Акционерное общество «Национальная платежная корпорация Национального Банка Республики Казахстан»

Уровень доступа: Общий

Утверждены
решением Правления АО «НПК»
от «02» мая 2024 г.
(протокол №9)

Дата вступления в силу с
«02» мая 2024 г.

Правила функционирования Центра обмена идентификационными данными Рег. № 63

г. Алматы

Содержание

Глава 1. Общие положения

1. Правила функционирования Центра обмена идентификационными данными (далее – Правила) разработаны в соответствии с законами «О банках и банковской деятельности в Республике Казахстан», «Об электронном документе и электронной цифровой подписи», «Об информатизации», «О платежах и платежных системах», «О персональных данных и их защите», Законом Республики Казахстан «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и определяют порядок организации и функционирования информационной системы «Центр обмена идентификационными данными» акционерного общества «Национальная платежная корпорация Национального Банка Республики Казахстана».

2. В Правилах используются понятия, предусмотренные действующим законодательством Республики Казахстан, а также следующие понятия и сокращения:

1) Общество – акционерное общество «Национальная платежная корпорация Национального Банка Республики Казахстана»;

2) ЦОИД – информационная система «Центр обмена идентификационными данными» Общества, обеспечивающая оказание услуг участникам рынка;

3) аутентификация личности Клиента – процедура проверки подлинности личности Клиента;

4) двухфакторная аутентификация личности Клиента – аутентификация личности Клиента, осуществляемая с применением двух различных идентификаторов (ввод одноразового (единовременного) кода, полученного на мобильное устройство Клиента, и биометрическая верификация личности);

5) одноразовый (единовременный) код – уникальная последовательность электронных цифровых символов, создаваемая программно-техническими средствами по запросу Клиента и предназначенная для одноразового использования при аутентификации Клиента;

6) биометрические данные – персональные данные, которые характеризуют физиологические и биологические особенности человека, на основе которых можно установить его личность;

7) биометрическая верификация личности – процедура установления личности Клиента на основе его биометрических данных, включает в себя liveness-проверку и сопоставление фотоизображения Клиента с фотоизображением из доступных источников;

8) deepfake технологии - методика синтеза изображения используется для соединения и наложения существующих изображений и видео на исходные изображения или видеоролики;

9) liveness-проверка - процесс выявления подмены личности Клиента, таких как использование фотографий, видеозаписей, масок или deepfake технологий для обхода системы;

10) сопоставление фотоизображений – процесс сверки фотоизображения лица Клиента, полученного из сессии liveness-проверки с фотоизображением, полученным из доступных источников;

11) биометрическое решение – программное обеспечение, основанное на биометрических технологиях, предназначенное для биометрической верификации личности человека;

12) FMR (False Match Rate) - показатель ложных срабатываний, который определяет вероятность неправильного сопоставления лиц, то есть система ошибочно утверждает, что два разных лица совпадают;

13) FNMR (False Non-Match Rate) - показатель ложных отказов, который определяет вероятность неправильного отказа системы от сопоставления двух одинаковых лиц, то есть система ошибочно утверждает, что два одинаковых лица не совпадают;

14) поставщик биометрического решения – юридическое лицо (поставщик/разработчик биометрического решения), биометрическое решение которого успешно протестировано Оператором и с которым заключен договор (присоединения) о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД;

15) доступные источники – государственные базы данных, содержащие сведения, позволяющие аутентифицировать личность Клиента;

16) аудиторский след – последовательная регистрация событий по обработке персональных данных и электронных сообщений в ЦОИД, информация по которым сохраняется ЦОИД и Участниками;

17) Клиент – совершеннолетнее, дееспособное физическое лицо - гражданин Республики Казахстан, иностранец или лицо без гражданства, постоянно проживающее на территории Республики Казахстан (при наличии вида на жительства в Республике Казахстан или удостоверения лица без гражданства, выданных уполномоченным государственным органом Республики Казахстан), обратившееся к Участнику за получением услуги;

18) Личный кабинет Клиента – персональная страница Клиента, доступная после прохождения Клиентом двухфакторной аутентификации личности и предоставляющая возможность управления выданными согласиями на сбор и передачу информации о текущих счетах и иных сведений, содержащих персональные данные и банковскую тайну, а также управления выпущенной облачной электронной цифровой подписью. Личный кабинет доступен для Клиентов по адресу: id.npck.kz;

19) НБРК – Национальный Банк Республики Казахстан;

20) АРРФР – Агентство Республики Казахстан по регулированию и развитию финансового рынка;

21) Оператор – Оператор ЦОИД, которым является Общество;

22) Участник – юридическое лицо, с которым Оператором заключен Договор о предоставлении услуг;

23) Сайт – официальный интернет-ресурс Общества, доступный по адресу https://npck.kz/;

24) Портал – платформа Общества, предоставляющая Участникам функционал подключения к сервисам ЦОИД, доступная по адресу cabinet.npck.kz;

25) приложение Участника – веб/мобильное приложение, посредством которого Участник оказывает финансовую/платежную или иную услугу Клиенту;

26) диспут – спорная и/или конфликтная ситуация, при которой Участник оспаривает результаты оказанной услуги сервисами ЦОИД;

27) участник межбанковской системы обмена информацией по открытым программным интерфейсам (OpenAPI) - юридическое лицо, зарегистрированное на территории Республики Казахстан, использующее систему в целях обмена данными;

28) МФЦА – Международный финансовый центр «Астана»;

29) лицензированные участники МФЦА – юридические лица, зарегистрированные или аккредитованные МФЦА, получившие лицензию Комитета МФЦА по регулированию финансовых услуг на осуществление деятельности, требующей наличия лицензии;

30) ИИН - индивидуальный идентификационный номер;

31) облачная ЭЦП - сервис удостоверяющего центра Общества, позволяющий создавать, использовать, хранить и удалять закрытые ключи электронной цифровой подписи в аппаратном, криптографическом модуле защиты (HSM) удостоверяющего центра Общества, где доступ к закрытому ключу осуществляется владельцем удаленно посредством не менее двух факторов аутентификации, одним из которых является биометрический;

32) сервис управления облачной ЭЦП - сервис ЦОИД, предоставляющий услуги подписания электронных документов с применением облачной ЭЦП, а также иные функции по выпуску/перевыпуску и отзыву регистрационных свидетельств, а также просмотра списка подписанных документов;

33) Договор о предоставлении услуг - договор присоединения о предоставлении услуг ЦОИД и/или договор (присоединения) о предоставлении услуг сопоставления ЦОИД;

34) в контексте настоящих Правил под персональными данными Клиента понимаются следующие данные:

- ИИН;
- фамилия, имя, отчество;
- дата рождения;
- пол;
- национальность;
- гражданство;
- данные документа, удостоверяющего личность (номер документа, дата выдачи, срок действия, и орган, выдавший документ);
- сведения о месте рождения;
- сведения об адресе регистрации;
- номер телефона;
- биометрические данные (фото/видеоизображение).

Глава 2. Функционирование ЦОИД

3. ЦОИД разработан и функционирует в целях предоставления Участникам сервисов по сопоставлению фотоизображений, аутентификации Клиентов, а также по управлению облачной ЭЦП применяемых при дистанционном (удаленном) оказании услуг.

4. ЦОИД обеспечивает хранение запросов, а также результатов оказания услуг Участникам в течение пяти лет с даты их получения и обработки. Все данные, полученные от Участника и обработанные ЦОИД должны оставлять аудиторский след.

5. Участники принимают необходимые меры по обеспечению информационной безопасности и защите персональных данных Клиентов в соответствии с Законом Республики Казахстан «О персональных данных и их защите», а также иными правовыми актами, регламентирующими требования к обеспечению информационной безопасности.

6. В случае недоступности инфраструктуры основного центра обработки данных Оператора, Участник подключается к резервному центру.

7. Подлинность электронных сообщений обеспечивается применением подтвержденного идентификационного средства. Порядок формирования и проверки подлинности электронных сообщений определяется Оператором. Для подтверждения получения и обработки электронных сообщений используются ответные электронные сообщения.

8. Оператор предоставляет Участникам посредством сервисов ЦОИД следующие виды услуг:

1) услуга сопоставления фотоизображений Клиента – предоставление результата сопоставления фотоизображений Клиента, и персональных данных Клиента по запросу Участника, в соответствии с действующим законодательством Республики Казахстан и Правилами. Персональные данные Клиента не предоставляются лицензированным участникам МФЦА и субъектам рынка, осуществляющим предпринимательскую деятельность в сфере электронной коммерции.

2) услуга двухфакторной аутентификации личности Клиента - предоставление результата двухфакторной аутентификации личности Клиента, а также персональных данных Клиента по запросу Участника, в соответствии с действующим законодательством Республики Казахстан и Правилами;

3) услуга подписания электронных документов с применением облачной ЭЦП - юридически значимое подписание электронных документов с использованием облачной электронной цифровой подписи без необходимости применения физических носителей.

