Зарегистрирован в Министерстве юстиции Республики Казахстан
25 февраля 2016 года № 13256

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҰЛТТЫҚ БАНКІ»

РЕСПУБЛИКАЛЫҚ МЕМЛЕКЕТТІК МЕКЕМЕСІ

БАСҚАРМАСЫНЫҢ ҚАУЛЫСЫ

28 января 2016 года

Алматы қаласы

РЕСПУБЛИКАНСКОЕ ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ

«НАЦИОНАЛЬНЫЙ БАНК РЕСПУБЛИКИ КАЗАХСТАН»

ПОСТАНОВЛЕНИЕ ПРАВЛЕНИЯ

№ 34

город Алматы

Об утверждении Требований к безопасности и беспрерывности работы информационных систем банков и организаций, осуществляющих отдельные виды банковских операций

(с изменениями и дополнениями от 22.12.2017 г.)

В целях реализации Закона Республики Казахстан от 24 ноября 2015 года «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам неработающих кредитов и активов банков второго уровня, оказания финансовых услуг и деятельности финансовых организаций и Национального Банка Республики Казахстан» и в целях установления требований к безопасности и беспрерывности работы информационных систем банков и организаций, осуществляющих отдельные виды банковских операций, при оказании электронных банковских услуг Правление Национального Банка Республики Казахстан **ПОСТАНОВЛЯЕТ**:

1. Утвердить прилагаемые Требования к безопасности и беспрерывности работы информационных систем банков и организаций, осуществляющих отдельные виды банковских операций.

2. Департаменту развития и управления платежными системами (Мусаев Р.Н.) в установленном законодательством Республики Казахстан порядке обеспечить:

1) совместно с Департаментом правового обеспечения (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 получения Национальным Банком

Республики Казахстан после государственной регистрации в Министерстве юстиции Республики Казахстан;

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

3. Департаменту международных отношений и связей с общественностью (Казыбаев А.К.) обеспечить направление настоящего постановления на официальное опубликование в периодических печатных изданиях в течение десяти календарных дней после его государственной регистрации в Министерстве юстиции Республики Казахстан.

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

5. Настоящее постановление вводится в действие с 1 января 2017 года и подлежит официальному опубликованию.

Председатель
Национального Банка **Д. Акишев**

Утверждены
постановлением Правления
Национального Банка
Республики Казахстан
от 28 января 2016 года № 34

Требования
к безопасности и беспрерывности работы информационных систем банков и организаций,
осуществляющих отдельные виды банковских операций

Заголовок главы 1 изложен в редакции постановления Правления Национального Банка РК от 22.12.17 г. № 248 (см. стар. ред.)

Глава 1. Общие положения

Пункт 1 изложен в редакции постановления Правления Национального Банка РК от 22.12.17 г. № 248 (см. стар. ред.)

1. Настоящие Требования к безопасности и беспрерывности работы информационных систем банков и организаций, осуществляющих отдельные виды банковских операций (далее - Требования), разработаны в соответствии с законами Республики Казахстан от 30 марта 1995 года «О Национальном Банке Республики Казахстан», от 31 августа 1995 года «О банках и банковской деятельности в Республике Казахстан» (далее - Закон о банках), от 26 июля 2016 года «О платежах и платежных системах» (далее - Закон о платежах и платежных системах) и устанавливают требования к безопасности и беспрерывности работы информационных систем банков и организаций, осуществляющих отдельные виды банковских операций (далее - банки), посредством которых обеспечивается оказание электронных банковских услуг.

В пункт 2 внесены изменения в соответствии с постановлением Правления Национального Банка РК от 22.12.17 г. № 248 (см. стар. ред.)

