Об утверждении Правил проведения биометрической аутентификации финансовыми и платежными организациями, включая случаи обязательного использования и (или) наполнения биометрическими данными национальной системы биометрической аутентификации, полученными центром обмена идентификационными данными Национального Банка Республики Казахстан

Совместное постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 26 июня 2026 года № 99 и постановление Правления Национального Банка Республики Казахстан от 29 июня 2026 года № 72. Зарегистрировано в Министерстве юстиции Республики Казахстан 2 июля 2026 года № 39186

Примечание ИЗПИ!

Порядок введения в действие см. п. 4.

В соответствии с пунктом 6 статьи 48 Цифрового кодекса Республики Казахстан Правление Агентства Республики Казахстан по регулированию и развитию финансового рынка и Правление Национального Банка Республики Казахстан ПОСТАНОВЛЯЮТ:

1. Утвердить прилагаемые Правила проведения биометрической аутентификации финансовыми и платежными организациями, включая случаи обязательного использования и (или) наполнения биометрическими данными национальной системы биометрической аутентификации, полученными центром обмена идентификационными данными Национального Банка Республики Казахстан (далее – Правила).

2. Департаменту информационной и кибербезопасности Агентства Республики Казахстан по регулированию и развитию финансового рынка в установленном законодательством Республики Казахстан порядке обеспечить:

1) совместно с Юридическим департаментом Агентства Республики Казахстан по регулированию и развитию финансового рынка государственную регистрацию настоящего совместного постановления в Министерстве юстиции Республики Казахстан;

2) размещение настоящего совместного постановления на официальном интернет-ресурсе Агентства Республики Казахстан по регулированию и развитию финансового рынка после его официального опубликования;

3) в течение десяти рабочих дней после государственной регистрации настоящего совместного постановления представление в Юридический департамент Агентства Республики Казахстан по регулированию и развитию финансового рынка сведений об исполнении мероприятия, предусмотренного подпунктом 2) настоящего пункта.

3. Контроль за исполнением настоящего совместного постановления возложить на курирующих заместителя Председателя Агентства Республики Казахстан по регулированию и развитию финансового рынка и заместителя Председателя Национального Банка Республики Казахстан.

4. Настоящее постановление подлежит официальному опубликованию и вводится в действие с 12 июля 2026 года, за исключением подпункта 2) и части второй пункта 24, подпункта 3) пункта 25, пунктов 26 и 27 Правил, которые вводятся в действие с 19 июля 2026 года.

Председатель
Национального Банка
Республики Казахстан
_____ *Т. Сулейменов*

и.о. Председателя Агентства
Республики Казахстан
по регулированию и развитию
финансового рынка
_____ *О. Кизатов*

Утверждены
совместным постановлением
Председатель
Национального Банка
Республики Казахстан
от 29 июня 2026 года № 72
и и.о. Председателя Агентства
Республики Казахстан
по регулированию и развитию
финансового рынка
от 26 июня 2026 года № 99

Правила проведения биометрической аутентификации финансовыми и платежными организациями, включая случаи обязательного использования и (или) наполнения биометрическими данными национальной системы биометрической аутентификации, полученными центром обмена идентификационными данными Национального Банка Республики Казахстан

Глава 1. Общие положения

1. Правила проведения биометрической аутентификации финансовыми и платежными организациями, включая случаи обязательного использования и (или) наполнения биометрическими данными национальной системы биометрической аутентификации, полученными центром обмена идентификационными данными Национального Банка Республики Казахстан (далее – Правила), разработаны в соответствии с пунктом 6 статьи 48 Цифрового кодекса Республики Казахстан (далее – Цифровой кодекс) и определяют порядок проведения биометрической аутентификации финансовыми и платежными организациями, включая случаи обязательного

использования и (или) наполнения биометрическими данными национальной системы биометрической аутентификации, полученными центром обмена идентификационными данными Национального Банка Республики Казахстан (далее – ЦОИД).

2. В Правилах используются понятия, предусмотренные Цифровым кодексом, Законами Республики Казахстан "О банках и банковской деятельности в Республике Казахстан", "О платежах и платежных системах" (далее – Закон о платежах), "О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций", а также следующие понятия:

1) аутентифицируемый – физическое лицо или физическое лицо, действующее от имени юридического лица, в отношении которого проводится процесс биометрической аутентификации;

2) технология проверки достоверности изображения – совокупность программно-технических методов и алгоритмов, направленных на подтверждение присутствия живого физического лица при получении биометрических данных (изображения лица) путем анализа динамических, объемных, световых и иных характеристик изображения в режиме реального времени (Liveness Detection);

3) текущее изображение лица – изображение лица, полученное в ходе сессии биометрической аутентификации;

