекса складывается впечатление, что ключевым органом в цифровых отношениях является Кабинет министров КР. Он определяет национального оператора телекоммуникаций, использует телекоммуникационные сервисы и сооружения в интересах государственного управления, устанавливает требования по защите персональных данных и основные правила в сфере использования цифровой подписи, цифровых архивов и систем искусственного интеллекта. Однако в случае со специальным регулированием неожиданно указан Президент КР как орган, разрешающий создание «песочницы».

Раздел второй

Раздел начинается с перечня объектов: цифровые данные, записи, документы, ресурсы, сервисы, экосистемы и технологические системы; далее следуют центры обработки данных и телекоммуникационные сети, а затем указаны земли, здания, строения, сооружения и иные аналогичные объекты. Возникает вопрос: как объекты гражданских правоотношений могут одновременно выступать объектами в цифровой среде?

Принудительное отчуждение или ограничение цифровых прав в отношении конкретного объекта допускается только на основании решения суда « в случаях, прямо предусмотренных законодательством» (ч. 6 ст. 24 Кодекса). В приведенной норме прослеживается недоработка законодателя: случаи принудительного отчуждения в самом Кодексе не установлены. Кодекс, регулирующий цифровые права, призван исчерпывающе определять соответствующие правила и не оставлять возможности влиять на них нижестоящим актам. При этом под законодательством понимаются не только законы, но и подзаконные акты — постановления и указы.

Согласно Кодексу участниками (субъектами) являются:

- владельцы цифровых записей,
- владельцы цифровых ресурсов,
- владельцы цифровых технологических систем,
- владельцы экосистем,
- поставщики цифровых сервисов,
- принципалы данных,
- пользователи,
- обработчики.

Нормы об «идентификаторах» представляются несколько противоречивыми. Идентификатор — любая информация (в том числе код, шифр, номер или адрес), позволяющая связывать цифровые записи, содержащие такую информацию, между собой и с субъектом правоотношений в цифровой среде. Идентификатор, использованный в цифровой записи в соответствии с правилами системы цифровой идентификации, считается цифровым документом, аналогичным документу на бумажном носителе, подписанному собственноручной подписью. Другими словами, данный инструмент предоставляет информацию, известную ограниченному кругу лиц, которая позволяет из общей группы идентифицировать конкретное лицо, с которым строятся определенные правовые отношения. Однако ст. 42 Кодекса к уникальному публичному идентификатору для физических лиц относит персональный идентификационный номер (ПИН) и указывает, что уникальные публичные идентификаторы являются общедоступными данными. Возникает вопрос: как может «персональный» номер стать «публичным»? Тем более что ПИН содержит дату рождения лица,[4] которая относится к персональным

[4] Пункт 3 Порядка присвоения и изменения персонального идентификационного номера, утвержденного постановлением Кабинета Министров Кыргызской Республики от 17 апреля 2025 года № 207.

данным в соответствии с п. 7 ч. 4 ст. 48 Кодекса. Слишком много чувствительной информации отнесено к общедоступным данным. Такой подход законодателя вызывает множество вопросов и создает существенные правовые неопределенности. Ранее примерно такую роль выполняла «простая электронная подпись»[5] (далее — ПЭП). После того, как утратил силу Закон «Об электронной подписи», данный вид перестал быть актуальным. Таким образом, финансовым институтам необходимо внести изменения в шаблоны договоров (публичной оферты), размещаемые на сайтах или в приложениях, а также в свои локальные нормативные акты, в которых упоминается ПЭП.

Цифровая идентификация и цифровая аутентификация являются основанием для возникновения, изменения, прекращения правоотношений, в том числе для целей доказывания (ч. 3 ст. 46). Весьма важная норма для развития бизнеса, если не учитывать, что ч. 4 этой же статьи неожиданно добавляет формулировку *«подтверждает личность физического лица»* при цифровой аутентификации. Соответственно, эти слова могут дать основание для вывода, что цифровая идентификация и аутентификация предназначены только для физических лиц. Вместе с тем цифровую идентификацию можно проводить и в отношении юридических лиц.

Положения относительно биометрических данных должны вызвать повышенный интерес у представителей финансового сектора. Обработка биометрических данных *(изображение лица, узоры пальцев, собственноручная подпись)* не допускается, за исключением целей проведения выборов и референдумов, получения и предоставления госсервисов или прямо предусмотренных законом (ч. 2 ст. 48 Кодекса). Таким образом, есть вероятность признания запрета использования биометрических данных для банковской деятельности, пока специальный закон[6] прямо не разрешит это. В настоящее время Закон Кыргызской Республики «О банках и банковской деятельности» ничего существенного о цифровизации (к примеру, по цифровой подписи или удаленной идентификации) не содержит, хотя в свое время я лично предлагал включить положения,[7] которые уже

---

5 Джусупов А. Т. Электронная подпись как подпись на расстоянии // Официальный сайт ОЮЛ «Союз банков Кыргызстана». — URL: https://ub.kg/ru/elektronnaya-podpis-kak-podpis-na-rasstoyanii/ (дата обращения: 09.06.2026).

