Акционерное общество «Национальная платежная корпорация Национального Банка Республики Казахстан»

Уровень доступа: Общий

Утверждены
решением Правления АО «НПК»
от «04» 11 2025 г.
(приложение № 10
к протоколу № 19)

Дата вступления в силу с
«04» 11 2025 г.

Правила функционирования Центра обмена идентификационными данными

Рег. № 44

г. Алматы

Содержание

Глава 1. Общие положения

1. Правила функционирования Центра обмена идентификационными данными (далее – Правила) разработаны в соответствии с законами Республики Казахстан «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», «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) АРРФР – Агентство Республики Казахстан по регулированию и развитию финансового рынка;

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

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

4) биометрическая аутентификация личности – процесс сравнения и проверки соответствия биометрических данных Клиента, включающий liveness-проверку и сопоставление фотоизображения Клиента с фотоизображением из доступных источников;

Данный подпункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

5) биометрические данные – персональные данные, позволяющие охарактеризовать физиологические и биологические особенности человека, на основе которых можно установить его личность;

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

7) deepfake технологии – методика синтеза изображения, используемая для соединения и наложения существующих изображений и видео на исходные изображения или видеоролики;

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

9) двухфакторная аутентификация личности Клиента – аутентификация личности Клиента с применением двух различных способов идентификации (ввод одноразового (единовременного) кода, полученного на мобильное устройство Клиента, и биометрическая аутентификация личности);

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

11) Договор о предоставлении услуг – договор присоединения о предоставлении услуг ЦОИД и/или договор (присоединения) о предоставлении услуг сопоставления фотоизображений ЦОИД;

12) ИИН – индивидуальный идентификационный номер;

13) Клиент – физическое лицо или физическое лицо, действующее от имени юридического лица, обратившееся и/или пользующееся услугами Участника. Для физических лиц клиентом признается совершеннолетнее, дееспособное лицо - гражданин Республики Казахстан, иностранец или лицо без гражданства, постоянно проживающее на территории Республики Казахстан (для иностранцев и лиц без гражданства обязательным является наличие вида на жительства в Республике Казахстан или удостоверения лица без гражданства, выданных уполномоченным государственным органом Республики Казахстан);

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

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

16) Личный кабинет Клиента – персональная страница Клиента, доступная после прохождения Клиентом двухфакторной аутентификации личности и предоставляющая возможность управления выданными согласиями на сбор, обработку и передачу третьим лицам персональных данных и сведений, относящихся к банковской тайне, а также управления выпущенной облачной электронной цифровой подписью. Личный кабинет доступен для Клиентов по адресу: id.npck.kz;

17) матрица полномочий – реестр, содержащий перечень лиц, уполномоченных подписывать электронные документы от имени юридического лица с использованием облачной ЭЦП, заверенный (подписанный) первым руководителем организации, от имени которой предоставлены данные полномочия;

18) МФЦА – Международный финансовый центр «Астана»;

19) НБРК – Национальный Банк Республики Казахстан;

20) 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;

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

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

23) Оператор – Оператор ЦОИД, которым является Общество;

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

25) 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;

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

27) 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;

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

29) сопоставление фотоизображений – процесс сверки фотоизображения лица Клиента, полученного из доступных источников, с фотоизображением, полученным из сессии liveness-проверки, или при очном (личном) обращении Клиента;

30) Участник – юридическое лицо, которое присоединилось к Договору о предоставлении услуг ЦОИД и/или договору (присоединения) о предоставлении услуг сопоставления фотоизображений ЦОИД;

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

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

33) 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;

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);
- сведения о дееспособности/недееспособности физического лица;
- сведения об исключении из национального реестра индивидуальных идентификационных номеров;
- сведения о лице, признанным без вести пропавшим;

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

Глава 2. Взаимоотношения Оператора с Участниками

Параграф 1. Требования к Участникам

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

4. Договор о предоставлении услуг заключается Оператором со следующими юридическими лицами:

1) финансовой организацией, осуществляющей предпринимательскую деятельность по предоставлению финансовых услуг;

2) юридическим лицом, состоящим в реестре платежных организаций, формируемом НБРК;

3) дочерней организацией НБРК;

4) юридическим лицом, получившим лицензию МФЦА;

5) юридическим лицом, состоящим в реестре коллекторских агентств, формируемом АРРФР;

6) юридическим лицом, осуществляющим предпринимательскую деятельность в сфере игорного бизнеса;

7) участником экосистемы Open Banking и Open API, прошедшим аккредитацию Оператора;

8) государственным органом;

9) иными юридическими лицами по усмотрению Оператора.