2. В Требованиях используются понятия, предусмотренные Законом о платежах и платежных системах, Законом Республики Казахстан от 24 ноября 2015 года «Об информатизации», Правилами оказания банками и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг, утвержденными постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 212, зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 14337 (далее - Правила № 212), а также следующие понятия:

1) объект информационной системы - отдельный компонент информационной системы, предназначенный для передачи, обработки и хранения информации для выполнения отдельной функции при оказании электронных банковских услуг;

2) основной центр информационной системы банка (далее - основной центр) - совокупность программно-технических средств и обслуживающего персонала, обеспечивающих оказание электронных банковских услуг в штатном (повседневном) режиме;

3) резервный центр информационной системы банка (далее - резервный центр) - совокупность программно-технических средств и обслуживающего персонала, обеспечивающих оказание электронных банковских услуг при возникновении нестандартных ситуаций или проведении плановых технических работ в основном центре;

4) информационная система банка для оказания электронных банковских услуг (далее - информационная система) - система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением аппаратно-программного комплекса, посредством которой обеспечивается оказание электронных банковских услуг;

5) ответственный работник - работник банка, ответственный за работу в информационной системе в соответствии с должностными обязанностями;

6) рабочее место - персональный компьютер (сервер), на котором установлен программно-пользовательский интерфейс для управления информационной системой либо объектами информационной системы;

7) команда восстановления - работники банка и организаций, оказывающих услуги по обеспечению доступности и полноценного функционирования информационной системы или объектов информационной системы, которые обеспечивают полное восстановление с учетом времени простоя, установленным внутренними документами банка, либо перевод работы информационной системы в резервный центр;

8) пользователь - клиент банка, обращающийся к информационной системе за получением электронных банковских услуг, либо ответственный работник;

9) идентификация - подтверждение подлинности субъекта или объекта доступа к информационной системе путем определения соответствия предъявленных реквизитов доступа.

3. Управление операционным риском, непрерывностью деятельности, рисками информационных технологий, информационной безопасностью в целях обеспечения безопасности и беспрерывности работы информационных систем банков, за исключением организаций, осуществляющих отдельные виды банковских операций, осуществляется в соответствии с постановлением Правления Национального Банка Республики Казахстан от 26 февраля 2014 года № 29 «Об утверждении Правил формирования системы управления рисками и внутреннего контроля для банков второго уровня», зарегистрированным в Реестре государственной регистрации нормативных правовых актов под № 9322.

Заголовок главы 2 изложен в редакции постановления Правления Национального Банка РК от 22.12.17 г. № 248 (см. стар. ред.)

Глава 2. Требования к рабочим местам

4. На рабочих местах банк обеспечивает:

1) установку и функционирование программного или программно-аппаратного комплекса защиты от несанкционированного доступа, включающего в себя средства идентификации и аутентификации ответственного работника;

2) установку и функционирование технических средств бесперебойного электропитания, позволяющих осуществлять работу рабочего места при отсутствии напряжения в электросети в течение времени, необходимого для корректного завершения работы в информационной системе, но не менее десяти минут. Допускается использование общего источника бесперебойного питания, установленного в здании банка;

3) установку и функционирование средств обнаружения вредоносного программного кода и/или программы. В случае выявления факта заражения данная информация доводится до сведения подразделения безопасности банка;

4) программную либо программно-аппаратную защиту передаваемой информации и каналов связи. Допускается централизованная защита передаваемой информации путем установки соответствующих программно-аппаратных средств на специально выделенных рабочих местах.

5. Порядок хранения и использования технических средств, паролей или другой информации, предоставляющих доступ к рабочему месту, обеспечивает защиту данных от несанкционированного доступа.

6. Порядок доступа к ресурсам (дисковое пространство, директории, сетевые ресурсы, базы данных), выделенным для накопления в них информации для передачи в информационную систему, получения информации из информационной системы, хранения, архивирования либо другой обработки информации, обеспечивает защиту от доступа к этим ресурсам лиц, не имеющих допуска к работе с ними.

7. Доступ к рабочему месту ответственным работником осуществляется в соответствии с его должностными обязанностями.

8. Одному системному имени пользователя, по которому идентифицируется пользователь на входе в информационные системы, соответствует один ответственный работник, за исключением работников, выполняющих функции администратора. Для работника, выполняющего функции администратора, допускается создание нескольких системных имен пользователя.

9. Порядок доступа к рабочему месту посредством сети и иных технических каналов передачи данных минимизирует возможность несанкционированного доступа.

10. Во внутренних документах банка, предусматривающих порядок работы ответственных работников, имеющих доступ в информационную систему, определяются:

1) порядок назначения ответственных работников;

2) режим работы ответственных работников;

3) права и обязанности ответственных работников, включая должностные инструкции;

4) список команды восстановления.

Заголовок главы 3 изложен в редакции постановления Правления Национального Банка РК от 22.12.17 г. № 248 (см. стар. ред.)

