

УТВЕРЖДАЮ
Председатель Правления
АО ЮниКредит Банка
_____ А.А. Оборин
« » _____ 2026 г.

РЕГЛАМЕНТ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА БЕЗОПАСНОСТИ
АО ЮНИКРЕДИТ БАНКА ПЛАТФОРМЫ ЦИФРОВОГО РУБЛЯ БАНКА
РОССИИ

(Редакция 1, 12.03.2026)

Москва, 2026

Содержание

1.	Термины, определения и сокращения.....	3
2.	Общие положения.....	6
3.	Присоединение к Регламенту.....	7
4.	Публикация Регламента.	8
5.	Порядок внесения изменений в Регламент	8
6.	Прекращение деятельности УЦБ	Error! Bookmark not defined.
7.	Основные функции УЦБ	9
8.	Условия конфиденциальности.....	10
9.	Права и обязанности УЦБ.....	10
9.1.	Права УЦБ	10
9.2.	Обязанности УЦБ	11
10.	Права и обязанности субъекта информационного обмена	13
10.1.	Права субъекта информационного обмена	13
10.2.	Обязанности субъекта информационного обмена.....	13
11.	Ответственность сторон	14
12.	Сроки действия криптографических ключей и сертификатов безопасности	15
12.1.	Сроки действия криптографических ключей и сертификата УЦБ.....	15
12.2.	Сроки действия криптографических ключей и сертификата безопасности субъекта информационного обмена	15
13.	Хранение сертификатов безопасности в УЦБ.....	16
14.	Регистрация СИО в Реестре УЦБ.....	16
15.	Порядок создания и выдачи сертификатов безопасности	16
15.1.	Порядок создания и выдачи сертификата безопасности для ФЛ	16
15.2.	Порядок создания и выдачи сертификата безопасности представителю Клиента-юридического лица	17
16.	Отзыв сертификата безопасности	18
17.	Смена криптографических ключей УЦБ	18
18.	Смена криптографических ключей субъектов информационного обмена	19
19.	Порядок действий владельца сертификата безопасности при компрометации его закрытого ключа безопасности	19
20.	Содержание и форма сертификата безопасности	20
21.	Хранение материалов.....	20

1. Термины, определения и сокращения

1.1. Термины и определения

Аутентификация клиента (АК) – процедура установления подлинности источника информации.

Владелец сертификата безопасности – субъект информационного обмена, которому УЦБ создал и выдал сертификат безопасности.

Внеплановая смена сертификата безопасности – смена ключевой пары сертификата безопасности, вызванная компрометацией закрытого ключа безопасности, выходом из строя ключевого носителя или изменением данных СИО, содержащихся в сертификате безопасности.

Запрос на выдачу сертификата безопасности – электронное сообщение определенного формата и синтаксиса, созданное в соответствии со стандартом PKCS#10 и содержащее необходимую информацию для создания сертификата безопасности.

Запрос на отзыв сертификата безопасности – электронное сообщение определенного формата, содержащее необходимую информацию для отзыва сертификата безопасности.

Идентификация Субъекта информационного обмена (Идентификация СИО) – процесс мероприятий по установлению сведений о СИО и их проверке.

Клиенты – физические лица, юридические лица (за исключением кредитных организаций).

Закрытый ключ безопасности - закрытый ключ, соответствующий сертификату безопасности.

Ключ электронной подписи УЦБ – ключ, соответствующий ключу проверки электронной подписи, содержащемуся в сертификате УЦБ. Используется УЦБ для подписания сертификатов безопасности и списка отозванных сертификатов безопасности, создаваемых и публикуемых УЦБ.

Ключевой носитель¹ – мобильное устройство или отчуждаемый носитель информации, предназначенный для размещения ключевой информации, используемой для выполнения криптографических процедур шифрования, расшифрования и аутентификации клиента.

Компрометация закрытого ключа безопасности – установленный факт раскрытия закрытого ключа безопасности или подозрение на раскрытие закрытого ключа безопасности; утрата доверия к тому, что используемый закрытый ключ безопасности и соответствующий ему сертификат безопасности обеспечивают подлинность, защищенность и безопасность информации. К фактам, которые могут рассматриваться как компрометация (или подозрение на компрометацию) закрытого ключа безопасности, относятся следующие события:

- утрата ключевых носителей,

¹ Хранение сертификата безопасности субъекта информационного обмена, должно осуществляться на устройстве субъекта информационного обмена или внешних отчуждаемых носителях ключевой информации в соответствии с требованиями эксплуатационной документации к используемым СКЗИ, прошедшим процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

- утрата ключевых носителей с последующим их обнаружением,
- увольнение работника Клиента-юридического лица, имевшего доступ к закрытому ключу безопасности и (или) к ключевому носителю, на который записан указанный закрытый ключ безопасности,
- нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа безопасности,
- возникновение подозрений на утечку конфиденциальной информации или ее искажение;
- нарушение целостности упаковки ключевых носителей и (или) печати на хранилище, где хранились данные носители,
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что выход из строя произошел в результате несанкционированных действий злоумышленника).

