



**Акционерное общество «Национальная платежная корпорация
Национального банка Республики Казахстан»**

Уровень доступа: Общий

Утверждены
решением Правления АО «НПК»
от «21» 08 2026 года
(протокол № 15)

Дата вступления в силу с
«21» 08 2026 г.

Регламент по взаимодействию с Платформой цифрового тенге

Рег. № 45

г. Алматы

Содержание

Глава 1. Общие положения.....	4
Глава 2. Условия и порядок подключения к Платформе	6
Глава 3. Тестовая среда Платформы	8
Глава 4. Промышленная среда Платформы.....	9
Глава 5. Способы взаимодействия участников с Платформой	10
Глава 6. Электронные сообщения на Платформе	11
Глава 7. Технические работы и недоступность Платформы	11
Глава 8. Порядок обращения участников к Национальному центру.....	12
Глава 9. Требования к проектированию информационных систем участника.....	14
Глава 10. Меры информационной безопасности	15
Глава 11. Порядок урегулирования спорных ситуаций по операциям.....	16
Приложение.....	18

Тасганова Г.Т. 

Глава 1. Общие положения

1. Настоящий Регламент по взаимодействию с Платформой цифрового тенге (далее – Регламент) разработан в соответствии с Законом Республики Казахстан «О платежах и платежных системах» (далее – Закон о платежах и платежных системах) и Правилами выпуска, обращения и погашения цифровых тенге, утверждёнными постановлением Правления Национального Банка Республики Казахстан от 29 апреля 2026 года № 42 (далее — Правила).

2. Регламент входит в состав технической документации акционерного общества «Национальная платежная корпорация Национального Банка Республики Казахстан» (далее - Национальный центр) и является неотъемлемой частью типовой формы договора о предоставлении услуг на Платформе цифрового тенге, утвержденной решением Правления акционерного общества «Национальная платежная корпорация Национального Банка Республики Казахстан» от 30 июня 2026 года (протокол № 8) (далее – Договор о предоставлении услуг). Присоединяясь к Договору о предоставлении услуг, участник принимает на себя обязательство соблюдать требования настоящего Регламента в полном объёме.

3. Целью Регламента является предоставление участникам дополнительных сведений к положениям Правил в части:

- 1) порядка подключения к Платформе цифрового тенге (далее — Платформа);
- 2) процессов операционного взаимодействия при работе с Платформой;
- 3) режима работы Платформы и порядка взаимодействия при проведении технических работ и при недоступности Платформы;
- 4) требований к проектированию информационных систем участника;
- 5) порядка урегулирования спорных ситуаций по операциям на Платформе.

4. Регламент предназначен для специалистов-участников, осуществляющих или планирующих подключение к Платформе, включая подразделения информационных технологий, команды разработки, участвующие в проекте интеграции с Платформой, подразделения информационной безопасности, подразделения операционного сопровождения и подразделения, ответственные за урегулирование спорных ситуаций.

5. Для взаимодействия участников с Платформой Национальный центр разрабатывает справочные материалы и документацию (далее — Документация), включающую, помимо прочего:

- 1) API-спецификацию для работы с Платформой (OpenAPI-спецификация, текстовое описание, перечень кодов ошибок);
- 2) документацию к криптосервису (инструкция по развёртыванию, OpenAPI-спецификация);
- 3) инструкцию по формированию и проверке транспортной ЭЦП;
- 4) Рекомендации к пользовательским интерфейсам.

Документация направляется участнику Национальным центром по обращению участника после заключения договоров, предусмотренных пунктом 8



Регламента. Изменения Документации доводятся до участников не менее чем за 30 (тридцать) календарных дней до даты введения их в действие.

