**О внесении изменений и дополнений в некоторые постановления Правления Национального Банка Республики Казахстан по вопросам платежей и платежных услуг**

Постановление Правления Национального Банка Республики Казахстан от 29 апреля 2026 года № 44. Зарегистрировано в Министерстве юстиции Республики Казахстан 30 апреля 2026 года № 38624

Примечание ИЗПИ!

Порядок введения в действие см. п. 4.

Правление Национального Банка Республики Казахстан ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемый Перечень некоторых постановлений Правления Национального Банка Республики Казахстан, в которые вносятся изменения и дополнения по вопросам платежей и платежных услуг (далее – Перечень).

2. Департаменту платежных систем и цифровых финансовых технологий Национального Банка Республики Казахстан в установленном законодательством Республики Казахстан порядке обеспечить:

1) совместно с Юридическим департаментом Национального Банка Республики Казахстан государственную регистрацию настоящего постановления в Министерстве юстиции Республики Казахстан;

2) размещение настоящего постановления на официальном интернет-ресурсе Национального Банка Республики Казахстан после его официального опубликования;

3) в течение десяти рабочих дней после государственной регистрации настоящего постановления представление в Юридический департамент Национального Банка Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктом 2) настоящего пункта.

3. Контроль за исполнением настоящего постановления возложить на курирующего заместителя Председателя Национального Банка Республики Казахстан.

4. Настоящее постановление вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования, за исключением:

абзацев третьего, четвертого, пятого, шестого, седьмого, восьмого, девятого, десятого, одиннадцатого, двенадцатого, тринадцатого, четырнадцатого, пятнадцатого, шестнадцатого, семнадцатого, восемнадцатого, девятнадцатого, сорокового, сорок первого, сорок второго, сорок третьего, сорок четвертого, сорок пятого, сорок шестого, сорок седьмого, сорок восьмого, сорок девятого, пятидесятого, пятьдесят первого, пятьдесят второго, пятьдесят третьего, пятьдесят четвертого, пятьдесят пятого, пятьдесят шестого, пятьдесят седьмого, пятьдесят восьмого, пятьдесят девятого, шестидесятого, шестьдесят первого, шестьдесят второго, шестьдесят третьего,

шестьдесят четвертого, шестьдесят пятого, шестьдесят шестого, шестьдесят седьмого, шестьдесят восьмого, шестьдесят девятого, семидесятого, семьдесят первого, семьдесят второго, семьдесят третьего, семьдесят четвертого, семьдесят пятого, семьдесят шестого, семьдесят седьмого, семьдесят восьмого, семьдесят девятого, восьмидесятого, восемьдесят первого, восемьдесят второго, восемьдесят третьего, восемьдесят четвертого, восемьдесят пятого, восемьдесят шестого, восемьдесят седьмого, восемьдесят восьмого, восемьдесят девятого, девяностого, девяносто первого, девяносто второго, девяносто третьего, девяносто четвертого, девяносто пятого, девяносто шестого, девяносто седьмого, девяносто восьмого пункта 1 Перечня, которые вводятся в действие с 12 июля 2026 года;

абзацев двадцатого, двадцать первого, двадцать второго, двадцать третьего, двадцать четвертого, двадцать пятого, двадцать шестого, двадцать седьмого, двадцать восьмого, двадцать девятого, тридцатого, тридцать первого, тридцать второго, тридцать третьего, тридцать четвертого, тридцать пятого, тридцать шестого пункта 1 Перечня, которые вводятся в действие по истечении шести месяцев после дня первого официального опубликования настоящего постановления;

абзацев третьего, четвертого, пятого, шестого, седьмого, восьмого, девятого, десятого, одиннадцатого, двенадцатого, тринадцатого, четырнадцатого, девятнадцатого , двадцатого, двадцать седьмого, двадцать восьмого, двадцать девятого, тридцатого, тридцать первого, тридцать второго, тридцать третьего, тридцать четвертого, тридцать пятого, тридцать шестого, пятьдесят шестого, пятьдесят седьмого, пятьдесят восьмого, пятьдесят девятого, шестидесятого, шестьдесят первого, шестьдесят второго, шестьдесят третьего, шестьдесят четвертого, шестьдесят пятого, шестьдесят шестого, шестьдесят седьмого, шестьдесят восьмого, шестьдесят девятого, семидесятого, семьдесят первого, семьдесят второго, семьдесят третьего, семьдесят четвертого, семьдесят пятого, семьдесят шестого, семьдесят седьмого, семьдесят восьмого, семьдесят девятого, восьмидесятого, восемьдесят первого, восемьдесят второго, восемьдесят третьего, восемьдесят четвертого, восемьдесят пятого, восемьдесят шестого, восемьдесят седьмого, восемьдесят восьмого, восемьдесят девятого, девяностого, девяносто первого, девяносто второго, девяносто третьего, девяносто четвертого, девяносто пятого, девяносто шестого, девяносто седьмого, девяносто восьмого, девяносто девятого, сотого, сто первого, сто второго, сто третьего, сто четвертого, сто пятого, сто шестого, сто седьмого, сто восьмого, сто девятого, сто десятого, сто одиннадцатого, сто двенадцатого, сто тринадцатого, сто четырнадцатого, сто пятнадцатого, сто шестнадцатого, сто семнадцатого, сто восемнадцатого, сто девятнадцатого, сто двадцатого, сто двадцать первого, сто двадцать второго, сто двадцать третьего, сто двадцать четвертого, сто двадцать пятого, сто двадцать шестого, сто двадцать седьмого, сто двадцать восьмого, сто двадцать девятого, сто тридцатого пункта 3 Перечня, которые вводятся в действие с 12 июля 2026 года;

абзацев сорокового, сорок первого, сорок второго, сорок третьего, сорок четвертого , сорок пятого, сорок шестого, сорок седьмого, сорок восьмого, сорок девятого, пятидесятого, пятьдесят первого, пятьдесят второго, пятьдесят третьего, пятьдесят четвертого и пятьдесят пятого пункта 3 Перечня, которые вводятся в действие по истечении шести месяцев после дня первого официального опубликования настоящего постановления;

приложения 1 к Перечню, которое вводится в действие с 12 июля 2026 года;

подпунктов 2), 3) пункта 2, части третьей пункта 23, абзаца четвертого части шестой пункта 24, части седьмой пункта 24 и главы 4 Правил оказания электронных банковских услуг, которые вводятся в действие с 19 июля 2026 года;

части девятой пункта 24 Правил оказания электронных банковских услуг, которая вводится в действие с 12 июля 2026 года;

приложений 4, 5, 6 к Перечню, которые вводятся в действие с 12 июля 2026 года.

5. Приостановить до 12 июля 2026 года действие:

абзацев шестнадцатого, семнадцатого, восемнадцатого пункта 3 Перечня, установив , что в период приостановления данные абзацы действуют в следующей редакции:

"4. Для прохождения учетной регистрации в Национальном Банке платежная организация представляет в Национальный Банк через веб-портал "электронного правительства" заявление по форме согласно приложению 1 к Правилам, содержащее, в том числе сведения о руководителе (членах) исполнительного органа платежной организации (с приложением копий диплома (дипломов) и документа, подтверждающего трудовую деятельность руководителя (члена) исполнительного органа платежной организации в соответствии с Трудовым кодексом Республики Казахстан).

К заявлению также прилагаются документы, предусмотренные подпунктами 2), 3), 4), 5), 6) и 7) пункта 2 статьи 16 Закона о платежах и платежных системах.

Копия диплома (дипломов) не представляется, в случае наличия интеграции веб-портала "электронного правительства" с соответствующими государственными информационными системами, посредством которых обеспечивается получение указанных сведений, за исключением дипломов зарубежных организаций высшего и ( или) послевузового образования.";

абзацев двадцать четвертого, двадцать пятого, двадцать шестого пункта 3 Перечня, установив, что в период приостановления данные абзацы действуют в следующей редакции:

"15-2. Работник Национального Банка, уполномоченный на прием и регистрацию корреспонденции, в день поступления заявления осуществляет его прием, регистрацию и направление на исполнение в подразделение, ответственное за оказание государственной услуги по учетной регистрации (далее – ответственное подразделение ). При поступлении заявления после окончания рабочего времени, в выходные и

праздничные дни согласно трудовому законодательству Республики Казахстан прием заявлений осуществляется следующим рабочим днем.

При направлении платежной организацией заявления через веб-портал " электронного правительства" в личном кабинете автоматически отображается статус о принятии запроса на оказание государственной услуги с указанием даты и времени получения результата.

Национальный Банк получает из соответствующих государственных информационных систем через шлюз "электронного правительства" сведения о документах, удостоверяющих личность руководителя платежной организации, и о государственной регистрации (перерегистрации) юридического лица, а также копии диплома (дипломов) руководителя платежной организации с учетом положения части третьей пункта 4 Правил.";

абзаца первого пункта 2 Правил оказания электронных банковских услуг, установив , что в период приостановления данный абзац действует в следующей редакции:

"2. В Правилах используются понятия, предусмотренные законами Республики Казахстан "О банках и банковской деятельности в Республике Казахстан" (далее – Закон о банках и банковской деятельности), "Об электронном документе и электронной цифровой подписи", "Об информатизации", "О платежах и платежных системах" (далее – Закон о платежах и платежных системах), а также следующие понятия:";

часть восьмую пункта 24 Правил оказания электронных банковских услуг, установив, что в период приостановления данная часть действует в следующей редакции:

"Биометрическая аутентификация посредством ЦОИД осуществляется с использованием доступных источников.".

*Председатель*
*Национального Банка*
*Республики Казахстан* *Т. Сулейменов*

СОГЛАСОВАНО
Министерство юстиции
Республики Казахстан

СОГЛАСОВАНО
Министерство национальной экономики
Республики Казахстан

СОГЛАСОВАНО
Министерство искусственного интеллекта
и цифрового развития
Республики Казахстан

СОГЛАСОВАНО
Агентство Республики Казахстан

по регулированию и развитию
финансового рынка

Приложение
к постановлению Председатель
Национального Банка
Республики Казахстан
от 29 апреля 2026 года № 44

**Перечень некоторых постановлений Правления Национального Банка Республики Казахстан, в которые вносятся изменения и дополнения по вопросам платежей и платежных услуг**

1. Внести в постановление Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 202 "Об утверждении Правил выпуска, использования и погашения электронных денег, а также требований к эмитентам электронных денег и системам электронных денег на территории Республики Казахстан" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 14298) следующие изменения:

в Правилах выпуска, использования и погашения электронных денег, а также в требованиях к эмитентам электронных денег и системам электронных денег на территории Республики Казахстан, утвержденных указанным постановлением:

пункт 2 изложить в следующей редакции:

"2. В Правилах используются понятия, предусмотренные статьей 1 Закона Республики Казахстан "О платежах и платежных системах", а также следующие понятия:

1) кибербезопасность – состояние защищенности цифровых объектов от нарушения их конфиденциальности, целостности или доступности;

2) угроза кибербезопасности – совокупность условий и факторов, создающих предпосылки к возникновению инцидента кибербезопасности;

3) обеспечение кибербезопасности – процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информационных активов оператора системы электронных денег;

4) процедура безопасности – комплекс организационных мер и программно-технических средств защиты информации, предназначенных для удостоверения прав владельца электронных денег на использование электронных денег и обнаружения ошибок и (или) изменений в содержании передаваемых и получаемых электронным способом сообщений (далее – электронное сообщение) при использовании электронных денег;

