

О внесении изменений и дополнений в постановление Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 200 "Об утверждении Требований к организационным мерам и программно-техническим средствам, обеспечивающим доступ в платежные системы"

Постановление Правления Национального Банка Республики Казахстан от 30 июня 2026 года № 74. Зарегистрировано в Министерстве юстиции Республики Казахстан 1 июля 2026 года № 39185

Примечание ИЗПИ!

Вводится в действие с 12.07.2026 г.

Правление Национального Банка Республики Казахстан ПОСТАНОВЛЯЕТ:

1. Внести в постановление Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 200 "Об утверждении Требований к организационным мерам и программно-техническим средствам, обеспечивающим доступ в платежные системы" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 14289) следующие изменения и дополнения:

в Требованиях к организационным мерам и программно-техническим средствам, обеспечивающим доступ в платежные системы, утвержденных указанным постановлением:

пункт 3 изложить в следующей редакции:

"3. В Требованиях используются понятия, предусмотренные Законом Республики Казахстан "О платежах и платежных системах", постановлением Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 3 апреля 2026 года № 53 "Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций" (зарегистрировано в Реестре государственной регистрации нормативных правовых актов под № 38336) (далее – Требования № 53), и следующие понятия:

1) аутентификация – комплекс мер для подтверждения подлинности пользователей системы при обмене платежными и информационными сообщениями, при удаленном подключении к виртуальной среде с установленным терминалом платежной системы, а также для подтверждения подлинности платежных и информационных сообщений;

2) программно-аппаратный комплекс – совокупность программного обеспечения и технических средств, совместно применяемых для взаимодействия пользователя платежной системы с Центром;

3) гипервизор – программное или аппаратно-программное обеспечение, позволяющее создавать и запускать одновременно несколько операционных систем на одном и том же сервере или компьютере;

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

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

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

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

8) несанкционированный доступ – доступ к цифровым и программным ресурсам с нарушением законодательства Республики Казахстан, а также порядка доступа к ним, установленным пользователем платежной системы;

9) средства защиты от несанкционированного доступа – совокупность технических и (или) программных средств, реализующих функции аутентификации, разграничения прав доступа, контроля действий пользователей платежной системы;

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

11) пользователь платежной системы – юридическое лицо, заключившее договор с Центром об оказании услуг в платежной системе, и оператор (операционный центр) других платежных систем;

12) цифровая 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;

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

14) 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;

15) 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;

16) центр обработки данных пользователя платежной системы – объект цифровой инфраструктуры, предназначенный для размещения и обеспечения среды функционирования программно-технических средств пользователя платежной системы, используемых для доступа к платежной системе;

17) рабочее место пользователя платежной системы – персональный компьютер, на котором установлен терминал платежной системы, обеспечивающий доступ в платежную систему, либо совокупность программно-аппаратного комплекса, включающая виртуальную среду с установленным терминалом платежной системы, физический ресурс (сервер), на базе которого она развернута, и персональный компьютер с настроенным удаленным подключением по защищенным каналам связи к этой виртуальной среде, обеспечивающие в совокупности доступ в платежную систему ;

18) администратор рабочего места пользователя платежной системы – лицо, непосредственно осуществляющее администрирование терминала платежной системы, виртуальной среды, на которой он установлен, и гипервизора, на базе которого работает виртуальная среда;

19) подразделение безопасности пользователя платежной системы – структурное подразделение пользователя платежной системы, обеспечивающее безопасность и защиту цифровых и программных ресурсов пользователя платежной системы;

20) офицер безопасности рабочего места пользователя платежной системы – лицо, обеспечивающее установку и функционирование на рабочем месте пользователя платежной системы средств защиты информации от несанкционированного доступа, утечки, в том числе по электромагнитным каналам в случае установки терминала платежной системы на персональном компьютере, гипервизора, на базе которого работает виртуальная среда, удаленного подключения по защищенным каналам связи к виртуальной среде, на которой установлен терминал платежной системы, а также осуществляющее мониторинг за их работоспособностью и за выполнением требований безопасности;

21) 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;

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

23) приложение терминала платежной системы – специальное программное обеспечение, предназначенное для удаленной работы с терминалом платежной системы;

24) физический ресурс (сервер) – аппаратно-программный комплекс, представляющий собой вычислительное оборудование, используемое для размещения и функционирования программного обеспечения и (или) виртуальной среды.";

пункт 5 изложить в следующей редакции:

"5. В случае установки терминала платежной системы на персональном компьютере, рабочее место пользователя платежной системы размещается в помещении по месту нахождения пользователя платежной системы с ограниченным доступом (далее – Помещение).

