«ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҰЛТТЫҚ БАНКІ»

РЕСПУБЛИКАЛЫҚ МЕМЛЕКЕТТІК МЕКЕМЕСІ

БАСҚАРМАСЫНЫҢ ҚАУЛЫСЫ

31 августа 2016 года

Алматы қаласы

РЕСПУБЛИКАНСКОЕ ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ

«НАЦИОНАЛЬНЫЙ БАНК РЕСПУБЛИКИ КАЗАХСТАН»

ПОСТАНОВЛЕНИЕ ПРАВЛЕНИЯ

№ 200

город Алматы

Об утверждении Требований к организационным мерам и программно-техническим средствам, обеспечивающим доступ в платежные системы

Зарегистрировано Министерством юстиции Республики Казахстан 5 октября 2016 года за № 14289

(с изменениями и дополнениями по состоянию на 27.08.2018 г.)

В соответствии с законами Республики Казахстан от 30 марта 1995 года «О Национальном Банке Республики Казахстан», от 26 июля 2016 года «О платежах и платежных системах», в целях установления требований к организационным мерам и программно-техническим средствам, обеспечивающим доступ в платежные системы Правление Национального Банка Республики Казахстан **ПОСТАНОВЛЯЕТ**:

1. Утвердить прилагаемые Требования к организационным мерам и программно-техническим средствам, обеспечивающим доступ в платежные системы, (далее - Требования).

2. Признать утратившими силу:

1) постановление Правления Национального Банка Республики Казахстан от 24 августа 2012 года № 269 «Об утверждении Требований к организационным мерам и программно-техническим средствам, обеспечивающим доступ в платежные системы» (зарегистрированное в Реестре государственной регистрации нормативных правовых актов под № 7950, опубликованное 8 декабря 2012 года в газете «Казахстанская правда» № 427-428 (27246-27247);

2) постановление Правления Национального Банка Республики Казахстан от 28 января 2016 года № 35 «О внесении изменений и дополнений в постановление Правления Национального Банка Республики Казахстан от 24 августа 2012 года № 269 «Об утверждении Требований к организационным мерам и программно-техническим средствам, обеспечивающим доступ банкам и организациям, осуществляющим отдельные виды банковских операций, в платежные системы» (зарегистрированное в Реестре государственной регистрации нормативных правовых актов № 13187, опубликованное 14 марта 2016 года в информационно-правовой системе «Әділет» республиканского государственного предприятия на праве хозяйственного ведения «Республиканский центр правовой информации Министерства юстиции Республики Казахстан»).

3. Департаменту платежных систем (Ашыкбеков Е.Т.) в установленном законодательством Республики Казахстан порядке обеспечить:

1) совместно с Юридическим департаментом (Сарсенова Н.В.) государственную регистрацию настоящего постановления в Министерстве юстиции Республики Казахстан;

2) направление настоящего постановления в республиканское государственное предприятие на праве хозяйственного ведения «Республиканский центр правовой информации Министерства юстиции Республики Казахстан»:

на официальное опубликование в информационно-правовой системе «Әділет» в течение десяти календарных дней после его государственной регистрации в Министерстве юстиции Республики Казахстан;

для включения в Государственный реестр нормативных правовых актов Республики Казахстан, Эталонный контрольный банк нормативных правовых актов Республики Казахстан в течение десяти календарных дней со дня его государственной регистрации в Министерстве юстиции Республики Казахстан;

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

4. Управлению по защите прав потребителей финансовых услуг и внешних коммуникаций (Терентьев А.Л.) обеспечить направление настоящего постановления на официальное опубликование в периодические печатные издания в течение десяти календарных дней после его государственной регистрации в Министерстве юстиции Республики Казахстан.

5. Контроль за исполнением настоящего постановления возложить на заместителя Председателя Национального Банка Республики Казахстан Пирматова Г.О.

6. Настоящее постановление вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования, за исключением пунктов 58, 59, 60, 61, 62, 63 и 64 Требований, которые вводятся в действие с 1 января 2017 года.

