

**ПОЛОЖЕНИЕ
ОБ ЭЛЕКТРОННОМ ДОКУМЕНТООБОРОТЕ И
ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ
В ОАО «ДОС-КРЕДОБАНК»**

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение «Об электронном документообороте и использовании электронной цифровой подписи в ОАО «Дос-Кредобанк»» (далее по тексту - Положение) регулирует порядок организации, ведения и контроля электронного документооборота и использования электронной цифровой подписи в ОАО «Дос-Кредобанк» (далее по тексту — Банк).
2. Электронные документы, подписанные электронной цифровой подписью (простой или квалифицированной электронной подписью) обладают юридической силой, эквивалентной документам на бумажном носителе в соответствии с законодательством Кыргызской Республики.
3. Положение направлено на обеспечение безопасности, эффективности и прозрачности процессов управления электронными документами внутри Банка, а также при взаимодействии с клиентами, уполномоченными государственными органами Кыргызской Республики и партнерами/контрагентами Банка.
4. Электронный документооборот может быть использован в любой деятельности Банка, включая, но не ограничиваясь: взаимодействие с государственными органами, НБКР, партнерами и контрагентами Банка, клиентами (в том числе и в документах/информации, которые были переданы клиентами Банку либо созданы Банком, либо возникли иным образом в связи со взаимоотношением Банка с клиентами, включая их преддоговорные отношения, в ходе осуществления банковской деятельности).
5. В рамках настоящего Положения используются следующие термины и определения
 - **Электронный документооборот (ЭДО)** – процесс создания, подписания, передачи, хранения и обработки электронных документов.
 - **Электронный документ** – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком, с использованием электронных вычислительных машин.
 - **Электронная цифровая подпись (ЭЦП)** – информация в электронной форме, которая присоединена к другой информации в электронной форме и (или) логически связана с ней и которая используется для определения лица, от имени которого подписана информация.
 - **Система электронного документооборота (система ЭДО)** – программно-аппаратный комплекс, используемый Банком для управления электронными документами.

II. ОСНОВНЫЕ ПРИНЦИПЫ ВЕДЕНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА И ПРИМЕНЕНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

6. В целях успешного применения электронного документооборота (ЭДО) и электронной цифровой подписи (ЭЦП), являющимися важными инструментами цифровой трансформации Банка, обеспечивающих эффективность, безопасность и юридическую значимость документов, необходимо соблюдать следующие принципы:

6.1. Принципы электронного документооборота:

6.1.1. Законность и соответствие нормативным требованиям законодательства Кыргызской Республики.

- Электронные документы должны создаваться, передаваться, храниться и уничтожаться в соответствии с законодательством Кыргызской Республики.
- Применяемые технологии ЭДО должны соответствовать требованиям стандартов безопасности, конфиденциальности и актуальности.

6.1.2. Юридическая значимость и достоверность.

- Электронные документы должны содержать все обязательные реквизиты, подтверждающие их подлинность.
- Применение ЭЦП на электронных документах обеспечивает их неизменность и авторство владельца ЭЦП.

6.1.3. Безопасность и защита данных.

- Электронные документы должны быть защищены от несанкционированного доступа, изменения и уничтожения.
- При создании и использовании электронных документов рекомендуется использовать сертифицированные средства защиты информации и шифрования.

6.1.4. Эффективность и оперативность.

- Автоматизация документооборота сокращает сроки согласования документов и повышает производительность и эффективность сотрудников.
- Исключается дублирование информации и ручная обработка документов, что снижает риск совершения ошибок.

6.1.5. Прозрачность и контроль.

- Все операции с электронными документами фиксируются в системах ЭДО, обеспечивая их сохранность и контролируемость.
- Внедряются механизмы контроля доступа и разграничения прав пользователей.

6.1.6. Долговременное хранение и архивирование.