Данный пункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

5. Договор о предоставлении услуг заключается Оператором с юридическим лицом при условии его соответствия следующим требованиям в совокупности:

1) юридическое лицо обеспечивает наличие службы технической поддержки, доступной Клиенту для консультаций в режиме 24/7;

2) юридическое лицо не находится в процессе банкротства либо на стадии ликвидации.

6. Юридическое лицо приобретает статус Участника после регистрации Оператором Договора о предоставлении услуг. Номер и дата заключения Договора присваивается и заполняется Оператором на заявлении Участника.

7. С целью ознакомления юридического лица с условиями подключения к сервисам ЦОИД необходимая документация размещается на Сайте Оператора.

Параграф 2. Подача заявок на подключение к сервисам ЦОИД

8. Для подключения к сервисам ЦОИД юридическое лицо, соответствующее требованиям, установленным Правилами, представляет Оператору заявление о присоединении по форме, установленной Договором о предоставлении услуг.

9. Юридическое лицо представляет заявление о присоединении с приложением копий следующих документов:

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

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

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

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) уведомление или разрешение 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) иные подтверждающие документы (при необходимости).

Данный подпункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

10. Предоставление заявления о присоединении к Договору о предоставлении услуг по сопоставлению фотоизображений ЦОИД с приложением документов, предусмотренных в пункте 9 Правил, осуществляется нарочно либо заказным почтовым направлением по адресу Оператора.

11. Подача заявления о присоединении к Договору о предоставлении услуг двухфакторной аутентификации личности, биометрической аутентификации и подписания электронных документов с применением облачной ЭЦП

осуществляется Участником в электронном виде на Портале. Оригинал заявления о присоединении к Договору о предоставлении услуг двухфакторной аутентификации личности и подписания электронных документов с применением облачной ЭЦП заказным почтовым направлением по адресу Оператора. Прилагаемые к заявлению документы подаются в копиях.

Данный пункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

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

13. Особенности подключения к сервисам ЦОИД:

Данный абзац изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

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

14. После получения от юридического лица заявления о присоединении к Договору о предоставлении услуг, Оператор в течение 7 (семи) рабочих дней проверяет:

1) соответствие юридического лица требованиям, установленным в пункте 5 Правил;

2) отнесение юридического лица к категориям юридических лиц, допускающихся к заключению Договора, предусмотренных в пункте 4 Правил;

3) полноту и правильность составления заявления о присоединении к Договору, а также полномочие лица, подписавшего его;

4) пакет документов, приложенных согласно перечню, предусмотренному пунктом 9 Правил.

Данный пункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

15. В случае, если юридическое лицо и (или) представленное заявление о присоединении к Договору с приложенными документами, не соответствуют условиям, предусмотренным в пунктах 4 и 5 Правил, Оператор отказывает в предоставлении услуг и заключении Договора о предоставлении услуг.

Данный абзац изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

Оператор вправе по своему усмотрению отказать в заключении Договора, в том числе при наличии оснований, предусмотренных законодательством Республики Казахстан и внутренними документами Оператора.

При этом отказ не влечёт возникновения у Оператора каких-либо обязательств перед пользователем.

16. При прохождении юридического лица и представленного заявления о присоединении к Договору о предоставлении услуг с приложенными документами проверки Оператора на соответствие условиям, предусмотренным пунктами 4 и 5 Правил, Оператор осуществляет регистрацию Договора о предоставлении услуг.

Данный абзац изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

Регистрационный номер и дата его заключения доводится до сведения Участника путем отметки в заявлении о присоединении к Договору о предоставлении услуг либо направления сообщения одним из следующих способов:

1) посредством Портала Общества;
2) по электронной почте, указанной в заявлении о присоединении;
3) посредством системы электронного документооборота.

17. Юридическое лицо приобретает статус Участника после регистрации Оператором Договора о предоставлении услуг.

18. 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.

