Об утверждении Инструкции о требованиях к организационным мерам и программно-техническим средствам, обеспечивающим доступ банков и организаций, осуществляющих отдельные виды банковских операций, в платежные системы Республиканского государственного предприятия на праве хозяйственного ведения "Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан"

Утративший силу

Постановление Правления Национального Банка Республики Казахстан от 28 ноября 2008 года № 95. Зарегистрировано в Министерстве юстиции Республики Казахстан 29 декабря 2008 года № 5411. Утратило силу постановлением Правления Национального Банка Республики Казахстан от 24 августа 2012 года № 269

Сноска. Утратило силу постановлением Правления Национального Банка РК от 24.08.2012 № 269 (вводится в действие по истечении шести месяцев после его первого официального опубликования).

В целях установления требований к организационным мерам и программно-техническим средствам, обеспечивающим доступ банков и организаций, осуществляющих отдельные виды банковских операций, в платежные системы Республиканского государственного предприятия на праве хозяйственного ведения "Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан" Правление Национального Банка Республики Казахстан **ПОСТАНОВЛЯЕТ:**

1. Утвердить прилагаемую Инструкцию о требованиях к организационным мерам и программно-техническим средствам, обеспечивающим доступ банков и организаций, осуществляющих отдельные виды банковских операций в платежные системы Республиканского государственного предприятия на праве хозяйственного ведения "Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан" (далее - Центр).

2. Настоящее постановление вводится в действие по истечении трех месяцев со дня государственной регистрации в Министерстве юстиции Республики Казахстан.

3. Со дня введения в действие настоящего постановления признать утратившими силу нормативные правовые акты Национального Банка Республики Казахстан, согласно приложению к настоящему постановлению.

4. Департаменту платежных систем (Мусаев Р.Н.):

1) совместно с Юридическим департаментом (Шарипов С.Б.) принять меры к государственной регистрации в Министерстве юстиции Республики Казахстан настоящего постановления;

2) в десятидневный срок со дня государственной регистрации в Министерстве юстиции Республики Казахстан настоящего постановления довести его до сведения заинтересованных подразделений центрального аппарата и филиалов Национального Банка Республики Казахстан, Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций, Центра и пользователей платежных систем Центра.

5. Управлению по обеспечению деятельности руководства Национального Банка Республики Казахстан (Терентьев А.Л.) в трехдневный срок со дня получения от Департамента платежных систем заявки на опубликование принять меры к опубликованию настоящего постановления в средствах массовой информации Республики Казахстан.

6. Контроль за исполнением настоящего постановления возложить на заместителя Председателя Национального Банка Республики Казахстан Сартбаева М.М.

Председатель

Национального Банка *А. Сайденов*

Приложение
к постановлению Правления
Национального Банка Республики Казахстан
от 28 ноября 2008 года № 95

Перечень нормативных правовых актов Национального Банка Республики Казахстан, признаваемых утратившими силу

1. Постановление Правления Национального Банка Республики Казахстан от 7 октября 1999 года № 325 "Об утверждении Правил обеспечения безопасности рабочего места пользователя платежной системы Республиканского государственного предприятия на праве хозяйственного ведения "Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан" (зарегистрированное в Реестре государственной регистрации нормативных правовых актов под № 1059).

2. Постановление Правления Национального Банка Республики Казахстан от 28 февраля 2002 года № 61 "О внесении изменений и дополнений в постановление Правления Национального Банка Республики Казахстан "Об утверждении Правил обеспечения безопасности рабочего места пользователя

платежной системы Республиканского государственного предприятия на праве хозяйственного ведения "Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан" от 7 октября 1999 года № 325" (зарегистрированное в Реестре государственной регистрации нормативных правовых актов под № 1825).

3. Постановление Правления Национального Банка Республики Казахстан от 25 июля 2003 года № 235 "Об утверждении Правил доступа в платежную систему Республики Казахстан, оператором которой является Республиканское государственное предприятие на праве хозяйственного ведения "Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан" (зарегистрированное в Реестре государственной регистрации нормативных правовых актов под № 2458).