6. В Регламенте используются понятия, предусмотренные Законом о платежах и платежных системах, Правилами и Договором о предоставлении услуг, а также следующие понятия:

1) график работы Платформы — график взаимодействия между Национальным Банком Республики Казахстан (далее — НБРК), Национальным центром и участниками платформы цифрового тенге, утверждённый НБРК. График работы Платформы опубликован на интернет-ресурсе НБРК;

2) клиентская подпись — цифровая подпись, формируемая с использованием криптографических ключей пользователя Платформы для подтверждения операций по его цифровому счёту;

3) криптосервис — программное средство участника, обеспечивающее формирование клиентской подписи и работу с криптографическими ключами;

4) программно-аппаратный модуль — специализированное оборудование, предназначенное для криптографической обработки данных, работы с криптографическими ключами Пользователей и их надежного хранения.

5) средства криптографической защиты информации — это специальные программы, устройства или системы, которые преобразуют данные с помощью математических алгоритмов для обеспечения их безопасности.

6) транспортная электронная цифровая подпись (транспортная ЭЦП) — электронная цифровая подпись, которой участник подписывает запросы к Платформе, формируемая с использованием регистрационного свидетельства, выпущенного Удостоверяющим центром Национального центра;

7) учётные данные участника — идентификационные данные (api-key, bankName), предоставляемые Национальным центром для вызова API Платформы;

8) Удостоверяющий центр Национального центра (УЦ НПК) — подразделение Национального центра, выполняющее функции удостоверяющего центра по созданию, выдаче и управлению регистрационными свидетельствами, используемыми при выполнении операций на Платформе;

9) эталонное тестирование — тестирование информационных систем участника на соответствие требованиям Документации, включающее выполнение эталонных запросов к тестовой среде и демонстрацию пользовательских интерфейсов участника, по результатам которого принимается решение о допуске участника к промышленной среде Платформы;

10) Service Desk — система регистрации и обработки обращений участников, размещённая по адресу <https://help.npsk.kz/>;

11) API — это набор правил, инструкций и готовых команд, которые позволяют разным программам общаться и передавать друг другу данные.

12) 7. Вопросы выпуска, обращения и погашения цифровых тенге, открытия, ведения и закрытия цифровых счетов пользователей Платформы, а также меры информационной безопасности регулируются Правилами. Порядок оплаты услуг

Национального центра, ответственность сторон и меры, применяемые к участнику за нарушение требований, регулируются договорами, предусмотренными в пункте 8 Регламента.

Глава 2. Условия и порядок подключения к Платформе

8. Для получения статуса участника и доступа к Платформе банки, организации, осуществляющие отдельные виды банковских операций, АО «Центральный депозитарий ценных бумаг», Комитет государственных доходов Министерства финансов Республики Казахстан, иные поставщики платёжных услуг и юридические лица, определённые НБРК, заключают:

- 1) с Оператором договор участия на Платформе (далее — Договор участия);
- 2) с Национальным центром договор о предоставлении услуг.

Требования, которым должен соответствовать участник для заключения Договора участия, установлены пунктом 68 Правил, в том числе обеспечение технической поддержки по работе на Платформе, доступной в круглосуточном режиме.

9. Требования к технологическому взаимодействию информационных систем участников с Платформой, API-спецификация, процедуры аутентификации и порядок использования криптографических ключей определяются Документацией.

10. При заключении с участником Договора участия Оператор уведомляет Национальный центр об этом в течение 3 (трёх) рабочих дней после его заключения и предоставляет Национальному центру информацию об индивидуальном идентификационном коде цифрового счёта участника.

11. Заключение Договора о предоставлении услуг с Национальным центром осуществляется путем присоединения на основании заявления участника о присоединении к типовой форме данного договора с представлением пакета документов, предусмотренных в данном заявлении. Актуальная редакция договора о предоставлении услуг размещена на интернет-ресурсе Национального центра (<https://npck.kz/>).

12. Датой заключения Договора о предоставлении услуг является дата, указанная в отметке Национального центра о получении Заявления. От этой даты исчисляются сроки, установленные настоящей Главой.

13. Участник получает регистрационные свидетельства, необходимые для работы в тестовой среде Платформы, в порядке, предусмотренном в Главе 3 Регламента.