Параграф 4. Основания для приостановления или прекращения предоставления услуг Участнику

19. Предоставление услуг Участнику приостанавливается в следующих случаях:

1) при неисполнении или ненадлежащем исполнении, и иных нарушений Участником условий Договора о предоставлении услуг, Правил и иных 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 сроков оплаты услуг более чем на 15 (пятнадцать) календарных дней;

5) в иных случаях, установленных законодательством Республики Казахстан и Правилами.

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

21. Предоставление услуг Участнику прекращается в следующих случаях:

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

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

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

4) в случае нарушения сроков оплаты услуг более чем на 30 (тридцать) календарных дней;

5) 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;

6) в иных случаях, установленных законодательством Республики Казахстан.

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

23. В случае подтвержденного факта лишения Участника лицензии АРРФР Оператор расторгает Договор в одностороннем порядке в соответствии с условиями Договора о предоставлении услуг.

24. В случае если выявлен факт приостановления АРРФР лицензии Участника, Оператор незамедлительно блокирует 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).

25. Участник обязуется незамедлительно, но не позднее 1 (один) рабочего дня, уведомлять Оператора о приостановлении/лишении/возобновлении действия лицензии АРРФР Участника. В случае несвоевременного уведомления/ отсутствия уведомления Оператора о факте лишения/приостановления/возобновления лицензии АРРФР ответственность несет Участник.

26. В случае несвоевременного уведомления или не уведомления Оператора о вышеуказанных фактах:

1) Оператор не несёт какой-либо ответственности за последствия предоставления услуг Участнику в период отсутствия у него действующей лицензии;

2) все риски, убытки, претензии третьих лиц, а также возможные мошеннические действия, совершённые в указанный период, полностью и исключительно возлагаются на Участника;

3) Участник обязуется возместить Оператору все понесённые убытки, штрафы и расходы (включая судебные издержки и расходы на представительство), возникшие в связи с неисполнением указанных обязательств

27. Оператор вправе, но не обязан, осуществлять самостоятельную проверку статуса лицензии Участника по официальным источникам. Осуществление такой проверки не освобождает Участника от обязанности по уведомлению и не влечёт за собой возникновение у Оператора какой-либо ответственности в случае непредоставления или несвоевременного предоставления уведомления.

Параграф 5. Условия тарификации и оплаты услуг Участниками

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

29. Условия тарификации и размеры тарифов публикуются на Сайте.

30. Оператор ежемесячно взимает оплату за услуги, фактически оказанные Участнику (Клиенту). Условия и порядок оплаты услуг определяются Договором о предоставлении услуг. Сессия по услугам двухфакторной аутентификации личности и биометрической аутентификации прерванная Клиентом, подлежит оплате в полном объеме. Сессия подписания электронных документов с применением облачной ЭЦП, прерванная Клиентом в ходе прохождения двухфакторной аутентификации личности, подлежит оплате в соответствии с установленными Оператором тарифами на услуги двухфакторной аутентификации личности.

Данный пункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

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

Данный пункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

32. 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 Оператора, размещенной на Сайте.

Глава 3. Взаимоотношения Оператора с поставщиками биометрических решений

Параграф 1. Требования к поставщикам биометрических решений

33. Договор присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД заключается Оператором с юридическим лицом в совокупности соответствующим следующим требованиям:

1) юридическое лицо должно являться платежеспособным, не иметь срок налоговой задолженности свыше трех последних календарных месяцев;

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

3) юридическое лицо на момент подачи заявки не должно находиться в процессе банкротства либо находиться в стадии 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. Представление заявок на подключение биометрических решений к ЦОИД

34. Юридическое лицо, желающее стать поставщиком биометрического решения, предоставляет 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;

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

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

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

5) устав;

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

7) биометрическое решение для развертывания в контуре Оператора, соответствующее требованиям, предусмотренным в приложении 3 к Правилам, и соответствующую документацию для проведения интеграции и тестирования;

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

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

10) подписанное соглашение о проведении тестирования биометрического решения по форме, согласно приложению 4 к Правилам;

11) дополнительные документы (при необходимости).

35. В случае повторного заключения договора и неизменности версии биометрического решения, сведения указанные в подпунктах 7) и 10) Пункта 34 не предоставляются. Заявка и иные материалы направляются Оператору в официальном порядке нарочно либо заказным почтовым направлением по адресу Оператора. Прилагаемые к заявлению документы подаются в копиях.