Первые из четырех перечисленных выше событий должны трактоваться как безусловная компрометация закрытого ключа безопасности, остальные события – как подозрение на компрометацию закрытого ключа безопасности.

Конфиденциальная информация – информация, доступ к которой ограничивается в соответствии с требованиями законодательства Российской Федерации.

Несанкционированный доступ к информации – доступ к информации, нарушающий установленные правила разграничения доступа в результате случайных или преднамеренных действий субъекта информационного обмена или других субъектов, с использованием штатных аппаратных, аппаратно-программных, программных средств автоматизированной системы.

Платформа Цифрового рубля (ПлЦР) – информационная система, посредством которой взаимодействуют оператор платформы, участники платформы и пользователи платформы в целях совершения операций с цифровыми рублями. Оператором ПлЦР является Банк России, участниками ПлЦР являются банки, предоставляющие своим клиентам доступ к ПлЦР. Пользователями ПлЦР являются физические лица, юридические лица, включая индивидуальных предпринимателей или физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, которым предоставлен доступ к ПлЦР.

Подтверждение владения закрытым ключом безопасности – получение УЦБ доказательства того, что СИО владеет закрытым ключом безопасности, который соответствует криптографическому ключу, указанному СИО в Запросе на выдачу сертификата безопасности.

Представитель Клиента – физическое лицо, уполномоченное клиентом, являющимся юридическим лицом, на регистрацию в качестве субъекта информационного обмена в Реестрах УЦБ и получение таким субъектом информационного обмена сертификата безопасности.

Рабочий день – период с 10 часов 00 минут до 17 часов 00 минут с понедельника по пятницу по времени часовой зоны г. Москвы, за исключением нерабочих праздничных и выходных дней согласно законодательству Российской Федерации.

Регистрация субъекта информационного обмена – внесение в Реестры УЦБ регистрационной информации о субъекте информационного обмена.

Реестры УЦБ – набор документов УЦБ в электронной и/или бумажной форме, включающий следующую информацию:

- реестр запросов на регистрацию субъектов информационного обмена в УЦБ;
- реестр зарегистрированных субъектов информационного обмена;
- реестр запросов на сертификаты безопасности;
- реестр запросов на отзыв сертификатов безопасности;
- реестр сертификатов безопасности;
- реестр отозванных сертификатов безопасности;
- реестр изготовленных САС.

Сертификат УЦБ – электронный документ или документ на бумажном носителе, подтверждающий принадлежность ключа проверки электронной подписи Банку.

Сертификат безопасности – электронный документ, соответствующий уникальной последовательности символов однозначно связанной с закрытым ключом безопасности и предназначенный для аутентификации СИО.

Список аннулированных сертификатов (САС) – список серийных номеров сертификатов безопасности, которые были отозваны, а также информация о датах и причинах отзыва данных сертификатов.

Стандарты асимметричной криптографии с открытым ключом (Public Key Cryptography Standarts) – разработанные компанией RSA Security стандарты, определяющие формат и синтаксис передаваемых криптографических сообщений. УЦБ осуществляет свою работу в соответствии со следующими стандартами PKCS:

- PKCS#7 – стандарт, определяющий формат и синтаксис криптографических сообщений, тип данных PKCS#7 Signed – подписанные данные;
- PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат безопасности.

Субъект информационного обмена – присоединившиеся к настоящему Регламенту Клиент или Представитель Клиента, сведения о которых включены в Реестры УЦБ.

Удостоверяющий центр безопасности (УЦБ) АО ЮНИКРЕДИТ БАНКА платформы Цифрового рубля Банка России – комплекс аппаратно-программных средств и организационно-

технических мероприятий Банка, предназначенный для осуществления деятельности, включая функции по регистрации Клиентов Банка в УЦБ, созданию, выдаче и отзыву сертификатов безопасности Клиентам Банка, а также иные функции, предусмотренные настоящим Регламентом.

Система дистанционного банковского обслуживания для физических лиц (Система ДБО ФЛ) - система Enter.UniCredit для физических лиц в АО ЮниКредит Банке.

Система электронного документооборота для юридических лиц (Система ЭДО ЮЛ) - система Business.Online для юридических лиц и индивидуальных предпринимателей в АО ЮниКредит Банке.

Участники электронного взаимодействия – ПлЦР, Банк и субъекты информационного обмена, осуществляющие обмен информацией в электронной форме.

ФСБ России – Федеральная служба безопасности Российской Федерации.

Электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в Системе ДБО ФЛ или Системе ЭДО ЮЛ.

1.2. Сокращения

PKCS – Public Key Cryptography Standards.

Банк – АО ЮниКредит Банк.

ПлЦР – Платформа Цифрового рубля.