Председатель
Национального Банка **Д. Акишев**

Утверждены
постановлением Правления
Национального Банка
Республики Казахстан
от 31 августа 2016 года № 200

Требования к организационным мерам и программно-техническим средствам, обеспечивающим доступ в платежные системы

Глава 1. Общие положения
Глава 2. Размещение рабочего места пользователя платежной системы
Глава 3. Взаимодействие пользователя платежной системы и Центра
Глава 4. Терминал платежной системы
Глава 5. Ключевая информация
Глава 6. Требования к рабочему месту пользователя платежной системы
Глава 7. Организация работы обслуживающего персонала
Глава 8. Требования к управлению операционным риском и обеспечению непрерывности деятельности пользователя платежной системы
Глава 9. Заключительные положения

Глава 1. Общие положения

1. Требования к организационным мерам и программно-техническим средствам, обеспечивающим доступ в платежные системы, (далее - Требования) разработаны в соответствии с законами Республики Казахстан от 30 марта 1995 года «О Национальном Банке Республики Казахстан» (далее - Закон о Национальном Банке), от 26 июля 2016 года «О платежах и платежных системах» (далее - Закон о платежах и платежных системах) и определяют требования к организационным мерам и программно-техническим средствам, обеспечивающим доступ в платежные системы, оператором которых выступает Национальный Банк Республики Казахстан, (далее - платежная система).

Требования включают размещение рабочего места пользователя платежной системы, взаимодействие пользователя платежной системы и республиканского государственного предприятия на праве хозяйственного ведения «Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан» (далее - Центр), терминал платежной системы, ключевую информацию, требования к рабочему месту пользователя платежной системы, организацию работ обслуживающего персонала, требования к управлению операционным риском и обеспечению непрерывности деятельности пользователя платежной системы.

2. Требования распространяются на всех пользователей платежной системы.

3. В Требованиях используются понятия, предусмотренные Законом о платежах и платежных системах, и следующие понятия:

1) аутентификация - комплекс мер для подтверждения подлинности пользователей системы при обмене платежными и информационными сообщениями, а также для подтверждения подлинности платежных и информационных сообщений;

2) удостоверяющий центр - юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства;

3) средства контроля доступа - технические, программные или другие средства, позволяющие фиксировать информацию о доступе к объектам;

4) ключевая информация - криптографические ключи (открытые и закрытые) или другая информация, позволяющая осуществлять криптографические преобразования информации;

5) операционный риск - риск, связанный с нарушениями в работе информационных систем или внутренних процессов, ошибками, сбоями или нарушениями в управлении платежной системой, в том числе вследствие внешних событий;

6) несанкционированный доступ - доступ к информационным и программным ресурсам с нарушением законодательства Республики Казахстан, а также порядка доступа к ним, установленным пользователем платежной системы;

7) программно-аппаратный комплекс защиты от несанкционированного доступа - система защиты персонального компьютера от использования посторонними лицами, а также для разграничения полномочий зарегистрированных пользователей по доступу к информационным и программным ресурсам;

8) нестандартная ситуация - сбой (нарушение) функционирования программно-технического комплекса пользователя платежной системы вследствие реализации операционного риска;

9) пользователь платежной системы - юридические лица, заключившие договор с Центром об оказании услуг в платежной системе, и оператор (операционный центр) других платежных систем;

10) информационная система пользователя платежной системы - программное обеспечение пользователя платежной системы, используемое для формирования или преобразования электронных документов, предназначенных для дальнейшего направления в платежную систему посредством терминала платежной системы;

11) программно-технический комплекс пользователя платежной системы - технические, программные или другие средства, обеспечивающие работу пользователя платежной системы в платежной системе, включающие информационную систему, рабочее место пользователя платежной системы, средства коммуникации (передачи данных) с платежной системой;

12) основной центр программно-технического комплекса пользователя платежной системы (далее - основной центр) - программно-технический комплекс пользователя платежной системы, обеспечивающий работу пользователя платежной системы в платежной системе в обычном (повседневном) режиме;

