

**Республиканское государственное предприятие «Казахстанский центр  
межбанковских расчетов Национального Банка Республики  
Казахстан»**

Утверждены  
Приказом РГП «КЦМР НБ РК»  
от «19» 140-08 2019 года  
№ 47-н

**ПРАВИЛА  
функционирования системы  
«Центр обмена идентификационными данными»**

Рег. № 4602-48/31

г. Алматы

## Содержание

Глава 1. Общие положения.....	3
Глава 2. Договорные отношения Оператора Системы с Участниками .....	4
Глава 3. Условия участия в Системе .....	5
Глава 4. Функционирование Системы. ....	5
Глава 5. Порядок оказания Услуг в Системе.....	6
Глава 6. Тестовая среда Системы .....	8
Глава 7. Промышленная среда Системы.....	8
Глава 8. Порядок подключения в Систему Вендора .....	8
Глава 9. Оплата Услуг.....	9
Глава 10. Электронные сообщения в Системе .....	9
Глава 11. Меры информационной безопасности .....	9
Глава 12. Использование средств криптографической защиты информации.....	10
Глава 13. Система управления рисками.....	10

## Глава 1. Общие положения

1. Правила функционирования системы «Центр обмена идентификационными данными» (далее – Правила) разработаны в соответствии с законами Республики Казахстан от 26 июля 2016 года «О платежах и платежных системах» (далее - Закон о платежах и платежных системах), от 12 января 2007 года «О национальных реестрах идентификационных номеров» (далее - Закон о национальных реестрах идентификационных номеров), от 31 августа 1995 года «О банках и банковской деятельности в Республике Казахстан» (далее – Закон о банках), от 7 января 2003 года «Об электронном документе и электронной цифровой подписи» (далее - Закон об электронном документе и электронной цифровой подписи), от 28 августа 2009 года «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Закон о ПОДиФТ), от 21 мая 2013 года «О персональных данных и их защите» далее - Закон о персональных данных и их защите), Правилами оказания банками и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг, утвержденными постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 212, Требованиями к обеспечению информационной безопасности банков и организаций, осуществляющих отдельные виды банковских операций от 27 марта 2018 года №48 и определяют порядок организации и функционирования системы «Центр обмена идентификационными данными» (далее – Система) Республиканского государственного предприятия на праве хозяйственного ведения «Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан» (далее – КЦМР).

2. Система предназначена для определения степени соответствия по биометрическим показателям фотоизображения физического лица, полученного из сеанса видеоконференции с ним, или из документа, удостоверяющего личность и предоставления информации о результатах степени соответствия (далее – результаты степени соответствия), а также сведений, необходимых для идентификации физического лица в соответствии с требованиями законодательства Республики Казахстан о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

3. В Правилах используются понятия, предусмотренные законами Республики Казахстан о платежах и платежных системах, о банках, о национальных реестрах идентификационных номеров, об электронном документе и электронной цифровой подписи, о ПОДиФТ, о персональных данных и их защите, а также следующие понятия:

1) аутентификация – процесс проверки принадлежности субъекту прав доступа к информационным ресурсам системы или веб-сайта в соответствии с предъявленным им идентификатором;

2) аудиторский след – последовательная регистрация событий по обработке биометрических персональных данных в Системе, информация по которой сохраняется в Системе и Участниками Системы;

3) биометрическая идентификация – процедура установления личности Клиента с целью однозначного подтверждения его прав на получение услуг на основе его физиологических и биологических особенностей;

4) Вендор – компания–производитель биометрических процессов, поставляющая их под своей маркой;

5) биометрический процесс – технологическое решение Вендора по сопоставлению биометрических данных Клиента с биометрическими данными из доступных источников;

6) доступные источники – государственные базы данных, содержащие сведения, позволяющие идентифицировать личность Клиента;

7) идентификация – совокупность мероприятий по установлению определенных законодательством Республики Казахстан сведений о Клиенте и подтверждению достоверности этих сведений;

8) Клиент – физическое лицо, в отношении которого производится идентификация;

9) Оператор Системы – Оператор системы «Центр обмена идентификационными данными», которым выступает КЦМР;

10) Участник – банк второго уровня, организация, осуществляющая отдельные виды банковских операций, небанковские организации;

11) Услуга – предоставление Участнику сведений о степени соответствия предоставленных Участником биометрических персональных данных Клиента биометрическим персональным данным, содержащимся в доступных источниках, а также представление персональных данных Клиента, которые предназначены для выполнения требований Закона о ПОДиФТ;