5) информация об инцидентах кибербезопасности, включая сведения о нарушениях, сбоях в цифровых системах – информация об отдельно или серийно возникающих сбоях в работе цифровой инфраструктуры или отдельных ее объектов, создающих

угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования цифровых ресурсов оператора системы электронных денег;

6) инцидент кибербезопасности — событие или совокупность событий, негативно влияющих на кибербезопасность цифрового объекта;

7) периметр защиты цифровой инфраструктуры – совокупность программно-аппаратных средств, отделяющих цифровую инфраструктуру оператора системы электронных денег от внешних информационных сетей и обеспечивающих защиту от угроз кибербезопасности;

8) информационный актив оператора системы электронных денег – совокупность информации и объекта цифровой инфраструктуры, используемого для ее хранения и ( или) обработки;

9) цифровая инфраструктура оператора системы электронных денег (далее – цифровая инфраструктура) – совокупность объектов цифровой инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования цифровых ресурсов и предоставления доступа к ним;

10) внутренние правила системы электронных денег – правила, в соответствии с которыми производятся выпуск, реализация, приобретение, погашение электронных денег, а также осуществляются операции с их использованием в системе электронных денег;

11) личный кабинет владельца электронных денег – персональный раздел владельца электронных денег на интернет-ресурсе системы электронных денег, посредством которого владелец электронных денег имеет доступ к своему электронному кошельку для получения необходимой информации об остатке электронных денег, операциях, проведенных по нему, осуществления платежей и иных операций с использованием электронных денег в порядке, предусмотренном внутренними правилами системы электронных денег и договорами, заключенными между оператором системы электронных денег (далее – оператор) или эмитентом и владельцем электронных денег. Перечень предоставляемых услуг посредством личного кабинета владельца электронных денег устанавливается оператором;

12) обменные операции с электронными деньгами – операции по обмену электронных денег, выпущенных одним эмитентом, на электронные деньги другого эмитента, являющегося участником другой системы электронных денег;

13) принудительное погашение электронных денег – операция по погашению электронных денег, предусматривающая перечисление равной номинальной их стоимости на банковский счет владельца электронных денег либо на консолидированный счет эмитента до их востребования физическим лицом;

14) прекращение выпуска электронных денег – прекращение деятельности эмитента по оказанию платежной услуги, предусматривающей выдачу электронных денег

физическому лицу или агенту системы электронных денег (далее – агент) путем обмена на равную по их номинальной стоимости сумму денег;

15) блокирование электронного кошелька – полный или частичный запрет на использование электронных денег, хранящихся в электронном кошельке владельца электронных денег.";

пункт 24 изложить в следующей редакции:

"24. После осуществления платежа с использованием электронных денег их владельцу выдается торговый чек, подтверждающий факт осуществления операции с использованием электронных денег, в форме электронного сообщения либо на бумажном носителе (далее – торговый чек).

Торговый чек содержит следующие реквизиты:

1) сумма платежа;

2) время и дата совершения платежа;

3) порядковый номер торгового чека;

4) наименование (код) и индивидуальный идентификационный номер, бизнес-идентификационный номер индивидуального предпринимателя или юридического лица;

5) код транзакции или другой код, идентифицирующий платеж в системе электронных денег;

6) идентификационный код электронного кошелька отправителя и получателя электронных денег (уникальный идентификатор, статус идентификации владельца электронных денег);

7) контактные номера телефонов оператора, в том числе сотовой связи;

8) сведения об отправителе электронных денег (в случае наличия);

9) сведения о получателе электронных денег (поставщик товаров или услуг);

10) код назначения операции;

11) наименование поставщика платежных услуг (платежный посредник), в том числе иностранного, в пользу которого осуществляется перевод электронных денег от отправителя за оплату услуг третьих лиц, не представленных в системе электронных денег в качестве поставщиков услуг;

12) сведения о погашении электронных денег (банк, номер банковского счета).

Допускается отражение в торговом чеке дополнительных реквизитов.

При осуществлении перевода электронных денег от отправителя в пользу поставщика платежных услуг (платежный посредник), в том числе иностранного, за оплату услуг третьих лиц, не представленных в системе электронных денег в качестве поставщиков услуг, платежная организация обязана обеспечить отображение полной цепочки участников операции в платежном документе (чеке, квитанции, детализации)."
;

заголовок главы 6 изложить в следующей редакции:

"Глава 6. Удаленная идентификация владельца электронных денег - физического лица";

пункты 51, 52, 53 и 54 исключить;

заголовок главы 7 изложить в следующей редакции:

"Глава 7. Требования к программно-техническим средствам и системам управления кибербезопасностью операторов систем электронных денег, являющихся платежными организациями";

в пункте 55:

подпункт 4) изложить в следующей редакции:

"4) поиск информации по критериям и параметрам, определенным для данной цифровой системы, с сохранением запроса, а также сортировку информации по любым параметрам (определенным для данной цифровой системы) и возможность просмотра информации за предыдущие даты, если такая информация подлежит хранению в цифровой системе;";

подпункты 11) и 12) изложить в следующей редакции:

"11) регистрацию и идентификацию происходящих в цифровой системе событий с сохранением следующих атрибутов: дата и время начала события, наименование события, пользователь, производивший действие, идентификатор записи, дата и время окончания события, результат выполнения события;

12) изменение паролей учетных записей средств обеспечения безопасности периметра защиты цифровой инфраструктуры.";

пункты 56, 57, 57-1, 58, 58-1, 58-2, 58-3, 59, 60, 61, 62, 63, 64, 65 изложить в следующей редакции:

"56. Операторы систем электронных денег обеспечивают создание и функционирование системы управления кибербезопасностью, являющейся частью общей системы управления операторов систем электронных денег, предназначенной для управления процессом обеспечения кибербезопасности.

Операторы систем электронных денег утверждают внутренние документы, регламентирующие процесс управления кибербезопасностью, в том числе политику кибербезопасности.

Порядок и периодичность пересмотра внутренних документов, указанных в части второй настоящего пункта, определяются внутренними документами операторов систем электронных денег.

57. Система управления кибербезопасностью обеспечивает защиту информационных активов операторов систем электронных денег, допускающую минимальный уровень потенциального ущерба для бизнес-процессов операторов систем электронных денег.

57-1. Оператор системы электронных денег осуществляет обследование состояния кибербезопасности периметра защиты цифровой инфраструктуры не реже одного раз в

год. По результатам обследования составляется отчет с приложением материалов обследования, который доводится до сведения руководителя оператора системы электронных денег.

58. Оператор системы электронных денег обеспечивает надлежащий уровень системы управления кибербезопасностью, ее развитие и улучшение.

58-1. Оператор системы электронных денег, являющийся платежной организацией, прошедшей учетную регистрацию в Национальном Банке, в целях разграничения ответственности и функций в сфере обеспечения кибербезопасности создает подразделение кибербезопасности, являющееся структурным подразделением, обособленным от других структурных подразделений, занимающихся вопросами создания, сопровождения и развития цифровых объектов, или определяет лицо, ответственное за обеспечение кибербезопасности, не состоящее в штате структурных подразделений, занимающихся вопросами создания, сопровождения и развития цифровых объектов.

Подразделение кибербезопасности или лицо, ответственное за обеспечение кибербезопасности, осуществляет координацию работ по обеспечению кибербезопасности и контроль за исполнением требований кибербезопасности, определенных во внутренних документах оператора системы электронных денег.

Оператор системы электронных денег обеспечивает повышение квалификации работников подразделения кибербезопасности или лица, ответственного за обеспечение кибербезопасности, путем проведения:

1) внутренних мероприятий (лекции, семинары);

2) внешнего обучения (посещение курсов, семинаров – не реже одного раза в два года для каждого работника).

58-2. При приеме на работу нового работника, не позднее пяти рабочих дней с момента приема на работу, новый работник ознакомляется под подпись с основными требованиями по обеспечению кибербезопасности (вводный инструктаж). Результат ознакомления фиксируется в соответствующем журнале инструктажа или ином документе, подтверждающем прохождение инструктажа.

Требования настоящего пункта распространяются на операторов системы электронных денег, являющихся платежными организациями, прошедшими учетную регистрацию в Национальном Банке.

58-3. Трудовой договор, заключаемый с работником оператора системы электронных денег, являющегося платежной организацией, прошедшей учетную регистрацию в Национальном Банке, содержит обязанность работника по соблюдению требований по обеспечению кибербезопасности и неразглашению конфиденциальной информации.

59. Оператор системы электронных денег в целях обеспечения конфиденциальности , целостности и доступности информации осуществляет следующие функции:

1) организует систему управления кибербезопасностью, осуществляет координацию и контроль деятельности по обеспечению кибербезопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов кибербезопасности;

2) обеспечивает методологическую поддержку процесса обеспечения кибербезопасности;

3) осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля кибербезопасности в рамках своих полномочий;

4) осуществляет сбор, консолидацию, хранение и обработку информации об инцидентах кибербезопасности;

5) осуществляет анализ информации об инцидентах кибербезопасности;

6) обеспечивает внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения кибербезопасности, а также предоставление доступа к ним;

7) определяет ограничения по использованию привилегированных учетных записей;

8) организует и проводит мероприятия по обеспечению осведомленности работников оператора систем электронных денег в вопросах кибербезопасности;

9) осуществляет мониторинг состояния системы управления кибербезопасностью оператора систем электронных денег;

10) периодически (но не реже одного раза в год) осуществляет информирование руководства оператора системы электронных денег о состоянии системы управления кибербезопасностью;

11) поддерживает в актуальном состоянии схемы периметра защиты цифровой инфраструктуры и перечень администраторов средств обеспечения его безопасности;

12) устанавливает на периметре защиты цифровой инфраструктуры межсетевые экраны;

13) обеспечивает безопасность доступа пользователей к ресурсам сети Интернет из периметра защиты цифровой инфраструктуры;

14) в случае подключения ноутбуков или иных устройств к информационным активам оператора системы электронных денег, являющегося платежной организацией, прошедшей учетную регистрацию в Национальном Банке, из-за пределов периметра защиты оператора системы электронных денег на данных устройствах устанавливается лицензионное программное обеспечение для организации защищенного доступа ( шифрование канала связи, обеспечение двухфакторной аутентификации).

60. Оператор системы электронных денег управляет рисками кибербезопасности с указанием критериев приемлемого уровня по отношению к информационным активам.

При реализации рисков кибербезопасности разрабатывается план мероприятий, направленный на минимизацию возникновения подобных рисков.

61. Информация об инцидентах кибербезопасности, полученная в ходе мониторинга деятельности по обеспечению кибербезопасности, подлежит консолидации, систематизации и хранению.

62. Срок хранения информации об инцидентах кибербезопасности составляет не менее 5 (пяти) лет.

63. Оператором системы электронных денег определяется порядок принятия неотложных мер к устранению инцидента кибербезопасности, его причин и последствий.

64. Оператор систем электронных денег ведет журнал учета инцидентов кибербезопасности с отражением всей информации об инциденте кибербезопасности, принятых мерах и предлагаемых корректирующих мерах.

65. Оператор системы электронных денег предоставляет в Национальный Банк информацию о следующих выявленных инцидентах кибербезопасности:

1) эксплуатация уязвимостей в прикладном и системном программном обеспечении ;

2) несанкционированный доступ в цифровую систему;

3) атака "отказ в обслуживании" на цифровую систему или сеть передачи данных;

4) заражение сервера вредоносной программой или кодом;

5) совершение несанкционированного перевода электронных денег вследствие нарушения контролей кибербезопасности;

6) инцидентах кибербезопасности, несущих угрозу стабильности деятельности оператора системы электронных денег.