- Электронные документы должны храниться в соответствии с установленными сроками хранения согласно требованиям законодательства Кыргызской Республики¹.
- Обеспечивается защита архивов от потери, повреждения и несанкционированного изменения.

6.2. Принципы применения электронной цифровой подписи:

6.2.1. Надежность и уникальность.

¹ «Перечень основных документов, образующихся в деятельности коммерческих банков и финансово-кредитных организаций, лицензируемых Национальным банком Кыргызской Республики, с указанием сроков хранения» от 27 августа 2004 года N 22/9

- Право участников электронного взаимодействия по своему усмотрению использовать любой вид электронной подписи, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено законодательными актами, нормативными правовыми актами Кыргызской Республики (в случаях, когда законодательными актами предусмотрена такая возможность) либо соглашением участников электронного взаимодействия;
- Возможность использования участниками электронного взаимодействия по их усмотрению любой технологии и (или) технических средств, позволяющих выполнить требования Закона Кыргызской Республики «Об электронной подписи» применительно к использованию конкретных видов электронной подписи;
- ЭЦП должна гарантировать подлинность подписанта и целостность документа;
- Ключи ЭЦП хранятся в защищенных средах и не передаются третьим лицам;
- Недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на том основании, что подпись в электронном документе не является собственноручной подписью;

6.2.2. Разграничение уровней подписи.

В Банке возможно применение одного из или всех сразу видов ЭЦП:

- Простая электронная подпись** — электронная подпись, ключ подписи которой совпадает с самой электронной подписью (коды, пароли и иные идентификаторы) и применяется как для внутренних документов Банка, так и для документов клиентов в любой доступной и разрешенной форме, аутентификации пользователей.
- Неквалифицированная ЭЦП** — электронная подпись, которая используется для документов, не требующих максимального уровня защиты и соответствует следующим признакам:
 - ✓ получена в результате криптографического преобразования информации с использованием ключа подписи;
 - ✓ позволяет однозначно определить лицо, подписавшее электронный документ;
 - ✓ позволяет обнаружить факт внесения изменений в электронный документ после его подписания;
 - ✓ создается с использованием средств электронной подписи, которые лицо, подписавшее электронный документ, способно сохранять под своим контролем.
- Квалифицированная ЭЦП (КЭП)** — электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:
 - ✓ ключ проверки электронной подписи указан в квалифицированном сертификате;
 - ✓ для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным законодательством Кыргызской Республики.

КЭП применяется для подписания юридически значимых документов, контрактов, финансовой и прочей отчетности, которые передаются в уполномоченные государственные органы и НБКР.

6.2.3. Контроль и аудит использования.

- а) В Банке назначаются ответственные лица за выдачу, использование, учет и контроль использования ЭЦП.
 - б) Проводятся регулярные проверки на предмет несанкционированного использования ЭЦП.
- 6.2.4. Совместимость, защита и интеграция.
- а) ЭЦП должна поддерживаться используемыми системами ЭДО и взаимодействовать с внешними сервисами.
 - б) Обеспечивается соответствие стандартам электронной подписи для взаимодействия с партнерами/контрагентами Банка и государственными органами Кыргызской Республики.
 - в) В случае компрометации ЭЦП должна быть оперативно аннулирована и заменена.
- 6.3. Соблюдение данных принципов позволяет эффективно использовать систему ЭДО и ЭЦП, обеспечивая надежность, безопасность и юридическую значимость электронных документов в Банке.