14. В течение 5 (пяти) рабочих дней с даты заключения Договора о предоставлении услуг Национальный центр направляет участнику учётные данные участника для доступа к тестовой среде Платформы (api-key, bankName), а при отсутствии у участника действующей учётной записи в системе Service Desk — также учётные записи для доступа к ней. По обращению участника Национальный центр направляет ему Документацию.

15. Телекоммуникационные каналы доступа информационных систем участника к Платформе обеспечиваются участником самостоятельно и за его счёт. Взаимодействие с промышленной средой Платформы осуществляется по двум защищенным каналам связи (основному и резервному), предоставляемым разными поставщиками услуг связи, с использованием технологии VPN. При отсутствии выделенного канала связи с Национальным центром участник обеспечивает его организацию.

16. Участник выполняет подключение к тестовой среде Платформы в соответствии с Главой 3 Регламента, самостоятельно выполняет доработку своих информационных систем, включая пользовательские интерфейсы для выполнения операций на Платформе, в соответствии с Документацией и проводит интеграционное тестирование разработанных функций во взаимодействии с Платформой.

17. Участник и Национальный центр совместно определяют дату проведения эталонного тестирования. Эталонное тестирование включает выполнение участником эталонных запросов к тестовой среде Платформы в соответствии с Документацией, а также демонстрацию разработанных пользовательских интерфейсов для подтверждения готовности систем участника к взаимодействию с Платформой.

18. Национальный центр проверяет успешность выполнения участником тестовых операций со стороны Платформы и фиксирует результаты эталонного тестирования. При наличии невыполненных эталонных запросов участнику направляются рекомендации для доработки информационных систем и определяется дата следующего тестирования.

19. После успешного прохождения эталонного тестирования Национальным центром и участником подписываются в двух экземплярах Протокол проведения тестирования на соответствие требованиям Документации (форма Протокола приведена в приложении к Регламенту). После подписания Протокола Национальный центр предоставляет участнику учётные данные для работы в промышленной среде Платформы.

20. Участник выполняет подготовительные мероприятия, предусмотренные в Главе 4 Регламента, и согласовывает с Национальным центром дату начала работы в промышленной среде Платформы посредством направления обращения в систему Service Desk с указанием темы «Дата выхода в прод» и предполагаемой даты.

21. К дате, указанной в обращении участника, Национальный центр обеспечивает открытие цифрового счета на Платформе и предоставляет участнику доступ к промышленной среде Платформы. С указанной даты участник вправе совершать операции на Платформе в промышленном режиме.

22. Национальный центр вправе отказать в подключении участника к Платформе при выявлении несоответствия участника требованиям Документации. Об отказе участник уведомляется с указанием выявленных несоответствий, после



их устранения участник вправе повторно инициировать эталонное тестирование в порядке, предусмотренном пунктами 17–19 Регламента.

Глава 3. Тестовая среда Платформы

23. Тестовая среда Платформы предоставляется Национальным центром и предназначена для выполнения следующих задач:

1) тестирование процессов формирования и направления заявок на выпуск и погашение цифровых тенге;

2) тестирование видов операций с цифровыми тенге, предусмотренных Правилами;

3) тестирование электронных информационных и платёжных сообщений (запросов), включая проверку корректности процессов формирования и проверки ЭЦП, запросы на получение выписки;

4) тестирование операций по цифровым счетам, включая открытие и закрытие цифровых счетов, приостановление расходных операций, наложение ареста;

5) тестирование функциональности смарт-контрактов и программирования цифровых тенге, а также иных функциональных возможностей Платформы в соответствии с Правилами и API-спецификацией Национального центра.

24. Тестовая среда Платформы изолирована от промышленной среды Платформы и содержит только тестовые данные.

25. Для получения регистрационных свидетельств, необходимых для работы в тестовой среде Платформы, участник запрашивает у Национального центра значение системного имени и направляет заявку на адрес электронной почты SupportCA@npck.kz с указанием полученного значения системного имени. Форма заявки предоставляется в ответном письме либо контактным лицом Национального центра, курирующим подключение участника к Платформе. Выпуск регистрационных свидетельств осуществляется УЦ НПК в порядке, установленном УЦ НПК.