36. Допускается направление 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 заявки на подключение биометрических решений к ЦОИД

37. Рассмотрение заявки юридического лица осуществляется на ежеквартальной основе. Оператор рассматривает заявку в течение 20 (двадцати) рабочих дней и проверяет:

1) соответствие юридического лица требованиям, установленным в пункте 33 Правил;

2) полноту и правильность составления заявления о присоединении к Договору присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД, а также полномочие лица, подписавшего его;

5) пакет документов, приложенных согласно перечню, предусмотренному пунктом 34 Правил.

В пределах указанного срока Оператор также проводит функциональное тестирование биометрического решения и тестирование функций информационной безопасности.

38. Успешное прохождение тестирования функций информационной безопасности и функционального тестирования является обязательным условием одобрения заявки на подключение биометрического решения к ЦОИД.

39. 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 их проставления на заявлении о присоединении к Договору присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД или направления сообщения посредством:

1) электронной почты, указанной в заявлении о присоединении;
2) системы электронного документооборота.

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

41. 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.

42. В случае, если юридическое лицо и (или) представленное заявление о присоединении к Договору присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД с приложенными документами, не пройдут проверку Оператора на соответствие условиям, предусмотренным в пунктах 33 и 34 Правил, Оператор отказывает в предоставлении услуг и заключении Договора присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД.

Данный пункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

43. Причина отказа в предоставлении услуг и заключении Договора присоединения о предоставлении простой неисключительной лицензии на биометрическое решение для ЦОИД доводится Оператором до сведения юридического лица путем направления сообщения посредством электронной почты, указанной в заявлении о присоединении и/или системы электронного документооборота.

44. Оператор вправе приостановить использование биометрического решения, в случае выявления несоответствия требованиям, установленным Правилами и/или технической документацией Оператора.

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.

45. 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.

В случае успешных результатов функционального тестирования биометрического решения и не успешных результатов тестирования функций информационной безопасности Поставщику предоставляется 10 (десять) рабочих дней на их устранение с последующим повторным тестированием функций информационной безопасности. При этом сроки тестирования продлеваются на 20 (двадцать) рабочих дней, с момента повторного предоставления биометрического решения для тестирования. При сохранении неизменности алгоритмов и функциональной логики биометрического решения, повторное функциональное тестирование не проводится.

Данный абзац изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

Если выявленные уязвимости не будут устранены, формируется Протокол о несоответствии требованиям информационной безопасности.

Параграф 4. Условия тарификации и оплаты услуг поставщиков биометрических решений

46. Предельная стоимость услуг поставщиков биометрических решений устанавливается Оператором.

47. ЦОИД обеспечивает учет обработанных биометрическими решениями запросов на проведение биометрической аутентификации личности Клиента.

Данный пункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

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

49. В рамках оказания услуг двухфакторной и биометрической аутентификации распределение поступающих запросов между биометрическими решениями осуществляется Оператором в автоматическом режиме.

Данный пункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

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

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

Глава 4. Функционирование сервисов ЦОИД

Параграф 1. Общие требования по функционированию ЦОИД

52. ЦОИД функционирует в целях предоставления Участникам сервисов ЦОИД при оказании услуг Клиентам дистанционным (удаленным) способом, а также при очном (личном) обращении Клиента.

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

1) услуга по сопоставлению 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 по подписанию электронных документов с применением облачной ЭЦП - юридически значимое подписание электронных документов с использованием облачной электронной цифровой подписи без необходимости применения физических носителей;

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

Данный пункт дополнен подпунктом 4 решением Правления Общества от 30 января 2026 года (протокол № 2).

54. 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.

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

56. ЦОИД обеспечивает хранение запросов, а также результатов оказания услуг Участникам в течение 5 (пяти) лет с даты их получения и обработки. Все данные, полученные от Участника и обработанные ЦОИД, должны оставлять аудиторский след.

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

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

59. Участник обязан соблюдать требования законодательства Республики Казахстан о персональных данных и их защите в части обеспечения наличия согласия Клиента на сбор, обработку и передачи третьим лицам его персональных данных при передаче персональных данных Клиента Оператору и принимать необходимые меры по обеспечению информационной безопасности в соответствии с требованиями законодательства Республики Казахстан.