В случае установки терминала платежной системы на виртуальной среде, физический ресурс (сервер), на котором она развернута, размещается в центре обработки данных пользователя платежной системы, соответствующем требованиям главы 9 Требований № 53.

Персональный компьютер с настроенным удаленным подключением по защищенным каналам связи к виртуальной среде, на котором установлен терминал платежной системы, размещается в Помещении.

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.";

пункт 11 изложить в следующей редакции:

"11. За входом в Помещение, а также за персональным компьютером, на котором установлен терминал платежной системы, или персональным компьютером с настроенным удаленным подключением по защищенным каналам связи к виртуальной среде, на котором установлен терминал платежной системы, устанавливается видеонаблюдение с возможностью записи видеосигналов. Допускается запуск записи видеосигналов при обнаружении движения объектов. Архив видеозаписей хранится не менее периода контроля целостности печатей или пломб на системном блоке рабочего места пользователя платежной системы, установленного внутренними документами пользователя платежной системы.

В случае установки терминала платежной системы на виртуальной среде, видеонаблюдение дополнительно устанавливается за центром обработки данных

пользователя платежной системы, в котором установлен физический ресурс (сервер), на базе которого развернута эта виртуальная среда.

Видеонаблюдение центра обработки данных пользователя платежной системы обеспечивает наблюдение за всеми проходами, входами в центр обработки данных пользователя платежной системы. В центре обработки данных пользователя платежной системы расстановка видеокамер исключает наличие зон внутри помещения центра обработки данных пользователя платежной системы и перед его входом, не покрытых видеонаблюдением.

Запись видеосигналов центра обработки данных пользователя платежной системы ведется непрерывно или с использованием детектора движения.

Архив видеозаписей центра обработки данных пользователя платежной системы хранится не менее 3 (трех) месяцев.";

пункт 24 изложить в следующей редакции:

"24. Терминал платежной системы либо его приложение устанавливается на специально выделенном для этих целей персональном компьютере, имеющем инвентарный номер и паспорт с подробными данными по конфигурации, программным и аппаратным средствам, установленным на нем, или виртуальной среде, имеющей инвентарный номер и паспорт с подробным описанием установленных программных средств, параметров конфигурации, а также аппаратных характеристик физического ресурса (сервера), на котором она развернута, и выделенных для нее вычислительных ресурсов.";

дополнить пунктом 24-1 следующего содержания:

"24-1. В случае установки терминала платежной системы на виртуальной среде, пользователь платежной системы использует гипервизор, обеспечивающий изоляцию виртуальной среды от иных цифровых систем.

Пользователь платежной системы обеспечивает разграничение административного доступа к гипервизору, контроль целостности его конфигурации, учет действий администраторов рабочего места пользователя платежной системы, а также установку обновлений.";

пункт 26 изложить в следующей редакции:

"26. Работа с терминалом платежной системы осуществляется с рабочего места пользователя платежной системы. В случае установки терминала платежной системы на виртуальной среде, доступ к терминалу платежной системы осуществляется с персонального компьютера, предназначенного для работы с платежной системой и размещенного в Помещении, посредством удаленного подключения.

При удаленном подключении к терминалу платежной системы, пользователь платежной системы обеспечивает:

1) защиту каналов связи с рабочим местом пользователя платежной системы средствами шифрования и контроля целостности, обеспечивающими конфиденциальность и неизменность передаваемых данных;

2) использование механизмов аутентификации лиц, допущенных к работе с платежной системой, с использованием цифровых объектов и средств идентификации, соответствующих требованиям законодательства Республики Казахстан о кибербезопасности, о персональных данных и их защите;

3) реализацию автоматизированного логирования и мониторинга действий лиц, допущенных к работе с платежной системой, с фиксацией попыток доступа и изменений в конфигурации терминала платежной системы;

4) разграничение прав доступа лиц, допущенных к работе с платежной системой.

Не допускается установка и использование систем удаленного доступа на рабочем месте пользователя платежной системы при установке терминала платежной системы на персональный компьютер. Встроенные службы удаленного доступа на рабочем месте пользователя платежной системы (персональном компьютере) удаляются или отключаются.";

пункты 30, 31 и 32 изложить в следующей редакции:

"30. Ключевая информация хранится в персональном компьютере, на котором установлен терминал платежной системы, либо в персональном компьютере с настроенным удаленным подключением по защищенным каналам связи к виртуальной среде, на которой установлен терминал платежной системы, с применением программных средств защиты, обеспечивающих ее конфиденциальность, целостность и контроль доступа.

31. Наличие несанкционированных копий ключевой информации, в том числе на жестком диске рабочего места пользователя платежной системы, не допускается.