13) резервный центр программно-технического комплекса пользователя платежной системы (далее - резервный центр) - резервный программно-технический комплекс пользователя платежной системы, обеспечивающий работу пользователя платежной системы в платежной системе при возникновении нестандартных ситуаций или проведении плановых тестовых работ в основном центре;

14) рабочее место пользователя платежной системы - персональный компьютер (сервер), на котором установлен терминал платежной системы, обеспечивающий доступ в платежную систему;

15) администратор рабочего места пользователя платежной системы - лицо, непосредственно осуществляющее администрирование терминала платежной системы;

16) офицер безопасности рабочего места пользователя платежной системы - лицо, обеспечивающее установку и функционирование на рабочем месте пользователя платежной системы программно-аппаратного комплекса защиты информации от несанкционированного доступа, средств защиты информации от утечки по электромагнитным каналам, а также осуществляющее мониторинг за их работоспособностью и за выполнением требований безопасности;

17) оператор рабочего места пользователя платежной системы - лицо, непосредственно осуществляющее подготовку, передачу и прием сообщений платежной системы с использованием ключевой информации пользователя платежной системы, а также выработку

и регистрацию ключевой информации в удостоверяющем центре Центра в присутствии офицера безопасности рабочего места пользователя платежной системы;

18) подразделение безопасности пользователя платежной системы - структурное подразделение пользователя платежной системы, обеспечивающее безопасность и защиту информационных и программных ресурсов пользователя платежной системы;

19) терминал платежной системы - специальное программное обеспечение, обеспечивающее доступ в платежную систему, установленное у пользователя платежной системы;

20) приложение терминала платежной системы - специальное программное обеспечение, предназначенное для удаленной работы с терминалом платежной системы.

4. Процедуры обмена и форматы сообщений, применяемые в платежной системе, устанавливаются Центром по согласованию с Национальным Банком Республики Казахстан (далее - Национальный Банк).

Глава 2. Размещение рабочего места пользователя платежной системы

5. Рабочее место пользователя платежной системы размещается в помещении по месту нахождения пользователя платежной системы с ограниченным доступом (далее - Помещение). Не допускается размещение в Помещении рабочих мест, не предназначенных для работы с платежной системой, за исключением рабочих мест работников, выполняющих функции операторов рабочего места пользователя платежной системы.

6. Помещение оборудуется металлическими и (или) усиленными от проникновения входными дверями, на которые устанавливаются механические и (или) электромеханические замки.

7. Двери Помещения оборудуются средствами контроля доступа для осуществления мониторинга событий доступа в Помещение в режиме реального времени и записи событий доступа в Помещение в электронном журнале с возможностью получения отчета о событиях доступа в Помещение. Архив событий электронного журнала хранится пользователем платежной системы не менее шести месяцев.

8. Рабочее место пользователя платежной системы обеспечивается средствами защиты информации от утечки по электромагнитным каналам или жидкокристаллическим монитором с подключением его по цифровому интерфейсу.

9. При расположении Помещения на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц, прилегающих крыш иных строений, окна Помещения оборудуются металлическими решетками или аналогичными средствами защиты, предназначенными для предотвращения физического проникновения в Помещение путем разбития оконных стекол.

10. Двери и окна Помещения оборудуются охранной сигнализацией.

11. За входом в Помещение, а также за рабочим местом пользователя платежной системы устанавливается видеонаблюдение с возможностью записи видеосигналов. Допускается запуск записи видеосигналов на движение объектов. Архив записи видеосигналов хранится не менее периода контроля целостности печатей или пломб на системном блоке рабочего места пользователя платежной системы, установленного внутренними документами пользователя платежной системы.

12. Доступ в помещение имеют лица, допущенные к работе с платежной системой. Посещение Помещения лицами, не допущенными к работе с платежной системой, за исключением случаев возникновения нестандартных ситуаций, допускается только в присутствии лица, допущенного к работе с платежной системой.

Пункт 13 изложен в редакции постановления Правления Национального Банка РК от 22.12.17 г. № 248 (см. стар. ред.)