4. Постановление Правления Национального Банка Республики Казахстан от 2 февраля 2006 года № 6 "О внесении изменений в постановление Правления Национального Банка Республики Казахстан от 7 октября 1999 года № 325 "Об утверждении Правил обеспечения безопасности рабочего места пользователя платежной системы Республиканского государственного предприятия на праве хозяйственного ведения "Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан" (зарегистрированное в Реестре государственной регистрации нормативных правовых актов под № 4111).

5. Постановление Правления Национального Банка Республики Казахстан от 18 января 2007 года № 5 "О внесении изменений и дополнений в постановление Правления Национального Банка Республики Казахстан от 7 октября 1999 года № 325 "Об утверждении Правил обеспечения безопасности рабочего места пользователя платежной системы Республиканского государственного предприятия на праве хозяйственного ведения "Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан" (зарегистрированное в Реестре государственной регистрации нормативных правовых актов под № 4540).

Утверждена
постановлением Правления
Национального Банка
Республики Казахстан
от 28 ноября 2008 года № 95

Инструкция о требованиях к организационным мерам и программно-техническим средствам, обеспечивающим доступ банков и организаций, осуществляющих отдельные виды банковских операций, в платежные системы Республиканского

государственного предприятия на праве хозяйственного ведения "Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан"

Глава 1. Общие положения

1. Настоящая Инструкция разработана в соответствии с Законом Республики Казахстан "О Национальном Банке Республики Казахстан" от 30 марта 1995 года и устанавливает требования к организационным мерам и программно-техническим средствам, обеспечивающим доступ банков и организаций, осуществляющих отдельные виды банковских операций, в платежные системы Республиканского государственного предприятия на праве хозяйственного ведения "Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан" (далее - платежная система).

2. Нормы настоящей Инструкции распространяют свое действие на всех пользователей платежной системы, за исключением Национального Банка Республики Казахстан (далее - Национальный Банк).

3. В настоящей Инструкции используются следующие понятия:

1) аутентификация - комплекс мер для подтверждения подлинности участия Республиканского государственного предприятия на праве хозяйственного ведения "Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан" (далее - Центр) и пользователей платежной системы при обмене сообщениями платежной системы, а также для подтверждения подлинности таких сообщений;

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

3) ключевая информация - криптографические ключи или другая информация , позволяющая осуществлять криптографические преобразования информации;

4) несанкционированный доступ - доступ к информационным и программным ресурсам, с нарушением установленного пользователем платежной системы порядка доступа к ним;

5) пользователь платежной системы - банк второго уровня Республики Казахстан, акционерное общество "Банк Развития Казахстана", организация, осуществляющая отдельные виды банковских операций, заключившие договор с Центром о предоставлении услуг в платежной системе;

6) 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;

7) рабочее место пользователя платежной системы - персональный компьютер (сервер), на котором установлен терминал платежной системы;

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

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

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

11) терминал платежной системы - специальное программное обеспечение, обеспечивающее доступ в платежную систему, установленное у пользователей платежной системы.

4. Форматы передачи информации, применяемые в платежной системе, устанавливаются Центром.

Глава 2. Размещение рабочего места пользователя платежной системы

5. Рабочее место пользователя платежной системы размещается в специально выделенном помещении (далее - Помещение). Не допускается размещение в Помещении иных рабочих мест, непредназначенных для работы с платежной системой, за исключением рабочих мест сотрудников, выполняющих функции операторов, администратора и офицера безопасности платежной системы.

6. Место нахождения, специальное оборудование и охрана Помещения должны исключать возможность неконтролируемого проникновения в Помещение лиц, не допущенных к рабочему месту пользователя платежной системы.

7. Помещение должно находиться в контролируемой пользователем платежной системы зоне, иметь металлические входные двери, на которые устанавливаются механические замки.