СИО – субъект информационного обмена.

УЦБ – Удостоверяющий центр безопасности.

2. Общие положения

2.1. В данном документе описан Регламент Удостоверяющего центра безопасности АО ЮниКредит Банка платформы Цифрового рубля Банка России.

2.2. Настоящий Регламент разработан в соответствии с законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров, а также нормативно-правовыми актами Банка России, регулирующими порядок проведения операций на Платформе ЦР, включая требования к обеспечению защиты информации при осуществлении действий на Платформе ЦР и операций с ЦР.

2.3. Настоящий Регламент определяет условия предоставления услуг УЦБ, включая права, обязанности и ответственность СИО и УЦБ, порядок регистрации СИО в УЦБ, порядок создания, смены и отзыва сертификатов безопасности.

2.4. УЦБ осуществляет свою деятельность на территории Российской Федерации на основании имеющейся у Банка лицензии, выданной Федеральной службой безопасности Российской Федерации, на осуществление видов деятельности, связанных с предоставлением услуг удостоверяющего центра:

- Лицензия на осуществление распространения шифровальных (криптографических) средств (за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных ФСБ России) и информационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ по техническому обслуживанию шифровальных (криптографических) средств, предоставления услуг по шифрованию и имитозащите информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей.

2.5. Адрес Удостоверяющего центра безопасности АО ЮниКредит Банка платформы Цифрового рубля Банка России для почтовой переписки: 119034, Россия, Москва, Пречистенская наб. д. 9.

3. Присоединение к Регламенту

3.1. Настоящий Регламент является договором присоединения в соответствии со ст. 428 Гражданского кодекса Российской Федерации.

3.2. Присоединение к Регламенту Клиента - физического лица осуществляется путем направления таким Клиентом - физическим лицом Запроса на выдачу сертификата безопасности посредством Системы ДБО ФЛ. С момента подачи Запроса на выдачу сертификата безопасности Клиентом - физическим лицом такой Клиент считается присоединившимся к настоящему Регламенту и становится Стороной Регламента.

3.3. Присоединение к Регламенту Клиента - юридического лица (за исключением кредитных организаций) осуществляется путем присоединения представителя юридического лица и направления таким представителем Запроса на выдачу сертификата безопасности посредством Системы ЭДО ЮЛ. С момента подачи Запроса на выдачу сертификата безопасности представителем Клиента, такой Клиент считается присоединившимся к настоящему Регламенту и становится Стороной Регламента.

3.4. Клиент/СИО обязуется обеспечить ознакомление с требованиями настоящего Регламента, изменениями и/или дополнениями, внесенными Банком в настоящий Регламент, и их неукоснительное соблюдение.

4. Публикация Регламента.

4.1. Настоящий Регламент размещается в электронной форме в виде файла формата PDF на официальном сайте Банка в сети Интернет по адресу: <https://www.unicreditbank.ru>.

4.2. В случае прекращения действия настоящего Регламента, в том числе в случае, предусмотренном разделом 6 настоящего Регламента, соответствующая информация размещается на официальном сайте Банка в сети Интернет по адресу: <https://www.unicreditbank.ru>.

5. Порядок внесения изменений в Регламент

5.1. Внесение изменений и/или дополнений в настоящий Регламент (в том числе, утверждение Банком новой редакции настоящего Регламента) производится в порядке, предусмотренным настоящим разделом, и в соответствии с действующим законодательством Российской Федерации.

5.2. Изменения и дополнения в настоящий Регламент вносятся Банком в одностороннем порядке.

5.3. Банк не несет ответственности за возможные убытки Клиента/СИО, причиненные его неосведомленностью в случае, если Банк надлежащим образом выполнил свои обязательства.

5.4. Любые изменения и/или дополнения в настоящий Регламент, в том числе утвержденная Банком новая редакция настоящего Регламента, с момента вступления их в силу равно распространяются на всех лиц, присоединившихся к настоящему Регламенту, в том числе присоединившихся к настоящему Регламенту ранее даты вступления изменений в силу, если иное не предусмотрено соответствующими изменениями и/или дополнениями в настоящий Регламент.

5.5. Уведомление Клиента/СИО о внесении изменений в Регламент осуществляется способом, указанным в разделе «Публикация Регламента».

6. Прекращение деятельности УЦБ

6.1. Деятельность УЦБ может быть прекращена в случаях и порядке, установленных действующим законодательством Российской Федерации. При этом информация, внесенная в Реестры УЦБ, уничтожается или передаётся лицу, к которому перешли функции удостоверяющего центра, прекратившего свою деятельность, в соответствии с порядком, установленным действующим законодательством Российской Федерации. При прекращении деятельности УЦБ настоящий Регламент прекращает свое действие.

6.2. Официальное уведомление о прекращении деятельности УЦБ и прекращении действия настоящего Регламента осуществляется путем публикации текста официального уведомления на официальном сайте Банка в сети Интернет по адресу: <https://www.unicreditbank.ru>.