Информация об инцидентах кибербезопасности, указанных в настоящем пункте, предоставляется оператором системы электронных денег в возможно короткий срок, но не позднее 48 часов с момента выявления, в виде карты инцидента кибербезопасности по форме согласно приложению 2 к Правилам.

Информация по обработанным инцидентам кибербезопасности представляется в электронном формате с использованием платформы Национального Банка для обмена событиями и инцидентами кибербезопасности.

На каждый инцидент кибербезопасности заполняется отдельная карта инцидента кибербезопасности.";

часть первую пункта 66 изложить в следующей редакции:

"66. Оператор системы электронных денег, являющийся платежной организацией, прошедшей учетную регистрацию в Национальном Банке, для обмена событиями и инцидентами кибербезопасности использует статический IP-адрес и предоставляет информацию о нем в течение десяти рабочих дней со дня прохождения учетной регистрации в Национальном Банке.";

часть третью пункта 68 изложить в следующей редакции:

"В случае отсутствия у оператора системы электронных денег серверного помещения (центра обработки данных), требования настоящего пункта распространяются на арендуемые помещения или помещения, в которых размещены цифровые объекты оператора системы электронных денег.";

приложение 2 изложить в редакции согласно приложению 1 к настоящему Перечню некоторых постановлений Правления Национального Банка Республики Казахстан, в которые вносятся изменения и дополнения по вопросам платежей и платежных услуг ( далее – Перечень).

2. Внести в постановление Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 212 "Об утверждении Правил оказания банками, филиалами банков-нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг" ( зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 14337) следующее изменение:

Правила оказания банками, филиалами банков-нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг, утвержденные указанным постановлением, изложить в редакции согласно приложению 2 к Перечню (далее – Правила оказания электронных банковских услуг).

3. Внести в постановление Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 215 "Об утверждении Правил организации деятельности платежных организаций" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 14347) следующие изменения и дополнение:

в Правилах организации деятельности платежных организаций, утвержденных указанным постановлением:

часть вторую пункта 1 изложить в следующей редакции:

"Порядок организации деятельности платежных организаций включает учетную регистрацию платежных организаций в Национальном Банке Республики Казахстан ( далее – Национальный Банк), ведение Национальным Банком реестра платежных организаций (далее – реестр), оказание платежных услуг платежными организациями, уведомление платежными организациями об открытии филиалов, требования к программно-техническим средствам платежных организаций и системе управления кибербезопасности.";

пункт 2 изложить в следующей редакции:

"2. В Правилах используются понятия, предусмотренные Законом Республики Казахстан "О платежах и платежных системах" (далее – Закон о платежах и платежных системах), и следующие понятия:

1) кибербезопасность – состояние защищенности цифровых объектов от нарушения их конфиденциальности, целостности или доступности;

2) угроза кибербезопасности – совокупность условий и факторов, создающих предпосылки к возникновению инцидента кибербезопасности;

3) обеспечение кибербезопасности – процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информационных активов платежной организации;

4) информационный актив платежной организации – совокупность информации и объекта цифровой инфраструктуры, используемого для ее хранения и (или) обработки;

5) цифровая инфраструктура платежной организации (далее – цифровая инфраструктура) – совокупность объектов цифровой инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования цифровых ресурсов и предоставления доступа к ним;

6) информация об инцидентах кибербезопасности, включая сведения о нарушениях, сбоях в цифровых системах – информация об отдельно или серийно возникающих сбоях в работе цифровой инфраструктуры или отдельных ее объектов, создающих угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования цифровых ресурсов платежной организации;

7) инцидент кибербезопасности – событие или совокупность событий, негативно влияющих на кибербезопасность цифрового объекта;

8) периметр защиты цифровой инфраструктуры – совокупность программно-аппаратных средств, отделяющих цифровую инфраструктуру платежной организации от внешних информационных сетей и обеспечивающих защиту от угроз кибербезопасности."

пункт 4 изложить в следующей редакции:

"4. Для прохождения учетной регистрации в Национальном Банке платежная организация представляет в Национальный Банк через веб-портал "цифрового правительства" заявление по форме согласно приложению 1 к Правилам, содержащее, в том числе сведения о руководителе (членах) исполнительного органа платежной организации (с приложением копий диплома (дипломов) и документа, подтверждающего трудовую деятельность руководителя (члена) исполнительного органа платежной организации в соответствии с Трудовым кодексом Республики Казахстан.

К заявлению также прилагаются документы, предусмотренные подпунктами 2), 3), 4), 5), 6) и 7) пункта 2 статьи 16 Закона о платежах и платежных системах.

Копия диплома (дипломов) не представляется, в случае наличия интеграции веб-портала "цифрового правительства" с соответствующими государственными цифровыми системами, посредством которых обеспечивается получение указанных сведений, за исключением дипломов зарубежных организаций высшего и (или) послевузового образования.";

подпункт 7 пункта 7 изложить в следующей редакции:

"7) порядок соблюдения мер кибербезопасности;";

пункт 12-1 изложить в следующей редакции:

"12-1. Платежная организация, прошедшая учетную регистрацию в Национальном Банке, в случае необходимости включения в перечень оказываемых платежных услуг дополнительных платежных услуг представляет в Национальный Банк документы, предусмотренные подпунктами 2), 3), 4) и 7) пункта 2 статьи 16 Закона о платежах и платежных системах, с внесенными изменениями и (или) дополнениями с учетом планируемых к оказанию платежных услуг в течение десяти календарных дней со дня внесения таких изменений и (или) дополнений.";

пункт 15-2 изложить в следующей редакции:

"15-2. Работник Национального Банка, уполномоченный на прием и регистрацию корреспонденции, в день поступления заявления осуществляет его прием, регистрацию и направление на исполнение в подразделение, ответственное за оказание государственной услуги по учетной регистрации (далее – ответственное подразделение ). При поступлении заявления после окончания рабочего времени, в выходные и праздничные дни согласно трудовому законодательству Республики Казахстан прием заявлений осуществляется следующим рабочим днем.

При направлении платежной организацией заявления через веб-портал "цифрового правительства" в личном кабинете автоматически отображается статус о принятии запроса на оказание государственной услуги с указанием даты и времени получения результата.

Национальный Банк получает из соответствующих государственных цифровых систем через шлюз "цифрового правительства" сведения о документах, удостоверяющих личность руководителя платежной организации и о государственной регистрации (перерегистрации) юридического лица, а также копии диплома (дипломов) руководителя платежной организации с учетом положения части третьей пункта 4 Правил.";

часть четвертую пункта 15-4 изложить в следующей редакции:

"На веб-портале "цифрового правительства" результат оказания государственной услуги по учетной регистрации направляется платежной организации в личный кабинет в форме электронного документа, удостоверенного электронной цифровой подписью (далее – ЭЦП) уполномоченного лица.";

пункт 15-5 изложить в следующей редакции:

"15-5. Информация о стадии оказания государственной услуги по учетной регистрации обновляется в автоматическом режиме в цифровой системе мониторинга оказания государственных услуг.";

часть первую пункта 23-1 изложить в следующей редакции:

"23-1. Выдача согласия на проведение добровольной реорганизации платежной организации осуществляется при предоставлении платежной организацией в Национальный Банк через веб-портал "цифрового правительства" решения о добровольной реорганизации.";

часть четвертую пункта 23-4 изложить в следующей редакции:

"На веб-портале "цифрового правительства" результат оказания государственной услуги по добровольной реорганизации направляется платежной организации в личный кабинет в форме электронного документа, удостоверенного ЭЦП уполномоченного лица.";

пункт 23-5 изложить в следующей редакции:

"23-5. Информация о стадии оказания государственной услуги по добровольной реорганизации обновляется в автоматическом режиме в цифровой системе мониторинга оказания государственных услуг.";

дополнить пунктом 24-1 следующего содержания:

"24-1. Платежными организациями, являющимися операторами системы электронных денег, в случаях, предусмотренных Законом о платежах и платежных системах, биометрическая аутентификация владельцев электронных денег осуществляется посредством Центра обмена идентификационными данными Национального Банка (далее – ЦОИД), функционирование которого предусмотрено Законом о платежах и платежных системах.

Биометрическая аутентификация владельцев электронных денег посредством ЦОИД осуществляется в порядке, предусмотренном Правилами оказания банками, филиалами банков-нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг, утвержденными постановлением Правления Национального Банка Республики Казахстан № 212 от 31 августа 2016 года (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 14337).";

пункт 25 изложить в следующей редакции:

"25. При оказании платежной организацией платежных услуг, предусмотренных подпунктами 1) и 4) пункта 3 Правил, документ, подтверждающий факт оказания платежной услуги, содержит следующие реквизиты:

1) номер документа, дата и время его выписки;

2) наименование платежной организации;

3) сумма операции;

4) валюта операции;

5) сумма комиссионного вознаграждения;

6) назначение платежа;

7) наименование поставщика услуг;

8) наименование поставщика платежных услуг (платежный посредник), в том числе иностранного, участвующего в операции;

9) код категории субъекта предпринимательства (Merchant Category Code) (в случае оказания платежной услуги, предусмотренной подпунктом 4) пункта 3 Правил);

10) наименование либо банковский идентификационный код банка, филиала банка-нерезидента Республики Казахстан или организации, осуществляющей отдельные виды банковских операций, которому (которой) платежная организация представляет информацию для осуществления платежа и (или) перевода либо принятия денег по данным платежам в соответствии с подпунктом 9) пункта 1 статьи 12 Закона о платежах и платежных системах (в случае оказания платежной услуги, предусмотренной подпунктом 4) пункта 3 Правил);

11) идентификатор транзакции внутри системы платежной организации;

12) уникальный 12-значный идентификатор операции (Reference Retrieval Number или Receiver Reference Number) и иные технические реквизиты (в случае оказания платежной услуги, предусмотренной подпунктом 4) пункта 3 Правил).

Не допускается при указании наименований использование сокращений, торговых обозначений, аббревиатур и кодов, допускающих неоднозначное толкование.

Допускается проставление платежной организацией в документе, подтверждающем факт оказания платежной услуги, дополнительных реквизитов по оказанной платежной услуге.";

заголовок главы 6 изложить в следующей редакции:

"Глава 6. Требования к программно-техническим средствам платежных организаций и системе управления кибербезопасностью";

в пункте 34:

подпункт 4) изложить в следующей редакции:

"4) поиск информации по критериям и параметрам, определенным для данной цифровой системы, с сохранением запроса, а также сортировку информации по любым параметрам (определенным для данной цифровой системы) и возможность просмотра информации за предыдущие даты, если такая информация подлежит хранению в цифровой системе;";

подпункты 11) и 12) изложить в следующей редакции:

"11) регистрацию и идентификацию происходящих в цифровой системе событий с сохранением следующих атрибутов: дата и время начала события, наименование события, пользователь, производивший действие, идентификатор записи, дата и время окончания события, результат выполнения события;

12) изменение паролей учетных записей средств обеспечения безопасности периметра защиты цифровой инфраструктуры.";

пункты 35, 36, 36-1, 37, 37-1, 37-2, 37-3, 38, 39, 40, 41, 42, 43 и 44 изложить в следующей редакции:

"35. Платежные организации обеспечивают создание и функционирование системы управления кибербезопасностью, являющейся частью общей системы управления платежной организации, предназначенной для управления процессом обеспечения кибербезопасности.