12) модуль матчинга – модуль Системы, предназначенный для получения степени соответствия фотоизображения Клиента, полученного от Участника, с фотоизображением, полученным из доступных источников;

13) Интернет-ресурс – официальный интернет портал Оператора Системы [www.kisc.kz](http://www.kisc.kz);

14) небанковская организация – юридическое лицо, состоящее в реестре Национального Банка Республики Казахстан в качестве платежной организации, либо получившее лицензию в Агентстве Республики Казахстан по регулированию и развитию финансового рынка и/или осуществляющее деятельность по обязательному гарантированию депозитов, привлечению пенсионных взносов и пенсионных выплат, а также субъекты рынка, осуществляющие предпринимательскую деятельность в сфере электронной коммерции;

15) IPSec-туннель – набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет;

## **Глава 2. Договорные отношения Оператора Системы с Участниками**

4. Взаимодействие Участников с Оператором Системы осуществляется на основании договора о предоставлении Услуг в Системе, заключаемого между Участниками и Оператором Системы (далее – Договор).

5. Удален

6. Договор содержит условия, предусмотренные подзаконными актами Республики Казахстан, регулирующими порядок предоставления дистанционных финансовых услуг или услуг в сфере электронной коммерции.

7. Форма Договора, утверждается Оператором Системы, с учетом требований настоящей главы Правил.

## **Глава 3. Условия участия в Системе**

8. Статус Участника Системы приобретается после подписания Заявления/Соглашения о безусловном присоединении к Договору.

С целью ознакомления Участников Системы с положениями Договора, Договор размещается на Интернет-ресурсе.

8-1. Участники, являющиеся субъектами финансового мониторинга, при установлении дистанционных деловых отношений с Клиентами, а также при совершении операций в рамках дистанционно установленных отношений, руководствуются Законом о ПОДиФТ, Правилами и правилами внутреннего контроля Участников.

9. Предоставление Услуг Участнику в Системе приостанавливается в следующих случаях:

- 1) неисполнение или ненадлежащее исполнение Участником условий Договора;
- 2) нарушение Участником требований Правил;
- 3) невозможность и/или отказ от исполнения Участником обязательств по идентификации, предусмотренные правовыми актами Республики Казахстан, регулирующими порядок предоставления дистанционных финансовых услуг;
- 4) на основании полученного указания, уполномоченного на то государственного органа, должностного лица или судебного исполнителя;
- 5) использование Системы в не коммерческих целях;
- 6) передача данных, полученных через Систему, третьим лицам.

10. Приостановление предоставления Услуг Участнику в Системе не лишает его статуса Участника Системы.

11. Предоставление Услуг Участнику в Системе прекращается в следующих случаях:

- 1) расторжение Договора либо признание утратившими силу условий об участии в Системе, содержащихся в Договоре;
- 2) на основании полученного уведомления уполномоченного на то государственного органа, должностного лица или судебного исполнителя;
- 3) в случае утраты права на оказание платежных услуг и/или финансовых услуг.

12. При приостановлении либо прекращении предоставления Услуг Участнику в Системе Оператор Системы в соответствии с условиями Договора уведомляет Участника о дате и причинах приостановления, либо прекращения предоставления Услуг в Системе.

#### **Глава 4. Функционирование Системы**

13. Информационный обмен в Системе осуществляется как в синхронном, так и в асинхронном режиме. Обмен данными Участника с Системой проходит через портал Оператора Системы в электронном формате с организацией защищенного канала связи.

14. Для мониторинга функционирования Системы портал Оператора Системы оповещает сотрудников Оператора Системы обо всех неуспешных попытках сетевого доступа к сервису с указанием времени обращения, IP адреса, имени Клиента (DN) при аутентификации, кода ошибки.

15. Сообщения подразделяются на два типа: «запрос» и «ответ». Инициализирующим информационный обмен сообщением является сообщение типа «запрос» от Участника (далее – запрос). На сообщение типа «запрос» Система должна выслать Участнику сообщение типа «ответ» (далее - ответ).

16. Система принимает следующие параметры запросов:

- 1) запрос на получение результатов степени соответствия, который содержит: ИИН Клиента;

фотоизображение Клиента, полученное из сеанса видеоконференции, или с применением специализированного приложения, реализующего технологию выявления движения клиента, интервьюируемого в процессе дистанционной идентификации, или из документа, удостоверяющего личность;

2) запрос на получение персональных данных Клиента, содержащий подписанное ЭЦП Участника подтверждение наличия согласия Клиента на сбор и обработку его персональных данных третьими лицами.