7. Основные функции УЦБ

7.1. УЦБ предназначен для оказания услуг по созданию, выдаче и отзыву сертификатов безопасности. В рамках своей деятельности УЦБ осуществляет следующие функции:

- регистрирует субъекта информационного обмена;
- создает и выдает сертификат безопасности по обращению субъекта информационного обмена,
- отзывает по обращению субъекта информационного обмена сертификаты безопасности, созданные и выданные УЦБ,
- устанавливает сроки действия сертификатов безопасности,
- ведет реестр сертификатов безопасности и реестр отозванных сертификатов безопасности, в том числе включающий в себя информацию, содержащуюся в выданных УЦБ сертификатах безопасности, и информацию о датах отзыва сертификатов безопасности и об основаниях отзыва,
- устанавливает порядок ведения Реестров УЦБ и порядок доступа к ним, а также обеспечивает доступ субъектов информационного обмена к информации, содержащейся в реестре сертификатов безопасности,
- проверяет уникальность криптографических ключей, содержащихся в Запросах на выдачу сертификатов безопасности, в реестре сертификатов безопасности,
- изготавливает и публикует актуальный САС, обеспечивает возможность свободного доступа субъектов информационного обмена к САС,
- осуществляет по обращениям субъектов информационного обмена процедуру разбора конфликтных ситуаций,
- осуществляет подтверждение владения СИО закрытым ключом безопасности, соответствующим криптографическому ключу, содержащемуся в Запросе на сертификат безопасности, указанному СИО для получения сертификата безопасности,
- предъявляет требования по обеспечению информационной безопасности при использовании закрытого ключа безопасности и сертификата безопасности в процессе взаимодействия Клиента с системами Банка.

7.2. Порядок проверки действительности сертификата безопасности состоит в проверке одновременного соблюдения следующих условий:

- сертификат безопасности действителен на момент аутентификации клиента;
- имеется положительный результат проверки принадлежности сертификата безопасности СИО, с помощью которого осуществляется аутентификация в ПлЦР;
- сертификат безопасности используется в отношениях, определенных областями действия, указанными в сертификате безопасности.

8. Условия конфиденциальности

8.1. Конфиденциальная информация:

- Закрытый ключ безопасности, связанный с сертификатом безопасности субъекта информационного обмена, является конфиденциальной информацией данного субъекта информационного обмена. УЦБ не осуществляет хранение закрытых ключей безопасности СИО.
- Реестры УЦБ, за исключением реестра сертификатов безопасности и реестра отозванных сертификатов безопасности, являются конфиденциальной информацией УЦБ и относятся к коммерческой тайне.
- Персональные данные субъекта информационного обмена и информация о Клиенте, от лица которого действует субъект информационного обмена, ставшие известными УЦБ в силу его деятельности и не подлежащая включению в сертификат безопасности, являются конфиденциальной информацией.

8.2. Информация, не относящаяся к конфиденциальной информации:

- Настоящий Регламент, сведения, включаемые в сертификат безопасности и САС, издаваемые УЦБ.

8.3. Предоставление конфиденциальной информации УЦБ:

- УЦБ имеет право раскрывать конфиденциальную информацию третьим лицам исключительно в порядке и случаях, установленных законодательством Российской Федерации.

9. Права и обязанности УЦБ

9.1. Права УЦБ

9.1.1. Отказать в предоставлении услуг по регистрации субъекта информационного обмена в УЦБ в случае нарушения указанным субъектом требований настоящего Регламента, с указанием причин отказа.

9.1.2. Отказать в предоставлении услуг по созданию сертификата безопасности субъекту информационного обмена в случае нарушения указанным субъектом требований настоящего Регламента с указанием причин отказа.

9.1.3. Отказать субъекту информационного обмена в предоставлении услуг по созданию сертификата безопасности в случае, если использованное средство для формирования Запроса на выдачу сертификата безопасности не поддерживается УЦБ.

9.1.4. Отозвать сертификат безопасности субъекта информационного обмена в случаях, когда:

- установлен факт компрометации закрытого ключа безопасности, в том числе и без соответствующего Запроса со стороны владельца соответствующего сертификата безопасности,
- в случае если УЦБ стало достоверно известно о прекращении действия документа, на основании которого СИО был выдан сертификат безопасности,
- если установлено, что сертификат безопасности содержит сведения, утратившие свою достоверность в связи с изменением данных СИО или Клиента,
- если установлено, что в результате технической ошибки сертификат безопасности содержит недостоверные или неполные сведения.

9.2. Обязанности УЦБ

9.2.1. Использовать для создания ключа электронной подписи УЦБ и формирования электронной подписи, исключительно сертифицированные ФСБ России средства.

9.2.2. Использовать ключ электронной подписи УЦБ исключительно для подписи выдаваемых УЦБ сертификатов безопасности и публикуемых САС.