8. 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 одного года.

9. При отсутствии охраняемой и контролируемой зоны в радиусе 50 (пятидесяти) метров от здания, где расположено рабочее место пользователя платежной системы, а также в случае нахождения в данном здании других организаций, рабочее место пользователя платежной системы обеспечивается средствами защиты информации от утечки по электромагнитным каналам.

10. 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.

11. Двери и окна Помещения оборудуются исправной охранной сигнализацией.

12. За входом в Помещение, а также за рабочим местом пользователя платежной системы устанавливается видеонаблюдение в режиме реального времени с возможностью записи видеосигналов. 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.

13. При создании рабочего места пользователя, получившего доступ в платежную систему, или переноса рабочего места пользователя платежной системы на новое место пользователь платежной системы в течение десяти рабочих дней с момента эксплуатации рабочего места пользователя платежной системы уведомляет об этом Национальный Банк.

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.

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 используемый для взаимодействия с платежной системой канал передачи данных, должен предусматривать ответственность при сбоях в работе такого канала передачи данных.

18. Пользователь платежной системы имеет резервный канал передачи данных с платежной системой. Основной канал передачи данных подключается к основному серверу платежной системы, а резервный канал передачи данных - к резервному серверу платежной системы.

Глава 4. Терминал платежной системы

19. Терминал платежной системы осуществляет прием и передачу сообщений платежной системы и является обязательным для использования пользователем платежной системы.

20. Терминал платежной системы обрабатывает сообщения платежной системы в соответствии с форматами передачи информации, применяемыми в платежной системе.

21. Терминал платежной системы выполняет следующие функции:

1) аутентификация пользователя платежной системы и Центра;

2) обеспечение конфиденциальности и аутентификации передаваемой и получаемой информации;

3) прием и передача сообщений от пользователя платежной системы к Центру и от Центра к пользователю платежной системы;

4) проверка целостности полученных сообщений платежной системы;

5) проверка целостности терминала платежной системы;

6) применение ключевой информации;

7) иные функции, связанные с приемом и передачей пользователем платежной системы сообщений платежной системы.

22. Терминал платежной системы обеспечивает ведение электронных журналов, в которых регистрируются следующие ключевые события и действия операторов и администраторов платежной системы:

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

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

3) время начала и время завершения действий операторов и администраторов платежной системы над сообщениями платежной системы, описание совершенных действий.

23. Терминал платежной системы обеспечивает доступ операторов и администраторов платежной системы посредством технических средств, паролей или иным способом.

24. Эксплуатация терминала платежной системы осуществляется с использованием технических средств, которые должны обеспечивать надежную и бесперебойную работу терминала платежной системы и соответствовать требованиям, указанным в документации к терминалу платежной системы.

25. 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. Сведения, указанные в таком паспорте, должны соответствовать действительным .

26. 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.

27. Обязательным условием подключения пользователя платежной системы к платежной системе является использование пакета криптографической защиты информации "ТУМАР", который должен обеспечить:

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

28. Ключевая информация должна находиться на внешнем носителе.

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

30. Порядок хранения и использования внешних носителей с ключевой информацией должен исключать возможность несанкционированного доступа к н и м .

31. Лица, имеющие доступ к ключевой информации, обеспечивают сохранность и неразглашение информации, полученной в результате работы с п л а т е ж н о й с и с т е м о й .

32. Плановая смена ключевой информации осуществляется не реже одного р а з а в г о д .

33. Для хранения внешних носителей с ключевой информацией в помещении сотрудников, ответственных за хранение внешних носителей с ключевой информацией, устанавливаются сейфы, оборудованные запирающими устройствами. При неиспользовании ключевой информации внешние носители с ключевой информацией находятся в сейфах.

34. В случаях увольнения сотрудников, 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 сотрудника, имеющего доступ к ключевой информации, либо не позднее дня выявления попытки несанкционированного доступа к ключевой информации.