Параграф 2. Порядок оказания услуги сопоставления фотоизображений Клиента

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

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

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

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

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

63. 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, или полученное при очном (личном) обращении Клиента соответствующее требованиям, установленным в приложении 1 к Правилам;

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, предусмотренными в пунктах 57 и 59 Правил.

64. Сервис сопоставления фотоизображений осуществляет обработку запроса Участника, соответствующего 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, предусмотренными в пунктах 57 и 59 Правил, направляет в доступные источники запрос на получение персональных данных Клиента. Полученные персональные данные перенаправляются Участнику;

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.

65. В случае неуспешного проведения процедуры биометрической аутентификации 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.

66. Персональные данные Клиента, 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 аутентификации личности Клиента с использованием результатов степени соответствия фотоизображений.

67. 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.

68. 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.

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

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

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

Параграф 3. Порядок оказания услуги двухфакторной аутентификации личности Клиента

72. 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 аутентификацию 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 (пятнадцать) 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;

3) СМС проверку путем направления 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.

Данный подпункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

73. 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.

74. Согласие Клиента с условиями Пользовательского соглашения, оформленного по форме приложения 2 к Правилам, является обязательным

условием продолжения процедуры двухфакторной аутентификации. В случае отсутствия такого согласия услуга по двухфакторной аутентификации личности Клиента не оказывается.

Данный пункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

75. Исключен.

Данный пункт исключен решением Правления Общества от 30 января 2026 года (протокол № 2).

76. Двухфакторная аутентификация юридического лица осуществляется посредством аутентификации первого руководителя организации или других лиц, уполномоченных в соответствии с матрицей полномочий.

77. В составе сервиса двухфакторной аутентификации ЦОИД при осуществлении между Участниками обмена информацией и иных сведений, содержащих персональные данные и банковскую тайну, а также при проведении платежей и (или) 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 персональных данных и сведений, относящихся к банковской тайне;

3) ведение реестра согласий Клиента на сбор, обработку и передачу персональных данных третьим лицам и сведений, относящихся к банковской тайне

4) проверка Оператором наличия ранее зарегистрированного согласия Клиента на сбор, обработку и передачу третьим лицам персональных данных и сведений, относящихся к банковской тайне;

5) предоставление Клиенту возможности просмотра зарегистрированных/отозванных согласий на сбор, обработку и передачу третьим лицам персональных данных и сведений, относящихся к банковской тайне.

78. Отзыв согласия на сбор, обработку и передачу третьим лицам персональных данных и сведений, содержащих банковскую тайну, а также на проведение платежей и (или) переводов денег посредством межбанковской системы обмена информацией по открытым программным интерфейсам (OpenAPI) осуществляется Клиентом посредством Личного кабинета (id.npck.kz).

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

80. В случае неуспешного завершения процедуры двухфакторной аутентификации личности Клиента, в ответном сообщении Участнику ЦОИД направляет информацию о неуспешном проведении соответствующих процедур.

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

82. 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 третьим лицам персональных данных и сведений, относящихся к банковской тайне.

83. 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, либо через выделенный канал связи посредством IP VPN или IPSEC.

Параграф 3-1. Порядок оказания услуги биометрической аутентификации

83-1. Для оказания услуги биометрической аутентификации используется сервис двухфакторной аутентификации ЦОИД. Услуга биометрической аутентификации обеспечивает по запросу Участника комплексное проведение мероприятий по аутентификации личности Клиента включающее в себя:

1) запрос подтверждения ИИН Клиента;

2) биометрическую аутентификацию 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 (пятнадцать) 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;

3) принятие решения по результатам проведенной процедуры биометрической аутентификации личности и отправка результата Участнику;

4) предоставление персональных данных Клиента по запросу Участника с согласия Клиента.

83-2. В запросе на проведение биометрической аутентификации личности Участник направляет Оператору ИИН Клиента;

83-3. Согласие Клиента с условиями Пользовательского соглашения, оформленного по форме приложения 2 к Правилам, является обязательным условием продолжения процедуры биометрической аутентификации личности. В случае отсутствия такого согласия услуга по биометрической аутентификации не оказывается.

83-4. В случае успешного завершения процедуры биометрической аутентификации личности, в ответном сообщении Участнику ЦОИД направляет код авторизации, который в дальнейшем используется Участником в процессе получения персональных данных.