9.2.3. Принимать меры по защите ключа электронной подписи УЦБ от несанкционированного доступа.

9.2.4. Обеспечивать уникальность серийных номеров создаваемых сертификатов безопасности УЦБ для субъектов информационного обмена.

9.2.5. Проверять уникальность криптографических ключей, содержащихся в сертификатах безопасности в реестре сертификатов безопасности.

9.2.6. Обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования или иных неправомерных действий.

9.2.7. Отказать субъекту информационного обмена в создании сертификата безопасности в случае, если не было подтверждено то, что субъект информационного обмена владеет закрытым ключом безопасности соответствующему криптографическому ключу, который указан в Запросе

на выдачу сертификата безопасности, переданному субъектом информационного обмена для получения сертификата безопасности.

9.2.8. Отказать субъекту информационного обмена в создании сертификата безопасности в случае отрицательного результата проверки в реестре сертификатов уникальности криптографического ключа, указанного в Запросе на выдачу сертификата безопасности, переданного субъектом информационного обмена для получения сертификата безопасности.

9.2.9. Соблюдать сроки отзыва сертификатов безопасности субъектов информационного обмена.

9.2.10. Осуществлять регистрацию субъектов информационного обмена на основании Запросов на выдачу сертификатов безопасности, в соответствии с положениями, определенными настоящим Регламентом.

9.2.11. Обеспечивать занесение регистрационной информации о субъектах информационного обмена в Реестры УЦБ и обеспечивать уникальность регистрационной информации, используемой для идентификации владельцев сертификатов безопасности.

9.2.12. Обеспечивать конфиденциальность регистрационной информации субъектов информационного обмена, за исключением информации, заносимой в сертификаты безопасности, выдаваемые УЦБ.

9.2.13. Осуществлять создание сертификатов безопасности субъектов информационного обмена в соответствии с нормами, определенными настоящим Регламентом.

9.2.14. Обеспечивать внесение информации о созданном сертификате безопасности субъекта информационного обмена в реестр сертификатов безопасности не позднее указанной в нем даты начала действия сертификата безопасности.

9.2.15. Отозвать сертификат безопасности субъекта информационного обмена путем внесения записи об его отзыве в САС с указанием даты, времени внесения и причины отзыва не позднее 12 (двенадцати) рабочих часов как УЦБ стало известно или должно было стать известно об обстоятельствах, влекущих необходимость отзыва сертификата безопасности.

9.2.16. Уведомлять владельца сертификата безопасности о фактах отзыва, принадлежащего ему сертификата безопасности, путём информирования посредством Системы ДБО ФЛ в случае Клиентов-физических лиц или Системы ЭДО ЮЛ в случае Клиентов-юридических лиц.

9.2.17. Обеспечивать сохранность и контроль доступа к конфиденциальной информации в соответствии с действующими нормативными актами Российской Федерации.

9.2.18. Гарантировать конфиденциальность сведений, полученных в связи с исполнением своих

обязательств по настоящему Регламенту, в течение срока хранения документов, установленного законодательством об архивном деле в Российской Федерации.

9.2.19. Поддерживать во всех технических и программных средствах УЦБ единое системное время, соответствующее времени часовой зоны г. Москвы, с точностью до 01 минуты.

9.2.20. Отозвать сертификат безопасности в случаях когда:

- не подтверждено, что владелец сертификата безопасности владеет закрытым ключом безопасности, соответствующим криптографическому ключу, указанному в сертификате безопасности,
- установлено, что содержащийся в сертификате безопасности криптографический ключ уже содержится в ином ранее созданном УЦБ сертификате безопасности,
- установлено, что сертификат безопасности содержит недостоверную информацию,
- на основании Запроса на отзыв сертификата безопасности, поданного СИО посредством Системы ДБО ФЛ или Системы ЭДО ЮЛ,
- в иных случаях, установленных федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами.

10. Права и обязанности субъекта информационного обмена

10.1. Права субъекта информационного обмена

10.1.1. Применять закрытый ключ безопасности и сертификат безопасности, владельцем которого указанный субъект информационного обмена является, для осуществления защищенного подключения к системам Банка.

10.1.2. Для сертификата безопасности, выданного в форме электронного документа, получить по запросу копию сертификата безопасности на бумажном носителе, заверенную УЦБ.

10.1.3. Получить Сертификат ключа проверки электронной подписи УЦБ и использовать его для проверки электронной подписи УЦБ в сертификатах безопасности, выданных УЦБ.

10.1.4. Получить актуальный САС УЦБ и применять его для проверки статуса сертификата безопасности, выданного УЦБ.

10.1.5. Обращаться в соответствии с настоящим Регламентом в УЦБ для отзыва сертификата безопасности, в течение срока действия данного сертификата безопасности.

10.2. Обязанности субъекта информационного обмена

10.2.1. Формировать криптографические ключи согласно требованиям, предъявляемым к СКЗИ.