4) эталонное изображение лица – биометрические данные на основе изображения лица аутентифицируемого, содержащиеся в доступных источниках и (или) в базе биометрических данных Национальной системы биометрической аутентификации (далее – НСБА), доступ к которым предоставляется ЦОИД;

5) провайдер биометрической аутентификации – организация, осуществляющая получение достоверного текущего изображения лица аутентифицируемого и (или) сличение текущего и эталонного образца изображения лица аутентифицируемого, в том числе ЦОИД;

6) база данных верифицированных изображений провайдера биометрической аутентификации – база данных, создаваемая и хранимая провайдером биометрической аутентификации, содержащая верифицированные изображения лиц аутентифицируемых, прошедшие успешное сличение с эталонным образцом из доступных источников и (или) из базы биометрических данных НСБА посредством ЦОИД, или полученные посредством аппаратных устройств провайдера биометрической аутентификации при личном присутствии аутентифицируемого;

7) заказчик биометрической аутентификации – финансовая или платежная организация, в интересах которой осуществляется процесс биометрической аутентификации;

8) система сличения биометрических данных – цифровая система, осуществляющая сличение изображений;

9) система проверки биометрических данных – цифровая система, осуществляющая процедуру проверки достоверности изображения;

10) доступные источники – государственные базы данных, включающие эталонные данные физических лиц, эталонные изображения физических лиц, а также индивидуальные идентификационные номера (далее - ИИН) физических лиц и (или) бизнес-идентификационные номера (далее - БИН) юридических лиц;

11) лицо с инвалидностью – лицо, имеющее нарушение здоровья со стойким расстройством функций организма, обусловленное заболеваниями, увечьями (ранениями, травмами, контузиями), их последствиями, нарушениями, которое приводит к ограничению жизнедеятельности и необходимости его социальной защиты;

12) правила ЦОИД – внутренние правила национального центра по управлению национальной цифровой финансовой инфраструктурой, регламентирующие порядок предоставления услуг ЦОИД финансовым и платежным организациям для проведения процедур аутентификации.

3. Принципы использования и защиты биометрических данных:

1) сбор и хранение биометрических данных проводится в соответствии с главой 2 Правил;

2) биометрические данные защищаются от несанкционированного доступа и распространения;

3) документирование процессов сбора, хранения и уничтожения биометрических данных.

4. Заказчик биометрической аутентификации утверждает описание процесса биометрической аутентификации, сведения о системах проверки биометрических данных и сличения биометрических данных, а также критерии принятия решения об успешности биометрической аутентификации, выраженные количественными показателями.

5. Биометрическая аутентификация проводится по изображению лица аутентифицируемого.

Глава 2. Порядок биометрической аутентификации по изображению лица аутентифицируемого

6. Процесс биометрической аутентификации по изображению лица аутентифицируемого включает в себя следующие этапы:

1) получение достоверного текущего изображения лица аутентифицируемого;

2) получение эталонного изображения лица аутентифицируемого из доступных источников и (или) базы биометрических данных НСБА или изображения лица аутентифицируемого из базы данных верифицированных изображений провайдера биометрической аутентификации (далее – верифицированное изображение);

3) сличение текущего и эталонного изображения лица аутентифицируемого или текущего и верифицированного изображения лица аутентифицируемого (далее – сличение изображений).

7. Получение достоверного текущего изображения лица аутентифицируемого, а также ИИН осуществляется провайдером биометрической аутентификации посредством программного обеспечения на мобильном устройстве или компьютере. При этом в программном обеспечении реализуются как минимум следующие меры защиты: контроль собственной целостности, проверка на запуск в эмулируемой среде, защита от подмены встроенной камеры устройства или компьютера.

8. При получении достоверного текущего изображения лица аутентифицируемого, с целью предотвращения подмены текущего изображения лица аутентифицируемого, осуществляется процедура проверки достоверности изображения, включающая в себя направление аутентифицируемому не менее трех сигналов и (или) команд, направленных на создание визуальных изменений в кадре, с последующим анализом видеопотока на предмет выявления в нем несоответствий направленным сигналам и командам.

Выявленное несоответствие любому из направленных сигналов и (или) команд приводит к повторению процедуры проверки достоверности изображения. Три неуспешных повтора означают отрицательный результат проверки достоверности изображения.

9. По результатам проверки достоверности изображения независимо от успешности проверки в системе проверки биометрических данных формируется электронный документ, содержащий:

1) результат проверки достоверности текущего изображения лица;

2) ИИН;

3) перечень выбранных системой сигналов и (или) команд, набор соответствующих сигналам и (или) командам изображений с указанием использованных сигналов и (или) команд;

4) реквизиты заказчика биометрической аутентификации (наименование, БИН, адрес);

5) дату и время проведения проверки достоверности изображения;

6) реквизиты провайдера биометрической аутентификации (наименование, БИН, адрес).