83-5. В случае неуспешного завершения процедуры биометрической аутентификации личности, в ответном сообщении Участнику ЦОИД направляет информацию о неуспешном проведении соответствующих процедур.

83-6. При успешном завершении процедуры биометрической аутентификации личности, Участник может направить запрос на получение персональных данных Клиента с приложением полученного кода авторизации.

83-7. 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 третьим лицам персональных данных и сведений, относящихся к банковской тайне.

83-8. Взаимодействие услуги биометрической аутентификации ЦОИД с Участниками осуществляется посредством глобальной сети Интернет с учетом наличия публичного статического IPv4 адреса, зарегистрированного (RIPE-NCC) в Республике Казахстан, либо через выделенный канал связи посредством IP VPN или IPSEC.

Данный параграф дополнен решением Правления Общества от 30 января 2026 года (протокол № 2).

Параграф 4. Порядок оказания услуги подписания электронных документов с применением облачной ЭЦП

84. Подписание электронных документов с использованием облачной ЭЦП доступно для физических и юридических лиц.

85. Для подписания электронных документов с применением облачной ЭЦП 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;

2) подписание электронных документов с использованием облачной ЭЦП;

3) просмотр перечня электронных документов, подписанных с применением облачной ЭЦП.

86. Подписание электронных документов с применением облачной ЭЦП юридическими лицами осуществляется в соответствии с матрицей полномочий.

87. Создание, внесение изменений и деактивация матрицы полномочий осуществляется Участником на Портале.

88. Для использования сервиса подписания электронных документов с применением облачной ЭЦП юридическими лицами Участнику требуется:

1) создать и оформить матрицу полномочий на Портале в отношении своей организации, а при необходимости, также в отношении своего Клиента, уполномоченного на подписание соответствующих документов;

2) направить сгенерированную ЦОИД ссылку на указанный в матрице полномочий электронный адрес или номер телефона первого руководителя организации. Участник имеет возможность также самостоятельно направить сгенерированную ЦОИД ссылку на утверждение сформированной матрицы полномочий первому руководителю организации Участника или Клиента по любому из доступных и самостоятельно выбранных каналов связи (электронная почта, мессенджеры, пуш-уведомления в мобильном приложение и т.д.);

3) обеспечить утверждение (заверение) матрицы полномочий первым руководителем организации путём её подписания облачной ЭЦП, выпущенной на его имя и соответствующей юридическому лицу, в отношении которого формируется данная матрица полномочий.

89. После утверждения (заверения) матрицы полномочий указанные в ней лица приобретают право подписи электронных документов от имени данной организации на основании предоставленных им полномочий первым руководителем организации, подписавшим матрицу полномочий своей облачной ЭЦП.

90. Участник несет ответственность за полноту, достоверность и актуальность матрицы полномочий, сформированной Участником как в отношении собственной организации, так и в отношении организации Клиента. Участник обязан обеспечить своевременное обновление матрицы полномочий, в случае изменения организационной структуры организации, смены уполномоченных лиц или прекращения их полномочий.

91. Сервис управления облачной ЭЦП используется Участником при дистанционном оказании услуг Клиенту либо при очном (личном) обращении Клиента.

92. 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. В случае подписания электронных документов от имени юридического лица дополнительно осуществляется проверка наличия Клиента в утверждённой матрице полномочий;

4) сервис управления облачной ЭЦП предлагает Клиенту подписать электронные документы путем ввода пароля для доступа к закрытым ключам облачной ЭЦП 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.

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

94. В случае отсутствия у Клиента действующих ключей облачной ЭЦП, Клиенту предоставляется заявление на выдачу регистрационного свидетельства согласно форме, опубликованной на Сайте по адресу: https://npck.kz/docs-uuc/, на основании которого осуществляется выпуск ключей облачной ЭЦП и подписание необходимых документов. Отсутствие согласия Клиента на выпуск регистрационного свидетельства является основанием для отказа в оказании услуги.

95. При успешном прохождении процедуры выпуска регистрационного свидетельства и подписания электронных 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 информации о ранее подписанных электронных документах.

96. При неуспешном прохождении процедуры выпуска регистрационного свидетельства Клиенту направляется информация с указанием соответствующей ошибки.

97. Хранение закрытых ключей Клиента осуществляется на защищенном ресурсе Общества в соответствии с требованиями внутренних нормативных документов Общества, определяющими политику применения регистрационных свидетельств и порядок работы Удостоверяющего центра Общества.