Данный пункт дополнен решением Правления Общества от 12 августа 2025 года (протокол № 15)

9. Персональные данные Клиента, предоставляются Участнику с согласия Клиента в соответствии с действующим законодательством Республики Казахстан и Правилами без права трансграничной передачи данных.

9-1. Участник обязан обеспечить соответствие требованиям законодательства передачи персональных данных Клиента Оператору, а также

наличие согласия Клиента на сбор, обработку персональных данных и их передачу третьим лицам.

Данный пункт включен решением Правления Общества от 22 ноября 2024 года (протокол № 30)

10. Конфиденциальность передаваемых данных в ЦОИД обеспечивается участниками информационного взаимодействия шифрованием при их обмене.

Параграф 1. Порядок оказания услуги сопоставления фотоизображений Клиента

11. Для проведения сопоставления фотоизображений Клиента в ЦОИД используется сервис сопоставления фотоизображений, который посредством биометрического решения определяет степень соответствия фотоизображений по биометрическим данным.

12. Услуга сопоставления фотоизображений Клиента, оказываемая ЦОИД, является одним из этапов процедур проверок и/или аутентификации и/или идентификации личности Клиента, проводимых Участником. Выбор биометрического решения для сопоставления фотоизображений осуществляется Участником. Решение о результатах этих процедур, а также решение об установлении деловых отношений с Клиентом и/или оказании ему услуг принимается Участником самостоятельно.

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

13. До отправки запроса на сопоставление фотоизображения Клиента Участник должен:

1) получить согласие Клиента на сбор, обработку и передачу его персональных данных, в том числе третьими лицами;

2) убедиться в том, что Клиентом не используются фотоизображения, видеозаписи, маски и иные средства/технологии для подмены личности Клиента.

14. Сервис сопоставления фотоизображения Клиента принимает следующие виды и параметры запросов:

1) запрос на получение результатов степени соответствия фотоизображения Клиента, который содержит:

- ИИН Клиента;
- фотоизображение Клиента, полученное от Участника с применением специализированного программного обеспечения, реализующего технологию выявления подмены личности Клиента в процессе дистанционной идентификации, удовлетворяющее требованиям, приведенным в Приложении 1.

2) запрос на получение персональных данных Клиента, содержащий подписанное электронной цифровой подписью Участника подтверждение наличия согласия Клиента на сбор, обработку и передачу его персональных данных третьим лицам в соответствии с условиями пунктов 9 и 9-1 Правил.

Данный пункт включен решением Правления Общества от 22 ноября 2024 года (протокол № 30)

15. Сервис сопоставления фотоизображений осуществляет обработку запроса Участника, удовлетворяющего форматам обмена запросами, в следующем порядке:

1) направляет в доступные источники запрос на получение фотоизображения Клиента;

2) направляет фотоизображения Клиента, полученные от Участника и доступных источников биометрическому решению сопоставления фотоизображений для сопоставления;

3) перенаправляет Участнику ответ биометрического решения сопоставления фотоизображений о степени соответствия обработанных фотоизображений;

4) в случае если степень соответствия фотоизображений выше 85%, сервис сопоставления фотоизображений по запросу Участника в соответствии с условиями пунктами 9 и 9-1 Правил направляет в доступные источники запрос на получение персональных данных Клиента. Полученные персональные данные перенаправляются Участнику;

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

5) если степень соответствия фотоизображений ниже 85% сервис сопоставления фотоизображений направляет Участнику результат степени соответствия. При степени соответствия фотоизображений ниже 85%, сервис сопоставления фотоизображений не предоставляет персональные данные Клиента Участнику.

16. В случае неуспешного проведения процедуры биометрической верификации личности Клиента более двух раз Участник проводит процедуру дополнительной проверки Клиента в оффлайн режиме либо отказывает Клиенту в установлении деловых отношений и/или предоставлении услуг.

17. Персональные данные Клиента, за исключением биометрических данных, предоставляются Участнику при соблюдении следующих условий (в совокупности):

1) результат степени соответствия фотоизображения Клиента не ниже 85%;

2) наличие запроса Участника на получение персональных данных Клиента;

3) наличие и отправка Участником подтверждения, подписанного электронной цифровой подписью, о наличии согласия Клиента на сбор, обработку и передачу его персональных данных третьим лицам;

4) принятие Участником положительного решения об успешности биометрической верификации личности Клиента с использованием результатов степени соответствия фотоизображений.

18. Для получения услуг при авторизации Участника используется защищенный канал информационного обмена (с двусторонней аутентификацией, TLS не ниже v. 1.2 Mutual), обеспечивающий процесс аутентификации лица, а также конфиденциальность и целостность передаваемых данных с использованием криптографической защиты на базе сертификатов, предоставляемых Участнику удостоверяющим центром Оператора.

19. Взаимодействие Участника и ЦОИД осуществляется по выделенным каналам связи или по IPSec-туннелю через глобальную сеть Интернет, с учетом

наличия публичного статического IPv4 адреса, зарегистрированного (RIPE-NCC) в Республике Казахстан.

20. При авторизации сторон информационного взаимодействия в поле «Username» указывается системное имя Участника (идентификатор пользователя), соответствующее имени, указанному в сертификате, полученном в удостоверяющем центре Оператора.

21. Оператор устанавливает меры информационной безопасности, определяет сертифицированные средства криптографической защиты информации и аккредитованный удостоверяющий центр, обеспечивающий выдачу регистрационных свидетельств, и порядок их использования.

22. Порядок аутентификации при доступе к сервису сопоставления фотоизображений включает необходимость использования аутентификации с проверкой сторон информационного взаимодействия, основанной на криптографических алгоритмах.

Параграф 2. Порядок оказания услуги двухфакторной аутентификации личности Клиента

23. Для оказания услуги двухфакторной аутентификации личности Клиента используется сервис двухфакторной аутентификации ЦОИД, который по запросу Участника обеспечивает комплексное проведение мероприятий по аутентификации личности Клиента и включает в себя:

1) запрос подтверждения ИИН Клиента;

2) биометрическую верификацию личности Клиента:

- liveness – проверка. В случае неуспешного результата liveness-проверки, проводится повторная проверка. Допускается проведение не более 4 (четырех) liveness-проверок в пределах одной сессии, после чего сессия с Клиентом завершается и возможность проведения liveness-проверок для верифицируемого лица блокируется на 15 минут. Участник имеет возможность самостоятельно настроить параметр временной блокировки, при этом принимает на себя полную ответственность за последствия, связанные с изменением указанного параметра, включая возможные риски несанкционированного доступа и нарушения требований к обеспечению безопасности аутентификации;

- получение фотоизображения Клиента из сеанса liveness - проверки для проведения процедуры сопоставления фотоизображений;

- проведение процедуры сопоставления фотоизображения, полученного из сеанса liveness-проверки с эталонным фотоизображением из доступных источников.

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

3) СМС проверку путем отправки Клиенту одноразового (единовременного) кода на указанный в запросе номер телефона. Допускается отправка не более 2 (двух) СМС в пределах одной сессии двухфакторной аутентификации;

4) принятие решения по результатам проведенной процедуры двухфакторной аутентификации личности Клиента и отправка результата Участнику;

5) предоставление персональных данных Клиента по запросу Участника с согласия Клиента, за исключением биометрических данных.

24. В запросе на проведение двухфакторной аутентификации личности Клиента Участник направляет Оператору следующие данные:

1) ИИН Клиента;

2) номер мобильного телефона, по которому Клиент зарегистрирован в приложении Участника.

25. До начала проведения процедуры двухфакторной аутентификации личности Оператор предоставляет Клиенту пользовательское соглашение по форме согласно Приложению 2 к настоящим Правилам, согласие с условиями которого является обязательным условием для продолжения процедуры двухфакторной аутентификации личности Клиента. Несогласие Клиента с условиями пользовательского соглашения приводит к отказу в оказании услуги двухфакторной аутентификации личности.

25-1. В рамках услуги двухфакторной аутентификации Участник имеет возможность настраивать порядок проведения процедур, а именно использование биометрической верификации в качестве отдельного фактора без применения SMS-проверки.

Данный пункт включен решением Правления Общества от 12 августа 2025 года (протокол № 15)

26. В составе сервиса двухфакторной аутентификации ЦОИД при осуществлении между Участниками обмена информацией о банковских счетах и иных сведений, содержащих персональные данные и банковскую тайну, а также при проведении платежей и переводов денег посредством межбанковской системы обмена информацией по открытым программным интерфейсам (OpenAPI) функционирует сервис управления согласиями, который осуществляет следующие функции:

1) регистрация согласия Клиента на сбор, обработку и передачу третьим лицам персональных данных и сведений, относящихся к банковской тайне по запросу Участника;

2) отзыв ранее зарегистрированного согласия Клиента на сбор, обработку и передачу третьим лицам сведений, содержащих его персональные данные и сведения, относящиеся к банковской тайне;

3) ведение реестра согласий Клиента на сбор, обработку и передачу персональных данных третьим лицам:

4) проверка Оператором наличия ранее зарегистрированного согласия Клиента;

5) предоставление Клиенту возможности просмотра зарегистрированных/отозванных согласий.