32. Порядок хранения и использования ключевой информации на рабочем месте пользователя платежной системы исключает возможность несанкционированного доступа к ним.";

пункт 35 исключить;

пункт 37 исключить;

подпункты 4) и 5) пункта 39 исключить;

пункты 40 и 41 изложить в следующей редакции:

"40. На рабочем месте пользователя платежной системы обеспечивается реализация функций защиты от несанкционированного доступа, включая:

1) аутентификацию лиц, допущенных к работе с платежной системой;

2) контроль и разграничение прав доступа лиц, допущенных к работе с платежной системой;

3) регистрацию событий доступа и действий лиц, допущенных к работе с платежной системой.

Указанные функции реализуются с использованием средств защиты от несанкционированного доступа, соответствующих требованиям главы 9 Требований № 53.

41. На рабочее место пользователя платежной системы устанавливаются средства обнаружения вредоносного программного кода и (или) программы.

В случае установки терминала платежной системы на виртуальной среде, пользователем платежной системы обеспечивается использование средств обнаружения вредоносного программного кода и (или) программы встроенных функций безопасности виртуальных сред, при отсутствии таких возможностей – подтверждение производителя о тестировании средств обнаружения вредоносного программного кода и (или) программы в виртуальных средах, используемых пользователем платежной системы.

При выявлении факта заражения данная информация немедленно сообщается в подразделение безопасности пользователя платежной системы.";

пункты 43 и 44 изложить в следующей редакции:

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

44. В случае установки терминала платежной системы на персональном компьютере, 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.

В случае установки терминала платежной системы на виртуальной среде, опечатывается или опломбируется системный блок персонального компьютера с настроенным удаленным подключением по защищенным каналам связи к этой виртуальной среде с указанием на стикере или пломбе даты последнего опечатывания или опломбирования и инвентарного номера учета персонального компьютера.";

пункты 49 и 50 изложить в следующей редакции:

"49. Персональный компьютер, на котором установлен терминал платежной системы, либо физический ресурс (сервер), на базе которого развернута виртуальная среда с установленным терминалом платежной системы, и персональный компьютер с настроенным удаленным подключением по защищенным каналам связи к этой виртуальной среде, оснащается техническими средствами бесперебойного электропитания, обеспечивающими функционирование оборудования при отсутствии напряжения в электросети в течение времени, необходимого для корректного завершения работы в системе, но не менее тридцати минут.

50. В случае внесения изменений в программное обеспечение, посредством которого осуществляется связь между пользователем платежной системы и Центром, в средства защиты от несанкционированного доступа рабочего места пользователя

платежной системы, а также в технологию передачи электронных документов, подготовленных в цифровой 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.";

абзац первый подпункта 3) пункта 53 изложить в следующей редакции:

"3) журнал опломбирования и проверки целостности пломб и печатей системного блока персонального компьютера, на котором установлен терминал платежной системы, или персонального компьютера с настроенным удаленным подключением по защищенным каналам связи к виртуальной среде с установленным терминалом платежной системы с указанием:";

в пункте 56:

подпункт 7) изложить в следующей редакции:

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

дополнить подпунктами 11) и 12) следующего содержания:

"11) порядок предоставления удаленного подключения к терминалу платежной системы на виртуальной среде, включая условия предоставления доступа, используемые механизмы аутентификации, разграничение прав доступа лиц, допущенных к работе с платежной системой, а также регистрацию и хранение сведений о подключениях;

12) порядок функционирования гипервизора, на базе которого работает виртуальная среда, включая порядок контроля целостности и конфигурации гипервизора, установки обновлений, административного доступа, а также учета действий администраторов рабочего места пользователя платежной системы, мониторинга событий кибербезопасности и выявления попыток несанкционированного доступа.";

пункт 61 изложить в следующей редакции:

"61. Пользователь платежной системы обеспечивает:

1) 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;

2) функционирование механизма динамического переключения взаимодействия с основным центром на резервный центр платежной системы Центра.";

пункт 63 изложить в следующей редакции:

"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 других транспортных систем, включая систем электронного документооборота, 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 других транспортных систем, включая систем электронного документооборота, 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 других транспортных систем, включая систем электронного документооборота, Национальному Банку письмо о результате перевода программно-технического комплекса обратно на основной центр в течение трех часов после завершения работ по переводу.";

часть вторую пункта 64 изложить в следующей редакции:

"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 десяти рабочих дней после дня завершения мероприятий после перевода программно-технического комплекса с резервного на основной центр."

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 с 12 июля 2026 года и подлежит официальному опубликованию.

*Председатель Национального
Банка Республики Казахстан*

Т. Сулейменов