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

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

37. Пользователю платежной системы запрещается:

1) снимать несанкционированные копии ключевой информации;

2) знакомить с содержанием внешних носителей с ключевой информацией или передавать их лицам, не имеющим к ним 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.

Глава 6. Требования к рабочему месту пользователя платежной системы

38. На рабочем месте пользователя платежной системы устанавливается программно-аппаратный комплекс защиты от несанкционированного доступа, включающий в себя средства опознавания пользователя, возможность ведения электронных журналов в течение срока хранения электронных документов платежной системы с целью контроля событий, связанных с доступом к рабочему месту пользователя платежной системы и действиями пользователей.

39. На рабочее место пользователя платежной системы устанавливаются средства обеспечения целостности программного обеспечения. В случае подозрения на нарушение целостности или получения предупреждений о

нарушении целостности этих средств или программного обеспечения данная информация немедленно сообщается в подразделение безопасности пользователя платежной системы.

40. Установка на рабочем месте пользователя платежной системы аппаратных и программных средств, не предусмотренных настоящей Инструкцией и не предназначенных для решения задач по подготовке, обработке, передаче или ведения электронных документов в рамках платежной системы, не допускается.

41. Одному системному имени пользователя, по которому идентифицируется пользователь на входе в информационные системы пользователя платежной системы, должно соответствовать одно физическое лицо.

42. 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.

43. Порядок хранения и использования технических средств, паролей или другой информации, обеспечивающих доступ к рабочему месту пользователя платежной системы, должен исключать возможность их несанкционированного использования.

44. Права по установлению и изменению настроек средств защиты от несанкционированного доступа рабочего места пользователя платежной системы предоставляются только сотрудникам, выполняющим функции офицера безопасности платежной системы.

45. Технология передачи электронных документов (определенный порядок передачи электронных документов), подготовленных в информационной системе пользователя платежной системы, на рабочее место пользователя платежной системы должна исключать возможность несанкционированного доступа к этим электронным документам.

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

47. Порядок доступа к рабочему месту пользователя платежной системы посредством сети и иных технических каналов передачи данных должен исключать возможность несанкционированного доступа.

48. 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 30 (тридцати) минут.

49. 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 с момента эксплуатации уведомляет об этом Национальный Банк.

Глава 7. Организация работ обслуживающего персонала

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

1) администратор платежной системы - лицо, непосредственно осуществляющее выработку и использование собственных открытых и секретных ключей, а также регистрацию ключей в Центре;

2) оператор платежной системы - лицо, непосредственно осуществляющее подготовку, передачу и прием сообщений платежной системы;

3) офицер безопасности 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 контроль за их работоспособностью и за выполнением требований безопасности.

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

1) журнал пломбирования и контроля целостности пломб системного блока рабочего места пользователя платежной системы;

2) журнал посещений Помещения;

3) журнал использования ключевой информации.

52. Журналы регистрации, указанные в пункте 51 настоящей Инструкции, пронумеровываются, прошнуровываются и скрепляются печатью пользователя платежной системы. Ошибочные записи в журналах регистрации подлежат корректировке и заверяются подписью ответственного лица.

53. Журналы регистрации, указанные в пункте 51 настоящей Инструкции, хранятся пользователем платежной системы не менее одного года с момента внесения последней записи.