III. ПОРЯДОК ИСПОЛЬЗОВАНИЯ И ОБЛАСТИ ПРИМЕНЕНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

7. В Банке используется система ЭДО, обеспечивающая:
- создание, использование и хранение электронных документов;
 - маршрутизацию и согласование электронных документов;
 - применение ЭЦП;
 - взаимодействие с контрагентами/клиентами/партнерами Банка через системы ЭДО, соответствующие законодательным требованиям Кыргызской Республики.
8. Документы, подлежащие обработке в ЭДО, включают:
- договоры (в том числе и кредитные, залога и пр.), соглашения, счета-фактуры, накладные;
 - кадровые документы (при наличии соответствующего согласия работников);
 - внутренние приказы, распоряжения и служебные записки;
 - иные документы, допускающие электронную форму в соответствии с законодательством Кыргызской Республики.
9. Доступ к ЭДО предоставляется уполномоченным сотрудникам/контрагентам/партнерам/клиентам Банка, а также при необходимости уполномоченным государственным органам в соответствии с требованиями законодательства Кыргызской Республики.
10. Все участники ЭДО обязаны соблюдать требования по защите информации и не разглашать учетные данные для входа в систему ЭДО.
11. Все вопросы, связанные с использованием ЭДО и подписанием документов при помощи ЭЦП регулируются внутренними нормативными документами, определяющими порядок работы ЭДО в Банке.

IV. ПОРЯДОК ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

12. Получение и использование ЭЦП осуществляется в соответствии с законодательством Кыргызской Республики.
13. Ответственность за выдачу и контроль использования ЭЦП в Банке возлагается на следующие структурные подразделения (включая, но не ограничиваясь):
 - Управление информационной безопасности (установление стандартов или правил безопасности, общий мониторинг контролей безопасности, аудиты безопасности, оценка рисков);
 - IT-департамент (техническое сопровождение, технический мониторинг);
 - Юридический департамент (контроль соответствия требованиям законодательства Кыргызской Республики).
 - уполномоченные сотрудники и руководители структурных подразделений.
14. Владелец ЭЦП несет ответственность за сохранность закрытого ключа и не имеет права передавать его третьим лицам.

V. БЕЗОПАСНОСТЬ И ЗАЩИТА ДАННЫХ

15. Банк обеспечивает защиту информации в ЭДО путем:
 - использования комплексных мер защиты (по результатам оценки рисков безопасности);
 - регулярного обновления программного обеспечения;
 - шифрования и резервного копирования данных.
16. В случае компрометации ЭЦП сотрудник обязан незамедлительно сообщить об этом ответственному лицу.
17. Общий контроль за соблюдением стандартов и правил безопасности при использовании ЭЦП осуществляется Управлением информационной безопасности.

VI. ОТВЕТСТВЕННОСТЬ И КОНТРОЛЬ

18. Персональную ответственность за соблюдение Положения несут все сотрудники, использующие ЭДО и ЭЦП.
19. За нарушение порядка использования ЭЦП могут применяться дисциплинарные меры, предусмотренные законодательством Кыргызской Республики и внутренними нормативными документами Банка.
20. Регулярные проверки соблюдения требований Положения осуществляются:
 - 1-я линия защиты: Руководители структурных и самостоятельных подразделений Банка, IT-департамент;
 - 2-я линия защиты: Управление информационной безопасности.
 - 3-я линия защиты: Служба внутреннего аудита Банка.

VII. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

21. Настоящее Положение вступает в силу с момента утверждения Правлением Банка и подлежит обязательному исполнению всеми структурными подразделениями Банка, должностными лицами Банка, являющимися участниками описываемого процесса.

22. Ответственность за организацию своевременного ознакомления, изучения, порядок применения и использования настоящего Положения сотрудниками несут руководители структурных подразделений Банка.
23. Положение подлежит пересмотру при выявлении новых уязвимостей и рисков, замечаний аудита, после инцидентов безопасности и по мере необходимости. Все изменения и дополнения в настоящее Положение утверждаются Правлением после согласования с Управлением информационной безопасности.
24. В случае коллизии между настоящим Положением и нормативными правовыми актами субъекты правоотношений руководствуются нормативным правовым актом, обладающим более высокой юридической силой.
25. Вопросы, не урегулированные настоящим Положением, регулируются действующим законодательством Кыргызской Республики и нормативными правовыми актами Национального банка Кыргызской Республики, решениями Совета директоров Банка и иными внутренними документами Банка.