Платежная организация утверждает внутренние документы, регламентирующие процесс управления кибербезопасностью, в том числе политику кибербезопасности.

Порядок и периодичность пересмотра внутренних документов, указанных в части второй настоящего пункта, определяются внутренними документами платежной организации.

36. Система управления кибербезопасностью обеспечивает защиту информационных активов платежной организации, допускающую минимальный уровень потенциального ущерба для бизнес-процессов платежной организации.

36-1. Подразделение кибербезопасности или лицо, ответственное за обеспечение кибербезопасности, осуществляют обследования состояния кибербезопасности не реже одного раз в год. По результатам обследования подразделением кибербезопасности или лицом, ответственным за обеспечение кибербезопасности, составляется отчет с приложением материалов обследования, который доводится до сведения руководителя платежной организации.

37. Платежная организация обеспечивает надлежащий уровень системы управления кибербезопасностью, ее развитие и улучшение.

37-1. В платежной организации в целях разграничения ответственности и функций в сфере обеспечения кибербезопасности создается подразделение кибербезопасности, являющееся структурным подразделением, обособленным от других структурных подразделений, занимающихся вопросами создания, сопровождения и развития цифровых объектов, или определяется лицо, ответственное за обеспечение кибербезопасности, не состоящее в штате структурных подразделений, занимающихся вопросами создания, сопровождения и развития цифровых объектов.

Подразделение кибербезопасности или лицо, ответственное за обеспечение кибербезопасности, осуществляет координацию работ по обеспечению кибербезопасности и контроль за исполнением требований кибербезопасности, определенных во внутренних документах платежной организации.

Платежная организация обеспечивает повышение квалификации работников подразделения кибербезопасности или лица, ответственного за обеспечение кибербезопасности путем проведения:

1) внутренних мероприятий (лекции, семинары);

2) внешнего обучения (посещение курсов, семинаров – не реже одного раза в два года для каждого работника).

37-2. При приеме на работу нового работника, не позднее пяти рабочих дней с момента приема на работу, новый работник ознакомляется под подпись с основными

требованиями по обеспечению кибербезопасности (вводный инструктаж). Результат ознакомления фиксируется в соответствующем журнале инструктажа или ином документе, подтверждающем прохождение инструктажа.

37-3. Трудовой договор, заключаемый с работником платежной организации, содержит обязанность работника по соблюдению требований по обеспечению кибербезопасности и неразглашению конфиденциальной информации.

38. Платежная организация в целях обеспечения конфиденциальности, целостности и доступности информации платежной организации осуществляет следующие функции :

1) организует систему управления кибербезопасностью, осуществляет координацию и контроль деятельности по обеспечению кибербезопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов кибербезопасности;

2) обеспечивает методологическую поддержку процесса обеспечения кибербезопасности;

3) осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля кибербезопасности в рамках своих полномочий;

4) осуществляет сбор, консолидацию, хранение и обработку информации об инцидентах кибербезопасности;

5) осуществляет анализ информации об инцидентах кибербезопасности;

6) обеспечивает внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения кибербезопасности, а также предоставление доступа к ним;

7) определяет ограничения по использованию привилегированных учетных записей;

8) организует и проводит мероприятия по обеспечению осведомленности работников платежной организации в вопросах кибербезопасности;

9) осуществляет мониторинг состояния системы управления кибербезопасностью платежной организации;

10) периодически (но не реже одного раза в год) осуществляет информирование руководства платежной организации о состоянии системы управления кибербезопасностью платежной организации;

11) поддерживает в актуальном состоянии схемы периметра защиты цифровой инфраструктуры и перечень администраторов средств обеспечения его безопасности;

12) устанавливает на периметре защиты цифровой инфраструктуры межсетевые экраны;

13) обеспечивает безопасность доступа пользователей к ресурсам сети Интернет из периметра защиты цифровой инфраструктуры;

14) в случае подключения ноутбуков или иных устройств к информационным активам платежной организации из-за пределов периметра защиты платежной

организации на данных устройствах устанавливается лицензионное программное обеспечение для организации защищенного доступа (шифрование канала связи, обеспечение двухфакторной аутентификации).

39. Платежная организация управляет рисками кибербезопасности с указанием критериев приемлемого уровня по отношению к информационным активам.

При реализации рисков кибербезопасности разрабатывается план мероприятий, направленный на минимизацию возникновения подобных рисков.

40. Информация об инцидентах кибербезопасности, полученная в ходе мониторинга деятельности по обеспечению кибербезопасности, подлежит консолидации, систематизации и хранению.

41. Срок хранения информации об инцидентах кибербезопасности составляет не менее 5 (пяти) лет.

42. Платежной организацией определяется порядок принятия неотложных мер к устранению инцидента кибербезопасности, его причин и последствий.

43. В платежной организации ведется журнал учета инцидентов кибербезопасности с отражением всей информации об инциденте кибербезопасности, принятых мерах и предлагаемых корректирующих мерах.

44. Платежная организация предоставляет в Национальный Банк информацию о следующих выявленных инцидентах кибербезопасности:

1) эксплуатация уязвимостей в прикладном и системном программном обеспечении ;

2) несанкционированный доступ в цифровую систему;

3) атака "отказ в обслуживании" на цифровую систему или сеть передачи данных;

4) заражение сервера вредоносной программой или кодом;

5) совершение несанкционированного перевода денежных средств вследствие нарушения контролей кибербезопасности;

6) инцидентах кибербезопасности, несущих угрозу стабильности деятельности платежной организации.

Информация об инцидентах кибербезопасности, указанных в настоящем пункте, предоставляется платежной организацией в возможно короткий срок, но не позднее 48 часов с момента выявления, в виде карты инцидента кибербезопасности по форме согласно приложению 7 к Правилам.

Информация по обработанным инцидентам кибербезопасности представляется в электронном формате с использованием платформы Национального Банка для обмена событиями и инцидентами кибербезопасности.

На каждый инцидент кибербезопасности заполняется отдельная карта инцидента кибербезопасности.";

часть первую пункта 45 изложить в следующей редакции:

"45. Платежная организация для подключения к платформе Национального Банка для обмена событиями и инцидентами кибербезопасности использует статический IP-адрес и предоставляет информацию о нем в течение десяти рабочих дней со дня прохождения учетной регистрации в Национальном Банке.";

часть третью пункта 47 изложить в следующей редакции:

"В случае отсутствия в платежной организации серверного помещения (центра обработки данных), требования настоящего пункта распространяются на арендуемые помещения или помещения, в которых размещены цифровые объекты платежной организации.";

заголовок главы 7 изложить в следующей редакции:

"Глава 7. Порядок актуализации сведений по учетной регистрации платежной организации в цифровой системе "Государственная база данных "Е-лицензирование";

пункт 50 изложить в следующей редакции:

"50. Актуализация сведений по учетной регистрации платежной организации в цифровой системе "Государственная база данных "Е-лицензирование" осуществляется в следующих случаях:

1) изменения наименования платежной организации;

2) включения дополнительных платежных услуг в перечень оказываемых платежных услуг;

3) исключения отдельных платежных услуг из перечня оказываемых платежных услуг.";

пункты 52 и 53 изложить в следующей редакции:

"52. Национальный Банк вносит соответствующие изменения в сведения по учетной регистрации платежной организации в цифровой системе "Государственная база данных "Е-лицензирование".

53. В случае исключения платежной организации из реестра платежных организаций Национальный Банк вносит соответствующую запись о прекращении действия учетной регистрации в цифровой системе "Государственная база данных " Е-лицензирование".";

приложения 1 и 2 изложить в редакции согласно приложениям 3 и 4 к Перечню;

в приложении 5:

в Перечне основных требований к оказанию государственной услуги "Выдача согласия на проведение добровольной реорганизации (присоединение, слияние, разделение, выделение, преобразование) платежных организаций":

строку 2 изложить в следующей редакции:

"

| | | |
|---|---|---|
| 2. | Способы предоставления государственной услуги | Веб-портал "цифрового правительства" www.egov.kz, www.elicense.kz (далее – портал). |

";

строку 7 изложить в следующей редакции:

"

| | | |
|---|---|---|
| 7. | График работы услугодателя, Государственной корпорации и цифровых объектов | 1) услугодателя – с понедельника по пятницу с 9.00 до 18.30 часов с перерывом на обед с 13.00 до 14.30 часов, кроме выходных и праздничных дней, в соответствии с трудовым законодательством Республики Казахстан.<br>График приема документов и выдачи результатов оказания государственной услуги – с понедельника по пятницу с 9.00 до 17.30 часов с перерывом на обед с 13.00 до 14.30 часов;<br>2) портала – круглосуточно, за исключением технических перерывов в связи с проведением ремонтных работ (при обращении услугополучателя после окончания рабочего времени, в выходные и праздничные дни, согласно трудовому законодательству Республики Казахстан, прием заявлений и выдача результатов оказания государственной услуги осуществляется на следующий рабочий день). |

";

приложения 6 и 7 изложить в редакции согласно приложениям 5 и 6 к Перечню.

Приложение 1
к Перечню некоторых
постановлений Правления
Национального Банка
Республики Казахстан,
в которые вносятся изменения
и дополнения по вопросам
платежей и платежных услуг

Приложение 2
к Правилам выпуска,
использования и погашения
электронных денег,
а также требованиям к эмитентам
электронных денег и системам
электронных денег
на территории
Республики Казахстан

Форма

# Карта инцидента кибербезопасности

| № | Общие сведения | |
|---|---|---|
| | Характеристики инцидента кибербезопасности | Информация об инциденте кибербезопасности |
| 1 | Наименование инцидента кибербезопасности | |
| 2 | Дата и время выявления ( дд.мм.гггг и чч:мм с указанием часового пояса UTC+X) | |
| 3 | Место выявления (организация, филиал, сегмент цифровой инфраструктуры ) | |
| 4 | Источник информации об инциденте кибербезопасности ( пользователь, администратор, администратор кибербезопасности , работник подразделения кибербезопасности или техническое средство) | |
| 5 | Использованные методы при реализации инцидента кибербезопасности (социальная инженерия, внедрение вредоносного кода) | |
| Содержание инцидента кибербезопасности | | |
| 6 | Симптомы, признаки инцидента кибербезопасности | |
| 7 | Основные события (эксплуатация уязвимостей в прикладном и системном программном обеспечении;<br>несанкционированный доступ в цифровую систему;<br>атака "отказ в обслуживании" на цифровую систему или сеть передачи данных;<br>заражение сервера вредоносной программой или кодом;<br>совершение несанкционированного перевода денежных средств;<br>инциденты кибербезопасности, несущие угрозу стабильности деятельности оператора системы электронных денег) | |
| | Пораженные активы (физический уровень цифровой инфраструктуры, уровень сетевого оборудования, уровень сетевых | |

| | | |
|---|---|---|
| 8 | приложений и сервисов, уровень операционных систем, уровень технологических процессов и приложений и уровень бизнес-процессов оператора системы электронных денег) | |
| 9 | Статус инцидента кибербезопасности ( свершившийся инцидент кибербезопасности, попытка осуществления инцидента кибербезопасности, подозрение на инцидент кибербезопасности) | |
| 10 | Ущерб | |
| 11 | Источник угрозы (выявленные идентификаторы) | |
| 12 | Преднамеренность (намеренный, ошибочный) | |
| Предпринятые меры по инциденту кибербезопасности | | |
| 13 | Предпринятые действия ( идентификация уязвимости, блокирование, восстановление) | |
| 14 | Запланированные действия, направленные на минимизацию возникновения рисков кибербезопасности | |
| 15 | Оповещенные лица (фамилия, имя , отчество (при его наличии) должностных лиц, наименование государственных органов, организаций) | |
| 16 | Привлеченные специалисты ( фамилия, имя, отчество (при его наличии) место работы, должность, номер телефона) | |

Ответственный работник по кибербезопасности

_____ _____

(фамилия, имя, отчество (при его наличии) (подпись)

Дата "____" _____ 20 ___ года

Приложение 2
к Перечню некоторых
постановлений Правления
Национального Банка
Республики Казахстан,
в которые вносятся изменения
и дополнения по вопросам
платежей и платежных услуг
Утверждены
постановлением Правления
Национального Банка

Республики Казахстан
от 31 августа 2016 года № 212

# Правила оказания банками, филиалами банков-нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг

## Глава 1. Общие положения

1. Настоящие Правила оказания банками, филиалами банков-нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг (далее – Правила) разработаны в соответствии с подпунктом 37) абзаца второго части второй пункта 19 Положения о Национальном Банке Республики Казахстан, утвержденного Указом Президента Республики Казахстан от 31 декабря 2003 года № 1271 "Об утверждении Положения и структуры Национального Банка Республики Казахстан", и определяют порядок оказания банками, филиалами банков-нерезидентов Республики Казахстан и организациями, осуществляющими отдельные виды банковских операций (далее – банки), электронных банковских услуг.