26. Участник выполняет мероприятия по сетевому подключению к тестовой среде с использованием выделенного сетевого канала Национального центра, а при отсутствии такого канала выполняет мероприятия по его организации.

27. Запросы для взаимодействия с тестовой средой направляются на URL, предоставляемый Национальным центром при подключении участника.

28. Каждый запрос участника к тестовой среде Платформы подписывается транспортной ЭЦП. На основании временных ключей участник выпускает ключ сроком действия 1 (один) год в соответствии с инструкцией, приведённой в Документации, и использует его в сервисе формирования транспортной подписи, который организует на своей стороне. Для тестовой среды Национальный центр по запросу участника предоставляет пример реализации сервиса формирования транспортной подписи и документацию по формированию и проверке подписи с использованием указанного сервиса. Требования к формированию транспортной подписи определяются Документацией.



29. Для проверки подключения к тестовой среде участник выполняет контрольный запрос получения баланса своего цифрового счёта методом, предусмотренным API-спецификацией. Успешное получение ответа на контрольный запрос свидетельствует о корректности сетевого подключения, аутентификации и формирования транспортной подписи.

30. Участник обеспечивает развёртывание и функционирование на своей стороне криптосервиса, предназначенного для генерации криптографических ключей и формирования клиентской подписи при выполнении операций на Платформе. В тестовой среде допускается имитация криптосервисом взаимодействия с криптографическим программно-аппаратным модулем. В промышленной среде применяется криптографический программно-аппаратный модуль, соответствующий требованиям пункта 38 Регламента.

31. Показатели режима работы, установленные Регламентом для Платформы, на тестовую среду не распространяются. Обращения по вопросам работы тестовой среды направляются в порядке, предусмотренном Главой 8 Регламента.

Глава 4. Промышленная среда Платформы

32. Промышленная среда Платформы предназначена для промышленной эксплуатации Платформы в рамках оказания услуг участникам. Промышленная среда изолирована от тестовой среды, содержит реальные данные и доступна только по выделенным каналам связи при условии использования регистрационных свидетельств УЦ НПК, выданных для работы на Платформе ЦТ.

33. Для получения регистрационных свидетельств, необходимых для работы в промышленной среде Платформы, участник присоединяется к Договору о предоставлении услуг Удостоверяющего центра, размещённому на интернет-ресурсе Национального центра.

33. Участник запрашивает у Национального центра значение системного имени ключа в формате CBDC.XXXX.XXXX.

35. После получения системного имени, участник направляет предварительно заполненное приложение 1 к Договору о предоставлении услуг Удостоверяющего центра на адрес электронной почты SupportCA@npck.kz для получения регистрационного свидетельства для системы «Цифровой тенге».

36. Порядок выпуска, использования, перевыпуска и отзыва регистрационных свидетельств устанавливается УЦ НПК.

37. Участник обеспечивает выпуск, управление и хранение криптографической пары ключей для открытия цифровых счетов пользователей платформы и для подтверждения операций по цифровым счетам с использованием криптографического программно-аппаратного модуля, соответствующего не ниже, чем третьему уровню безопасности согласно СТ РК 1073-2007 «Средства криптографической защиты информации. Общие технические требования».

38. Участник выполняет мероприятия по сетевому подключению к промышленной среде с использованием выделенных каналов связи (основного и резервного) в соответствии с пунктом 15 Регламента.

39. Запросы для взаимодействия с промышленной средой направляются на URL, предоставляемый Национальным центром при подключении участника.

40. Каждый запрос участника к промышленной среде Платформы подписывается транспортной ЭЦП. При обмене данными с Платформой применяется сертифицированное средство криптографической защиты информации и электронная цифровая подпись регистрационного свидетельства, предоставляемые участнику Национальным центром. Участник организует разработку сервиса формирования и проверки транспортной подписи для взаимодействия с Платформой в соответствии с Документацией. В случае использования в промышленной среде примера сервиса, предоставленного Национальным центром, Национальный центр не несёт ответственности за его использование. Регистрационное свидетельство тестовой среды для взаимодействия с промышленной средой не применяется.