27. Отзыв согласия на сбор, обработку и передачу информации о банковских счетах и иных сведений, содержащих персональные данные и банковскую тайну, а также на проведение платежей и переводов денег посредством межбанковской системы обмена информацией по открытым программным интерфейсам (OpenAPI) осуществляется Клиентом посредством Личного кабинета (id.npck.kz).

28. В случае успешного завершения процедуры двухфакторной аутентификации личности Клиента, в ответном сообщении Участнику ЦОИД возвращает код авторизации, который в дальнейшем используется Участником в процессе получения персональных данных.

29. В случае не успешного завершения процедуры двухфакторной аутентификации личности Клиента в ответном сообщении Участнику ЦОИД возвращает признак неуспешности проведения соответствующих процедур.

30. При успешном завершении процедуры двухфакторной аутентификации личности Клиента, Участник, может направить запрос на получение персональных данных Клиента с приложением полученного кода авторизации.

31. Запрос на получение Участником сведений по Клиенту, содержащих его персональные данные и сведения, относящиеся к банковской тайне, обрабатывается Оператором исключительно в случае предоставления самим Клиентом согласия на сбор, обработку и передачу данных посредством сервиса управления согласиями;

32. Взаимодействие сервиса двухфакторной аутентификации ЦОИД с Участниками осуществляется посредством глобальной сети Интернет с учетом наличия публичного статического IPv4 адреса, зарегистрированного (RIPE-NCC) в Республике Казахстан, посредством IPSEC, либо через выделенный канал связи IP VPN.

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

Параграф 3. Порядок оказания услуги подписания электронных документов с применением облачной ЭЦП

33. Для оказания услуги подписания электронных документов применяется сервис управления облачной ЭЦП ЦОИД, который включает в себя комплекс функций для Участников и Клиентов и обеспечивает:

1) выпуск/перевыпуск и отзыв регистрационного свидетельства облачной ЭЦП для физических лиц;

2) подписание электронных документов с использованием облачной ЭЦП;

3) просмотр списка подписанных документов.

34. Оказание услуг с использованием сервиса управления облачной ЭЦП применяется Участником при дистанционном оказании услуг Клиенту.

35. Подписание электронных документов с применением облачной ЭЦП осуществляется в следующем порядке:

1) Участник осуществляет вызов сервиса управления облачной ЭЦП и передает для подписания электронные документы (*.pdf, *.xml, blob), в ответ получает уникальные идентификаторы загруженных документов;

2) Участник перенаправляет Клиента на сервис двухфакторной аутентификации ЦОИД для прохождения процедуры аутентификации и передает перечень ранее полученных уникальных идентификаторов загруженных документов;

3) сервис двухфакторной аутентификации ЦОИД проводит аутентификацию личности Клиента;

4) сервис управления облачной ЭЦП предлагает Клиенту подписать электронные документы путем ввода пароля, для доступа к закрытым ключам Клиента. Пароль, заданный Клиентом, не хранится в информационных системах ЦОИД и удостоверяющего центра. Для проверки пароля от закрытого ключа Клиента, хранится только хэш пароля в HSM;

5) Клиент вводит пароль, шифрование которого осуществляется на устройстве Клиента и передается в Сервис облачной ЭЦП для его проверки;

6) сервис управления облачной ЭЦП осуществляет вызов сервиса облачной ЭЦП на подписание электронных документов;

7) подписанные документы возвращаются Участнику.

36. Доступ к закрытому ключу обеспечивается на базе сервиса двухфакторной аутентификации ЦОИД.

37. В случае отсутствия у Клиента действующих ключей облачной ЭЦП Клиенту предоставляется Заявление на выдачу регистрационного свидетельства от физического лица согласно форме, опубликованной на Сайте по адресу: **https://npck.kz/docs-uuc/**, на основании которого осуществляется выпуск ключей облачной ЭЦП и подписание необходимых документов. Несогласие Клиента с выпуском регистрационного свидетельства приводит к отказу в оказании услуги.

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

38. При успешном прохождении процедуры выпуска и подписания документов с применением облачной ЭЦП сервис ЦОИД перенаправляет Клиента на ранее указанную Участником веб-страницу, а также предоставляет код авторизации, который используется для доступа к получению списка ранее подписанных документов.

39. При неуспешном прохождении возвращается соответствующая ошибка.

40. Хранение закрытых ключей Клиента осуществляется на защищенном ресурсе Общества в соответствии с Политикой применения регистрационных свидетельств и Регламентом Удостоверяющего центра, размещенных на Сайте Общества.

40-1. Срок хранения подписанных документов в течение одного года после истечения срока действия ключей ОЭЦП.

Данный пункт включен решением Правления Общества от 12 августа 2025 года (протокол № 15)

41. Отзыв регистрационного свидетельства осуществляется Клиентом путем подачи заявления на отзыв (аннулирование) регистрационного свидетельства от физического лица согласно форме, опубликованной на Сайте по адресу: **https://npck.kz/docs-uuc/**.

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

42. Отзыв регистрационного свидетельства осуществляется в электронном формате в Личном кабинете Клиента (id.npck.kz).

43. Взаимодействие сервиса управления облачной ЭЦП с Участниками осуществляется посредством глобальной сети Интернет с учетом наличия публичного статического IPv4 адреса, зарегистрированного (RIPE-NCC) в Республике Казахстан, посредством IPSEC, либо через выделенный канал связи IP VPN.

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

Глава 3. Взаимоотношения Оператора с Участниками

Параграф 1. Требования к Участникам

44. Взаимодействие Участников с Оператором осуществляется на основании Договора о предоставлении услуг. Типовая форма Договора о предоставлении услуг утверждается Оператором и размещается на Сайте.

45. Договор о предоставлении услуг может быть заключен Оператором со следующими юридическими лицами:

1) банком второго уровня;

2) юридическим лицом, осуществляющим отдельные виды банковских операций;

3) организацией, состоящей в реестре НБРК в качестве платежной организации, либо получившей лицензию в АРРФР;

4) юридическим лицом, осуществляющим деятельность по обязательному гарантированию депозитов, привлечению пенсионных взносов и пенсионных выплат;

5) юридическим лицом, осуществляющим деятельность по формированию и ведению Единой базы данных по страхованию;

6) субъектом рынка, осуществляющим предпринимательскую деятельность в сфере электронной коммерции;

7) юридическим лицом, получившим лицензию Комитета МФЦА по регулированию финансовых услуг на осуществление деятельности требующей наличие лицензии.

8) участником экосистемы Open Banking и Open API, прошедшего аккредитацию Оператора.

9) профессиональным участником рынка ценных бумаг, осуществляющим брокерскую и/или дилерскую деятельность;

10) юридическим лицом, осуществляющим деятельность по возврату просроченной задолженности (коллекторская деятельность) на основании соответствующего уведомления или разрешения уполномоченного органа;

11) страховой (перестраховочной) организацией, имеющей лицензию на осуществление страховой деятельности.

Данный пункт дополнен решением Правления Общества от 12 августа 2025 года (протокол № 15)

46. Договор о предоставлении услуг может быть заключен Оператором с юридическим лицом, в совокупности отвечающим следующим требованиям:

1) Юридическое лицо должно обеспечить наличие службы технической поддержки, доступной Клиенту для консультаций в режиме 24/7;

2) Юридическое лицо не должно подлежать процедуре банкротства либо ликвидации.

47. Юридические лица приобретают статус Участника после регистрации Оператором Договора о предоставлении услуг. Номер и дата заключения Договора присваивается и заполняется Оператором на заявлении Участника.

48. С целью ознакомления юридических лиц с условиями подключения к сервисам ЦОИД, необходимая документация размещается на Сайте Оператора.

49. Предоставление услуг Участнику приостанавливается в следующих случаях:

1) неисполнение или ненадлежащее исполнение, нарушение Участником условий Договора о предоставлении услуг, настоящих Правил и иных регламентирующих документов, являющихся неотъемлемой частью Договора о предоставлении услуг;

2) в соответствии со вступившим в законную силу решением суда или предписанием уполномоченного органа;

3) в случае выявления факта аномального трафика, подозрительной активности, чрезмерно больших объемов трафика, попыток сканирования большого количества сетевых портов/адресов, зарегистрированных системами обнаружения вторжений и т.д.;

4) в случае нарушения Участником установленных Договором о предоставлении услуг сроков оплаты услуг более чем на 15 (пятнадцать) календарных дней;

5) иных случаях, установленных законодательством Республики Казахстан и Договором о предоставлении услуг.