Порядок оказания банками электронных банковских услуг включает предоставление электронных банковских услуг, процедуры безопасности, меры от несанкционированного доступа, приостановление и прекращение предоставления электронных банковских услуг, хранение электронных документов при предоставлении электронных банковских услуг.

Действие Правил не распространяется на услуги, связанные с приемом платежей с использованием платежных карточек в пользу лиц, реализующих товары и услуги в сети Интернет (интернет-эквайринг).

2. В Правилах используются понятия, предусмотренные законами Республики Казахстан "О банках и банковской деятельности в Республике Казахстан" (далее – Закон о банках и банковской деятельности), "О платежах и платежных системах" ( далее – Закон о платежах и платежных системах), цифровым законодательством Республики Казахстан, а также следующие понятия:

1) аутентификация – подтверждение подлинности и правильности составления электронного документа в соответствии с требованиями процедуры безопасности;

2) операционная документация оператора системы открытого банкинга – внутренние документы, утверждаемые оператором системы открытого банкинга, определяющие технические и организационные требования к взаимодействию участников системы открытого банкинга, включая стандарты интерфейсов программирования приложений (API), требования к кибербезопасности, уровни и показатели доступности сервисов, сроки обработки запросов, форматы и иные требования оператора системы открытого банкинга;

3) оператор системы открытого банкинга – национальный центр по управлению национальной цифровой финансовой инфраструктурой, осуществляющий сбор, хранение и обработку согласий клиентов участников системы открытого банкинга на оказание электронных банковских услуг сторонними поставщиками платежных услуг на основании согласия клиента, идентификацию клиентов участников системы открытого банкинга, ведение реестра авторизованных поставщиков платежных услуг, обмен информацией между поставщиками платежных услуг;

4) одноразовый (единовременный) код – уникальная последовательность электронных цифровых символов, создаваемая программно-техническими средствами по запросу клиента и предназначенная для одноразового использования при предоставлении доступа клиенту к электронным банковским услугам;

5) динамическая идентификация – процедура установления личности клиента с целью однозначного подтверждения его прав на получение электронных банковских услуг путем использования одноразового (единовременного) кода;

6) процедура безопасности – комплекс организационных мер и программно-технических средств защиты информации, предназначенных для идентификации клиента при составлении, передаче и получении электронных документов с целью установления его прав на получение электронных банковских услуг и обнаружения ошибок и (или) изменений в содержании передаваемых и получаемых электронных документов;

7) код доступа – уникальная последовательность электронных цифровых символов ( от четырех до шести цифр), устанавливаемая клиентом или автоматически формируемая системами поставщика платежных услуг, используемая для входа в мобильное приложение и (или) подтверждения выполняемых клиентом операций, включая осуществление платежей и переводов;

8) уникальный идентификатор пользователя – цифровой, буквенный или содержащий иные символы код, присваиваемый банком клиенту для входа в систему банка, в которой предоставляется доступ к электронным банковским услугам;

9) пароль – совокупность цифровых, буквенных и иных символов, создаваемая для подтверждения прав на вход в систему банка для получения электронных банковских услуг;

10) центр обмена идентификационными данными (ЦОИД) – цифровая система, обеспечивающая взаимодействие с финансовыми и платежными организациями по обмену данными клиентов из доступных источников для проведения процедур идентификации, в том числе биометрической аутентификации клиентов;

11) Правила ЦОИД – внутренние правила национального центра по управлению национальной цифровой финансовой инфраструктурой, регламентирующие порядок предоставления услуг ЦОИД банкам при проведении процедур идентификации ( аутентификации) клиентов;

12) электронный документ – документ, в котором информация представлена в электронно-цифровой форме и удостоверена идентификационными средствами, составленный отправителем и не содержащий искажений и (или) изменений, внесенных в него после составления, в порядке, предусмотренном Правилами;

13) электронные платежные услуги – электронные банковские услуги, связанные с проведением платежей и (или) переводов денег, обменных операций с иностранной валютой с использованием банковского счета и осуществлением иных видов банковских операций, не относящихся к информационным банковским услугам.

## Глава 2. Предоставление электронных банковских услуг

3. Электронные банковские услуги предоставляются посредством систем удаленного доступа, в том числе посредством интернет-ресурса и (или) мобильного приложения.

4. При открытии интернет-ресурса или мобильного приложения для предоставления электронных банковских услуг банк в течение десяти рабочих дней после дня открытия интернет-ресурса или мобильного приложения уведомляет в произвольной письменной форме Национальный Банк (далее – Национальный Банк).

Уведомление содержит:

1) доменное имя и электронный адрес интернет-ресурса, а также идентификатор мобильного приложения, включая ссылки на мобильные приложения в соответствующих магазинах приложений;

2) перечень электронных банковских услуг, предоставляемых посредством Интернета и мобильного приложения;

3) подтверждение о наличии в банке утвержденных процедур безопасности и защиты информации от несанкционированного доступа при оказании электронных банковских услуг.

5. При изменении доменного имени, электронного адреса интернет-ресурса или идентификатора мобильного приложения банк в течение десяти рабочих дней со дня изменений уведомляет в произвольной письменной форме Национальный Банк.

6. Банк предоставляет электронные банковские услуги только по банковским операциям, которые предусмотрены лицензией, выданной уполномоченным государственным органом.

Банк до оказания электронных банковских услуг обеспечивает предоставление клиенту информации о размере взимаемой комиссии в денежном выражении по оказываемым электронным банковским услугам.

При оказании платежных услуг через электронный терминал допускается указание размера взимаемой комиссии в денежном выражении после внесения клиентом наличных денег в терминал.

7. Банк разрабатывает и утверждает процедуры и принимает меры по предотвращению использования действующих или внедряемых способов и технологий предоставления электронных банковских услуг в схемах легализации (отмывания) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения.

Банк при предоставлении электронных банковских услуг применяет необходимые меры, предусмотренные Законом Республики Казахстан "О противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения" ( далее – Закон о ПОД/ФТ/ФРОМУ), а также обеспечивает осуществление функций агента валютного контроля.

8. Электронные банковские услуги предоставляются посредством применения идентификационных средств, предусмотренных Законом о платежах и платежных системах, с соблюдением порядка, установленного Правилами. Предоставление банком электронных банковских услуг клиенту с использованием электронной цифровой подписи производится при наличии у клиента сертификата электронной цифровой подписи, выданного аккредитованным удостоверяющим центром Республики Казахстан или иностранным удостоверяющим центром, зарегистрированным в доверенной третьей стороне Республики Казахстан.

9. Электронные банковские услуги предоставляются клиенту на основании договора о предоставлении электронных банковских услуг либо договора банковского обслуживания, содержащего условие по оказанию электронных банковских услуг ( далее – договор).

10. Договор содержит следующие условия:

1) перечень электронных банковских услуг;

2) порядок и максимальный срок оказания электронных банковских услуг;

3) способы (способ) предоставления электронных банковских услуг и получения доступа к ним (через Интернет, средства телекоммуникаций, цифровые технологии, программное обеспечение и оборудование или другие устройства);

4) размеры взимаемых комиссий или указание интернет-ресурса, содержащего информацию о них, и порядок их взимания;

5) порядок и сроки предоставления банком подтверждения об отправке и (или) получении электронных документов, на основании которых клиенту предоставлены электронные банковские услуги;

6) права и обязанности сторон;

7) процедуры безопасности, также порядок аутентификации и подтверждения прав клиента на получение электронных банковских услуг;

8) ответственность сторон за неисполнение или ненадлежащее исполнение своих обязательств по договору;

9) основания приостановления, прекращения предоставления электронных банковских услуг с указанием порядка и формы уведомления клиента;

10) порядок предъявления претензий и способы разрешения спорных ситуаций, возникающих при предоставлении банком электронных банковских услуг;

11) контактные телефоны и адреса, в том числе для обращения в банк по вопросам, связанным с предоставлением электронных банковских услуг;

12) условие о неразглашении банком информации, полученной от клиента при предоставлении электронных банковских услуг;

13) право клиента на расторжение договора;

14) порядок определения курса обмена валют, применяемого при оказании электронных банковских услуг в иностранной валюте.

Допускается включение в договор иных условий, не содержащихся в настоящем пункте.

11. При заключении договора банк предоставляет клиенту информацию об электронных банковских услугах.

12. В случае указания в договоре отсылки на электронный документ, размещенный на интернет-ресурсе банка и содержащий дополнительные условия к договору, банк обеспечивает клиенту возможность беспрепятственного доступа к указанному электронному документу в течение срока действия договора.

13. В случае предоставления банком электронной банковской услуги через Интернет порядок и условия предоставления электронных банковских услуг определяются внутренними документами банка, которые размещаются на интернет-ресурсе банка.

14. Электронные платежные услуги предоставляются юридическим лицам с использованием следующих способов идентификации: электронной цифровой подписи, динамической идентификации, биометрической аутентификации их уполномоченных лиц.

15. Электронные платежные услуги предоставляются физическим лицам с использованием одного из следующих способов идентификации: электронной цифровой подписи, динамической идентификации, биометрической аутентификации или уникального идентификатора пользователя и пароля.

16. Банки при оказании электронных банковских услуг осуществляют идентификацию личности клиента с использованием средств биометрической аутентификации при:

1)превышении общей суммы переводов денег клиента - физического лица в пользу другого клиента – физического лица двух миллионов тенге в течение календарного дня. Биометрическая аутентификация проводится в совокупности с применением динамической идентификации;

2)изменении кода доступа и (или) пароля к мобильному приложению;

3)первичной регистрации клиента в мобильном приложении и (или) интернет-ресурсе банка.

17. При использовании динамической идентификации для получения физическими и юридическими лицами электронных платежных услуг одноразовый (единовременный ) код создается банком и направляется клиенту в соответствии с условиями договора, заключенного между ними.