41. Участник указывает учётные данные промышленной среды, полученные в соответствии с пунктом 19 Регламента, в своих информационных системах, взаимодействующих с Платформой.

42. После предоставления доступа к промышленной среде, согласно пункту 21 Регламента, и перед началом проведения операций участник выполняет контрольный запрос получения баланса своего цифрового счёта в промышленной среде методом, предусмотренным API-спецификацией. Успешное получение ответа подтверждает готовность участника к проведению операций.

Глава 5. Способы взаимодействия участников с Платформой

43. Взаимодействие участника с Платформой осуществляется информационными системами участника исключительно посредством вызова API-методов Платформы в соответствии с документом «API-спецификация Платформы цифрового тенге». Иные способы взаимодействия информационных систем участника с Платформой не применяются.

44. Участник предоставляет пользователям платформы сервис для совершения операций на Платформе посредством своих пользовательских интерфейсов. При проектировании пользовательских интерфейсов участнику рекомендуется следовать Рекомендациям к пользовательским интерфейсам Национального центра, определяющим пользовательский сценарий работы с цифровыми тенге и рекомендации по оформлению. Готовность пользовательских интерфейсов к работе с Платформой подтверждается их демонстрацией при проведении эталонного тестирования, согласно пункту 17 Регламента. Участник обеспечивает, чтобы операции, инициированные пользователями Платформы,

направлялись на Платформу в порядке, установленном в Правилах, Регламентом и Документацией.

45. Взаимодействие участника с Национальным центром по вопросам, не являющимся операционными (инциденты, проблемы, запросы, консультации), осуществляется через систему Service Desk в порядке, предусмотренном Главой 8 Регламента, либо иными каналами связи, определёнными по согласованию с Национальным центром.

46. Национальный центр вправе вносить изменения в Документацию, включая API-спецификацию, и требовать от участников их соблюдения. Порядок доведения изменений Документации до участников установлен пунктом 5 Регламента.

Глава 6. Электронные сообщения на Платформе

47. Передача, приём, обработка, учёт и хранение электронных сообщений на Платформе осуществляются в соответствии с Правилами и Документацией. Форматы электронных сообщений и процедуры обмена платёжными и информационными сообщениями определяются API-спецификацией Платформы.

48. Порядок и сроки направления электронных сообщений в рамках запросов на выпуск и погашение цифровых тенге определяются Правилами и графиком работы Платформы.

49. По запросу участника Национальный центр в течение операционного дня предоставляет информационное сообщение, содержащее информацию о балансе цифрового счёта участника по состоянию на дату и время, указанные в запросе, а также перечень транзакций по цифровому счёту участника, выполненных за указанный в запросе период.

Глава 7. Технические работы и недоступность Платформы

50. Платформа доступна участникам непрерывно, 24 (двадцать четыре) часа в сутки 7 (семь) дней в неделю, за исключением времени проведения технических работ.

Участник обеспечивает непрерывный доступ к Платформе для своих клиентов в соответствии с Графиком работы Платформы.

51. Технические работы на Платформе проводятся Национальным центром. Национальный центр уведомляет участников о проведении и продолжительности плановых профилактических и восстановительных работ с указанием даты, времени и продолжительности работ, а также ожидаемого времени восстановления сервиса. Уведомление направляется на адрес электронной почты, указанный участником в Заявлении, и (или) иными способами по усмотрению Национального центра, в том числе через каналы оповещения Национального центра.

52. Плановые профилактические работы проводятся в окне с предельной длительностью и сроком предварительного уведомления участников, установленными Договором о предоставлении услуг.

53. Внеплановые работы при внештатных ситуациях, требующих немедленной реакции, проводятся в любое время суток. Уведомление о таких работах направляется участникам незамедлительно — одновременно с началом работ либо непосредственно после их начала.

54. Национальный центр уведомляет участников о завершении внеплановых работ и восстановлении доступности сервисов Платформы.