- 10.2.2. Соблюдать условия и порядок использования криптографических ключей и СКЗИ.
- 10.2.3. Обеспечивать конфиденциальность своего закрытого ключа безопасности, принимать все возможные меры для предотвращения утраты, раскрытия, искажения и несанкционированного использования закрытого ключа безопасности, его компрометации.
- 10.2.4. Применять для подключения к системам Банка для осуществления операций с цифровыми рублями, только действующий не скомпрометированный закрытый ключ безопасности.
- 10.2.5. Не применять свой закрытый ключ безопасности, если стало известно или имеются подозрения, что данный закрытый ключ безопасности используется или использовался ранее другими лицами.
- 10.2.6. Немедленно обратиться в соответствии с настоящим Регламентом в УЦБ с Запросом на отзыв своего сертификата безопасности при наличии оснований полагать, что закрытый ключ безопасности скомпрометирован.
- 10.2.7. Не использовать закрытый ключ безопасности, связанный с сертификатом безопасности, Запрос на отзыв которого подан в УЦБ, с момента подачи такого Запроса.
- 10.2.8. Не использовать закрытый ключ безопасности, связанный с сертификатом безопасности, который был отозван в УЦБ.
- 10.2.9. Применять свой закрытый ключ безопасности исключительно в отношениях, определенных областями действия, указанными в связанном с данным закрытым ключом безопасности сертификате безопасности.

11. Ответственность сторон

- 11.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему Регламенту стороны несут ответственность в порядке, предусмотренном действующим законодательством Российской Федерации.
- 11.2. УЦБ не несет ответственности за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникших в связи с этим убытков, в случаях:
- если УЦБ обоснованно полагался на сведения, указанные в Запросе на выдачу сертификата безопасности субъекта информационного обмена, Запросе на отзыв сертификата безопасности,
 - вследствие компрометации закрытого ключа безопасности субъекта информационного обмена.
- 11.3. УЦБ несет ответственность за убытки, возникшие вследствие или в связи с использованием субъектом информационного обмена сертификата безопасности, выданного

УЦБ только в случае, если указанные убытки возникли вследствие компрометации ключа электронной подписи УЦБ. Субъект информационного обмена понимает и принимает риски, связанные с использованием сертификата безопасности, включая компрометацию закрытого ключа безопасности и несанкционированное использование сертификата безопасности при ненадлежащем соблюдении субъектом информационного обмена мер безопасности.

11.4. Ответственность сторон, не урегулированная настоящим Регламентом, регулируется в соответствии с действующим законодательством Российской Федерации.

12. Сроки действия криптографических ключей и сертификатов безопасности

12.1. Сроки действия криптографических ключей и сертификата УЦБ

12.1.1. Срок действия ключа электронной подписи УЦБ составляет 36 (тридцать шесть) календарных месяцев. Срок действия сертификата УЦБ, соответствующего ключу ЭП УЦБ, составляет 18 (восемнадцать) лет.

12.1.2. В течение 15 (пятнадцати) календарных месяцев ключ ЭП УЦБ используется для подписания сертификатов безопасности и САС УЦБ, остальное время ключ ЭП УЦБ используется для подписания САС УЦБ.

12.1.3. Плановая смена криптографических ключей УЦБ осуществляется в порядке, предусмотренном разделом 17 настоящего Регламента.

12.2. Сроки действия криптографических ключей и сертификата безопасности субъекта информационного обмена

12.2.1. Срок действия закрытого ключа безопасности субъекта информационного обмена составляет 15 (пятнадцать) календарных месяцев.

12.2.2. Срок действия сертификата безопасности, соответствующего закрытому ключу безопасности субъекта информационного обмена, составляет 15 (пятнадцать) месяцев, и определяется по атрибутам сертификата безопасности «Действителен с» - «Действителен по».

12.2.3. Сертификат безопасности прекращает свое действие:

- в связи с истечением установленного срока его действия,
- на основании Запроса на отзыв сертификата безопасности, подаваемого в порядке, предусмотренном разделом 16 (шестнадцать) настоящего Регламента,
- в случае прекращения деятельности УЦБ без перехода его функций другим лицам;

- в случае если УЦБ стало достоверно известно о прекращении действия документа, на основании которого выдан сертификат безопасности, в том числе прекращении действия в отношении Договора использования Системы ДБО ФЛ или Системы ЭДО ЮЛ в части операций с цифровыми рублями, включая расторжение договора счета цифрового рубля,
- в иных случаях, согласно требованиям законодательства Российской Федерации.

13. Хранение сертификатов безопасности в УЦБ

13.1. Хранение сертификата безопасности в Реестре УЦБ осуществляется в течение всего срока деятельности УЦБ, если более короткий срок не установлен нормативными правовыми актами.

14. Регистрация СИО в Реестре УЦБ

14.1. Под регистрацией СИО в Реестрах УЦБ понимается внесение регистрационных данных СИО в информационную систему УЦБ.