6 О банках и банковской деятельности: Закон Кыргызской Республики от 11 августа 2022 года № 93 // Официальный сайт Министерства юстиции КР. — URL: https://cbd.minjust.gov.kg/4-3214/edition/1241184/ru (дата обращениея: 09.06.2026).

7 Джусупов А. Т. Эксперт высказался о законопроектах, регулирующих работу Нацбанка // Портал Banks.kg. — 02.06.2022. — URL: https://banks.kg/news/expert-on-draft-laws-

работали на тот момент на основании подзаконных актов. Поэтому если банки желают продолжать использовать биометрические данные клиентов для своих цифровых сервисов и соответствовать ст. 48 Кодекса, в первую очередь необходимо прямо предусмотреть это в Законе КР «О банках и банковской деятельности». Кодекс также целую статью посвятил ответственности за нарушение права на идентичность, а также утвердил, что цифровая запись может содержать юридический факт, а принадлежность цифровых прав может подтверждаться метаданными.

КР внедряет новые институты «доверенных цифровых сервисов», которые встречаются в законодательстве ЕС, в частности eIDAS.[8] eIDAS имеет важное трансграничное значение для ЕС, поскольку устанавливает единые правила взаимного признания государствами-членами национальной цифровой идентификации в рамках ЕС, создавая единую правовую и техническую основу, обеспечивающую интероперабельность и признание национальных схем цифровой идентификации для цифровых транзакций на внутреннем рынке.[9] Кодекс КР регулирует более широкий круг отношений, чем eIDAS. Даже в части доверенных цифровых сервисов он в ст. 55 предусмотрел пять следующих направлений (в том числе иностранных):

1. сервисы цифровой аутентификации;
2. сервисы цифровых подписей;
3. сервисы цифровых архивов;
4. сервисы гарантированной доставки сообщений;
5. сервисы аутентификации сайтов.

Что касается цифровых записей (цифровые данные, которые могут быть идентифицированы с использованием метаданных), то доступ к ним или их распространение в соответствии со ст. 61 Кодекса могут быть ограничены с учетом метаданных таких записей на основании закона исключительно в следующих случаях:

---

regulating-work-of-nbkr (дата обращениея: 09.06.2026).

8 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

9 Polánski, Przemyslaw, «Towards the single digital market for e-identification and trust services». *Computer Law and Security Review*, Volume 31, Issue 6 (December, 2015), pp. 773–781.

- если ограничение доступа является осуществлением цифровых прав;
- если метаданные цифровых записей указывают на их отнесение к охраняемой законом тайне;
- если распространение цифровых записей или доступ к ним запрещены законом или решением суда.

Исследователи и научные организации имеют право на доступ к цифровым записям, содержащим персональные данные или отнесенным к охраняемой законом тайне, в научных, статистических или иных исследовательских целях при условии обеспечения их конфиденциальности (ч. 3 ст. 61 Кодекса).

Раздел третий

Данный раздел начинается с Главы 10 («*Общие положения об обработке цифровых данных*»), в которой устанавливаются общие принципы и правила обработки[10] цифровых данных в КР. В частности, указываются четыре принципа: добровольности участия (1), добросовестности (2), повторного использования (3), совместимости и переносимости (4).

Запрещается недобросовестная обработка, включая использование неточных данных, нарушение идентичности, дискриминацию, избыточные сборы, навязывание условий, несоразмерность и неизвестность целей обработки (ст. 71). Принципалы данных имеют широкий круг прав на получение информации об обработке и доступ к своим данным, за исключением случаев, прямо ограниченных законом *(оперативно-розыскная, уголовно-процессуальная, деятельность в сфере государственной тайны)*. Согласно ст. 75 и 76 владельцы записей обязаны исправлять и дополнять данные, обеспечивать их переносимость в стандартных форматах и информировать принципалов о произведённых изменениях, соблюдая установленные сроки.

---

[10] Обработка — любое действие (операция) или совокупность действий (операций), совершаемых с цифровыми данными (цифровыми записями), включая сбор, запись, организацию, структурирование, накопление, хранение, адаптацию или изменение, загрузку, просмотр, использование, раскрытие посредством передачи, распространение, обмен или иной вид предоставления доступа, сопоставление или комбинирование, сокращение, удаление или уничтожение (Кодекс, ст. 1).

Глава 11 «Обработка персональных данных» (ПД) содержит новые правила в отношении чувствительной информации, в частности регулирует любую обработку ПД *(цифровых и бумажных)*, кроме обработки в личных и семейных целях. Кодекс устанавливает шесть принципов обработки ПД, соблюдение которых возлагается на владельцев записей: (1) законности, справедливости, прозрачности, (2) ограничения цели, (3) минимизации данных, (4) точности, (5) ограничения хранения, (6) целостности и конфиденциальности.