50. Приостановление предоставления услуг Участнику не лишает его статуса Участника.

51. Предоставление услуг Участнику прекращается в следующих случаях:

1) передачи данных, полученных через ЦОИД, третьим лицам без согласия Клиента;

2) в соответствии со вступившим в законную силу решением суда или предписанием уполномоченного органа;

3) утраты Участником права на оказание платежных услуг и/или финансовых услуг;

4) применения к Участнику ограничений и запретов, предусмотренных санкциями;

5) в случае нарушения Участником установленных Договором об оказании услуг сроков оплаты услуг более чем на 30 (тридцать) календарных дней;

6) включения Участника в перечень организаций и лиц, связанных с финансированием распространения оружия массового уничтожения, и (или) в перечне организаций и лиц, связанных с финансированием терроризма и экстремизма;

7) иных случаях, установленных законодательством Республики Казахстан и Договором о предоставлении услуг.

52. При приостановлении либо прекращении предоставления услуг Участнику Оператор письменно уведомляет Участника о дате и причинах приостановления, либо прекращения предоставления услуг.

52-1. В случае подтвержденного факта лишения лицензии Участника Оператор вправе расторгнуть Договор в одностороннем порядке в соответствии с условиями Договора о предоставлении услуг.

Данный пункт включен решением Правления Общества от 22 ноября 2024 года (протокол № 30)

52-2. В случае если выявлен факт приостановления лицензии Участника, Оператор вправе незамедлительно заблокировать Участника до момента возобновления действия лицензии, с последующим уведомлением Участника по электронной почте, указанной в заявлении о присоединении (Приложение 1 к Договору о предоставлении услуг).

Данный пункт включен решением Правления Общества от 22 ноября 2024 года (протокол № 30)

52-3. Участник обязуется незамедлительно уведомлять Оператора о приостановлении/лишении/возобновлении действия лицензии Участника. В случае несвоевременного уведомления/ не уведомления Оператора о факте лишения/приостановления/возобновления лицензии ответственность несет Участник.

Данный пункт включен решением Правления Общества от 22 ноября 2024 года (протокол № 30)

Параграф 2. Подача заявок на подключение к сервисам ЦОИД

53. Для подключения к сервисам ЦОИД юридическое лицо, соответствующее требованиям, установленным настоящими Правилами, подает Оператору заявление о присоединении по форме, установленной соответствующим Договором о предоставлении услуг.

54. Юридическое лицо подписывает заявление о присоединении и прикладывает к нему следующие документы:

1) свидетельство/справка о государственной регистрации/ перерегистрации юридического лица;

2) протокол (решение) уполномоченного органа юридического лица и приказ о назначении первого руководителя;

3) свидетельство о постановке на регистрационный учет по налогу на добавленную стоимость;

4) устав юридического лица;

5) доверенность, подтверждающая полномочия заявителя (если Заявление подписывает не первый руководитель);

6) свидетельство о регистрации в реестре НБ РК или АРРФР (при наличии);

7) лицензия, выданная АРРФР (при наличии);

8) лицензия, выданная Комитетом МФЦА по регулированию финансовых услуг (при наличии);

9) подписанное Согласие о неиспользовании персональных данных в целях трансграничной передачи по форме Приложения 3 к Договору о предоставлении услуг;

10) соответствующие уведомления или разрешения уполномоченного органа на осуществление деятельности по возврату просроченной задолженности (коллекторская деятельность) (при необходимости);

11) лицензия на осуществление страховой деятельности (при необходимости);

12) подтверждающие документы об осуществлении брокерской и/или дилерской деятельность (лицензии) (при наличии);

13) подтверждающие документы на осуществление предпринимательской деятельности в сфере электронной коммерции.

Данный пункт дополнен решением Правления Общества от 12 августа 2025 года (протокол № 15)

55. Подача заявления о присоединении к Договору о предоставлении услуг по сопоставлению фотоизображений ЦОИД осуществляется лично либо заказным почтовым направлением по адресу: г. Алматы, микрорайон Коктем-3, здание 21. Прилагаемые к заявлению документы подаются в копиях.

56. Подача заявления о присоединении к Договору о предоставлении услуг двухфакторной аутентификации личности и подписания облачной ЭЦП осуществляется Участником в электронном виде на Портале. Оригинал заявления о присоединении к Договору о предоставлении услуг двухфакторной аутентификации личности и подписания облачной ЭЦП заказным почтовым направлением по адресу: г. Алматы, микрорайон Коктем-3, здание 21. Прилагаемые к заявлению документы подаются в копиях.

57. Допускается передача подписанного заявления о присоединении к Договору о предоставлении услуг посредством системы электронного документооборота в соответствии с действующим законодательством Республики Казахстан.

58. Особенности подключения к сервисам двухфакторной аутентификации личности и управления облачной ЭЦП:

1) подключение Участников к сервисам ЦОИД осуществляется путем регистрации на Портале приложения Участника и выбора Участником соответствующей услуги для подключения;

2) авторизация сторон в информационном обмене осуществляется по учетным данным (clientID/clientSecret), генерируемым для каждого приложения Участника;

3) учетные данные (clientID/clientSecret) являются уникальными для каждого зарегистрированного на Портале приложения Участника;

4) учетные данные (clientID/clientSecret) являются едиными при подключении одного зарегистрированного на Портале приложения Участника к различным сервисам ЦОИД;

5) с момента регистрации приложения Участника и его подключения к соответствующему сервису ЦОИД на Портале Участник приобретает право пользования сервисом ЦОИД;

6) факт подключения Участника к сервису(ам) ЦОИД отображается на Портале на странице информации о приложении Участника;

7) в целях пользования сервисом ЦОИД Участник направляет запрос Оператору. Учет обработанных сервисом ЦОИД запросов Участника

осуществляется с момента подключения приложения Участника к сервису ЦОИД.

Параграф 3. Рассмотрение Оператором заявок Участников на подключение к сервисам ЦОИД

59. После получения от юридического лица заявления о присоединении к Договору о предоставлении услуг, Оператор в течение 7 рабочих дней проверяет полноту и правильность его заполнения, полномочия лица, подписавшего заявление, наличие оснований для заключения договора (соответствие юридического лица требованиям, предусмотренным настоящими правилами), наличие копий прилагаемых документов.

60. При отсутствии оснований для отказа в предоставлении услуг, Оператор осуществляет регистрацию Договора о предоставлении услуг. Регистрационный номер Договора о предоставлении услуг и дата его заключения доводится до сведения Участника путем направления сообщения посредством Портала и/или на электронную почту, указанную в заявлении о присоединении и/или их проставления на заявления о присоединении к Договору об оказании услуг Участника и/или посредством системы электронного документооборота.

61. После заключения Договора присоединения о предоставлении услуг Центра обмена идентификационными данными (ЦОИД) Оператор предоставляет Участнику учетные данные, используемые для аутентификации и авторизации сторон при взаимодействии в личном кабинете Участника на Портале.

62. При наличии оснований для отказа в предоставлении услуг, регистрация Договора о предоставлении услуг не производится, причины отказа доводятся до сведения юридического лица путем направления сообщения посредством Портала и/или электронной почты, указанной в заявлении о присоединении, и/или указания в заявлении о присоединении к Договору об оказании услуг и/или посредством системы электронного документооборота.

63. При необходимости после устранения замечаний, послуживших основанием для отказа в предоставлении услуг, юридическое лицо вправе подать новое заявление о присоединении к Договору о предоставлении услуг.

Параграф 4. Условия тарификации и оплаты услуг Участниками

64. Стоимость услуг (тарифы), оказываемых Оператором Участникам посредством ЦОИД, утверждается Оператором.

65. Условия тарификации и тарифы публикуются на Сайте.

66. Оператор ежемесячно взимает плату за услуги, фактически оказанные Участнику (Клиенту). Условия и порядок оплаты услуг определяются Договором о предоставлении услуг. Сессия двухфакторной аутентификации личности, прерванная Клиентом, подлежит оплате в полном объеме. Сессия подписания облачной ЭЦП, прерванная Клиентом в ходе прохождения двухфакторной аутентификации личности, подлежит оплате в соответствии с установленными Оператором тарифами двухфакторной аутентификации личности.

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

67. Для Участников, подключенных к сервисам двухфакторной аутентификации ЦОИД и управления облачной ЭЦП ЦОИД, на Портале доступна информация о фактическом количестве обработанных запросов на аутентификацию личности Клиентов.

68. Для Участников, подключенных к сервису сопоставления фотоизображений ЦОИД получение информации о фактическом количестве обработанных запросов, осуществляется в автоматизированном режиме путем вызова соответствующих методов, описанных в технической документации, доступной на Сайте.