10. Электронный документ по результатам проверки достоверности изображения удостоверяется электронной цифровой подписью провайдера биометрической аутентификации, осуществлявшего проверку, и хранится у заказчика биометрической аутентификации.

11. Сличение биометрических данных осуществляется путем сравнения изображения лица аутентифицируемого, полученного по результатам проверки

достоверности, с эталонным изображением лица или верифицированным изображением. Алгоритм формирования результата сличения определяется провайдером биометрической аутентификации.

12. По результатам сличения изображений, независимо от успешности проверки в системе сличения биометрических данных, формируется электронный документ, содержащий:

1) изображение лица аутентифицируемого, полученное по результатам проверки достоверности изображения;

2) ИИН;

3) результат сличения изображений;

4) реквизиты заказчика биометрической аутентификации (наименование, БИН, адрес);

5) дату и время проведения сличения изображений;

6) реквизиты провайдера биометрической аутентификации (наименование, БИН, адрес).

13. Электронный документ по результатам сличения биометрических данных:

1) удостоверяется электронной цифровой подписью провайдера биометрической аутентификации, осуществлявшего сличение изображений;

2) сохраняется в базе данных верифицированных изображений провайдера биометрической аутентификации, осуществлявшего сличение изображений, при наличии такой базы данных;

3) хранится у заказчика биометрической аутентификации.

14. С целью обеспечения конфиденциальности, а также предотвращения подмены передаваемых данных обеспечивается шифрование используемых в рамках процесса биометрической аутентификации каналов связи, выходящих за пределы цифровой инфраструктуры провайдера биометрической аутентификации или заказчика биометрической аутентификации.

15. На основании результатов проверки достоверности изображения, результатов сличения изображений, а также критериев, определенных в соответствии с пунктом 4 Правил, заказчиком биометрической аутентификации принимается решение об успешности биометрической аутентификации.

16. Хранение результатов проверки достоверности изображения, результатов сличения изображений и итогового решения об успешности биометрической аутентификации осуществляется заказчиком биометрической аутентификации в соответствии с требованиями Закона о платежах, а также требованиями к хранению документов, предъявляемыми к финансовой услуге, в рамках которой осуществлялась биометрическая аутентификация, с обеспечением возможности извлечения и предоставления указанных результатов по запросу в виде электронного документа, пригодного для визуального восприятия без применения процедур преобразования

данных (за исключением средств проверки электронной цифровой подписи) и содержащего сведения, необходимые для подтверждения подлинности и действительности электронной цифровой подписи.

Глава 3. Порядок проведения биометрической аутентификации посредством ЦОИД, а также случаи обязательного использования и (или) наполнения биометрическими данными НСБА, полученными ЦОИД

17. Подключение финансовых и платежных организаций к ЦОИД и получение указанными организациями сведений о результатах биометрической аутентификации посредством ЦОИД осуществляется в соответствии с Правилами ЦОИД. Правила ЦОИД размещаются на официальном интернет-ресурсе национального центра по управлению национальной цифровой финансовой инфраструктурой.

18. В случаях, предусмотренных пунктами 24, 29 и 30 Правил, финансовая и (или) платежная организация получает согласие аутентифицируемого на проведение биометрической аутентификации и согласие аутентифицируемого на сбор, обработку и представление, в том числе при необходимости третьим лицам, его персональных данных, подтвержденные посредством идентификационного средства.

Финансовая и (или) платежная организация проводит с аутентифицируемым с использованием имеющихся у аутентифицируемого устройств и (или) иных устройств организации сеанс видеоконференции либо использует технологию проверки достоверности изображения с применением ЦОИД или самостоятельно выбранных сторонних решений.

Содержательная часть сеанса видеоконференции (перечень контрольных вопросов при их наличии), а также перечень и объемы услуг, оказываемых финансовыми и (или) платежными организациями, устанавливаются финансовыми и (или) платежными организациями самостоятельно.

19. Финансовая и (или) платежная организация передает в ЦОИД ИИН аутентифицируемого либо БИН юридического лица, от имени которого действует аутентифицируемый, и изображение аутентифицируемого, полученное из сеанса видеоконференции либо с помощью технологии проверки достоверности изображения в процессе биометрической аутентификации.

20. В отношении аутентифицируемого, являющегося лицом с инвалидностью, финансовая и (или) платежная организация до начала процедуры биометрической аутентификации обеспечивает возможность выбора способа получения изображения лица путем проведения сеанса видеоконференции либо с использованием технологии проверки достоверности изображения.