ПД обрабатываются на основании договора, закона, защиты жизненных интересов субъекта ПД или иного лица, общественно полезных задач владельца записей *(например, жизнь человека, интересы общества, гуманитарные и экологические задачи)*, законных интересов владельца записей или третьего лица *(при условии ненарушения прав субъекта ПД)*. Большинство из этих оснований представляются обоснованными, за исключением отдельных расплывчатых описаний. В частности, формулировки *«общие интересы»* и *«законные интересы владельца записей»* могут способствовать чрезмерному использованию ПД, противоречащему принципам *«ограничения цели»* и *«минимизации данных».*

Согласие должно быть конкретным и может быть отозвано в любой момент *(процедура отзыва не должна быть сложнее выдачи)*. Если запрос на согласие написан непонятным языком или спрятан внутри другого документа, такое согласие считается недействительным.

Запрещена обработка детских и чувствительных данных о расе, этносе, политике, религии, генетике, биометрии и здоровье (особая категория), за исключением случаев, прямо прописанных в законе *(например, исполнение договора или закона, медицинский диагноз, общественное здравоохранение, правосудие, статистика, нацэкосистема или национальная безопасность)*. Данные детей обрабатываются строго в их интересах.

Удаление данных, возражения и ограничения обработки (ст. 83–85). Можно ли утверждать, что в КР внедряется «*право быть забытым*» — норма, давно существующая в ЕС?[11] Владелец записей обязан удалять данные по требованию субъекта или при утрате оснований обработки. Однако такое право не имеет безусловного характера: владелец вправе не удалять данные в целях обеспечения свободы

[11] Оганесян Т. Правовые основы, пределы и стандарты применения права быть забытым: опыт Европейского союза // Вестник Санкт-Петербургского университета. Право. — 2023. — Т. 14. — № 3. — С. 750–767.

слова, исследований, защиты правовых обязательств. Субъект также может возразить против обработки, после чего владелец записей обязан прекратить ее при наличии оснований *(автоматические решения, дискриминация, отказ от записей, выход из сообщества и другие)*. На время рассмотрения возражения или при возникновении оснований для исправления или удаления данных обработка должна быть ограничена с обязательным уведомлением субъекта.

ПД могут обрабатываться не только владельцами записей, но и третьими лицами (обработчиками) на основании правового акта или договора. Договор должен детально регулировать тип ПД, обязанности, сроки, безопасность и учёт операций. При совместном владении данные обрабатываются по опубликованному порядку распределения обязанностей; субъект может обращаться к любому из совместных владельцев. В экосистемах и сообществах ответственность за соблюдение правил несёт владелец экосистемы или уполномоченное лицо.

В части защиты ПД внедрены новые требования по сравнению с утрачивающим силу Законом КР «Об информации персонального характера». В частности:

- если у владельца записей более 10 сотрудников, должно быть определено лицо, ответственное за обработку ПД из числа сотрудников либо внешних лиц;
- конструктивная защита при создании цифровых продуктов;
- ведение учета операций;
- обучение правилам обработки ПД.

В части регулирования «трансграничной передачи» (ст. 89) Агентство по ПД *(уполномоченный госорган)* ведет реестр государств, обеспечивающих адекватную защиту ПД, и передача ПД в эти страны не может быть запрещена. Но в государства, которые не признаны обеспечивающими адекватную защиту, ПД можно передавать только при наличии специальных оснований *(согласие, договор, интересы безопасности, защита жизни и др.)* или договорных гарантий защиты.

Раздел четвертый

Общие правила предоставления цифровых сервисов[12] устанавливаются самими поставщиками с соблюдением баланса интересов пользователей и международной практики и основываются на следующих принципах: инклюзивность, обоюдная защита, отсутствие разрешения (без бюрократии), свобода устройств, недискриминация, взаимное обеспечение устойчивости.

Пользование сервисами допускается только на основании пользовательского соглашения (в любой форме), которое должно быть доступным, информативным и изменяемым с предварительным уведомлением (ст. 114). Поставщик обязан хранить связанные с ним и конкретным пользователем цифровые записи в период действия соглашения и не менее трех лет после прекращения.

Важное положение Кодекса касается порядка изменения условий «пользовательского соглашения». Во-первых, уведомление о вносимых изменениях должно направляться пользователю не позднее чем за один месяц. Во-вторых, в случае несогласия пользователя с новыми условиями соглашение прекращается, а поставщик обязан вернуть все неиспользованные денежные средства за вычетом стоимости фактически оказанных услуг.

Поставщики сервиса должны четко идентифицировать себя (если поставщиков два и более — один из них должен быть уполномоченным представителем), действовать добросовестно, не заниматься недобросовестной конкуренцией (манипулированием алгоритмами поиска, ценами и приоритетностью товаров и услуг, созданием предусловий, требованием уступки прав, ограничением ухода, принудительными акциями, созданием фаворитов) и не ограничивать права пользователей (ст. 115–117).