Глава 4. Взаимоотношения Оператора с поставщиками биометрических решений

Параграф 1. Требования к поставщикам биометрических решений

69. Договор присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД может быть заключен Оператором с юридическим лицом, в совокупности отвечающим следующим требованиям:

1) юридическое лицо должно являться платежеспособным, не иметь налоговой задолженности сроком, превышающим три месяца;

2) юридическое лицо должно предоставить документальное подтверждение наличия исключительных прав на предоставляемое биометрическое решение в соответствии с законодательством Республики Казахстан;

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

3) юридическое лицо, на момент подачи заявки, не должно подлежать процедуре банкротства либо ликвидации;

4) юридическое лицо на момент подачи заявки, не должно состоять в реестре недобросовестных участников на портале закупок НБРК и реестре недобросовестных поставщиков на портале государственных закупок;

5) юридическое лицо, руководитель или учредитель юридического лица, на момент подачи заявки, не должно состоять в перечне организаций и лиц, связанных с финансированием распространения оружия массового уничтожения, и (или) в перечне организаций и лиц, связанных с финансированием терроризма и экстремизма;

6) юридическое лицо должно обеспечить наличие службы технической поддержки, доступной Оператору для консультаций в режиме 24/7.

Параграф 2. Подача заявок на подключение биометрических решений к ЦОИД

70. Юридическое лицо, желающее стать поставщиком биометрического решения, должно предоставить заявку на подключение к ЦОИД, включая, но не ограничиваясь:

1) оригинал подписанного заявления о присоединении к Договору присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД по форме, согласно приложению 1 к

Договору присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД;

Данный пункт включен решением Правления Общества от 22 ноября 2024 года (протокол № 30)

2) доверенность от первого руководителя (если Заявление подписывает не первый руководитель);

3) протокол (решение) уполномоченного органа юридического лица и приказ о назначении первого руководителя;

4) свидетельство о постановке на регистрационный учет по налогу на добавленную стоимость;

5) устав;

6) документы, подтверждающие государственную регистрацию/перерегистрацию юридического лица;

7) биометрическое решение для развертывания в контуре Оператора, соответствующее требованиям, приведенным в Приложении 5 к настоящим Правилам, и соответствующую документацию для проведения интеграции и тестирования;

8) документальное подтверждение наличия исключительных прав на биометрическое решение в соответствии с законодательством Республики Казахстан;

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

8-1) подписанное соглашение о проведении тестирования биометрического решения по форме согласно приложению 6 к Правилам;

Данный пункт включен решением Правления Общества от 22 ноября 2024 года (протокол № 30)

9) письмо подтверждение наличия службы технической поддержки и указанием ее контактов;

10) подписанное соглашение о проведении тестирования биометрического решения;

11) дополнительные документы (при необходимости).

71. Заявка и иные материалы направляются Оператору в официальном порядке лично либо заказным почтовым направлением по адресу: г. Алматы, микрорайон Коктем-3, здание 21. Прилагаемые к заявлению документы подаются в копиях.

72. Допускается подача заявления о присоединении к Договору присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД посредством системы электронного документооборота в соответствии с действующим законодательством Республики Казахстан.

Параграф 3. Рассмотрение Оператором заявок на подключение биометрических решений к ЦОИД

73. Рассмотрение заявок юридических лиц осуществляется на ежеквартальной основе в соответствии с утвержденным Оператором планом. Оператор рассматривает заявку в течение 20 (двадцати) рабочих дней (проверяет

заявку на полноту и правильность заполнения заявления о присоединении к Договору присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД, полномочия лица, подписавшего заявление, наличие оснований для заключения договора (соответствие юридического лица требованиям, предусмотренным Правилами), наличие копий прилагаемых документов). В пределах указанного срока Оператор также проводит тестирование биометрического решения.

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

74. Успешное прохождение функционального и нагрузочного тестирования является обязательным условием одобрения заявки на подключение биометрического решения к ЦОИД.

75. В случае положительного рассмотрения заявки юридического лица, Оператор осуществляет регистрацию Договора присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД. Регистрационный номер Договора присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД и дата его заключения доводится до сведения Поставщика биометрического решения путем направления сообщения посредством электронной почты, указанной в заявлении о присоединении и/или их проставления на заявлении о присоединении к Договору присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД и/или посредством системы электронного документооборота.

76. После заключения Договора присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД Оператор осуществляет интеграцию биометрического решения в ЦОИД.

Данный пункт включен решением Правления Общества от 22 ноября 2024 года (протокол № 30)

76-1. Поставщик предоставляет дополнительную лицензию для развертывания его биометрического решения в тестовом контуре Оператора сроком действия не ранее окончания срока действия Договора присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД.

Данный пункт включен решением Правления Общества от 12 августа 2025 года (протокол № 15)

77. При наличии оснований для отказа в предоставлении услуг, регистрация Договора присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД Оператором не производится, причины отказа доводятся до сведения юридического лица путем направления сообщения посредством электронной почты, указанной в заявлении о присоединении и/или указания в заявлении о присоединении к Договору присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД и/или посредством системы электронного документооборота.

77-1. Оператор вправе приостановить использование биометрического решения в случае выявления несоответствия требованиям, установленным настоящими Правилами и/или технической документацией.

При этом Оператор за 14 (четырнадцать) календарных дней до даты отключения направляет соответствующее уведомление Участникам, а также направляет Поставщику официальное письмо с требованием предоставить исправленную версию решения для проведения повторного тестирования.

В случае непрохождения повторного тестирования, Оператор оставляет за собой право в одностороннем порядке расторгнуть договор с Поставщиком.

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

78. При необходимости, после устранения замечаний, послуживших основанием для отказа в заключении Договора присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД, юридическое лицо вправе подать новую заявку на подключение биометрических решений к ЦОИД, но не ранее двух месяцев с даты подписания Протокола тестирования.

Данный пункт включен решением Правления Общества от 22 ноября 2024 года (протокол № 30)

Параграф 4. Условия тарификации и оплаты услуг поставщиков биометрических решений

79. Предельная стоимость услуг поставщиков биометрических решений устанавливается Оператором.

80. ЦОИД обеспечивает учет обработанных биометрическими решениями запросов на проведение биометрической верификации личности Клиента.

81. В рамках функционирования сервиса сопоставления фотоизображений Участник самостоятельно выбирает биометрическое решение, с использованием которого будет проведено сопоставление фотоизображений.

82. В рамках функционирования сервиса двухфакторной аутентификации распределение поступающих запросов между биометрическими решениями осуществляется Оператором в автоматическом режиме.

83. Оплата производится за фактически обработанное биометрическим решением количество запросов.

84. Порядок оплаты услуг поставщика биометрического решения определяются Договором присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД.

Глава 5. Рассмотрение диспутных ситуаций

85. Рассмотрение диспутных ситуаций возможно исключительно по результатам оказания ЦОИД услуги двухфакторной аутентификации ЦОИД. Рассмотрение диспутных ситуаций по результатам оказания ЦОИД услуги сопоставления фотоизображений не проводится.

86. При несогласии Клиента с результатами проведенной аутентификации, Клиент обращается в службу поддержки Участника.

87. Участник на основании запроса Клиента направляет официальный запрос Оператору, с указанием сути запроса, реквизитов документа, на основании которого проводится разбирательство, хронологии взаимодействия информационных систем Участника с ЦОИД и иных деталей проведенной процедуры аутентификации личности Клиента.

Данный пункт включен решением Правления Общества от 22 ноября 2024 года (протокол № 30)

88. Оператор проводит разбирательство по существу диспута, по результатам которого формируется заключение.

89. В заключении указываются следующие сведения (не ограничиваясь):

1) дата и время проведения аутентификации личности Клиента;
2) поставщик биометрического решения, чье биометрическое решение использовалось при аутентификации личности Клиента;
3) биометрическое решение, которое использовалось при аутентификации личности Клиента;
4) сведения из подсистемы доставки СМС сообщений;
5) сведения из подсистемы логирования;
6) результат анализа фото и (или) видео, на основании которых проводилась liveness-проверка лица;
7) результат анализа фотоизображений лица Клиента, представленных для сопоставления;
8) итоговое заключение по результатам проведенного разбирательства.

90. Оператор несет перед Участником ответственность по доказанным фактам неправильного положительного результата по итогам двухфакторной аутентификации личности (положительная аутентификация злоумышленника вместо корректной личности) на стороне ЦОИД. Размер ответственности Оператора перед Участником определяется условиями Договора о предоставлении услуг ЦОИД с Участником.

91. Причиненный Участнику ущерб по доказанным фактам некорректной аутентификации личности (положительная аутентификация злоумышленника вместо корректной личности) возмещается Оператором, в соответствии с условиями Договора о предоставлении услуг.

92. Участник самостоятельно несет ответственность перед Клиентами и любыми третьими лицами за любой ущерб и/или убытки вследствие неправильного положительного результата по итогам двухфакторной аутентификации личности (положительная аутентификация злоумышленника вместо корректной личности).