Допускается использование клиентом устройства, генерирующего одноразовый ( единовременный) код, для получения электронных платежных услуг. Устройство, генерирующее одноразовый (единовременный) код, закрепляется за конкретным уполномоченным лицом юридического лица для совершения определенных им операций в рамках своих полномочий.

Допускается использование одного устройства, генерирующего одноразовый ( единовременный) код, одним уполномоченным лицом нескольких аффилированных юридических лиц, обсуживающихся в одном банке на основании соответствующих уполномочивающих документов. Данные полномочия предоставляются в соответствии с пунктом 47 Правил открытия, ведения и закрытия банковских счетов клиентов, утвержденных постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 207 "Об утверждении Правил открытия, ведения и закрытия банковских счетов клиентов" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 14422).

Использование устройства, генерирующего одноразовый (единовременный) код, осуществляется путем ввода в него персонального идентификационного номера и указания при доступе к услугам набора других средств идентификации (уникальный идентификатор пользователя, пароль).

Не допускается использование уполномоченным лицом юридического лица устройства, генерирующего одноразовый (единовременный) код, принадлежащего другому уполномоченному лицу.

18. При использовании динамической идентификации для каждого доступа к электронным платежным услугам требуется создание нового одноразового ( единовременного) кода.

При повторном доступе клиента к электронным платежным услугам требуется создание и использование нового одноразового (единовременного) кода.

19. Информационные банковские услуги предоставляются с использованием одного из следующих способов идентификации: электронной цифровой подписи, динамической идентификации, биометрической аутентификации или уникального идентификатора и пароля. Пароль используется на многократной основе либо изменяется по желанию клиента.

20. Использование уникального идентификатора пользователя и пароля, указываемых в системе банка для доступа к электронным платежным услугам, не признается динамической идентификацией.

21. Допускается передача банком третьим лицам на основании договора о возмездном оказании услуг исполнения информационно-технологических функций, необходимых для оказания электронных банковских услуг (далее – договор об аутсорсинге). Порядок аутсорсинга по оказанию электронных банковских услуг определяется внутренними документами банка и договором об аутсорсинге и осуществляется в соответствии с требованиями пунктов 16, 17 статьи 13 Закона о платежах и платежных системах.

## Глава 3. Проведение биометрической аутентификации посредством ЦОИД

22. При оказании электронных банковских услуг деловые отношения с клиентом дистанционным способом устанавливаются в соответствии с Требованиями к надлежащей проверке клиентов в случае дистанционного установления деловых отношений субъектами финансового мониторинга, утвержденными постановлением Правления Национального Банка Республики Казахстан от 29 июня 2018 года № 140 " Об утверждении Требований к надлежащей проверке клиентов в случае дистанционного установления деловых отношений субъектами финансового мониторинга" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 17250).

23. Банки при оказании электронных банковских услуг в целях идентификации личности клиента используют услуги ЦОИД по предоставлению биометрической аутентификации при:

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

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

3) превышении суммы банковского займа размера, установленного нормативным правовым актом уполномоченного органа по регулированию, контролю и надзору финансового рынка и финансовых организаций;

4) проведении банком периодических обновлений данных клиента в соответствии с Законом о ПОД/ФТ/ФРОМУ.

В случае, если клиент ранее не был идентифицирован при личном присутствии в банке или с применением биометрической аутентификации посредством ЦОИД, то

банком создание электронной цифровой подписи клиента и выдача сертификата электронной цифровой подписи осуществляется при прохождении клиентом биометрической аутентификации посредством ЦОИД.

Согласие клиента на создание ключей электронной цифровой подписи и выдачу сертификата электронной цифровой подписи, в том числе полученных при личном присутствии клиента в банке, хранится в ЦОИД с возможностью отзыва клиентом ранее выданных согласий.

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

Банки обеспечивают хранение информации о согласиях клиентов, фотоизображения клиента с использованием технологии выявления движения и записи сеанса видеоконференции с клиентом, а также о результатах биометрической аутентификации, используемых при оказании электронных банковских услуг, не менее пяти лет со дня прекращения деловых отношений с клиентом.

24. В случаях, предусмотренных пунктом 23 Правил, банк получает согласие клиента на проведение биометрической аутентификации и согласие клиента на сбор, обработку и представление, в том числе при необходимости третьим лицам, его персональных данных, подтвержденные посредством идентификационного средства.

Банк проводит с клиентом с использованием имеющихся у клиента устройств и ( или) иных устройств банка сеанс видеоконференции либо использует технологию выявления движения клиента (Liveness Detection) 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 банками, устанавливаются банками самостоятельно.

Банк передает в ЦОИД индивидуальный либо бизнес-идентификационный номер клиента и фотоизображение клиента, полученное из сеанса видеоконференции либо с помощью технологии выявления движения (Liveness Detection) интервьюируемого в процессе биометрической аутентификации.

ЦОИД посредством программного обеспечения определяет степень соответствия по биометрическим показателям фотоизображения, полученного из сеанса видеоконференции либо при использовании технологии выявления движения клиента, с фотоизображением клиента из доступных источников. Видеозаписи обращений клиентов хранятся в банке.

Банками передаются в ЦОИД согласия клиента:

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

на проведение биометрической аутентификации клиента с использованием ЦОИД;

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

ЦОИД осуществляет сбор и регистрацию согласий клиента, предусмотренных частью 6 настоящего пункта Правил, с возможностью их отзыва клиентом в соответствии с законодательством Республики Казахстан.

Биометрическая аутентификация посредством ЦОИД осуществляется с использованием доступных источников и (или) биометрических данных национальной системы биометрической аутентификации, функционирование которой предусмотрено Цифровым кодексом Республики Казахстан (далее – национальная система биометрической аутентификации).

Фотоизображения клиентов, переданные банками в ЦОИД из сеанса видеоконференции либо с помощью технологии выявления движения (Liveness Detection), используются ЦОИД для целей биометрической аутентификации и (или) наполнения базы биометрических данных национальной системы биометрической аутентификации.

Банки получают сведения о результатах биометрической аутентификации посредством ЦОИД в соответствии с Правилами ЦОИД.

25. Допускается предоставление ЦОИД дополнительных сервисов банкам для идентификации клиента, предусмотренных Правилами ЦОИД. Правила ЦОИД размещаются на официальном интернет-ресурсе национального центра по управлению национальной цифровой финансовой инфраструктурой.

26. При предоставлении банком электронных банковских услуг банк использует систему и (или) программно-технические средства, автоматизирующие процесс противодействия несанкционированным платежам и (или) переводам денег.

## Глава 4. Оказание платежных услуг и информационных банковских услуг сторонним поставщиком платежных услуг

27. Допускается оказание клиенту с его согласия электронных банковских услуг сторонним поставщиком платежных услуг посредством системы открытого банкинга.

Банк при взаимодействии с системой открытого банкинга использует ЦОИД для регистрации согласия на обмен информацией о банковских счетах и иных сведениях, содержащих персональные данные и банковскую тайну, а также на инициирование платежей и переводов денег через систему удаленного доступа стороннего поставщика платежных услуг.

28. Сторонним поставщиком платежных услуг оказываются следующие электронные услуги:

предоставление доступа к информации о банковских счетах клиента, открытых у других поставщиков платежных услуг (далее – услуга по агрегации счетов);

предоставление клиенту возможности инициирования платежа и (или) перевода денег по запросу клиента с его банковского счета, открытого у другого поставщика платежных услуг;

информационные банковские услуги.

Электронные услуги, указанные в абзаце втором и третьем части первой настоящего пункта, не предоставляются по банковским счетам, режим функционирования которых в системе удаленного доступа поставщика платежных услуг не поддерживает возможности предоставления информации в режиме реального времени.

29. Электронные банковские услуги через систему открытого банкинга оказываются при выполнении следующих условий:

1) наличие стороннего поставщика платежных услуг, получающего доступ к банковскому счету клиента, в реестре поставщиков платежных услуг, авторизованных в системе открытого банкинга;

2) наличие согласия клиента на сбор и обработку персональных данных и информации, составляющей банковскую тайну, предоставленного через систему открытого банкинга и подтвержденного посредством идентификационного средства ( далее – согласие клиента, предоставленное посредством системы открытого банкинга).

30. Авторизация стороннего поставщика платежных услуг включает его проверку оператором системы открытого банкинга на соответствие операционной документации наличие положительных актов тестирования, прохождение первым руководителем стороннего поставщика платежных услуг регистрации в системе открытого банкинга путем двухфакторной аутентификации.

Оператор ведет реестр поставщиков платежных услуг, авторизованных в системе открытого банкинга, и размещает его на своем интернет-ресурсе.

31. Оператор системы открытого банкинга отказывает стороннему поставщику платежных услуг в авторизации для работы в системе открытого банкинга в следующих случаях:

1) несоответствия требованиям операционной документации оператора системы открытого банкинга;

2) непредставления либо представления недостоверных сведений и (или) документов, необходимых для авторизации в системе открытого банкинга;

3) непрохождения тестирования системы открытого банкинга;

4) несоблюдения необходимых мер защиты информации;

5) наличия фактов неисполнения либо ненадлежащего исполнения обязательств сторонним поставщиком платежных услуг в иных платежных системах Национального Банка;

6) наличия решения государственного органа, осуществляющего государственное регулирование, контроль и надзор финансового рынка и финансовых организаций, о

приостановлении действия или лишении лицензии на проведение банковских операций
.

32. Согласие клиента, предоставленное посредством системы открытого банкинга, содержит:

1) наименование стороннего поставщика платежных услуг, которому дается согласие;

2) номер банковского счета, к которому предоставляется доступ;

3) вид услуги, на оказание которой предоставляется согласие клиента;

4) дату и время предоставления, а также срок действия согласия.

33. Для инициирования электронной банковской услуги через систему удаленного доступа стороннего поставщика платежных услуг клиент авторизуется в системе удаленного доступа стороннего поставщика платежных услуг способом, установленным в договоре между ними.

34. После авторизации в системе удаленного доступа стороннего поставщика платежных услуг клиент предоставляет согласие на сбор и обработку данных посредством системы открытого банкинга.

35. При получении либо наличии ранее полученного согласия клиента, предоставленного посредством системы открытого банкинга, на основании запроса стороннего поставщика платежных услуг оператор системы открытого банкинга направляет запрос поставщику платежных услуг, обслуживающему банковский счет клиента, на получение запрошенной клиентом информации.

Информацию, полученную по результатам оказания услуги от поставщика платежных услуг, обслуживающего банковский счет клиента, оператор системы открытого банкинга передает стороннему поставщику платежных услуг с соблюдением операционной документации оператора системы открытого банкинга.

36. При инициировании клиентом услуги по агрегации счетов сторонний поставщик платежных услуг в своей системе удаленного доступа уведомляет клиента о результате оказания услуги и отображает клиенту соответствующую информацию.

37. При инициировании клиентом платежа и (или) перевода денег поставщик платежных услуг, обслуживающий банковский счет клиента, исполняет указание клиента, поступившее через систему удаленного доступа стороннего поставщика платежных услуг, в порядке и сроки, установленные Законом о платежах и платежных системах, с соблюдением операционной документации оператора системы открытого банкинга.

38. При непредставлении клиентом согласия на сбор и обработку данных в системе открытого банкинга электронная банковская услуга не оказывается.

39. Максимальный срок действия согласия клиента, предоставленного посредством системы открытого банкинга, составляет не более тридцати календарных дней.