Пользователи имеют право на создаваемые ими цифровые записи, обязаны сохранять свою идентичность и корректно использовать сервис. При этом потребители (физические лица) получают дополнительные права на отказ от сервиса, информационную поддержку и удаление своих данных после отказа от сервиса (ст. 118).
Если пользователь отказывается от сервиса, то поставщик обязан:

[12] Цифровой сервис — возможность использования цифровой технологической системы для создания, передачи, хранения цифровых данных или доступа к ним (Кодекс, ст. 1).

- произвести расчет (возврат денежных средств за неиспользованный сервис);
- предоставить имеющиеся данные о пользователе;
- предложить варианты копирования всех записей;
- обеспечить возможность удаления его цифровых записей;
- хранить данные в течение одного (1) года после прекращения соглашения.

Глава также регулирует порядок рассмотрения жалоб и споров, предписывая создание четкого канала подачи жалоб (через сайт или приложение). Жалоба подается первоначально поставщику, затем — в порядке обязательного досудебного обращения — регулятору, далее — в суд. Также главой устанавливается ответственность поставщиков за недоступность (штраф в размере двойной цены), задержку и ненадлежащее качество сервиса или данных (штраф в размере одной цены), а также причинение вреда пользователю; при этом поставщику предоставляется право приостанавливать доступ к сервису в случае нарушений со стороны пользователей.

Цифровые сервисы далее детально регулируются по следующим направлениям:

- сервисы цифрового благополучия (глава 15);
- телекоммуникационные сервисы (глава 16);
- доверенные сервисы (глава 17);
- госсервисы (глава 18).

Глава 15 «О сервисах цифрового благополучия»[13] посвящена сервисам, которые могут свободно создаваться и использоваться при соблюдении требований Кодекса и недопущении ущемления прав граждан, особенно при применении таких сервисов в медицине.

Устройства цифрового благополучия должны соответствовать техническим требованиям, сервис должен обеспечивать совмести-

[13] Сервис, направленный на улучшение качества жизни физического лица на основе обработки цифровых данных о его физиологических особенностях (Кодекс, ст. 1).

мость с любыми подходящими устройствами. Искусственный интеллект в таких сервисах относится к системам повышенной опасности, что требует соблюдения специальных требований. Потребители получают расширенную защиту — право на возмещение вреда, в том числе морального, либо получение фиксированной компенсации при нарушениях со стороны поставщика, при недоступности данных.

Положения о доверенных сервисах[14] (далее — Доверсер) не в полной мере согласованы с общей частью. Согласованность наблюдается в ст. 55 Кодекса: упоминаются сервисы аутентификации, подписей, архивов, гарантированной доставки сообщений и аутентификации сайтов. Однако в особенной части регулирование Доверсера начинается только с цифровых подписей и архивов как ключевых инструментов удостоверения юридически значимых действий в цифровой среде.

Подчеркивается, что законами могут устанавливаться особенности использования Доверсеров для следующих видов отношений:

- подготовка и проведение выборов и референдумов;
- совершение гражданско-правовых сделок;
- предоставление госсервисов;
- осуществление платежей и банковских операций;
- ведение бухгалтерского и налогового учета.

Перспективным для банковского сектора представляется принятие отдельных законов (или внесение изменений в действующие законы) с детально прописанными особыми возможностями для цифровых подписей, архивов, гарантированной доставки сообщений, аутентификации личности и сайтов. Пока такого специального закона нет, отдельные отношения регулируются подзаконными актами НБКР.

В процессе чтения Кодекса возникает обоснованный вопрос: почему «Цифровая подпись» (ЦП), представляющая самостоятельный институт, не выделена в отдельную главу регулирования? Раньше

[14] В свою очередь, доверенный цифровой сервис — цифровой сервис, направленный на удостоверение возникновения, изменения или прекращения отношений в цифровой среде (там же).

«электронной подписи» был посвящен отдельный закон.[15] Сейчас же она оказалась лишь частью главы о Доверсерах. Это странно, учитывая, что «простая электронная подпись» была исключена из данного определения, перейдя в другую главу как термин «идентификатор». Глава также определяет, что ЦП могут иметь неквалифицированный или квалифицированный статус, причем они обеспечивают полную юридическую силу, равнозначную юридической силе бумажного документа с собственноручной подписью и печатью.