13. При создании рабочего места пользователя платежной системы, получившего доступ в платежную систему, или переносе рабочего места пользователя платежной системы на новое место пользователь платежной системы в течение десяти рабочих дней с даты эксплуатации рабочего места пользователя платежной системы уведомляет об этом Национальный Банк в произвольной письменной форме для получения заключения (информации) о соответствии его деятельности Требованиям.

Глава 3. Взаимодействие пользователя платежной системы и Центра

14. Аутентификация пользователя платежной системы и Центра осуществляется путем двухстороннего обмена информацией с использованием средств криптографической защиты информации и ключевой информации, зарегистрированной в удостоверяющем центре Центра.

15. При возникновении ошибки в процессе аутентификации в платежной системе выдается сообщение об ошибке и связь разрывается.

16. Рабочее место пользователя платежной системы содержит средства, необходимые для обеспечения соединения по протоколу TCP (IP) с прикладными серверами Центра, обеспечивающими работоспособность пользователя платежной системы.

17. Договор, заключаемый между пользователем платежной системы и юридическим лицом, обеспечивающим канал передачи данных, используется для взаимодействия с платежной системой и предусматривает ответственность при сбоях в работе такого канала передачи данных.

Глава 4. Терминал платежной системы

18. Терминал платежной системы осуществляет прием и (или) передачу сообщений платежной системы и является обязательным для использования пользователям платежной системы.

19. Терминал платежной системы обрабатывает сообщения платежной системы в соответствии с процедурами обмена и форматами сообщений, применяемыми в платежной системе.

20. Терминал платежной системы выполняет следующие функции:

1) аутентификацию пользователя платежной системы и Центра;

2) взаимодействие с удостоверяющим центром Центра;

3) обеспечение конфиденциальности и аутентификации передаваемых и получаемых сообщений;

4) передачу и (или) прием сообщений от пользователя платежной системы к Центру и от Центра к пользователю платежной системы;

5) проверку целостности полученных сообщений платежной системы;

6) проверку целостности терминала платежной системы;

7) применение ключевой информации;

8) формирование и проверку электронной цифровой подписи сообщений;

9) проверку принадлежности электронной цифровой подписи сообщения пользователю платежной системы или Центру.

21. Терминал платежной системы обеспечивает ведение электронных журналов, регистрирующих следующие ключевые события и действия операторов и администраторов рабочего места пользователя платежной системы:

1) время и дату открытия и закрытия терминала платежной системы;

2) время и дату соединения с Центром и отсоединения от Центра;

3) время начала и время завершения действий операторов и администраторов платежной системы по сообщениям платежной системы, описание совершенных действий.

22. Доступ операторов и администраторов рабочего места пользователя платежной системы к терминалу платежной системы либо к его приложению обеспечивается исключительно после успешного выполнения идентификации и аутентификации.

23. Эксплуатация терминала платежной системы осуществляется с использованием технических средств, которые обеспечивают надежную и бесперебойную работу терминала платежной системы и соответствуют требованиям, указанным в документации к терминалу платежной системы.

24. Терминал платежной системы либо его приложение устанавливается на специально выделенном для этих целей персональном компьютере (сервере), имеющем инвентарный номер учета и паспорт с подробными данными по конфигурации, аппаратным и программным средствам, установленным на нем.

25. Администрирование терминала платежной системы или его приложения осуществляется непосредственно с рабочего места пользователя платежной системы и в присутствии офицера безопасности рабочего места пользователя платежной системы.

26. Работа с терминалом платежной системы осуществляется с рабочего места пользователя платежной системы. Не допускается установка и использование систем удаленного доступа на рабочем месте пользователя платежной системы. Встроенные службы удаленного доступа к рабочему месту пользователя платежной системы удаляются или отключаются.

27. В случае выявления некорректной работы терминала платежной системы, при которой может быть нанесен ущерб пользователям платежной системы или Центру, последний закрывает доступ этому терминалу платежной системы в платежную систему с одновременным извещением пользователя платежной системы и указанием соответствующих причин.