93. Участник самостоятельно несет ответственность перед Клиентами и любыми третьими лицами за любой ущерб и/или убытки вследствие нарушения информационной безопасности, а также сбоев в работе сервисов ЦОИД, вызванных действием или бездействием по своей вине.

94. Оператор не несет ответственности за любые возможные убытки Клиента и (или) Участника, связанные с отрицательным результатом проведенной аутентификации личности Клиента.

Глава 6. Система управления рисками

95. Управление рисками осуществляется в соответствии с Политикой управления рисками и другими внутренними документами Оператора, определяющих принципы и подходы к организации системы управления рисками и внутреннего контроля.

96. Для управления рисками, связанными с ложным пропуском в процессах аутентификации личности Клиента, применяются следующие методы:

1) тестирование биометрических решений на предмет противодействия атакам (противодействие подделке лица, такие как использование фотографий, видеозаписей, масок или deepfake технологий для обхода системы);

2) двухфакторная аутентификация личности Клиента;

3) ограничение количества попыток прохождения liveness-проверки лица.

97. Для управления рисками информационной безопасности Оператором предпринимаются организационные и технические меры по защите персональных данных в соответствии с требованиями действующего законодательства, а также требованиями международных и государственных стандартов в области информационной безопасности.

98. Для управления другими операционными рисками Оператором используются следующие контрольные меры:

1) проведение Оператором контроля за функционированием ЦОИД;

2) круглосуточный мониторинг и поддержание Оператором беспрерывной работы ЦОИД;

3) обеспечение надлежащего технического обслуживания оборудования ЦОИД для обеспечения его полной исправности и постоянной готовности, планирование приобретения и замена устаревшего оборудования;

4) обеспечение выполнения необходимых разработок и доработок по совершенствованию и устранению дефектов сервисов ЦОИД;

5) тестирование и регулярная установка обновлений стабильных версий прикладного/общесистемного программного обеспечения ЦОИД;

6) управление событиями и инцидентами, включая своевременное обнаружение, регистрацию, реагирование и анализ;

7) поддержание в актуальном состоянии плана восстановления функционирования сервисов ЦОИД с учетом возможных сценариев остановки работы системы и тестирование Оператором данного плана;

8) обеспечение работоспособности основного и резервного центров обработки данных ЦОИД;

9) перевод ЦОИД из основного центра обработки данных в резервный центр обработки данных при наличии сбоев или простоев в работе программно-технического комплекса ЦОИД, не подлежащих восстановлению в основном центре обработки данных;

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

10) обеспечение достаточного количества квалифицированного персонала, обеспечивающего сопровождение и поддержку ЦОИД, а также другие контрольные меры, предусмотренные системой внутреннего контроля Оператора.

Приложение 1
к Правилам функционирования
Центра обмена
идентификационными
данными

Требования к фотоизображению, предоставляемому в ЦОИД

Сервис сопоставления фотоизображений ЦОИД принимает фотоизображения, удовлетворяющие следующим требованиям:

1) изображение человека выше уровня груди;
2) изображение лица должно быть не менее 40% и не более 80% от общей площади фотоизображения;
3) голова может быть повернута и наклонена на не более чем 8° от фронтального положения;
4) расстояние между центрами глаз при минимальном горизонтальном размере 360 пикселей должна составлять не менее 70 пикселей;
5) размер входного изображения должен быть не менее 640x360 пикселей;

Данный пункт включен решением Правления Общества от 22 ноября 2024 года (протокол № 30)

6) изображение должно быть свободным от посторонних лиц в кадре;
7) плечи должны быть направлены к камере, исключая портретный стиль со взглядом через плечо;
8) лицо должно быть равномерно освещено без преобладающего направления света, с определенным соотношением интенсивности освещения;
9) изображение не должно содержать ярких пятен или бликов;
10) не допускается наличие головного убора. Необходимо обеспечить четкую видимость всех черт лица от подбородка до верхней линии лба, включая обе стороны лица;
11) разрешается использование очков только с прозрачными стеклами и без отражений вспышки. Окрашенные линзы запрещены. Необходимо избегать использования очков с толстыми оправами, отдавая предпочтение моделям с тонкими и прочными оправами, если они необходимы субъекту. Оправа очков не должна перекрывать глаза, обеспечивая их полную видимость;
12) недопустимы световые артефакты или отражения вспышки;
13) взгляд должен быть направлен прямо в камеру;
14) глаза должны быть открыты и четко видны. Волосы не должны закрывать глаза;
15) выражение лица должно быть нейтральным;
16) фотография лица должна четкой, лицо в фокусе.

Приложение 2
к Правилам функционирования
Центра обмена
идентификационными
данными

Пользовательское соглашение информационной системы «Центр обмена идентификационными данными» (ЦОИД)

Настоящее пользовательское соглашение информационной системы «Центр обмена идентификационными данными» (ЦОИД) (далее – Пользовательское соглашение) определяет условия взаимоотношений акционерного общества «Национальная платежная корпорация Казахстана Национального Банка Республики Казахстан», именуемое в дальнейшем «АО «НПК»» с одной стороны, и клиентом, присоединившемся к Пользовательскому соглашению, именуемое в дальнейшем «Клиент», также совместно именуемые «Стороны», а по отдельности «Сторона».

Условия Пользовательского соглашения принимаются Клиентом не иначе как путем присоединения к нему в целом, и являются стандартными для всех Клиентов, присоединившихся к Пользовательскому соглашению.

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

Присоединение Клиента к Пользовательскому соглашению осуществляется путем нажатия «Продолжить» (далее – Действия).

Выполнение указанных Действий означает, что Клиент ознакомлен с Пользовательским соглашением и согласен с тем, что условия Пользовательского соглашения принимаются им в редакции, действующей на момент выполнения Действий, полностью без каких-либо оговорок, изъятий, изменений и протоколов разногласий.

После присоединения к Пользовательскому соглашению путем выполнения Действий Клиент не может ссылаться на то, что он не ознакомлен с Пользовательским соглашением (полностью или частично), либо не признает его обязательность во взаимоотношениях с АО «НПК».

Клиент принимает изменения и дополнения, вносимые АО «НПК» в Пользовательское соглашение, в соответствии с условиями Пользовательского соглашения, при этом заключения дополнительного соглашения к Пользовательскому соглашению не требуется.

Актуальная редакция Пользовательского соглашения (Приложение 2 к Правилам ЦОИД) опубликована на официальном Сайте по адресу: https://npck.kz/pravila-coid/.

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

1. Термины и определения

1.1. аутентификация личности Клиента - процедура проверки подлинности личности Клиента;

1.2. двухфакторная аутентификация личности - услуга аутентификации личности Клиента с применением двух различных идентификаторов (ввод одноразового (единовременного) кода, полученного на мобильное устройство Клиента, и биометрическая верификация личности);

1.3. биометрические данные - персональные данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых можно установить его личность;

1.4. ГБД ФЛ - государственная база данных «Физические лица»;

1.5. доступные источники – государственные базы данных, содержащие сведения, позволяющие аутентифицировать личность Клиента;

1.6. Клиент – совершеннолетнее, дееспособное физическое лицо - гражданин Республики Казахстан, иностранец или лицо без гражданства, постоянно проживающее на территории Республики Казахстан (при наличии вида на жительства в Республике Казахстан или удостоверения лица без гражданства, выданных уполномоченным государственным органом Республики Казахстан), обратившееся к Участнику за получением услуги;

1.7. liveness–проверка – процесс выявления подмены личности Клиента, таких как использование фотографий, видеозаписей, масок или deepfake технологий для обхода системы;

1.8. deepfake технологии - методика синтеза изображения, используемая для соединения и наложения существующих изображений и видео на исходные изображения или видеоролики;

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

1.9. сопоставление фотоизображений – процесс сверки фотоизображения лица Клиента, полученного из сессии liveness-проверки с фотоизображением, полученным из доступных источников;

1.10. обработка персональных и биометрических данных – действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных и биометрических данных;

1.11. сбор персональных и биометрических данных – действия, направленные на получение персональных и биометрических данных;

1.12. Участник – юридическое лицо, с которым АО «НПК» заключен Договор присоединения о предоставлении услуг ЦОИД;

1.13. ЦОИД - информационная система «Центр обмена идентификационными данными» АО «НПК»;

1.14. Услуги – услуги ЦОИД, оказываемые по запросам Участника по двухфакторной аутентификации личности Клиента с предоставлением персональных данных из доступных источников и/или управления облачной ЭЦП, по запросу Участника;

1.15. Правила ЦОИД – Правила функционирования Центра обмена идентификационными данными, опубликованными на Сайте по адресу: https://npck.kz/pravila-coid/.

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

1.16. Сайт – официальный интернет-ресурс АО «НПК», доступный по адресу: https://npck.kz/.