14.2. Регистрация СИО в Реестрах УЦБ осуществляется на основании поданного СИО Запроса на выдачу сертификата безопасности в Системах ДБО ФЛ или ДБО ЮЛ, содержащего регистрационные данные Клиента, а в случае Клиента ЮЛ также и его представителя.

14.3. Инициирование регистрации субъектов информационного обмена в Реестрах УЦБ осуществляется субъектами информационного обмена соответственно с использованием Системы ДБО ФЛ или Системы ЭДО ЮЛ.

15. Порядок создания и выдачи сертификатов безопасности

Сертификат безопасности создаётся средствами УЦБ на основе сведений, указанных в Запросе на выдачу сертификата безопасности. Порядок создания и выдачи сертификата безопасности СИО зависит от технологии создания сертификата, предоставляемой Клиенту соответственно Системой ДБО ФЛ или Системой ЭДО ЮЛ.

15.1. Порядок создания и выдачи сертификата безопасности для ФЛ

15.1.1. Запрос на выдачу сертификата безопасности в электронной форме автоматически формируется и подается субъектом информационного обмена в УЦБ с использованием функциональности Системы ДБО ФЛ.

15.1.2. Клиент ФЛ с использованием Системы ДБО ФЛ автоматически иницирует передачу

Запроса на выдачу сертификата безопасности в УЦБ.

15.1.3. УЦБ принимает к исполнению Запрос на выдачу сертификата безопасности и, в случае принятия положительного решения, создает сертификат безопасности на основе Запроса и включает его в Реестры УЦБ не позднее 3 (трех) рабочих дней, следующих за рабочим днем, в течение которого Запрос был получен УЦБ.

15.1.4. В случае, если Запрос на выдачу сертификата безопасности не прошел положительную проверку, УЦБ отказывает в выдаче сертификата безопасности. Информирование СИО об отказе в выдаче сертификата безопасности осуществляется при помощи Системы ДБО ЮЛ.

15.2. Порядок создания и выдачи сертификата безопасности представителю Клиента-юридического лица

15.2.1. Представитель Клиента-ЮЛ (СИО) в целях получения доступа к функционалу счета цифрового рубля самостоятельно с использованием средств криптографической защиты информации, размещённых на его автоматизированном рабочем месте, создаёт криптографические ключи и формирует Запрос на выдачу сертификата безопасности.

15.2.2. СИО с использованием функциональности Системы ЭДО ЮЛ передаёт Запрос на выдачу сертификата безопасности в УЦБ по организованным каналам информационно-технологического взаимодействия. При передаче Запроса на выдачу сертификата безопасности СИО подписывает его своим ключом ЭП соответствующего сертификата ключа проверки электронной подписи для взаимодействия с Банком в Системе ЭДО ЮЛ.

15.2.3. УЦБ принимает к исполнению Запрос на выдачу сертификата безопасности и инициируется процесс создания сертификата безопасности. УЦБ осуществляет контроли Запроса на выдачу сертификата безопасности:

- проверяет целостность Запроса на выдачу сертификата безопасности,
- проверяет уникальность указанного в Запросе на выдачу сертификата безопасности криптографического ключа в Реестре сертификатов УЦБ,
- осуществляет форматно-логический контроль структуры и состава Запроса на выдачу сертификата безопасности.

15.2.4. УЦБ в случае положительного результата контролей, создает сертификат безопасности на основе Запроса на выдачу сертификата безопасности не позднее 3 (трех) рабочих дней, следующих за рабочим днем, в течение которого Запрос был получен УЦБ.

15.2.5. Сотрудник Банка через Систему ЭДО ЮЛ отправляет СИО созданный сертификат безопасности и инструкцию по установке сертификата безопасности. СИО скачивает сертификат безопасности и устанавливает его на свое устройство.

15.2.6. В случае если результат контролей Запроса на выдачу сертификата безопасности отрицательный, УЦБ отказывает СИО в выдаче сертификата безопасности. Сотрудник Банка через Систему ЭДО ЮЛ информирует СИО об отказе в выдаче сертификата безопасности.

16. Отзыв сертификата безопасности

16.1. Отзыв выданного УЦБ сертификата безопасности по инициативе СИО осуществляется на основании Запроса на отзыв сертификата безопасности, подаваемого СИО в электронной форме с использованием Системы ДБО ФЛ или Системы ЭДО ЮЛ.

16.2. Запрос на отзыв сертификата безопасности передаётся в УЦБ по организованным каналам информационно-технологического взаимодействия.

16.3. УЦБ, при положительном рассмотрении Запроса на отзыв сертификата безопасности, отзывает сертификат безопасности субъекта информационного обмена.

16.4. Датой и временем отзыва сертификата безопасности признается дата и время внесения информации о сертификате, который был отозван, в САС.