28. Условием подключения пользователя платежной системы к платежной системе является использование средства криптографической защиты информации, которое обеспечивает:

1) механизм формирования и проверки электронной цифровой подписи;

2) конфиденциальность информации (шифрование данных);

3) целостность передаваемой информации (имитационная защита данных);

4) целостность хранимой информации и программного обеспечения (хэширование данных).

Глава 5. Ключевая информация

29. Ключевая информация регистрируется пользователем в удостоверяющем центре Центра.

30. Ключевая информация находится на внешнем носителе. Доступ к носителю с ключевой информацией предоставляется исключительно операторам рабочего места пользователя платежной системы.

31. Ключевая информация загружается в терминал платежной системы с внешнего носителя. Наличие несанкционированных копий ключевой информации, в том числе на жестком диске рабочего места пользователя платежной системы, не допускается.

32. Порядок хранения и использования внешних носителей с ключевой информацией исключает возможность несанкционированного доступа к ним.

33. Лица, имеющие доступ к ключевой информации, обеспечивают сохранность и неразглашение информации, полученной в результате работы с платежной системой.

34. Плановая смена ключевой информации осуществляется не реже одного раза в год.

35. Внешние носители с ключевой информацией хранятся в сейфе, оборудованном запирающимся устройством, установленном в помещении работников, ответственных за хранение внешних носителей с ключевой информацией. В случае неиспользования ключевой информации внешние носители с ключевой информацией находятся в сейфах.

36. В случаях увольнения работников, имевших доступ к ключевой информации, или выявления попытки несанкционированного доступа к ключевой информации производится внеплановая смена ключевой информации. Новая ключевая информация вводится в действие не позднее дня увольнения работника, имеющего доступ к ключевой информации, либо не позднее дня выявления попытки несанкционированного доступа к ключевой информации.

Новая ключевая информация регистрируется пользователем в удостоверяющем центре Центра.

37. Процедуры по хранению и уходу за внешними носителями с ключевой информацией осуществляются в соответствии с рекомендациями производителя.

38. Устаревшая ключевая информация хранится пользователем платежной системы в течение срока хранения электронных документов, подписанных или зашифрованных с использованием этой ключевой информации.

39. Пользователю платежной системы не допускается:

1) снимать несанкционированные копии ключевой информации;

2) знакомить с ключевой информацией или передавать ее лицам, не имеющим к ней доступ;

3) выводить ключевую информацию на дисплей или принтер;

4) использовать внешний носитель с ключевой информацией в режимах, не предусмотренных условиями функционирования, установленными его производителем;

5) записывать на внешний носитель с ключевой информацией постороннюю информацию;

6) использовать чужую ключевую информацию.

Глава 6. Требования к рабочему месту пользователя платежной системы

40. На рабочем месте пользователя платежной системы устанавливается программно-аппаратный комплекс защиты от несанкционированного доступа, включающий в себя средства аутентификации лиц допущенных к работе с платежной системой, ведение электронных журналов в течение срока хранения электронных документов платежной системы с целью контроля событий, связанных с доступом к рабочему месту пользователя платежной системы и их действиями.

41. На рабочее место пользователя платежной системы устанавливаются средства обнаружения вредоносного программного кода и (или) программы. В случае выявления факта заражения данная информация немедленно сообщается в подразделение безопасности пользователя платежной системы.

42. Не допускается установка на рабочем месте пользователя платежной системы аппаратных и программных средств, не предусмотренных Требованиями и не

предназначенных для решения задач по подготовке, обработке, передаче или ведения электронных документов в рамках платежной системы.

43. Одному системному имени лица, допущенного к работе с платежной системой, по которому данное лицо идентифицируется на входе в информационные системы пользователя платежной системы, соответствует одно физическое лицо.

44. Системный блок рабочего места пользователя платежной системы опечатывается или опломбируется с указанием на стикере или пломбе даты последнего опечатывания или опломбирования и инвентарного номера учета персонального компьютера.

45. Порядок хранения и использования технических средств, паролей или другой информации, обеспечивающих доступ к рабочему месту пользования платежной системы, исключает возможность их несанкционированного использования.