55. Участник уведомляет Национальный центр через систему Service Desk о проведении на своей стороне технических работ, затрагивающих предоставление сервиса пользователям платформы, не позднее чем за 1 (один) рабочий день до начала работ.

56. Недоступность услуг Платформы может быть вызвана или связана с:

- 1) плановыми профилактическими работами;
- 2) внеплановыми работами при внештатных ситуациях;
- 3) аварийной ситуацией или сбоем в работе программно-технического комплекса Платформы;
- 4) кибератакой либо иной угрозой информационной безопасности.

57. При возникновении неисправностей Национальный центр оперативно устраняет их. В случае если устранение неисправности требует более длительного периода времени, Национальный центр сообщает об этом участникам и предпринимает необходимые меры для скорейшего восстановления функционирования Платформы.

58. При выявлении сбоев в работе Платформы, угроз информационной безопасности либо признаков несанкционированных операций Национальный центр вправе ограничить проведение операций и информирует об этом участников.

59. При недоступности Платформы участник:

- 1) прекращает направление новых платежных и информационных сообщений на Платформу до восстановления её доступности;
- 2) обеспечивает информирование пользователей платформы о временной недоступности операций с цифровыми тенге в порядке, установленном договором цифрового счёта;
- 3) регистрирует обращение в системе Service Desk, если недоступность выявлена участником самостоятельно и уведомление от Национального центра не поступало.

Глава 8. Порядок обращения участников к Национальному центру

60. Для регистрации обращений (инцидентов, проблем, запросов, претензий) участники используют систему Service Desk Национального центра: <https://help.npck.kz/>. Обращения также могут направляться на адрес электронной

почты Support-CBDC@npck.kz. Учётные записи для доступа к системе Service Desk предоставляются участнику в порядке, предусмотренном пунктом 14 Регламента.

61. Участники направляют обращения следующих типов:

1) инцидент — незапланированное прерывание или снижение качества предоставления услуг Платформы, в том числе недоступность Платформы, ошибки при обработке запросов, расхождения по результатам сверки;

2) проблема — причина одного или нескольких инцидентов, требующая анализа;

3) запрос — обращение за консультацией, нормативно-справочной информацией либо за изменением параметров подключения;

4) претензия — обращение за проведением анализа и предоставлением информации по операции с цифровыми тенге, в случае возникновения спорной ситуации.

62. Приоритет обращения определяет Национальный центр в соответствии с таблицей 2 и уведомляет о нём участника.

Приоритеты обращений и целевые сроки

Таблица 1.

Приоритет	Признаки	Время реакции	Время решения
Критичный	Полная недоступность Платформы для участника; невозможность проведения платежей и переводов; инцидент информационной безопасности, затрагивающий Платформу	15 минут, круглосуточно	4 часа
Высокий	Частичная деградация: недоступность отдельных API-методов, систематические ошибки обработки запросов, расхождения по результатам сверки	1 час, круглосуточно	8 часов
Средний	Единичные ошибки, не препятствующие проведению операций; вопросы, требующие анализа (проблемы)	4 часа в рабочее время	3 рабочих дня
Низкий	Консультации, запросы нормативно-справочной	1 рабочий день	10 рабочих дней

	информации, изменение параметров подключения		
--	--	--	--

Время реакции — срок, в течение которого Национальный центр подтверждает принятие обращения в работу. Время решения — срок восстановления работоспособности либо предоставления участнику решения или обходного пути. Указанные в таблице 2 сроки являются целевыми и не являются гарантированным сроком устранения.

63. Участник незамедлительно уведомляет Национальный центр о выявленных инцидентах информационной безопасности, затрагивающих взаимодействие с Платформой путём регистрации обращения в системе Service Desk с критичным приоритетом и последующей эскалацией в порядке, установленном пунктом 65 Регламента.

64. Экстренная эскалация по обращениям, зарегистрированным в системе Service Desk, выполняется звонком на номер колл-центра Национального центра: +7 727 297 91 00. При экстренной эскалации номер обращения в системе Service Desk сообщается оператору колл-центра.