16.5. Официальным уведомлением о факте отзыва сертификата безопасности является опубликование САС, который содержит сведения об отозванном сертификате.

16.6. Временем опубликования САС признаётся время его создания.

17. Смена криптографических ключей УЦБ

17.1. Плановая смена ключа электронной подписи УЦБ и соответствующего ему ключа проверки электронной подписи УЦБ выполняется через 12 (двенадцать) календарных месяцев и не позднее, чем через 15 (пятнадцать) календарных месяцев после начала действия ключа электронной подписи УЦБ².

17.2. Внеплановая смена ключа электронной подписи УЦБ выполняется в случае установления факта компрометации (или подозрения на наличие такого факта) ключа электронной подписи УЦБ. Сертификат электронной подписи УЦБ в таком случае отзывается. Все сертификаты безопасности, подписанные с использованием скомпрометированного ключа электронной подписи УЦБ, также считаются отозванными.

17.3. Уведомление субъекта информационного обмена о компрометации ключа электронной

² Актуальный срок указан в документе «Платформа цифрового рубля. Правила заполнения полей сертификатов.»

подписи УЦБ осуществляется посредством размещения данной информации на сайте Банка в сети Интернет по адресу: <https://www.unicreditbank.ru> и рассылки соответствующего сообщения при наличии данной функциональности соответственно в Системе ДБО ФЛ или Системе ЭДО ЮЛ.

17.4. Все подписанные с использованием скомпрометированного ключа электронной подписи УЦБ и действовавшие на момент компрометации ключа электронной подписи УЦБ сертификаты безопасности субъектов информационного обмена подлежат внеплановой смене в порядке, установленном настоящим Регламентом.

18. Смена криптографических ключей субъектов информационного обмена

18.1. Смена криптографических ключей субъектов информационного обмена выполняется в случае истечения срока действия закрытого ключа безопасности субъекта информационного обмена, установленного факта компрометации криптографических ключей субъекта информационного обмена, в случае выхода из строя ключевого носителя, в случае изменения данных субъекта информационного обмена, содержащихся в сертификате безопасности, а также в иных случаях, предусмотренных настоящим Регламентом.

18.2. Смена сертификата безопасности субъекта информационного обмена осуществляется согласно разделу 15 (пятнадцать) настоящего Регламента.

18.3. В случае установленного факта компрометации сертификата безопасности субъекта информационного обмена, в случае выхода из строя ключевого носителя, а также в случае изменения данных субъекта информационного обмена, содержащихся в учетной записи Реестра УЦБ и в сертификате безопасности, субъекту информационного обмена необходимо предварительно отозвать сертификат безопасности согласно разделу 16 (шестнадцать) настоящего Регламента.

19. Порядок действий владельца сертификата безопасности при компрометации его закрытого ключа безопасности

19.1. В случае подозрения о компрометации закрытого ключа безопасности владелец сертификата безопасности самостоятельно принимает решение о факте компрометации принадлежащего ему закрытого ключа безопасности.

19.2. В случае компрометации или подозрения о компрометации закрытого ключа безопасности

владелец сертификата безопасности отзывает сертификат безопасности в порядке, установленном разделом 16 (шестнадцать) настоящего Регламента.

20. Содержание и форма сертификата безопасности

20.1. Сертификат безопасности, выдаваемый Клиенту-физическому лицу, содержит серийный номер сертификата, даты начала и окончания срока действия, идентификатор алгоритма, значение криптографического ключа, а также информацию в поле «Владелец» сертификата:

- ID ФП (соответствующий идентификатор ФП, Участника ПлЦР, у которого обслуживается Пользователь платформы цифрового рубля согласно Альбому ЭС),
- фамилия, имя, отчество (если имеется),
- СНИЛС (страховой номер индивидуального лицевого счета),
- другую дополнительную информацию.

20.2. Сертификат безопасности, выдаваемый представителю Клиента-юридического лица, содержит серийный номер сертификата, даты начала и окончания срока действия, идентификатор алгоритма, значение криптографического ключа, а также информацию в поле «Владелец» сертификата:

- ID ФП (соответствующий идентификатор ФП, Участника ПлЦР, у которого обслуживается Пользователь платформы цифрового рубля согласно Альбому ЭС),
- фамилия, имя, отчество (если имеется) представителя Клиента-юридического лица,
- ИНН (индивидуальный номер налогоплательщика) представителя Клиента-юридического лица,
- другую дополнительную информацию.

21. Хранение материалов

21.1. Информация, внесенная в реестр сертификатов безопасности и реестр отозванных сертификатов безопасности, подлежит хранению в течение всего срока деятельности УЦБ.

21.2. Выданные УЦБ копии сертификатов безопасности в виде документов на бумажных носителях хранятся в порядке и в течение сроков, установленных законодательством Российской Федерации.

21.3. Документы, срок архивного хранения которых закончился, подлежат уничтожению в соответствии с действующей процедурой в Банке.