2. Предмет Пользовательского соглашения

2.1. Настоящим Пользовательским соглашением Клиент **дает свое безусловное и безоговорочное согласие АО «НПК»:**

2.1.1. на проведение в отношении Клиента по запросам Участника двухфакторной аутентификации личности Клиента, передачи результатов (итогов) проведенной в отношении Клиента аутентификации личности и/или сопоставления его фотоизображения Участнику;

2.1.2. на сбор и обработку персональных данных Клиента, в том числе передачу их Участнику, за исключением трансграничной передачи данных;

2.1.3. осуществление учета и хранения согласий Клиента на передачу персональных данных Клиента;

2.1.4. на выполнение АО «НПК» иных действий, бездействия, осуществление иных прав и обязанностей, в соответствии с Правилами ЦОИД, прямо или косвенно затрагивающих права и законные интересы Клиента.

3. Сбор и обработка персональных данных

3.1. К персональным данным, на сбор и обработку которых Клиент в соответствии с настоящим Пользовательским соглашением дает АО «НПК» согласие, относятся:

- ИИН;
- фамилия, имя, отчество;
- дата рождения;
- пол;
- национальность;
- гражданство;
- данные документа, удостоверяющего личность (номер документа, дата выдачи, срок действия, и орган, выдавший документ);
- сведения о месте рождения;
- сведения об адресе регистрации;
- биометрические данные (фото/видеоизображение);
- номер телефона.

3.2. Если иное не установлено законодательством или Пользовательским соглашением, согласия на сбор, обработку персональных данных, предоставленных Клиентом, действуют до их отзыва в установленном настоящим Пользовательским соглашением порядке.

4. Учет и хранение согласий на передачу персональных данных

4.1.Учет и хранение согласий Клиента на передачу персональных данных осуществляется АО «НПК» путем выполнения следующих функций:

4.1.1. регистрация согласия Клиента на передачу Участникам его персональных данных;

4.1.2. отзыв ранее зарегистрированного согласия Клиента на сбор, обработку и передачу его персональных данных третьим лицам.

Данный пункт включен решением Правления Общества от 22 ноября 2024 года (протокол № 30)

5. Права и обязанности сторон

5.1.Клиент имеет право:

5.1.1. в любое время отозвать согласие на сбор и обработку его персональных данных, предоставленное АО «НПК», путем отправки соответствующего сообщения в адрес технической поддержки: support@kisc.kz. При этом, АО «НПК» вправе продолжить сбор, обработку персональных данных без согласия Клиента, когда персональные данные сделаны общедоступными, а также при наличии оснований, указанных в статье 9 Закона Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите».

5.1.2. отказаться от проведения в отношении него двухфакторной аутентификации личности и/или сопоставления его фотоизображения (в том числе путем их прерывания до момента их завершения). При этом, Клиент предупрежден и соглашается с тем, что Услуги Участнику в отношении него в этом случае могут быть не оказаны либо оказаны не в полном объеме;

5.1.3. обжаловать неправомерные действия или бездействие АО «НПК» при обработке его данных, на защиту своих прав и законных интересов.

5.2.АО «НПК» имеет право:

5.2.1. Осуществлять проведения процедур и действий, указанных в настоящем Пользовательском соглашении с использованием средств автоматизации;

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

5.2.2. отказать в проведении двухфакторной аутентификации личности Клиента в случае нарушения условий использования сервисов ЦОИД, выявления признаков несанкционированных действий, нарушения требований установленных норм законодательства, Правил ЦОИД и других внутренних документов АО «НПК», или возможного применения средств подделки личности Клиента;

5.2.3. в целях обеспечения соблюдений действующего законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма хранить информацию о ранее проведенных процедурах аутентификации Клиента;

5.3. расторгнуть настоящее Пользовательское соглашение в одностороннем порядке (односторонний отказ) в случае неисполнения или ненадлежащего исполнения Клиентом условий настоящего Пользовательского соглашения.

5.4.АО «НПК» обязуется:

5.4.1. по запросам Участника оказывать в отношении Клиента Услуги;

5.4.2. прекратить сбор и обработку данных после отзыва Клиентом соответствующего согласия. За исключением сбора, обработки персональных данных без согласия Клиента, когда персональные данные сделаны

общедоступными, а также при наличии оснований, указанных в статье 9 Закона Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите».

5.4.3. принимать все необходимые меры для обеспечения конфиденциальности и обеспечения защиты персональных данных Клиента, полученных в рамках настоящего Пользовательского соглашения;

5.5.Клиент обязуется:

5.5.1. подавать запрос только от своего имени;

5.5.2. соблюдать Правила ЦОИД, а также иные требования, установленные и прописанные АО «НПК».

5.5.3. не осуществлять действия, указанные в п.5.6 Пользовательского соглашения.

5.6.Клиенту запрещается:

5.6.1. разглашать/ передавать третьим лицам информацию, полученную от АО «НПК» и используемую в процессе аутентификации личности Клиента, включая одноразовый пароль, отправляемый посредством СМС;

5.6.2. использовать любые средства подмены личности при прохождении процедуры аутентификации личности Клиента;

5.6.3. предпринимать действия, которые могут привести к непропорционально большой нагрузке на инфраструктуру АО «НПК» и иным образом нарушать работу сервисов АО «НПК»;

5.6.4. производить действия, направленные на получение незаконного доступа к информационным ресурсам, информационным системам и базам данных АО «НПК».

6. Конфиденциальность и безопасность данных

6.1. Каждая из Сторон сохраняет надлежащий режим конфиденциальности, в том числе хранения банковской тайны и защиты персональных данных, и принимает все необходимые меры по защите указанной информации от несанкционированного разглашения.

6.2. В целях повышения уровня безопасности, предотвращения мошеннических действий, недопущения разглашения конфиденциальной информации или иных противоправных действий АО «НПК» могут быть предусмотрены дополнительные условия, требования или действия для проверки подлинности, корректности, достоверности личности Клиента.

6.3. Доступ к персональным данным Клиента предоставляется только тем работникам АО «НПК», которым эта информация необходима для исполнения своих служебных обязанностей.

7. Ответственность

7.1. Клиент признает и соглашается, что АО «НПК» не несет ответственности за любые убытки (включая упущенную выгоду), которые могут быть причинены Клиенту в связи с ограничением доступности сервисов ЦОИД, используемых для оказания Услуг в отношении Клиента, независимо от оснований для такого ограничения.

7.2. Клиент принимает на себя риски, связанные с технологическими ограничениями и вероятностью ложного пропуска некорректной личности, и признает, что АО «НПК» не может гарантировать абсолютную точность в процессе аутентификации его личности. При выявлении фактов некорректной аутентификации личности Клиент обращается в техническую поддержку Участника.

7.3. АО «НПК» не несет ответственности за любые возможные убытки Клиента и (или) Участника, связанные с несогласием Клиента с отрицательным результатом проведенной аутентификации личности Клиента ЦОИД.

7.4. АО «НПК» освобождается от ответственности за неисполнение или ненадлежащее исполнение своих обязательств, если это явилось следствием обстоятельств, которые не могут быть предотвращены или преодолены АО «НПК», включая, но не ограничиваясь:

- действий обстоятельств непреодолимой силы;
- изменений/отмены нормативных правовых актов;
- действий государственных органов и третьих лиц;
- ухудшения качества услуг, предоставляемых операторами связи;
- работы любых устройств, техники, программ, приложений, информационных систем, со стороны Клиента, Участника и любых третьих лиц;
- других причин, не зависящих от АО «НПК».

7.5. АО «НПК» не несет ответственность за результат оказания услуги, в рамках которой АО «НПК» проведена процедура аутентификации личности.

8. Заключительные положения

8.1. Настоящее Пользовательское соглашение вступает в силу и считается заключенным с даты выполнения Действий Клиентом.

8.2. Внесение изменений и дополнений в Пользовательское соглашение производится АО «НПК» в одностороннем порядке.

8.3. Уведомление о внесении изменений и дополнений в Пользовательское соглашение осуществляется АО «НПК» путем размещения новой редакции Пользовательского соглашения на Сайте по адресу: https://npck.kz/pravila-coid/.

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

8.4. Если иное не предусмотрено настоящим Пользовательским соглашением, любые изменения и дополнения в Пользовательское соглашение вступают в силу с даты их размещения на Сайте и распространяются на всех Клиентов, присоединившихся к Договору, в том числе присоединившихся к Пользовательскому соглашению ранее даты внесения изменений и дополнений в Пользовательское соглашение.

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

8.5. Вопросы, не урегулированные настоящим Пользовательским соглашением, подлежат разрешению в соответствии с законодательством Республики Казахстан.

8.6. В случае возникновения любых споров или разногласий, связанных с исполнением настоящего Пользовательского соглашения, Клиент и АО «НПК» приложат все усилия для их разрешения путем проведения переговоров между ними с использованием обязательного досудебного (претензионного) порядка. В случае, если споры не будут разрешены путем переговоров, споры подлежат разрешению в судебном порядке, установленном действующим законодательством Республики Казахстан.