65. В соответствии с пунктом 68 Правил участник обеспечивает актуальность информации о контактных данных ответственных лиц, предоставленных Национальному центру.

Глава 9. Требования к проектированию информационных систем участника

66. Требования к программному обеспечению участника и к системе управления информационной безопасностью участника установлены Главой 6 Правил, в том числе пунктом 92 Правил (надёжное хранение информации и защита от несанкционированного доступа, многоуровневый доступ, контроль полноты обязательных полей, ведение внутрисистемных журналов, аудиторский след, резервирование и восстановление данных, хранение информации в течение 5 лет). Настоящий раздел устанавливает дополнительные требования, обусловленные особенностями операционного взаимодействия с Платформой.

67. При проектировании информационных систем для интеграции с Платформой участник обеспечивает:

- 1) корректную обработку повторных обращений к Платформе с учётом того, что повторное исполнение одного и того же платежа на Платформе не допускается;
- 2) выпуск, управление и хранение криптографических ключей пользователей с использованием программно-аппаратного модуля в соответствии с пунктом 38 Регламента;
- 3) резервирование каналов связи и переключение с основного канала на резервный при недоступности основного в соответствии с пунктом 15 Регламента;
- 4) техническую поддержку по работе на Платформе, доступную в круглосуточном режиме, в соответствии с пунктом 68 Правил.

Соблюдение требований настоящего пункта проверяется Национальным центром при проведении эталонного тестирования. При выявлении несоответствия Национальный центр вправе не допустить участника к промышленной среде Платформы.

68. При проектировании информационных систем для интеграции с Платформой участнику рекомендуется:

1) проектировать программное обеспечение с высокой доступностью, обеспечивая доступность используемых API-сервисов, а также конфиденциальность и целостность данных пользователей платформы при оказании им услуг с использованием сервисов Платформы;

2) оценивать ожидаемые объёмы операций и пиковые нагрузки и обеспечивать достаточную инфраструктуру для их обработки;

3) осуществлять мониторинг производительности на уровне собственной инфраструктуры и API — внутренний мониторинг аппаратных средств, гипервизора, операционной системы;

4) внедрять процессы мониторинга, которые оповещают (визуально или иным образом) персонал участника о несанкционированных, подозрительных и критических событиях;

5) при проектировании пользовательских интерфейсов для совершения пользователями платформы операций с цифровыми тенге руководствоваться Рекомендациями к пользовательским интерфейсам Национального центра.

69. Участник самостоятельно обеспечивает настройку, наладку, подключение и мониторинг работы своих информационных систем на Платформе, а также соответствие своего программного обеспечения и системы управления информационной безопасностью требованиям правил и Документации.

Глава 10. Меры информационной безопасности

70. Меры информационной безопасности, применяемые на Платформе, установлены Главой 6 Правил, Договором о предоставлении услуг и Документацией. Национальный центр и участники принимают меры по обеспечению информационной безопасности в соответствии с постановлением Правления Национального Банка Республики Казахстан от 27 марта 2018 года № 48 «Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах».

71. На Платформе применяется аутентификация участников, построенная на криптографическом протоколе двусторонней аутентификации, позволяющая аутентифицировать участника и Национальный центр. Порядок аутентификации информационных и платёжных сообщений устанавливается Национальным центром.



72. Национальный центр и участники применяют средства криптографической защиты информации для обеспечения конфиденциальности, целостности, подтверждения авторства и подлинности электронных сообщений. Применяемое средство криптографической защиты информации и электронной цифровой подписи, требования к программно-аппаратному модулю и порядок использования регистрационных свидетельств определены пунктами 38 и 41 Регламента и Договором о предоставлении услуг.

73. Конфиденциальность передаваемых данных обеспечивается их передачей по защищённым каналам связи (VPN) с использованием протокола TLS.

74. Участник незамедлительно уведомляет Национальный центр о выявленных инцидентах информационной безопасности в порядке, предусмотренном пунктом 64 Регламента. Национальный центр информирует участников о выявленных угрозах информационной безопасности и о принимаемых мерах по ограничению операций в порядке, предусмотренном пунктом 59 Регламента.