46. Права по установлению и изменению настроек средств защиты от несанкционированного доступа к рабочему месту пользователя платежной системы предоставляются исключительно работникам, выполняющим функции офицера безопасности рабочего места пользователя платежной системы.

47. Порядок доступа к ресурсам (дисковое пространство, директории, сетевые ресурсы, базы данных), выделенным для накопления в них информации для передачи в платежную систему, получения информации из платежной системы, хранения, архивирования либо другой обработки информации, исключает возможность доступа к этим ресурсам лиц, не допущенных к работе с ними.

48. Порядок доступа к рабочему месту пользователя платежной системы посредством сети и иных технических каналов передачи данных исключает возможность несанкционированного доступа.

49. Рабочее место пользователя платежной системы оснащается техническими средствами бесперебойного электропитания, позволяющего осуществлять работу персонального компьютера при отсутствии напряжения в электросети в течение времени, необходимого для корректного завершения работы в системе, но не менее тридцати минут.

Пункт 50 изложен в редакции постановления Правления Национального Банка РК от 22.12.17 г. № 248 (см. стар. ред.)

50. В случае внесения изменений в программное обеспечение, посредством которого осуществляется связь между пользователем платежной системы и Центром, в программно-аппаратный комплекс защиты от несанкционированного доступа рабочего места пользователя платежной системы, а также в технологию передачи электронных документов, подготовленных в информационной системе пользователя платежной системы, на рабочее место пользователя платежной системы, пользователь платежной системы в течение десяти рабочих дней со дня внесения изменений уведомляет об этом Национальный Банк в произвольной письменной форме для получения заключения (информации) о соответствии его деятельности Требованиям.

Глава 7. Организация работы обслуживающего персонала

51. Лица, допущенные к работе с платежной системой подразделяются на следующие категории:

1) администратор рабочего места пользователя платежной системы;

2) оператор рабочего места пользователя платежной системы;

3) офицер безопасности рабочего места пользователя платежной системы.

52. При наличии функции создания платежных сообщений в формате MT 100 и (или) MT 102 посредством терминала платежной системы либо его приложения при организации работ

обслуживающего персонала не допускается исполнение одним лицом функций (полностью или частично) разных категорий лиц, указанных в пункте 51 Требований.

53. Пользователь платежной системы осуществляет ведение следующих внутренних журналов регистрации:

1) журнал посещений Помещения лицами, не допущенными к работе с платежной системой, с указанием:

даты, времени входа и выхода посетителя и цели посещения;

фамилии и подписи посетителя;

фамилии и подписи сопровождающего лица из числа лиц, допущенных к работе с платежной системой;

2) журнал использования ключевой информации с указанием:

даты, времени начала и окончания использования ключевой информации;

фамилии и подписи лица, использующего ключевую информацию;

даты замены ключевой информации с указанием причин замены;

3) журнал опломбирования и проверки целостности пломб и печатей системного блока рабочего места пользователя платежной системы с указанием:

даты и времени опломбирования или проверки целостности пломб или печатей;

фамилии и подписи лица, осуществившего опломбирование или проверки целостности пломб или печатей;

причины опломбирования или проверки целостности пломб или печатей;

формы и материала пломбы или стикера для опечатывания.

Пункт 54 изложен в редакции постановления Правления Национального Банка РК от 27.08.18 г. № 182 (см. стар. ред.)

54. Внутренние журналы регистрации, указанные в пункте 53 Требований, пронумеровываются, прошнуровываются, сшиваются и удостоверяются подписью лица, допущенного к работе с платежной системой. Ошибочные записи во внутренних журналах регистрации, подлежащие корректировке, также удостоверяются подписью лица, допущенного к работе с платежной системой.

55. Внутренние журналы регистрации, указанные в пункте 53 Требований, хранятся пользователем платежной системы не менее одного года с даты внесения последней записи.