Значительное внимание уделено условиям признания иностранных подписей, роли доверенной третьей стороны и взаимодействию с зарубежными Доверсерами, а также закреплению принципов технологической нейтральности, свободы выбора Доверсеров. Включение нормы (ч. 4 ст. 137) о недопустимости отказа в юридической силе документов только по причине использования ЦП или иных электронных средств (в том числе иностранных, согласно ч. 3 ст. 140) поможет участникам судебного процесса использовать цифровые доказательства. Практикующая судья КР в своей статье отмечает активное использование социальных сетей в качестве доказательств в семейных спорах.[16] Введение таких норм в Кодекс рассматривается как весомый вклад в цифровизацию судопроизводства. Таким законодательным актом ЕС, регулирующим электронные доказательства, является Закон о сотрудничестве между судами государств-членов при собирании доказательств по гражданским или коммерческим делам (о получении доказательств).[17] В соответствии со статьей 7 данного Закона *«Документам, передаваемым через децентрализованную ИТ-систему, не может быть отказано в юридической силе или они не могут считаться недопустимыми в качестве доказательства в судебном разбирательстве исключительно на том основании, что они представлены в цифровой форме».*

---

[15] Об электронной подписи : Закон Кыргызской Республики от 19 июня 2017 года № 93. Утратил силу с 31 июля 2025 года // Официальный сайт Министерства юстиции Кыргызской Республики. — URL: https://cbd.minjust.gov.kg/4-2446/edition/985628/ru (дата обращения: 09.07.2026).

[16] Назирдинова Ч. Использование информационных технологий в гражданском судопроизводстве Кыргызской Республики и перспективы их дальнейшего развития // Ala-Too Academic Studies. — 2023. — № 1. — С. 391–405.

[17] Regulation (EU) 2020/1783 of the European Parliament and of the Council of 25 November 2020 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (taking of evidence) OJ L 405, 2.12.2020.

Отдельная часть главы посвящена обязанностям субъектов при использовании ЦП, включая обеспечение конфиденциальности ключей, своевременное уведомление о компрометации, проверку подлинности подписи и использование сертифицированных средств криптографической защиты. Детально регламентируются деятельность удостоверяющих центров (создающих сертификат ключа для ЦП), их аккредитация, ведение реестров сертификатов, обязанности по хранению данных, ответственность за нарушения и порядок передачи записей при прекращении работы (ст. 144). Государственные органы получают полномочия по аккредитации удостоверяющих центров, подтверждению соответствия средств подписи, ведению реестров сертификатов, обеспечению функционирования доверенной третьей стороны и круглосуточного доступа к ключевой информации.

Цифровизация жизнедеятельности — это прежде всего большие данные и документы, которые подлежат хранению где-то. Особенно актуально для банков, которые в среднем должны хранить не менее пяти лет документы 533 видо,[18] а учитывая клиентскую базу организаций финансового сектора, насчитывавшую 26 млн[19] клиентов на конец июня 2026 года, количество документов может исчисляться сотнями миллионов. Цифровые архивы (простые или квалифицированные) признаются самостоятельными Доверсерами, обеспечивающими долгосрочную неизменность и целостность цифровых записей на основании закона или соглашения (ст. 150). Квалифицированные архивы используются для хранения документов, подписанных квалифицированной цифровой подписью.

Вводится понятие «цифрового дубликата» документа, который может заменять подлинник (или пакет документов) на бумажном носителе при соблюдении требований к полноте воспроизведения и неизменности, при этом хранение даже подлинника может быть прекращено, если он не относится к документам, подлежащим обязательному сохранению (ст. 151). Причем если даже подлинника нет, то это не является основанием для отказа в признании его юридической силы.

---

[18] Перечень основных документов, образующихся в деятельности коммерческих банков и финансово-кредитных учреждений, лицензируемых Национальным банком Кыргызской Республики, с указанием сроков хранения. Утвержден постановлением Правления Национального банка КР от 27 августа 2004 года № 22/9.

[19] Число клиентов финансового сектора превысило 26 миллионов // Национальный статистический комитет Кыргызской Республики. — 25.08.2026. — URL: https://stat.gov.kg/ru/news/chislo-klientov-finansovogo-sektora-prevysilo-26-millionov/ (дата обращения: 09.07.2026).

В совокупности нормы главы формируют единый правовой механизм для обеспечения юридической значимости цифровых взаимодействий, безопасности цифровых документов и устойчивости национальной системы цифровой идентификации и архивного хранения. Авторы книги «Электронное правосудие»[20] подчеркивают требования, которым должны соответствовать национальные судебные системы стран ЕС при рассмотрении дел с использованием письменных электронных доказательств:

- обеспечение надежности электронных доказательств — личность подписанта может быть подтверждена, а целостность данных гарантирована возможностью проверки при возникновении объективных сомнений;

- обеспечение хранения доказательств, их читабельности, доступности, целостности, подлинности, надежности, а при необходимости и конфиденциальности.

Глава 18 Кодекса устанавливает правовые основы создания, функционирования и использования госсервисов в рамках нацэкосистемы, определяя их поставщиков — государственные органы, органы местного самоуправления и юридические лица — и подразделяя виды госсервисов на сервисы взаимодействия и пользовательские сервисы. До запуска сервис обязан пройти тестирование на фабрике госсервисов, которая обеспечивает проведение тестирования, мониторинг, взаимодействие и развитие сервисов. Регулятор нацэкосистемы ведёт реестр госсервисов, устанавливает требования к их созданию, контролирует их цифровую устойчивость и координирует деятельность государственных органов.