17. Система функционирует 24 (двадцать четыре) часа в сутки, за исключением времени проведения плановых профилактических работ и работ, осуществляемых АО «НИТ» (организация, обеспечивающая сопровождение и системно-техническое обслуживание национального шлюза Республики Казахстан).

18. Система функционирует на основе следующих принципов:

1) взаимодействие Участника и Системы 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 в соответствии с параметрами указанными в Приложении к Правилам;

2) в запросе Участника могут быть указаны данные только одного Клиента;

3) отсутствие приоритетов обработки запросов;

4) прием и обработка запросов в режиме реального времени;

5) предоставление персональных данных Клиента Участнику при результате степени соответствия 85% и выше;

6) предоставление банкам второго уровня, организациям, осуществляющим отдельные виды банковских операций или небанковским организациям, за исключением субъектов рынка, осуществляющих предпринимательскую деятельность в сфере электронной коммерции персональных данных Клиента при получении от Участника подтверждения наличия согласия Клиента на сбор и обработку его персональных данных третьими лицами;

7) проведение плановых профилактических работ только в выходные дни (дни отдыха) или ночное время (по времени г. Нур-Султан), общей длительностью не более 7 суток в год, с предварительным предупреждением Участников не менее, чем за двое суток до момента начала профилактических работ.

## **Глава 5. Порядок оказания Услуг в Системе**

19. Участник с целью проведения идентификации Клиента с использованием средств биометрической идентификации выбирает в Системе необходимый биометрический процесс Вендора и направляет в Систему запрос в соответствии с форматами, утвержденными Оператором Системы. Форматы запросов размещаются на Интернет-ресурсе.

20. Требования к фотоизображениям, принимаемым Системой:

размер изображения определяемого лица составляет от 160X240 до 1024x1024 пикселей;

на фотоизображении должно быть одно лицо;

размер входного изображения должен быть не менее 240X240 пикселей и не более 4096x4096 пикселей;

изображение должно быть без эффекта красных глаз или бликов на лице;

максимально прямой вид лица (недопустимо под углом, сверху или сбоку);

на изображении не должны быть предметы, скрывающие лицо (корректирующие зрение очки, солнцезащитные очки, капюшон, головной убор, маски и т.п.);

изображение человека выше уровня груди.

Фотоизображения, не соответствующие вышеуказанным параметрам, могут быть отклонены Системой.

21. Система по ИИН Клиента направляет запрос в доступные источники на получение его фотоизображения.

22. Модуль матчинга определяет степень соответствия по биометрическим показателям фотоизображения Клиента, полученного от Участника, и фотоизображения Клиента из доступных источников.

23. Система не представляет Участнику персональные данные Клиента при результате степени соответствия ниже 85%.

23-1. В случае неуспешной биометрической идентификации Клиента более двух раз попыток Участник проводит процедуру дополнительной проверки Клиента в офлайн режиме либо отказывает Клиенту в предоставлении услуг.

24. Участник направляет в Систему запрос на получение персональных данных Клиента с соблюдением условий, установленных пунктом 27 Правил.

25. После обработки запроса Участника на получение персональных данных Клиента, Система обращается в доступные источники для получения персональных данных Клиента. Доступные источники предоставляют результат в Систему.

26. Система представляет Участнику персональные данные Клиента, полученные из доступных источников.

27. Персональные данные Клиента представляются Участнику при соблюдении следующих условий (в совокупности):

- участник является банком второго уровня, организацией, осуществляющей отдельные виды банковских операций или небанковской организацией, за исключением субъектов рынка, осуществляющих предпринимательскую деятельность в сфере электронной коммерции;
- наличие запроса Участника на получение персональных данных Клиента;
- наличие подписанного ЭЦП подтверждения Участника о наличии согласия Клиента на сбор и обработку его персональных данных третьими лицами;
- результат степени соответствия фотоизображения Клиента не ниже 85%;
- принятие Участником с использованием результатов степени соответствия положительного решения об успешности идентификации Клиента.

28. Система обеспечивает хранение результатов степени соответствия, фотоизображения Клиентов, а также подтверждения о наличии согласия Клиента на сбор и обработку персональных данных Клиента третьими лицами, полученных от Участника, в течение пяти лет с даты их получения. Все данные, полученные от Участника и обработанные Системой, должны оставлять аудиторский след.

28-1. Участники, являющиеся субъектами финансового мониторинга, обеспечивают хранение результатов степени соответствия и видеозаписи обращений клиентов, полученные в ходе видеоконференций либо с помощью технологии выявления движения интервьюируемого в процессе дистанционной идентификации, согласно требованиям действующего Закона о ПОДиФТ и Правил.