Клиент имеет право в любое время до истечения срока действия отозвать предоставленное согласие путем инициирования соответствующего запроса в системе открытого банкинга.

После истечения срока действия согласия сторонний поставщик платежных услуг не вправе использовать ранее полученную информацию, кроме как для целей хранения в соответствии с требованиями законодательства Республики Казахстан.

40. Все согласия клиента на сбор и обработку данных и отзывы таких согласий регистрируются и хранятся оператором в системе открытого банкинга.

41. Сторонний поставщик платежных услуг обеспечивает использование данных клиента исключительно в соответствии с целью сбора этих данных.

42. Сторонний поставщик платежных услуг несет ответственность перед клиентом и поставщиком платежных услуг, обслуживающим банковский счет клиента, за последствия осуществления несанкционированных платежей и (или) мошеннических действий по платежам и (или) переводам денег, инициированным через его систему удаленного доступа.

## Глава 5. Процедуры безопасности

43. Предоставление банком электронных банковских услуг производится в соответствии с процедурами безопасности, установленными внутренними документами банка и договором.

44. Процедуры безопасности обеспечивают:

1) достоверную идентификацию (аутентификацию) клиента и его право на получение соответствующих электронных банковских услуг;

2) выявление наличия искажений и (или) изменений в содержании электронных документов, на основании которых клиенту предоставляются электронные банковские услуги;

3) защиту от несанкционированного доступа к персональным данным и информации, составляющей банковскую тайну, и целостность данной информации.

45. Предоставление электронных банковских услуг является санкционированным в случае выполнения клиентом процедур безопасности, установленных внутренними документами банка и договором.

46. Банк обеспечивает хранение подтверждения об отправке и (или) получении сообщений, на основании которых клиенту предоставлены электронные банковские услуги.

47. В интернет-ресурсе или мобильном приложении банк предоставляет клиенту подтверждение оказания электронных банковских услуг в порядке и сроки, предусмотренные договором.

48. При предоставлении физическим и юридическим лицам электронных банковских услуг либо платежных услуг банками обеспечиваются процедуры

безопасности от несанкционированного доступа к электронным банковским услугам и ( или) платежам и переводам денег.

## Глава 6. Меры от несанкционированного доступа

49. При обнаружении несанкционированного доступа к персональным данным и информации, составляющей банковскую тайну, их несанкционированного изменения, осуществления платежа с признаками мошенничества или несанкционированного платежа и (или) перевода денег и иных несанкционированных действий, банк уведомляет об этом клиента, в отношении которого были допущены такие действия, не позднее следующего рабочего дня после их обнаружения.

50. В случае возникновения несанкционированных действий, указанных в пункте 49 Правил, банк незамедлительно принимает все необходимые меры для устранения их последствий и предотвращения их допущения в будущем.

## Глава 7. Приостановление и прекращение предоставления электронных банковских услуг

51. Банк приостанавливает или прекращает предоставление клиенту электронных банковских услуг в случаях:

1) нарушения клиентом порядка и условий получения электронных банковских услуг, предусмотренных договором;

2) неисправности технических средств, обеспечивающих оказание электронных банковских услуг;

3) по иным основаниям, предусмотренным законами о банках и банковской деятельности, о платежах и платежных системах, о ПОД/ФТ/ФРОМУ, Гражданским кодексом Республики Казахстан (Особенная часть) и договором.

52. В случае приостановления или прекращения предоставления электронных банковских услуг по основаниям, предусмотренным пунктом 51 Правил, банк уведомляет клиента в порядке и сроки, установленные договором, за исключением случаев приостановления или прекращения предоставления электронных платежных услуг, предусмотренных подпунктом 3) пункта 51 Правил.

53. При устранении причин, повлекших приостановление права клиента на получение электронных банковских услуг, банк возобновляет оказание клиенту электронных банковских услуг с последующим его уведомлением письменно либо в электронной форме, за исключением случаев приостановления или прекращения предоставления электронных платежных услуг, предусмотренных подпунктом 3) пункта 51 Правил.

## Глава 8. Хранение электронных документов при предоставлении электронных банковских услуг

54. Электронные документы хранятся в том формате, в котором они были сформированы, отправлены или получены с соблюдением их целостности и неизменности и не требуют распечатки или иного отображения содержания электронного документа на бумажном носителе с целью хранения.

55. Порядок и сроки хранения электронных документов определяются внутренними документами банка, разработанными в соответствии с Законом о платежах и платежных системах и Законом о ПОД/ФТ/ФРОМУ.

Приложение 3
к Перечню некоторых
постановлений Правления
Национального Банка
Республики Казахстан,
в которые вносятся изменения
и дополнения по вопросам
платежей и платежных услуг
Приложение 1
к Правилам организации
деятельности
платежных организаций
Форма
Национальный Банк
Республики Казахстан

**Заявление**

_____

(наименование и бизнес-идентификационный номер платежной организации)
просит осуществить учетную регистрацию платежной организации и включить платежную организацию в реестр платежных организаций

1. Место нахождения платежной организации:

_____

_____

(индекс, город (область), район, улица, номер дома (офиса)

_____

_____

(телефон, факс, адрес электронной почты, интернет-ресурс (при наличии)

2. Сведения о государственной регистрации (перерегистрации) платежной организации:

_____

_____

(наименование документа, номер и дата выдачи, кем выдан)

3. Перечень планируемых к оказанию платежных услуг в соответствии с пунктом 3 Правил организации деятельности платежных организаций:

1) _____;
2) _____;
3) _____

4. Перечень представляемых документов в соответствии с пунктом 2 статьи 16 Закона Республики Казахстан "О платежах и платежных системах":
1) _____;
2) _____;

5. Сведения о руководителе (членах) исполнительного органа платежной организации:

Общие сведения:

| | |
|---|---|
| Фамилия, имя, отчество (при его наличии) | _____<br>(в соответствии с документом, удостоверяющим личность,<br>в случае изменения фамилии, имени, отчества - указать,<br>когда и по какой причине произошли изменения) |
| Индивидуальный идентификационный номер | |
| Данные документа, удостоверяющего личность | (наименование документа, номер, серия (при наличии)<br>и дата выдачи, кем выдан) |
| Место жительства | (место жительства, включая номера домашнего, служебного<br>телефонов, а также адрес электронной почты) |
| Гражданство | |

Полный перечень места работ и должностей:

| № | Период работы (месяц/год) | Наименование организации, занимаемые должности | Должностные обязанности |
|---|---|---|---|
| 1 | | | |

Иная информация:

| | |
|---|---|
| Наличие неснятой или непогашенной судимости | Да/нет<br>(если да, то указать реквизиты приговора суда, статью Уголовного кодекса Республики Казахстан) |
| Если ранее являлся руководителем, членом органа управления, руководителем, членом исполнительного органа, главным бухгалтером финансовой организации в период не более чем за один год до принятия решения о применении к банку режима урегулирования, лишении лицензии финансовой организации, повлекших ее ликвидацию и (или) прекращение осуществления деятельности на финансовом рынке, либо вступления в законную силу судебного акта о принудительной ликвидации финансовой организации или признании ее банкротом в порядке, | Да/нет<br>(если да, то указывается наименование организации, должность, реквизиты решения о применении к банку режима урегулирования, лишении лицензии финансовой организации, повлекших ее ликвидацию и (или) прекращение осуществления деятельности на финансовом рынке, либо вступившего в законную силу судебного акта о принудительной ликвидации финансовой организации или признании ее банкротом в порядке, определенном законодательством Республики |

| | |
|---|---|
| определенном законодательством Республики Казахстан или законодательством государства, резидентом которого является финансовая организация – нерезидент Республики Казахстан | Казахстан или законодательством государства, резидентом которого является финансовая организация-нерезидент Республики Казахстан) |
| Если ранее являлся руководителем исполнительного органа, учредителем или первым руководителем учредителя – юридического лица платежной организации, крупным участником либо первым руководителем крупного участника – юридического лица платежной организации в период не более чем за пять лет до ее исключения из реестра платежных организаций по основаниям, предусмотренным подпунктами 1) – 6), 9), 11) пункта 1 статьи 18 Закона о платежах и платежных системах либо платежной организации, ликвидированной на основании вступившего в законную силу судебного акта или признанной банкротом в порядке, установленном законодательством Республики Казахстан | Да/нет<br>(если да, то указывается наименование организации, должность, реквизиты решения уполномоченного органа либо вступившего в законную силу судебного акта о принудительной ликвидации платежной организации или признании ее банкротом в порядке, установленном законодательством Республики Казахстан) |
| Иная информация (при наличии) | |

Подтверждаю, что прилагаемые сведения мною проверены и являются достоверными и полными.

Согласен (согласна) на использование сведений, составляющих охраняемую законом тайну, содержащихся в цифровых системах.

Первый руководитель платежной организации
или лицо, уполномоченное на подписание

_____ _____

фамилия, имя, отчество (при его наличии) подпись

6. Сведения об учредителях (участниках) платежной организации:

| | |
|---|---|
| Фамилия, имя, отчество (при его наличии) / Наименование юридического лица / Наименование иностранной структуры без образования юридического лица | _____<br>(в соответствии с документом, удостоверяющим личность, в случае изменения фамилии, имени, отчества – указать, когда и по какой причине произошли изменения / в соответствии с учредительными документами) |
| Индивидуальный идентификационный номер / Бизнес идентификационный номер / Идентификационный номер | |
| Данные документа, удостоверяющего личность | (наименование документа, номер, серия (при наличии) и дата выдачи, кем выдан) |
| Место жительства / Место регистрации юридического лица или иностранной структуры без образования юридического лица | (место жительства, включая номера домашнего, служебного телефонов, а также адрес электронной почты / место регистрации юридического лица или иностранной структуры без образования юридического лица, включая номера служебного телефона, а также адрес электронной почты) |
| Гражданство / Страна регистрации | |
| | |

| | |
|---|---|
| Наличие неснятой или непогашенной судимости либо вступившее в законную силу решение суда о применении уголовного наказания в виде лишения права занимать должность руководящего работника финансовой организации, банковского и (или) страхового холдинга и являться крупным участником (крупным акционером) финансовой организации | Да/нет<br>(если да, то указать реквизиты приговора суда, статью Уголовного кодекса Республики Казахстан) |
| Если ранее являлся руководителем, членом органа управления, руководителем, членом исполнительного органа, главным бухгалтером финансовой организации, руководителем или заместителем руководителя филиала банка-нерезидента Республики Казахстан, филиала страховой (перестраховочной) организации-нерезидента Республики Казахстан, филиала страхового брокера-нерезидента Республики Казахстан в период не более чем за один год до принятия уполномоченным органом решения о применении к банку режима урегулирования, лишении лицензии финансовой организации, филиала банка-нерезидента Республики Казахстан, филиала страховой (перестраховочной) организации-нерезидента Республики Казахстан, филиала страхового брокера-нерезидента Республики Казахстан, либо вступления в законную силу судебного акта о принудительной ликвидации финансовой организации или признании ее банкротом в установленном законодательством Республики Казахстан порядке, либо вступления в законную силу судебного акта о принудительном прекращении деятельности филиала банка-нерезидента Республики Казахстан, филиала страховой (перестраховочной) организации-нерезидента Республики Казахстан в случаях, установленных законами Республики Казахстан | Да/нет<br>(если да, то указывается наименование организации, должность, реквизиты решения о применении к банку режима урегулирования, лишении лицензии финансовой организации, филиала банка-нерезидента Республики Казахстан, филиала страховой (перестраховочной) организации-нерезидента Республики Казахстан, филиала страхового брокера-нерезидента Республики Казахстан, либо вступившего в законную силу судебного акта о принудительной ликвидации финансовой организации или признании ее банкротом в установленном законодательством Республики Казахстан порядке либо вступившего в законную силу судебного акта о принудительном прекращении деятельности филиала банка-нерезидента Республики Казахстан, филиала страховой (перестраховочной) организации-нерезидента Республики Казахстан в случаях, установленных законами Республики Казахстан |
| Если ранее являлся учредителем или первым руководителем учредителя – юридического лица платежной организации, крупным участником либо первым руководителем крупного участника – юридического лица и (или) руководителем органа управления, руководителем исполнительного органа платежной организации в период не более чем за пять лет до ее исключения из реестра платежных организаций по основаниям, предусмотренным подпунктами 1) – 6), 9), 11) пункта 1 статьи 18 Закона о платежах и платежных системах либо платежной организации, ликвидированной на основании вступившего в законную силу судебного акта или признанной банкротом в порядке, установленном законодательством Республики Казахстан | Да/нет<br>(если да, то указывается наименование организации, должность, реквизиты решения уполномоченного органа либо вступившего в законную силу судебного акта о принудительной ликвидации платежной организации или признании ее банкротом в порядке, установленном законодательством Республики Казахстан) |
| Если имеет регистрацию, место жительства или место нахождения в офшорных зонах | Да/нет<br>(если да, то указывается наименование офшорной зоны) |