Пользовательские госсервисы доступны через государственные приложения и сайты, которые обеспечивают доступ к правилам, результатам обработки данных, а также позволяют загружать документы, отслеживать ход предоставления услуг, оплачивать их и подавать жалобы. Такие сервисы будут становиться всё более востребованными у пользователей. К примеру, в Италии разрешена подача правовых документов через электронный портал Министерства юстиции.[21]

---

[20] Электронное правосудие: монография / Е. В. Бурдина [и др.]; под ред. Е. В. Бурдиной, С. В. Зуева. — М. : РГУП, 2021. — 344 с.

[21] Контини Ф. Независимость судебной власти, равенство и судебные технологии: платформы электронного правосудия в Италии // Ala-Too Academic Studies. — 2023. — № 1. — С. 490–501.

Совокупность государственных и муниципальных цифровых ресурсов (включая сайты и приложения), технологических систем, госсервисов, Доверсеров и объектов инфраструктуры составляет нацэкосистему, которая строится на принципах общедоступности, модульности, независимости от конкретных технологических поставщиков, облачного подхода и вариативности, позволяя участникам подключаться к её элементам при соблюдении установленных правил.

Общее пространство данных формируется из цифровых ресурсов участников и регулируется нормами об открытости данных, защите персональных данных и охраняемых законом тайн, включая обязательный учет метаданных, прозрачность целей обработки и меры предотвращения вреда. Управление развитием, совместимостью, устойчивостью и взаимодействием элементов нацэкосистемы осуществляет отраслевой регулятор, который выступает владельцем ключевых систем (цифровое взаимодействие, идентификация, фабрика госсервисов, реестры) и наделён полномочиями по мониторингу, аккредитации, надзору, изданию обязательных предписаний и защите прав участников.

Раздел пятый

Начинается с общих положений о цифровых технологических системах[22] (далее — Цитес). Здесь закреплена свобода создания и использования Цитес, но регулирование вводится лишь там, где необходимо предотвратить вред жизни, здоровью, собственности, окружающей среде, а также угрозу безопасности.

Кодекс определяет четыре ключевых вида Цитес (ч. 2 ст. 171):

- телекоммуникационные сети;
- радиоэлектронные средства и высокочастотные устройства;
- государственные и муниципальные цифровые технологические системы;
- системы искусственного интеллекта.

[22] Система цифровых устройств, программ для них и баз данных, предназначенных для обработки цифровых данных (Кодекс, ст.1).

При этом обеспечивается технологическая нейтральность: владельцами и пользователями таких систем могут быть любые лица вне зависимости от гражданства или используемых технологий. Важным элементом является требование учитывать цифровую инфраструктуру в градостроительной деятельности и обеспечивать техническую совместимость Цитес с международными стандартами и практикой.

Примечательно, что регулирование касается системы противодействия мошенничеству (антифрод-системы), объединяющей операторов связи, банки, финансовые и платежные организации, а также правоохранительные органы. Антифрод-система прежде всего предназначена для обнаружения и предотвращения мошенничества, связанного с онлайн-банкингом, вишингом (телефонное мошенничество), фишингом, использованием поддельных веб-сайтов (фейк-сайтов) и другими цифровыми средствами. В этом плане существенные обязанности возложены на операторов телекоммуникаций и финансовые институты (банки, МФО, платежные организации).

Финансовые институты обязаны (ч. 4 ст. 186):

- выявлять подозрительные операции клиентов;
- для расследования мошенничества предоставлять по запросу правоохранительных органов информацию о подозрительных операциях, счетах и электронных кошельках, с соблюдением банковской тайны;
- обмениваться между собой информацией о выявленных мошеннических операциях, счетах, используемых методах и признаках мошенничества;
- информировать клиентов о рисках мошенничества, а также о мерах и действиях безопасного использования дистанционных финансовых услуг;
- применять меры по приостановлению или блокированию подозрительных операций.

Новым шагом является формирование Кодексом правовой основы для разработки и применения ИИ (глава 23). Основной посыл данной группы регулирования — свобода развития ИИ в пределах правил Кодекса.

Традиционно регулирование начинается с перечисления принципов:

- снижения рисков — по отношению к благам;
- открытости — последовательность и предсказуемость;
- объяснимости — понятность оснований;
- подконтрольности — эффективный контроль человеком;
- точности — достоверность результатов;
- надежности — устойчивость систем ИИ;
- безопасности — защищенность систем ИИ.

Закреплены общие правила относительно минимизации риска, запрета вредных разработок, а также соблюдения требований государства и самих объединений. Каждая система ИИ подлежит оценке опасности. Особое внимание уделено системам повышенной опасности. Для них предусмотрены обязательные требования к управлению рисками, качеству данных, технической документации и подтверждению соответствия через декларацию, размещаемую публично. Кабинет министров КР приступил к регулированию ИИ, утвердив Постановление[23] об оценке ИИ.