Глава 11. Порядок урегулирования спорных ситуаций по операциям

75. Настоящий раздел определяет порядок урегулирования спорных ситуаций, возникающих между участниками и Национальным центром в связи с совершением операций с цифровыми тенге на Платформе. Отношения участника и пользователя платформы, включая порядок уведомления пользователем участника об ошибочной передаче цифровых тенге, утере, краже или несанкционированном использовании цифрового счёта, а также ответственность участника перед пользователем платформы, регулируются Правилами и договором цифрового счёта.

76. При возникновении спора, связанного с совершением операции с цифровыми тенге, участник направляет претензию в Национальный центр и (или) другому участнику. Претензия предъявляется в течение 10 (десяти) рабочих дней со дня обнаружения спорной ситуации, но не позднее 180 (ста восьмидесяти) календарных дней с даты проведения спорной операции.

77. Претензия участника содержит:

- 1) наименование либо фамилию, имя, отчество (при его наличии) пользователя платформы;
- 2) индивидуальный идентификационный код цифрового счёта;
- 3) предмет претензии с указанием даты и суммы спорной операции;
- 4) иную информацию, необходимую для разрешения спора.

78. К претензии прилагаются:

- 1) копия платёжного и (или) информационного сообщения, подписанного ЭЦП, по которому возникла спорная ситуация;
- 2) связанные с ним другие электронные сообщения в электронном формате;
- 3) выписки с цифрового счёта, подтверждающие списание или зачисление цифровых тенге;



4) договор цифрового счета, заключённый между пользователем платформы и участником.

79. Претензия направляется посредством регистрации обращения в системе Service Desk Национального центра.

80. Претензия рассматривается Национальным центром в течение 10 (десяти) рабочих дней со дня её получения. При необходимости запроса дополнительных документов или сведений срок рассмотрения продлевается на период их предоставления, но не более чем на 5 (пять) рабочих дней. О продлении срока и о запрашиваемых документах Национальный центр уведомляет участника, инициировавшего претензию, для дальнейшего уведомления об этом заявителя.

81. В случае недостижения сторонами единого мнения относительно платёжного и (или) информационного сообщения, по которому возникла спорная ситуация, решение об удовлетворении либо об отказе в удовлетворении претензии принимает Национальный центр и уведомляет об этом стороны. При рассмотрении претензии Национальный центр исходит из данных Платформы, аудиторского следа электронных сообщений, приложенных к претензии электронных сообщений с ЭЦП, а также иных сведений, имеющих значение для разрешения спора.

82. По результатам рассмотрения претензии участник не позднее 10 (десяти) рабочих дней со дня получения ответа сообщает пользователю Платформы с обоснованием о полном либо частичном удовлетворении претензии или об отказе в её удовлетворении. Порядок и канал информирования пользователя Платформы определяются договором цифрового счёта.



Приложение
к Регламенту по взаимодействию с Платформой цифрового тенге

Протокол проведения тестирования

от «__» _____ 202__ года

Наименование объекта тестирования:

Интеграция информационных систем участника с Платформой цифрового тенге _____
(наименование участника)

Место проведения тестирования:

1. Тестовый стенд АО НПК: _____
2. Тестовый стенд информационной системы участника _____.

Сроки проведения тестирования _____ 2026г. – _____ 2026гг.

Список лиц, проводивших тестирование:

От Участника:

Должность:

ФИО

От Национального центра:

Должность:

ФИО:

Цель тестирования: удостовериться в готовности информационных систем участника для работы с Платформой ЦТ в промышленной среде.

Перечень сценариев тестирования

№	Наименование	Наименование сервисов (в документе API спецификации)	Статус (успешно\не успешно)

Заключение:

Результаты тестирования подтверждают соответствие информационной системы участника требованиям Документации Национального центра. Рекомендуется подключить информационную систему участника к промышленной среде Платформы цифрового тенге.