21. ЦОИД посредством программного обеспечения определяет степень соответствия по биометрическим показателям изображения, полученного из сеанса видеоконференции либо при использовании технологии проверки достоверности

изображения, с эталонным изображением лица аутентифицируемого из доступных источников и (или) из базы данных НСБА. Видеозаписи обращений аутентифицируемых хранятся в финансовой и (или) платежной организации не менее пяти лет со дня прекращения деловых отношений с клиентом.

22. Допускается предоставление ЦОИД дополнительных сервисов финансовым и платежным организациям для проведения аутентификации, предусмотренных Правилами ЦОИД.

23. Изображения лиц аутентифицируемых, переданные финансовыми и (или) платежными организациями в ЦОИД из сеанса видеоконференции либо с помощью технологии проверки достоверности изображения, используются ЦОИД для целей биометрической аутентификации и (или) наполнения базы данных НСБА.

Изображения лиц аутентифицируемых, полученные ЦОИД от финансовых и (или) платежных организаций, и прошедшие проверку с результатами соответствия не менее 95% достоверности и не менее 95% соответствия эталонному изображению лица, используются для наполнения базы данных НСБА.

24. Банки, филиалы банков-нерезидентов Республики Казахстан и организации, осуществляющие отдельные виды банковских операций (далее – банки), при оказании электронных банковских услуг в целях идентификации личности аутентифицируемого используют услуги ЦОИД по предоставлению биометрической аутентификации при:

1) установлении деловых отношений с аутентифицируемым дистанционным способом путем открытия банковского счета;

2) создании банком, являющимся аккредитованным удостоверяющим центром Республики Казахстан, электронной цифровой подписи и выдаче сертификата электронной цифровой подписи аутентифицируемому, в случаях, предусмотренных частью второй настоящего пункта;

3) превышении суммы банковского займа размера, установленного Требованиями к условиям осуществления банковской деятельности, утвержденными постановлением Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 15 мая 2026 года № 91 "Об утверждении Требований к условиям осуществления банковской деятельности" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 38748);

4) первичной регистрации аутентифицируемого в мобильном приложении и (или) на интернет-ресурсе банка;

5) в иных случаях, в соответствии с Требованиями к Правилам внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения для банков второго уровня, филиалов банков-нерезидентов Республики Казахстан и Национального оператора почты, утвержденным постановлением Правления Агентства Республики Казахстан по

регулированию и развитию финансового рынка от 22 марта 2020 года № 18 "Об утверждении Требований к Правилам внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения для банков второго уровня, филиалов банков-нерезидентов Республики Казахстан и Национального оператора почты" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 20160).

В случае, если аутентифицируемый ранее не был аутентифицирован при личном присутствии в банке или с применением биометрической аутентификации посредством ЦОИД, то банком создание электронной цифровой подписи аутентифицируемого и выдача сертификата электронной цифровой подписи осуществляется при прохождении аутентифицируемым биометрической аутентификации посредством ЦОИД.

25. Банками передаются в ЦОИД согласия аутентифицируемого:

1) на сбор, обработку его персональных данных, в том числе биометрических данных;

2) на проведение биометрической аутентификации аутентифицируемого с использованием ЦОИД;

3) на создание ключей электронной цифровой подписи и выдачу сертификата электронной цифровой подписи, в том числе, полученное при личном присутствии аутентифицируемого в банке.

26. ЦОИД осуществляет сбор и регистрацию согласий аутентифицируемого, предусмотренных пунктом 25 Правил, с возможностью их отзыва аутентифицируемым в соответствии с законодательством Республики Казахстан.

27. Согласия аутентифицируемых, полученные посредством ЦОИД, а также результаты биометрической аутентификации ЦОИД подлежат хранению в ЦОИД не менее 5 (пяти) лет с момента их получения и обработки.

28. Банки обеспечивают хранение информации о согласиях аутентифицируемого, используемых при оказании электронных банковских услуг, изображения аутентифицируемого с использованием технологии проверки достоверности изображения, записи сеанса видеоконференции с аутентифицируемым, а также результаты биометрической аутентификации аутентифицируемого, не менее 5 (пяти) лет со дня прекращения деловых отношений с аутентифицируемым.

29. Микрофинансовыми организациями услуги ЦОИД по биометрической аутентификации аутентифицируемых используются при превышении размеров суммы микрокредита, установленных Требованиями к осуществлению микрофинансовой деятельности, утвержденными постановлением Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 15 мая 2026 года № 92

"Об утверждении Требований к осуществлению микрофинансовой деятельности" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 38746).

30. Платежными организациями, являющимися операторами систем электронных денег, обеспечивается биометрическая аутентификация владельцев электронных денег посредством ЦОИД в соответствии с требованиями части третьей пункта 5 статьи 42 Закона о платежах.