56. Внутренними документами пользователя платежной системы определяются:

1) режим работы с платежной системой с указанием времени работы и перерывов, порядка работы в выходные и праздничные дни, а также случаев продления операционного дня платежной системы;

2) список работников (с указанием должности, фамилии и инициалов), допущенных к работе с платежной системой, с указанием по каждому работнику выполняемых им функций:

администратора, оператора или офицера безопасности рабочего места пользователя платежной системы;

архивирования и хранения электронных документов, переданных в платежную систему и полученных из платежной системы;

мониторинга целостности печатей или пломб на системном блоке рабочего места пользователя платежной системы;

3) список работников (с указанием должности, фамилии и инициалов), имеющих доступ к ресурсам, указанным в пункте 47 Требований, с указанием уровня доступа и выполняемых функций;

4) список работников (с указанием должности, фамилии и инициалов) и ресурсов, имеющих доступ к рабочему месту пользователя платежной системы посредством сети и иных технических каналов передачи данных, с указанием целей предоставления доступа;

5) порядок архивирования и дальнейшего хранения электронных документов, переданных в платежную систему и полученных из платежной системы, с указанием условий, сроков и места их хранения, а также порядка доступа к этим архивам;

6) порядок хранения и использования технических средств, паролей или другой информации, обеспечивающих доступ к рабочему месту пользователя платежной системы, с указанием условий и мест хранения, процедур доступа к ним и сроков смены;

7) порядок передачи электронных документов, подготовленных в информационной системе пользователя платежной системы, на рабочее место пользователя платежной системы;

8) порядок работы с программно-аппаратным комплексом защиты от несанкционированного доступа и средствами обеспечения целостности программного обеспечения, установленными на рабочем месте пользователя платежной системы;

9) порядок и процедуры работы с терминалом платежной системы;

10) порядок работы с основным и резервным каналами передачи данных с указанием случаев и процедур перехода с одного канала на другой.

57. Пользователь платежной системы получает с работников, допущенных к работе в платежной системе, обязательство о неразглашении и нераспространении паролей или другой информации, обеспечивающих доступ к рабочему месту пользователя платежной системы, а также конфиденциальной и ключевой информации.

Пункт 58 введен в действие с 1 января 2017 года

58. При необходимости решения текущих и оперативных вопросов в части безопасности оператор и офицер безопасности рабочего места пользователя платежной системы взаимодействуют с подразделением безопасности пользователя платежной системы.

Глава 8. Требования к управлению операционным риском и обеспечению непрерывности деятельности пользователя платежной системы

Пункт 59 введен в действие с 1 января 2017 года

59. В целях управления операционным риском пользователь платежной системы обеспечивает ведение внутренних документов, определяющих:

1) методы управления операционным риском;

2) порядок оценки качества и надежности функционирования программно-технического комплекса пользователя платежной системы;

3) план обеспечения непрерывности деятельности пользователя платежной системы.

Пункт 60 введен в действие с 1 января 2017 года

60. Пользователь платежной системы обеспечивает функционирование резервного центра для восстановления работы программно-технического комплекса пользователя платежной системы при нестандартных ситуациях, соответствующего условиям, установленным главами 2, 3, 4, 5, 6, 7 и настоящей главой Требований к основному центру, включая требования к рабочему месту пользователя платежной системы и его размещению, терминалу платежной системы, взаимодействию с Центром, порядку использования и хранения ключевой информации, организации работ обслуживающего персонала.

Пункт 61 введен в действие с 1 января 2017 года

61. Пользователь платежной системы обеспечивает функционирование резервного канала коммуникации (передачи данных) с платежной системой Центра. Предусматривается возможность подключения резервного канала коммуникации к сетевому (коммуникационному) оборудованию резервного и (или) основного центра платежной системы.