28-2. Решение о хранении видеозаписи обращений клиентов согласно требованиям действующих Правил принимается участником, не являющимся субъектом финансового мониторинга, самостоятельно.

29. Система обеспечивает целостность и неизменность сведений, получаемых от Участников и из доступных источников.

29-1. Собранные в ходе дистанционной идентификации посредством сеанса

видеоконференции фотоизображении должны проверяться Участником на предмет правильности решения об успешной идентификации согласно пункту 20 Правил.

29-2. В случае, если качество видеоизображения или звука не позволяют успешно провести идентификацию, и наблюдается вероятность возникновения рисков, приводящих к ложным результатам проверки, либо имеются сомнения в легитимности документа, удостоверяющего личность Клиента, Участник предпринимает меры для устранения препятствий либо завершает сеанс видеоконференции с указанием причин.

## **Глава 6. Тестовая среда Системы**

30. Тестовая среда Системы предназначена для выполнения следующих задач:

- тестирование уполномоченными сотрудниками Оператора Системы биометрических решений Вендоров, не имеющих доступ в промышленную среду Системы, или новых версий биометрических процессов, разработанных Вендором;
- тестирование Участником готовности Системы к взаимодействию и интеграции с информационными системами Участников.

Использование тестовой среды является обязательным условием при выполнении регламентных процедур подключения биометрических процессов Вендоров.

31. Тестовая среда Системы изолирована от промышленной среды Системы, и содержит только тестовые данные.

## **Глава 7. Промышленная среда Системы**

32. Промышленная среда Системы предназначена для промышленной эксплуатации Системы для оказания Услуг Участникам.

33. Промышленная среда Системы изолирована от тестовой среды Системы, доступна по выделенным каналам связи или с учетом требований пункта 18 Правил, недоступна без применения криптографической защиты на базе регистрационных свидетельств, и содержит реальные данные.

## **Глава 8. Порядок подключения в Систему Вендора**

34. Вендор с целью включения своего биометрического процесса в Систему направляет в произвольной форме письменное Заявление о включении в Систему

35. Ответственный сотрудник Оператора Системы после рассмотрения Заявления о включении в Систему производит анализ технических характеристик биометрического процесса Вендора, и включает его в тестовую среду Системы. Тестирование представляет собой выполнение Оператором Системы и Участником эталонных запросов к эмулятору доступных источников, расположенному в тестовой среде Системы, и по итогам которого составляется внутренний акт тестирования.

36. Надлежащие технические характеристики Вендора и успешное прохождение тестирования биометрического процесса являются обязательным условием включения биометрического процесса Вендора в промышленную среду Системы.

37. Вендор подписывает Соглашение о безусловном присоединении к Договору (присоединения) о предоставлении услуг в информационной системе «ЦОИД» по форме, утвержденной Оператором Системы.

38. Оператор Системы с целью ознакомления Вендоров с положениями Соглашения о безусловном присоединении к Договору (присоединения) о

предоставлении услуг в информационной системе «ЦОИД» размещает его на Интернет-ресурсе.

39. После заключения Соглашения Оператор Системы представляет доступ Участнику к биометрическому процессу Вендора в промышленной среде Системы.

39-1. Обновление биометрического процесса Вендора, включенного в промышленную среду Системы, осуществляется при соблюдении следующих условий: наличие официального письма от Вендора, с указанием причин обновления; обязательное тестирование обновленного биометрического процесса в тестовой среде Системы.

## **Глава 9. Оплата Услуг**

40. Стоимость Услуг (тарифы), оказываемых Оператором Системы Участнику, устанавливается Национальным Банком Республики Казахстан по согласованию с Оператором Системы.

41. Оператор Системы взимает плату за Услуги, оказываемые Участникам в Системе. Условия и порядок взимания платы за Услуги Оператора Системы определяются Договором.

## **Глава 10. Электронные сообщения в Системе**

42. Передача и прием сообщений в Системе осуществляется электронным способом с соблюдением мер по информационной безопасности. При этом Участник обменивается электронными сообщениями с Оператором Системы в форматах, утвержденных КЦМР и размещенных на Интернет-ресурсе.

43. Оператор Системы разрабатывает форматы электронных сообщений, меры информационной безопасности Системы и контролирует их соблюдение.

44. Система обеспечивает хранение электронных сообщений в течение пяти лет с даты их получения.

## **Глава 11. Меры информационной безопасности**

45. Оператор Системы устанавливает меры информационной безопасности для работы в Системе, определяет сертифицированные средства криптографической защиты информации и аккредитованный удостоверяющий центр, обеспечивающий выдачу регистрационных свидетельств, и порядок их использования.