8.7. Настоящее Пользовательское соглашение составлено на казахском и русском языках, имеющих одинаковую юридическую силу.

9. Юридический адрес и реквизиты АО «НПК»

Акционерное Общество «Национальная платежная корпорация Национального Банка Республики Казахстан»

адрес: A15C9T, Республика Казахстан, г. Алматы, м-н «Коктем-3», дом 21

БИН 960440000151

сектор экономики 5, признак резидентства 1,

ИИК KZ58601A861013807291 в АО «Народный Банк Казахстана»»

БИК HSBKKZKX.

Сәйкестендіру деректерімен алмасу
орталығының жұмыс істеу қағидаларына
3 қосымша

Приложение 3
к Правилам функционирования
Центра обмена
идентификационными данными

Данный пункт включен решением Правления Общества от 22 ноября 2024 года (протокол № 30)

Сәйкестендіру деректерімен алмасу
орталығының жұмыс істеу қағидаларына
4 қосымша

Приложение 4
к Правилам функционирования
Центра обмена
идентификационными данными

Данный пункт включен решением Правления Общества от 22 ноября 2024 года (протокол № 30)

Приложение 5
к Правилам функционирования
Центра обмена
идентификационными данными

Требования к биометрическим решениям

1. Биометрические решения используются ЦОИД для целей биометрической верификации личности Клиента.
2. Биометрическое решение должно функционировать в рамках инфраструктуры, предоставленной Оператором.
3. Администрирование и обновление биометрического решения осуществляется администраторами Оператора.
4. Биометрическое решение должно обеспечивать режим функционирования 24/7 с перерывом на обслуживание не более одного раза в три месяца, общей длительностью не более 168 часов в течение календарного года.

Данный пункт изменен решением Правления Общества от 12 августа 2025 года (протокол № 15)

5. Биометрическое решение должно быть предоставлено Оператору в виде docker образа.
6. Оператор проводит функциональное и нагрузочное тестирование биометрического решения в соответствии с утвержденной Оператором методикой тестирования биометрических решений.
7. Надлежащие технические характеристики биометрического решения и успешный результат проведенного тестирования являются обязательным условием включения биометрического решения в промышленную среду ЦОИД.
8. Биометрическое решение не должно содержать уязвимостей, выявленных Оператором по результатам проверки информационной безопасности с использованием имеющихся инструментов (антивирусы, системы анализа защищенности и т.п.) и признанных Оператором критичными. Критичные уязвимости подлежат исправлению поставщиком биометрического решения.

Требования к биометрическому решению liveness

9. Биометрическое решение liveness должно обеспечивать противодействие подделке лица и предотвращать попытки мошенничества, такие как использование фотографий, видеозаписей, масок или deepfake технологий для подлога личности. Оно должно обладать способностью распознавать и отличать живые лица от статичных или искусственных представлений, чтобы гарантировать, что процесс биометрической верификации осуществляется только с реальными живыми пользователями без использования средств подлога личности.
10. Биометрическое решение liveness должно предоставлять результат проведения проверки в виде «успешно/неуспешно».

11. Биометрическое решение liveness предоставляет ответ – «успешно» если обнаруживает признаки живого лица и устанавливает, что представленное лицо является реальным и не подвергается подмене или атаке.

12. Биометрическое решение liveness предоставляет ответ – «неуспешно» если обнаруживает несоответствия или подозрительные признаки, указывающие на возможность подделки или представления фотографии, маски или других атак.

13. Биометрическое решение liveness, при обработке сеанса связи с Клиентом, должно передавать на серверную часть серию фотоизображений либо видеофайл, на котором зафиксирован сеанс видеосвязи, объем которого не превышает 5 Мб.

14. Биометрическое решение liveness должно иметь в составе комплексное решение, реализующее фронтовую часть (WEB View) и бэковую в виде API.

14-1. Биометрическое решение liveness должно предоставлять возможность настройки интерфейса пользователя (цветовая гамма, текст, шрифты, логотип и т.д.).

Данный пункт включен решением Правления Общества от 12 августа 2025 года (протокол № 15)

15. Биометрическое решение должно обеспечивать возможность проведения liveness с применением стационарных/мобильных устройств под управлением наиболее распространенных операционных систем Windows/Linux/macOS/Android/iOS/WebOS и браузеров Chrome/Safari/Firefox последних версий).

16. Максимальное требование поставщика биометрического решения liveness по минимальному разрешению видеоизображения с камеры не должно быть менее 720p.

17. Биометрическое решение liveness должно обеспечивать обработку не менее 10 запросов в минуту в однопоточном режиме.

18. Тестирование биометрического решения liveness осуществляется в соответствии с утвержденной Оператором методикой тестирования биометрических решений. Для успешного прохождения тестирования биометрическое решение liveness должно успешно отразить все атаки, обеспечивая при этом отклонение корректной личности не более чем в 15% (пятнадцать процентов) случаях.

Требования к биометрическому решению сопоставления фотоизображений

19. Биометрическое решение сопоставления фотоизображений должно обеспечивать высокую точность (FMR не более 0,000001 (по методологии NIST) и не более 0.0005 (по методологии Оператора) при FNMR не более 0,01) и надежность при сравнении двух фотографий лица с целью определения принадлежат ли они одному и тому же человеку.

20. Поставщик должен предоставить Оператору рекомендованное пороговое значение коэффициента схожести фотоизображений, при котором сопоставление фотоизображений считается положительным. При этом биометрическое решение должно обеспечивать показатели точности сопоставления фотоизображений, указанные в пункте 19 настоящего раздела.

21. Биометрическое решение сопоставления фотоизображений должно предоставлять оценку степени сходства фотоизображений в виде коэффициента схожести фотоизображений.

22. API биометрического решения сопоставления фотоизображений должно работать в синхронном режиме.

23. Биометрическое решение сопоставления фотоизображений должно поддерживать работу с графическими процессорами.

24. Биометрическое решение сопоставления фотоизображений должно обеспечивать обработку не менее 100 запросов в минуту в однопоточном режиме.

25. Тестирование производительности и точности работы биометрического решения осуществляется на репрезентативной выборке, подготовленной Оператором.

Приложение 6
к Правилам функционирования
Центра обмена
идентификационными данными

Соглашение о проведении тестирования биометрического решения

Предмет соглашения

1. _____, в лице _____, действующего на основании _____ (далее – Потенциальный поставщик биометрического решения), соглашается с условиями настоящего Соглашения и предоставляет АО «Национальная платежная корпорация Национального Банка Республики Казахстан» (далее – АО «НПК») право на проведение тестирования ПО _____ (указать полное наименование) _____ (указать версию ПО) (далее – биометрическое решение).

Данный пункт включен решением Правления Общества от 22 ноября 2024 года (протокол № 30)

2. Потенциальный поставщик биометрического решения предоставляет АО «НПК» для тестирования биометрическое решение, соответствующее требованиям, изложенным в Приложении 5 к Правилам функционирования ЦОИД.

3. Тестирование биометрического решения проводится в целях определения возможности использования биометрического решения информационными системами АО «НПК» (далее – ИС АО «НПК») при проведении биометрической верификации личности.

4. Тестирование биометрического решения осуществляется в соответствии методикой тестирования биометрических решений АО «НПК», утвержденной АО «НПК».

5. Результаты тестирования биометрического решения публикуются на интернет-ресурсе АО «НПК» (http://npck.kz).

6. Для проведения тестирования Потенциальный поставщик биометрического решения предоставляет:

- простую неисключительную лицензию на биометрическое решение сроком не менее 30 календарных дней;
- биометрическое решение в виде docker контейнера;
- техническую документацию, описывающую вызов API биометрического решения.

Ответственность

7. Потенциальный поставщик биометрического решения соглашается с тем, что АО «НПК» не несет ответственности за косвенные, прямые и иные убытки, понесенные Потенциальным поставщиком биометрического решения в результате проведения тестирования и публикации результатов тестирования его биометрического решения.

Заключительные положения

8. Настоящее Соглашение вступает в силу с даты подписания Потенциальным поставщик биометрического решения настоящего Соглашения и действует в течение 30 (тридцати) календарных дней с момента его подписания.

9. Настоящее Соглашение составлено на казахском и русском языках, в двух экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон.

Поставщик: _____
ФИО, должность подписанта/подпись _____
МП

Дата получения АО «НПК» _____

Данный пункт включен решением Правления Общества от 22 ноября 2024 года (протокол № 30)

ЛИСТ ПОПРАВОК

1.	**Изменения и дополнения**	– утверждены решением Правления (протокол заседания от 22 ноября 2024 года № 30); – вступили в силу 22 ноября 2024 года
2.	**Изменения и дополнения**	– утверждены решением Правления (протокол заседания от 12 августа 2025 года № 15); – вступили в силу 12 августа 2025 года