Пункт 62 введен в действие с 1 января 2017 года

62. План обеспечения непрерывности деятельности пользователя платежной системы содержит следующие условия:

1) место нахождения резервного центра;

2) порядок информирования руководства пользователя платежной системы и Национального Банка о возникновении нестандартной ситуации, о результатах ее урегулирования;

3) перечень технических, программных или других средств, обеспечивающих работу пользователя с платежной системой Центра, восстановление которых требуется в резервном центре;

4) перечень систем жизнеобеспечения, предназначенных для поддержания функционирования программно-технического комплекса пользователя платежной системы, работы персонала (системы электроснабжения, отопления, вентилирования, водоснабжения, канализации, пожаротушения и пожарной сигнализации, охраны зданий), которые используются в резервном центре;

5) порядок дублирования и резервирования программно-технического комплекса пользователя платежной системы на резервный центр;

6) бизнес-процессы пользователя платежной системы, подлежащие восстановлению в резервном центре;

7) список команд восстановления пользователя платежной системы по каждому бизнес-процессу с описанием порядка их действий при переходе на работу резервного центра;

8) порядок извещения команды восстановления пользователя платежной системы о необходимости перевода работы на резервный центр и ее транспортировки к месту нахождения резервного центра;

9) контакты для внешнего взаимодействия;

10) порядок проведения тестирования функционирования резервного центра.

Пункт 63 изложен в редакции постановления Правления Национального Банка РК от 22.12.17 г. № 248 (см. стар. ред.)

63. При возникновении нестандартной ситуации в основном центре пользователь платежной системы:

1) обеспечивает перевод программно-технического комплекса пользователя платежной системы на резервный центр.

Стандартный норматив времени по переводу программно-технического комплекса пользователя платежной системы на резервный центр составляет не более трех часов с момента возникновения нестандартной ситуации.

При отсутствии возможности соблюдения стандартного норматива времени пользователь платежной системы принимает необходимые меры для перевода работы пользователя платежной системы на резервный центр с учетом необходимости исполнения принятых обязательств по платежам и переводам денег до завершения операционного дня платежной системы Центра;

2) направляет посредством защищенного канала связи транспортной системы «Финансовая автоматизированная система транспортной информации» (далее - ФАСТИ») или факсимильной связи Национальному Банку письмо о принятии решения перевести программно-технический комплекс на резервный центр в течение трех часов после принятия указанного решения;

3) направляет посредством защищенного канала связи ФАСТИ или факсимильной связи Национальному Банку письмо о результате перевода программно-технического комплекса на резервный центр в течение трех часов после завершения работ по переводу;

4) направляет посредством защищенного канала связи ФАСТИ или факсимильной связи Национальному Банку письмо о результате перевода программно-технического комплекса обратно на основной центр в течение трех часов после завершения работ по переводу.

Пункт 64 введен в действие с 1 января 2017 года

64. Пользователем платежной системы не менее одного раза в год проводится тестирование функционирования резервного центра путем планового перевода работы пользователя платежной системы на использование резервного центра. Пользователь платежной системы письменно уведомляет Национальный Банк о планируемых сроках тестирования за десять рабочих дней до начала планового перевода программно-технического комплекса на резервный центр.

Сведения о результатах тестирования с указанием выявленных проблем (при наличии) и принятых мер по их устранению представляются пользователем платежной системы в Национальный Банк в течение пяти рабочих дней после дня завершения мероприятий после перевода программно-технического комплекса с резервного на основной центр.

65. Документ, регламентирующий методы управления операционным риском, и план обеспечения непрерывности деятельности пользователя платежной системы подлежат ежегодному анализу пользователем платежной системы на предмет необходимости актуализации.

Глава 9. Заключительные положения

66. При расторжении (окончании срока действия) договора об оказании услуг в платежной системе, заключенного между пользователем платежной системы и Центром, Центр не позднее следующего рабочего дня после дня расторжения договора уведомляет об этом Национальный Банк в соответствии с договором.

67. Национальный Банк в течение десяти календарных дней со дня получения уведомления, предусмотренного пунктами 13 и 50 Требований, принимает решение о необходимости либо отсутствии необходимости проведения осмотра рабочего места пользователя платежной системы.

Допускается проведение осмотра в случаях, если ранее в деятельности пользователя платежной системы были выявлены нарушения Требований либо последний осмотр был проведен (осуществлен) более двух лет назад.

Национальный Банк проводит (осуществляет) осмотр рабочего места пользователя платежной системы в течение двух месяцев со дня принятия решения о проведении (осуществлении) осмотра либо со дня получения обращения.