46. Порядок аутентификации при доступе в Систему включает необходимость использования аутентификации с обоюдной проверкой каждой из сторон, основанный на криптографических алгоритмах.

47. Конфиденциальность передаваемых данных обеспечивается шифрованием при их обмене.

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

48-1. Участниками используются дополнительные факторы, установленные Участником для идентификации Клиента.

48-2. Участники принимают необходимые меры по обеспечению информационной

безопасности и защите персональных данных Клиентов в соответствии с Законом о персональных данных и их защите, а также правовыми актами, регламентирующими требования к обеспечению информационной безопасности Участников.

## **Глава 12. Использование средств криптографической защиты информации**

49. Для получения Услуг, при авторизации Участника в Системе, 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.

50. Основанием для получения и использования ключевой информации и средств криптографической защиты информации является присоединение Участника к Договору о предоставлении услуг удостоверяющего центра, расположенному по адресу <http://www.kisc.kz/ca/doc/dogovorcaps.rtf>, которое предусмотрено Договором о предоставлении услуг в Системе.

51. При авторизации Участника в Системе в поле «Username» указывается системное имя (идентификатор пользователя), которое должно быть тем же самым, что и указанное в сертификате, полученном в удостоверяющем центре.

## **Глава 13. Система управления рисками**

52. Управление рисками осуществляется в соответствии с Правилами управления рисками в КЦМР.

53. Для управления рисками технологий, связанными с подключением биометрических процессов Вендоров, подключения биометрических процессов Вендоров осуществляются при условиях:

обеспечения Вендором надлежащих технических характеристик биометрического процесса;

успешного прохождения тестирования биометрического процесса Вендора.

54. Для управления правовыми рисками и рисками информационной безопасности, связанными со сбором и обработкой персональных данных, Оператором Системы предпринимаются следующие меры:

1) персональные данные Клиента из доступных источников используются Оператором Системы только для реализации требований Правил;

2) Оператор Системы получает персональные данные Клиента из доступных источников при получении от Участника подтверждения наличия согласия Клиента на сбор и обработку персональных данных Клиента третьими лицами, а также при условии степени соответствия, определенной Правилами;

3) Оператором Системы предпринимаются организационные и технические меры по защите персональных данных в соответствии с требованиями действующего законодательства, а также требованиями международных и государственных стандартов в области информационной безопасности.

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

проведение Оператором контроля за функционированием Системы;

постоянный мониторинг и поддержание Оператором непрерывной работы системы;

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

обеспечение выполнения необходимых разработок и доработок по совершенствованию и устранению дефектов Системы;

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

управление инцидентами и проблемами, включая своевременное обнаружение, регистрацию, реагирование и анализ инцидентов;

поддержание в актуальном состоянии плана восстановления деятельности Системы с учетом возможных сценариев остановки работы системы и тестирование Оператором данного плана;

обеспечение работоспособности резервного центра Системы;

перевод работы Системы с основного центра на резервный центр при наличии сбоев или простоев в работе программно-технического комплекса системы, не подлежащих восстановлению в основном центре;

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

Приложение к Правилам функционирования системы  
«Центр обмена идентификационными данными»

Требования к параметрам IPSec-туннеля через Интернет			
	Параметр	Значение	Пояснение
Фаза 1	Authentication Method	Certificate (Сертификат)	Тип метода аутентификации: На основании запроса сгенерированный сертификат УЦ КЦМР.
	Diffie-Hellman Group	group 21	Определяет силу ключа, используемого в процессе обмена ключами. Чем выше группа, тем безопаснее ключ.
	Encryption Algorithm	AES 256 Preferred	AES (англ. Advanced Encryption Standard) — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит)
	Hashing Algorithm	SHA-256	Алгоритм SHA256 – это безопасный алгоритм хеширования, применяющийся для преобразования данных в зашифрованные строки длиной 256 бит.
	SA Lifetime * (for renegotiation) with no kbytes rekeying	86400 секунд	SA (Security Association), что можно приближённо перевести как "связь или ассоциация безопасности" - это термин IPSec для обозначения соединения.

Фаза 2	Encapsulation * (ESP or AH)	ESP	Encapsulating Security Payload. Индекс параметров безопасности (аналогичен соответствующему полю AH). Значение этого поля вместе с IP-адресом получателя и протоколом безопасности (ESP-протокол), однозначно определяет защищённое виртуальное соединение (SA) для данного пакета.
	Encryption Algorithm *	AES 256 Preferred	См. Выше
	Authentication Algorithm *	SHA-256	См. Выше
	Diffie-Hellman Group *	group 21	См. Выше