98. Срок хранения электронных документов, подписанных с применением облачной ЭЦП, составляет один год после истечения срока действия регистрационного свидетельства облачной ЭЦП.

99. Отзыв регистрационного свидетельства облачной ЭЦП осуществляется Клиентом путем подачи заявления на отзыв (аннулирование) регистрационного свидетельства согласно форме, опубликованной на Сайте по адресу: https://npck.kz/docs-uuc/.

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

100. 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, либо через выделенный канал связи посредством IP VPN или IPSEC.

Глава 6. Рассмотрение диспутных ситуаций

101. Рассмотрение диспутных ситуаций возможно исключительно по результатам оказания ЦОИД услуг двухфакторной и биометрической аутентификации. Рассмотрение диспутных ситуаций по результатам оказания ЦОИД услуги сопоставления фотоизображений не проводится.

Данный пункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

102. При несогласии Клиента с результатами проведенной аутентификации, Клиент обращается в Службу поддержки Участника.

103. 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.

104. Оператор проводит расследование по существу диспута, по результатам которого формирует заключение.

105. 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 решение по результатам проведенного разбирательства.

106. Оператор несет ответственность перед Участником только 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.

107. 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.

108. 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).

109. 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.

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

Глава 7. Система управления рисками

111. 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.

112. 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, блокирование сессии.

Данный подпункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

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

114. 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, неподлежащих восстановлению в основном центре обработки данных;

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

11) определение количественного показателя, отражающего долю времени корректного функционирования ЦОИД за определенный период, в порядке, установленном внутренним нормативным документом Оператора по определению доступности ЦОИД.

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;
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.

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/.

1. Термины и определения

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

1.2. биометрическая аутентификация личности - процесс сравнения и проверки соответствия биометрических данных Клиента, включающий liveness-проверку и сопоставление фотоизображения Клиента с фотоизображением из доступных источников;

Данный пункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

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;

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 аутентификации личности Клиента с предоставлением персональных данных из доступных источников и/или управления облачной ЭЦП, по запросу Участника;

Данный пункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

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

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 биометрической аутентификации личности по запросам Участника, передачу результатов (итогов) проведенной биометрической аутентификации личности;

Данный подпункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

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;
- сведения о дееспособности физического лица;
- сведения об исключении из национальных реестров;
- сведения о без вести пропавшем лице.

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.

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@npck.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 биометрической аутентификации личности (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;

Данный подпункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

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 проведение процедур и действий, указанных в настоящем Пользовательском соглашении с использованием средств автоматизации;

5.2.2. отказать в проведении биометрической аутентификации личности 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;

Данный подпункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

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» обязано:

5.4.1. по запросам Участника оказывать в отношении Клиента Услуги;

5.4.2. прекратить сбор и обработку персональных 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 обязан:

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.

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

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

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

5.5.7. не 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.

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.

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.

Приложение 3
к Правилам функционирования
Центра обмена идентификационными данными

Требования к биометрическим решениям

1. Биометрические решения используются ЦОИД для целей биометрической аутентификации личности.
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, длительностью не более 168 часов в течение календарного года.
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.
9. Биометрическое решение должно обеспечивать совместимость и корректное функционирование с актуальными версиями драйверов и системного программного обеспечения.

Требования к биометрическому решению liveness

10. 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 аутентификации личности осуществляется только с реальными живыми пользователями без использования средств подлога личности.
11. Биометрическое решение liveness должно предоставлять результат проведения проверки в виде «успешно/неуспешно».

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

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

14. 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.

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

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

17. 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).

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

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

20. 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

21. 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.

22. 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 21 настоящего раздела.

Данный пункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

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

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

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

26. Биометрическое решение сопоставления фотоизображений должно обеспечивать обработку не менее 100 запросов в минуту.

Данный пункт изменен решением Правления Общества от 30 января 2026 года (протокол № 2).

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

Приложение 4
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).

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 аутентификации 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), а также направляются потенциальному поставщику биометрического решения посредством официального письма.

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» _____

ЛИСТ ПОПРАВОК

1.	**Изменения и дополнения**	- утверждены решением Правления (протокол заседания от 30 января 2026 года № 2) - вступили в силу 30 января 2026 года