54. Внутренними документами пользователя платежной системы определяются:

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

2) список сотрудников, допущенных к рабочему месту пользователя платежной системы, с указанием занимаемых должностей и выполняемых функций;

3) список сотрудников, имеющих доступ к внешним носителям с ключевой информацией, с указанием занимаемых должностей;

4) список сотрудников, выполняющих функции офицера безопасности платежной системы, администратора платежной системы и оператора платежной системы, с указанием занимаемых должностей;

5) список сотрудников, осуществляющих архивирование и хранение электронных документов, переданных в платежную систему, и полученных из платежной системы, с указанием занимаемых должностей;

6) список сотрудников, осуществляющих пломбирование и дальнейший контроль целостности печатей или пломб на системном блоке рабочего места пользователя платежной системы, с указанием занимаемых должностей;

7) список лиц, допускаемых к рабочему месту пользователя платежной системы в случае необходимости устранения причин ненадлежащего функционирования рабочего места пользователя платежной системы и в других случаях, предусмотренных внутренними документами пользователя платежной системы, (далее - особые случаи) с указанием занимаемых должностей;

8) порядок и процедуры контроля доступа в Помещение с определением сотрудника, ответственного за допуск, и указанием порядка временного доступа в Помещение лиц, не допущенных к рабочему месту пользователя платежной системы и допущенных к рабочему месту пользователя платежной системы в особых случаях, а также действий при обнаружении вскрытия входных дверей и окон Помещения;

9) 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;

10) порядок пломбирования и дальнейшего контроля целостности печатей или пломб на системном блоке рабочего места пользователя платежной системы, с указанием периодичности такого контроля и действий при обнаружении нарушения целостности печати или пломбы;

11) порядок фиксирования в журнале регистрации полной информации (дата,

время, фамилия, роспись) об осуществлении пломбирования и контроля целостности печатей или пломб на системном блоке рабочего места пользователя платежной системы, с определением сотрудника, ответственного за его ведение;

12) функции и полномочия сотрудников, допущенных к рабочему месту пользователя платежной системы;

13) порядок отпусков, увольнения и замещения, в случае временного отсутствия сотрудников, допущенных к рабочему месту пользователя платежной системы;

14) порядок фиксирования в журнале регистрации полной информации (дата, время, фамилия, должность, цель посещения, роспись) обо всех посещениях Помещения лицами, допускаемыми к рабочему месту пользователя платежной системы в особых случаях и лицами, не допущенных к рабочему месту пользователя платежной системы, с определением сотрудника, ответственного за его ведение;

15) порядок хранения внешних носителей с ключевой информацией, с определением сотрудников, ответственных за их хранение с указанием условий и места хранения;

16) порядок хранения устаревшей ключевой информации, с определением сотрудников, ответственных за ее хранение с указанием условий, сроков и места хранения;

17) порядок фиксирования в журнале регистрации полной информации (дата, время, фамилия, роспись) о факте и продолжительности использования ключевой информации и о замене ключевой информации, с определением сотрудника, ответственного за его ведение;

18) 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;

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

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

21) порядок и процедуры работы с терминалом платежной системы;

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

55. В списках сотрудников, предусмотренных подпунктами 2)-6) пункта 54

настоящей Инструкции указываются фамилии и инициалы включенных в список сотрудников.

56. С сотрудников, допущенных к работе в платежной системе, пользователь платежных систем получает специальное обязательство о неразглашении и нераспространении технических средств, паролей или другой информации, обеспечивающих доступ к рабочему месту пользователя платежной системы, а также конфиденциальной и ключевой информации.

57. При необходимости решения текущих и оперативных вопросов в части безопасности, администратор платежной системы и офицер безопасности платежной системы взаимодействуют с подразделением безопасности платежной системы.

Глава 8. Заключительные положения

58. В случае наличия у пользователя платежной системы резервного рабочего места пользователя платежной системы, условия и требования, установленные настоящей Инструкцией, также распространяются и на такое рабочее место.

59. Национальный Банк в десятидневный срок со дня получения уведомления, предусмотренного пунктами 13 или 49 настоящей Инструкции, принимает решение о необходимости/отсутствии необходимости проведения проверки пользователя платежной системы.

При принятии решения о необходимости проведения проверки пользователя платежной системы Национальный Банк в течение двух месяцев со дня принятия указанного решения осуществляет проверку в порядке, установленном Законом Республики Казахстан "О Национальном Банке Республики Казахстан" от 30 марта 1995 года.