Статья 196 Кодекса устанавливает требования и к пользователям «опасных» ИИ, в частности они обязаны использовать по целевому назначению, контролировать работу системы, обеспечивать релевантность и сохранность данных (журналов), информировать затрагиваемых лиц о характеристиках ИИ, уведомлять владельца, если ИИ начинает причинять вред. Нарушение требований влечёт ответственность пользователя, в отдельных случаях даже без привлечения владельца ИИ.

Законодатель КР проявляет особую заботу о физических лицах (ч. 1 ст. 197), как и финансовое законодательство, которое рассматривает потребителя как «слабую сторону» и возлагает на финансовые

[23] Об утверждении требований к методике оценки опасности систем искусственного интеллекта, а также требований в отношении систем искусственного интеллекта повышенной опасности: постановление Кабинета Министров Кыргызской Республики от 2 декабря 2025 года № 770.

институты дополнительные обязательства (информирование потребителя о рисках и тарифах, шрифт договора и распечатка проектов для ознакомления, получение расписок и др.).[24] Поэтому при взаимодействии с ними с помощью ИИ физических лиц следует информировать. Например, при распознавании эмоций или биометрических признаков физические лица должны быть осведомлены о применении в отношении них таких систем.

Ранее выданные лицензии и разрешения автоматически признаются по новым нормам и продолжают действовать без перерывов. Сертификаты электронной подписи будут считаться сертификатами цифровой подписи, а к простым электронным подписям будут применяться правила, установленные для цифровых идентификаторах (ст. 198).

ЗАКЛЮЧЕНИЕ И РЕКОМЕНДАЦИИ

Ознакомившись с данным ключевым документом, можно сделать следующие выводы, значимые для финансового сектора Кыргызской Республики.

1. Главной целью регулирования Кодекса финансовый сектор не является, так как он представлен фрагментарно. Из императивных норм — только меры по противодействию мошенничеству, в которых детально расписаны права и обязанности финансовых институтов. Антифрод-система может быть улучшена за счёт взаимодействия финансовых организаций, возможно, придется в определенной мере ограничить банковскую тайну для защиты клиентов от нарастающей финансовой преступности.

2. Наступает новая эра «цифровой подписи» и выделения из нее «идентификаторов» как самостоятельного инструмента. Банкам и платежным организациям придется расстаться с практикой использования привычного термина «простая электронная подпись» в связи с утратой силы Закона «Об электронной подписи» и начать использовать «цифровые

[24] Положение о минимальных требованиях к порядку предоставления финансовых услуг и рассмотрения обращений потребителей от 24 июня 2015 года № 35/10 // Официальный сайт Министерства юстиции Кыргызской Республики. — URL: https://cbd.minjust.gov.kg/46-3590/edition/977528/ru (дата обращения: 09.07.2026).

идентификаторы», предложенные Кодексом. Из 26 банков[25] больше половины имеют мобильное приложение, которое можно использовать после акцепта публичной оферты с помощью шифров или кодов, ранее рассматривавшихся как «простая электронная подпись». Физические лица теперь вступают в правоотношения с финансовыми институтами с использованием идентификатора.

3. Финансовым институтам стоит пересмотреть свои подходы к работе с персональными данными. В частности, порядок получения согласия (оформлять как отдельный документ или как часть публичной оферты), условия сотрудничества с обработчиками персональных данных, в особенности находящихся за пределами Кыргызской Республики (трансграничная передача), а также назначение ответственного лица или даже формирование подразделения, в чьи функции будет входить регулирование всех требований по персональным данным.

4. Цифровые архивы могут стать неожиданным популярным цифровым сервисом для банков и платежных организаций, которые ежедневно десятки тысяч документов формируют в своей деятельности. К примеру, только банки в своей деятельности формируют 533 вида документов согласно Постановлению НБКР,[26] из которых большинство должны храниться в среднем пять лет. Естественно, в таких условиях цифровые архивы будут популярными, учитывая разрешение Кодекса уничтожать подлинник документа при наличии «цифрового дубликата».

Участники финансового сектора давно проводят цифровую идентификацию и аутентификацию своих клиентов, граждан Кыргызской Республики, посредством интеграции с государственной системой биометрической идентификации. Однако Кодекс ограничил использование биометрии только при проведении выборов и

---

[25] Список коммерческих банков Кыргызской Республики и их филиалов по состоянию на 6 июня 2026 года // Официальный сайт НБКР. — URL: https://www.nbkr.kg/index1.jsp?item=69&lang=RUS (дата обращения: 09.07.2026).

[26] Перечень основных документов, образующихся в деятельности коммерческих банков и финансово-кредитных учреждений, лицензируемых Национальным банком Кыргызской Республики, с указанием сроков хранения: утвержден постановлением Правления Национального банка Кыргызской Республики от 27 августа 2004 года № 22/9.

референдумов, получении и предоставлении госсервисов или в случаях, прямо предусмотренных законом. Поэтому важно обеспечить наличие разрешающих норм в специализированных законах финансовых институтов.