Приложение 4
к Перечню некоторых
постановлений Правления
Национального Банка
Республики Казахстан,
в которые вносятся
изменения и дополнения
Приложение 2
к Правилам организации
деятельности
платежных организаций
Форма

## Перечень основных требований к оказанию государственной услуги "Включение в реестр платежных организаций, прошедших учетную регистрацию в Национальном Банке Республики Казахстан"

| | | |
|---|---|---|
| 1. | Наименование услугодателя | Национальный Банк Республики Казахстан |
| 2. | Способы предоставления государственной услуги | Веб-портал "цифрового правительства" www.egov.kz, www.elicense.kz ( далее - портал). |
| 3. | Срок оказания государственной услуги | В течение пятнадцати рабочих дней со дня регистрации заявления и полного перечня документов. |
| 4. | Форма оказания государственной услуги | Электронная (автоматизированная ). |
| 5. | Результат оказания государственной услуги | Уведомление о прохождении учетной регистрации для предоставления разрешения ( права) на предоставление платежной организацией платежных услуг, установленных Законом Республики Казахстан "О платежах и платежных системах" ( далее – Закон) либо мотивированный отказ.<br>Форма результата оказания государственной услуги: электронная |
| 6. | Размер платы, взимаемой с услугополучателя при оказании государственной услуги, и способы ее взимания в случаях, предусмотренных законодательством Республики Казахстан | Услуга оказывается бесплатно. |
| | | 1) услугодателя – с понедельника по пятницу с 9.00 до 18.30 часов с |

| | | |
|---|---|---|
| 7. | График работы услугодателя, Государственной корпорации и цифровых объектов | перерывом на обед с 13.00 до 14.30 часов, кроме выходных и праздничных дней, в соответствии с трудовым законодательством Республики Казахстан.<br>График приема документов и выдачи результатов оказания государственной услуги – с понедельника по пятницу с 9.00 до 17.30 часов с перерывом на обед с 13.00 до 14.30 часов;<br>2) портала – круглосуточно, за исключением технических перерывов в связи с проведением ремонтных работ (при обращении услугополучателя после окончания рабочего времени, в выходные и праздничные дни, согласно трудовому законодательству Республики Казахстан, прием заявлений и выдача результатов оказания государственной услуги осуществляется на следующий рабочий день). |
| | | 1) заявление по форме согласно приложению 1 к Правилам организации деятельности платежных организаций, утвержденным постановлением Правления Национального Банка Республики Казахстан № 215 от 31 августа 2016 года (далее – Правила).<br>2) копия диплома (дипломов) руководителя (члена) исполнительного органа платежной организации;<br>3) копия документа, подтверждающего трудовую деятельность руководителя (члена) исполнительного органа платежной организации в соответствии с Трудовым кодексом Республики Казахстан;<br>4) копии документов, подтверждающих формирование уставного капитала;<br>5) устав;<br>6) документ, определяющий порядок взаимодействия платежной организации с соответствующим банком, |

| | | |
|---|---|---|
| 8. | Перечень документов, необходимых для оказания государственной услуги | филиалом банка-нерезидента Республики Казахстан или организацией, осуществляющей отдельные виды банковских операций, осуществляющими перевод денег по оказываемым платежным услугам;<br>7) сведения и документы, подтверждающие наличие в штате (приема на работу) руководителя структурного подразделения, отвечающего за администрирование цифровых объектов, и руководителя службы комплаенс-контроля или иного лица, на которое возлагается проведение комплаенс-контроля;<br>8) правила внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения для платежных организаций;<br>9) правила осуществления деятельности платежной организации, утвержденные органом управления платежной организации.<br>Перечень обязательных условий правил осуществления деятельности платежной организации, устанавливается в Правилах. |
| | | 1) представление неполных и (или) недостоверных сведений, подлежащих отражению в документах, указанных в пункте 2 статьи 16 Закона;<br>2) представление неполного перечня документов или несоответствие документов требованиям Закона и Правил;<br>3) если руководитель исполнительного органа платежной организации не соответствует требованиям, установленным в статье 19 Закона;<br>4) если платежная организация в течение одного года со дня ее государственной регистрации ( |

| | | |
|---|---|---|
| 9. | Основания для отказа в оказании государственной услуги, установленные законами Республики Казахстан | перерегистрации) в Государственной корпорации " Правительство для граждан" не обратилась с заявлением о прохождении учетной регистрации.<br>В случае отказа в учетной регистрации юридическое лицо повторно представляет заявление на учетную регистрацию при устранении причин, повлекших отказ в учетной регистрации платежной организации, или принимает решение об изменении своего наименования либо реорганизации или ликвидации.<br>Неустранение причин, повлекших отказ в учетной регистрации платежной организации, является основанием для отказа в повторном рассмотрении. |
| 10. | Иные требования с учетом особенностей оказания государственной услуги, в том числе оказываемой в электронной форме и через Государственную корпорацию | Адреса мест оказания государственной услуги размещены на портале и на официальном интернет-ресурсе услугодателя: www.nationalbank.kz , раздел "Государственные услуги" .<br>Услугополучателю открыт доступ для получения информации о порядке и статусе оказания государственной услуги в режиме удаленного доступа посредством Единого контакт-центра по вопросам оказания государственных услуг.<br>Контактные телефоны справочных служб по вопросам оказания государственной услуги размещены на официальном интернет-ресурсе услугодателя: www.nationalbank.kz, раздел " Государственные услуги". Единый контакт-центр по вопросам оказания государственных услуг: 8-800-080-7777, 1414. |

Приложение 5
к Перечню некоторых
постановлений Правления
Национального Банка
Республики Казахстан,

в которые вносятся изменения
и дополнения по вопросам
платежей и платежных услуг
Приложение 6
к Правилам организации
деятельности
платежных организаций
Форма
Национальный Банк
Республики Казахстан

**Уведомление об открытии филиала**

_____

(наименование, место нахождения и бизнес-идентификационный
номер платежной организации)
настоящим сообщает об открытии филиала:
□ на территории Республики Казахстан (в случае открытия):

_____

(наименование, место нахождения и бизнес-идентификационный
номер филиала платежной организации)
Данные о руководителе:

_____

(должность, фамилия, имя, отчество (при его наличии)
Перечень платежных услуг, оказываемых филиалом платежной организации,
в соответствии с пунктом 3 Правил организации деятельности платежных
организаций:
1) _____;
2) _____;
3) _____.
□ за пределами Республики Казахстан (в случае открытия):

_____

(наименование, место нахождения филиала платежной организации)
Данные о руководителе:

_____

(должность, фамилия, имя, отчество (при его наличии)
Перечень платежных услуг, оказываемых филиалом платежной организации
в соответствии с пунктом 3 Правил организации деятельности платежных
организаций:
1) _____;
2) _____;
3) _____.

Подтверждаю, что прилагаемые сведения мною проверены и являются достоверными и полными.
Согласен (согласна) на использование сведений, составляющих охраняемую законом тайну, содержащихся в цифровых системах.
Первый руководитель платежной организации или лицо, уполномоченное на подписание

_____ _____
фамилия, имя, отчество (при его наличии) подпись

Приложение 6
к Перечню некоторых
постановлений Правления
Национального Банка
Республики Казахстан,
в которые вносятся изменения
и дополнения по вопросам
платежей и платежных услуг
Приложение 7
к Правилам организации
деятельности
платежных организаций
Форма

## Карта инцидента кибербезопасности

| № | Общие сведения | |
|---|---|---|
| | Характеристики инцидента кибербезопасности | Информация об инциденте кибербезопасности |
| 1 | Наименование инцидента кибербезопасности | |
| 2 | Дата и время выявления ( дд.мм.гггг и чч:мм с указанием часового пояса UTC+X) | |
| 3 | Место выявления (организация, филиал, сегмент цифровой инфраструктуры) | |
| 4 | Источник информации об инциденте кибербезопасности ( пользователь, администратор, администратор кибербезопасности , работник подразделения кибербезопасности или техническое средство) | |
| 5 | Использованные методы при реализации инцидента кибербезопасности (социальная инженерия, внедрение вредоносного кода) | |
| Содержание инцидента кибербезопасности | | |

| | | |
|---|---|---|
| 6 | Симптомы, признаки инцидента кибербезопасности | |
| 7 | Основные события (эксплуатация уязвимостей в прикладном и системном программном обеспечении;<br>несанкционированный доступ в цифровую систему;<br>атака "отказ в обслуживании" на цифровую систему или сеть передачи данных;<br>заражение сервера вредоносной программой или кодом;<br>совершение несанкционированного перевода денежных средств;<br>инциденты кибербезопасности, несущие угрозу стабильности деятельности платежной организации) | |
| 8 | Пораженные активы (физический уровень цифровой инфраструктуры, уровень сетевого оборудования, уровень сетевых приложений и сервисов, уровень операционных систем, уровень технологических процессов и приложений и уровень бизнес-процессов платежной организации) | |
| 9 | Статус инцидента кибербезопасности ( свершившийся инцидент кибербезопасности, попытка осуществления инцидента кибербезопасности, подозрение на инцидент кибербезопасности) | |
| 10 | Ущерб | |
| 11 | Источник угрозы (выявленные идентификаторы) | |
| 12 | Преднамеренность (намеренный, ошибочный) | |
| Предпринятые меры по инциденту кибербезопасности | | |
| 13 | Предпринятые действия ( идентификация уязвимости, блокирование, восстановление) | |
| 14 | Запланированные действия, направленные на минимизацию возникновения рисков кибербезопасности | |
| | | |

| | | |
|---|---|---|
| 15 | Оповещенные лица (фамилия, имя, отчество (при его наличии) должностных лиц, наименование государственных органов, организаций) | |
| 16 | Привлеченные специалисты (фамилия, имя, отчество (при его наличии) место работы, должность, номер телефона) | |

Ответственный работник по кибербезопасности

_____ _____

(фамилия, имя, отчество (при его наличии) (подпись)

Дата "____" _____ 20 ___ года