Для удобства читателей рекомендации представлены в виде таблицы, в которой указаны вопросы, действия, исполнители и сроки реализации.

Предмет регулирования	**Рекомендация**	**Ответственный исполнитель**	**Ориентировочные сроки**
Цифровая подпись	Пересмотреть типовые договоры, публичные оферты и внутренние правила, ссылающиеся на бывшую «простую электронную подпись»	Банки, микрофинансовые организации, платежные организации, финтех-провайдеры	Немедленно / краткосрочно
Цифровые архивы	Пересмотреть правила хранения банковских документов и Перечень основных документов, образующихся в деятельности коммерческих банков и финансово-кредитных учреждений, лицензируемых Национальным банком Кыргызской Республики, с указанием сроков хранения	НБКР и профильные ведомства	Среднесрочно
Антифрод-система	Уточнить правовые, институциональные и безопасные механизмы обмена данными с соблюдением банковской тайны	НБКР, финансовые институты, профильные госорганы	Среднесрочно

Биометрические данные и цифровая идентификация	Уточнить правовые основания для обработки биометричских данных в банковской сфере и при удаленной идентификации	Парламент, НБКР, профильные исполнительные органы	Немедленно / краткосрочно
Персональные данные	Пересмотреть форму согласия, обновить комплаенс-процедуры, уведомления о конфиденциальности, учетные регистры и обучение персонала	Все компании, получающие и обрабатывающие персональные данные	Немедленно / краткосрочно

СПИСОК ЛИТЕРАТУРЫ

Цифровой кодекс Кыргызской Республики от 31 июля 2025 года № 178 // Официальный сайт Министерства юстиции Кыргызской Республики. — URL: https://cbd.minjust.gov.kg/3-48/edition/35412/ru (дата обращения: 09.07.2026.)

Электронное правосудие : монография / Е. В. Бурдина [и др.]; под ред. Е. В. Бурдиной, С. В. Зуева. — М. : РГУП, 2021. — 344 с.

Джусупов А. Т. Электронная подпись как подпись на расстоянии // Официальный сайт ОЮЛ «Союз банков Кыргызстана». — URL: https://ub.kg/ru/elektronnaya-podpis-kak-podpis-na-rasstoyanii/ (дата обращения: 09.07.2026.)

Джусупов А. Т. Эксперт высказался о законопроектах, регулирующих работу Нацбанка // Портал Banks.kg. — 02.06.2022. — URL: https://banks.kg/news/expert-on-draft-laws-regulating-work-of-nbkr (дата обращения: 09.07.2026.)

О банках и банковской деятельности: Закон Кыргызской Республики от 11 августа 2022 года № 93 // Официальный сайт Министерства юстиции Кыргызской Республики. — URL: https://cbd.minjust.gov.kg/4-3214/edition/1241184/ru (дата обращения: 09.07.2026.)

Контини Ф. Независимость судебной власти, равенство и судебные технологии: платформы электронного правосудия в Италии // Ala-Too Academic Studies. — 2023. — № 1. — С. 490–501.

Назирдинова Ч. Использование информационных технологий в гражданском судопроизводстве Кыргызской Республики и перспективы их дальнейшего развития // Ala-Too Academic Studies. — 2023. — № 1. — С. 391–405.

Оганесян Т. Правовые основы, пределы и стандарты применения права быть забытым: опыт Европейского союза // Вестник Санкт-Петербургского университета. Право. — 2023. — Т. 14. — № 3. — С. 750–767.

Polański P. Towards the single digital market for e-identification and trust services // Computer Law and Security Review. — 2015. — Vol. 31. — Issue 6. — pp. 773–781.

Перечень основных документов, образующихся в деятельности коммерческих банков и финансово-кредитных учреждений, лицензируемых Национальным банком Кыргызской Республики, с указанием сроков хранения : утвержден постановлением Правления Национального банка Кыргызской Республики от 27 августа 2004 года № 22/9 // Официальный сайт Министерства юстиции Кыргызской Республики. — URL: https://cbd.minjust.gov.kg/31389/edition/456652/ru (дата обращения: 09.07.2026.)

Положение о минимальных требованиях к порядку предоставления финансовых услуг и рассмотрения обращений потребителей: утверждено постановлением Правления Национального банка Кыргызской Республики от 24 июня 2015 года № 35/10 // Официальный сайт Министерства юстиции Кыргызской Республики. — URL: https://cbd.minjust.gov.kg/46-3590/edition/977528/ru (дата обращения: 09.07.2026.)

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Regulation (EU) 2020/1783 of the European Parliament and of the Council of 25 November 2020 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (taking of evidence) OJ L 405, 2.12.2020.

Список коммерческих банков Кыргызской Республики и их филиалов по состоянию на 6 июня 2026 года // Официальный сайт НБКР. — URL: https://www.nbkr.kg/index1.jsp?item=69&lang=RUS (дата обращения: 09.07.2026.)