Глава 3. Требования к документации по структуре и функционированию информационной системы

11. В документации банка по структуре и функционированию информационных систем указывается:

1) перечень информационных систем и их объектов, их назначение и основные характеристики, требования к числу уровней иерархии и степени централизации систем, в том числе, перечень функций, задач по каждому объекту информационной системы;

2) требования к способам и средствам связи для информационного обмена между компонентами информационных систем;

3) планы восстановления работы информационных систем (далее - план восстановления);

4) требования к режимам функционирования информационных систем;

5) требования к мониторингу функционирования информационных систем;

6) требования к классификации, количеству и режиму работы ответственных работников команды восстановления.

12. Документация банка по структуре и функционированию информационных систем подлежит пересмотру на предмет актуализации на периодической основе, определенной банком, но не реже одного раза в год.

Заголовок главы 4 изложен в редакции постановления Правления Национального Банка РК от 22.12.17 г. № 248 (см. стар. ред.)

Глава 4. Требования к безопасности работы информационных систем

13. При обращении пользователя к информационной системе для получения электронной банковской услуги банк обеспечивает:

1) регистрацию действий по получению клиентами электронных банковских услуг в электронных журналах без возможности изменения внесенных в них данных, в том числе, как успешных, так и неудачных, начиная от попытки установления связи, с указанием времени совершения операций. Период хранения сведений электронных журналов составляет не менее 2 (двух) месяцев;

2) функционирование программного обеспечения, предназначенного для автоматического мониторинга, выявления и блокирования в информационной системе несанкционированных операций или действий, направленных на создание условий для проведения несанкционированных операций;

3) архитектуру «клиент-сервер», позволяющую при выводе из строя рабочего места пользователя или получении злоумышленником несанкционированного доступа к нему не влиять на работу серверной части системы, а при сбое сервера приложений не влиять на состояние данных системы;

4) резервное копирование и архивацию данных с возможностью их последующего восстановления;

5) выполнение действий, предусмотренных подпунктом 4) пункта 4 Требований.

14. При оказании электронных банковских услуг осуществляется шифрование относящихся к банковской тайне передаваемых данных и (или) информационно-коммуникационной сети для их передачи от персональных компьютеров, телефонов, электронных терминалов и иных устройств до конечной системы обработки передаваемых данных.

Пункт 15 изложен в редакции постановления Правления Национального Банка РК от 22.12.17 г. № 248 (см. стар. ред.)

15. Требования к процедурам безопасности при оказании электронных банковских услуг устанавливаются Правилами № 212.

Заголовок главы 5 изложен в редакции постановления Правления Национального Банка РК от 22.12.17 г. № 248 (см. стар. ред.)

Глава 5. Требования к обеспечению беспрерывности работы информационных систем

16. В целях обеспечения беспрерывности предоставления электронных банковских услуг банки определяют во внутренних документах план восстановления, порядок его пересмотра и тестирования.

17. Разработка плана восстановления осуществляется с учетом следующих факторов:

1) виды и характер нестандартных ситуаций, их степень воздействия на деятельность банка;

2) перечень информационных систем и их объектов, обеспечивающих оказание электронных банковских услуг, с указанием приоритетности их восстановления;

3) ущерб, возникающий при остановке работы информационных систем, и затраты для восстановления их работы.

18. При указании перечня информационных систем определяются допускаемые сроки их восстановления. Сроки устанавливаются банком в зависимости от критичности простоя в работе информационной системы.

19. План восстановления содержит следующие условия:

1) наличие и место нахождения резервного центра;

2) перечень бизнес-процессов, объектов информационной системы, технических, программных или других средств, обеспечивающих работу информационной системы, восстановление которых требуется в резервном центре;

3) порядок проведения, периодичность и сценарии тестирования функционирования резервного центра информационной системы;

4) порядок восстановления нарушенных информационных систем после ликвидации последствий нестандартных ситуаций, критерии, позволяющие принять решение о завершении работы в нестандартном режиме, и порядок принятия такого решения, а также порядок возврата в штатный режим функционирования.

20. В целях проверки готовности работы резервного центра и резервных каналов связи для восстановления деятельности информационной системы банк не менее одного раза в год проводит тестирование функционирования резервного центра и резервных каналов связи в соответствии с планом восстановления (далее - тестирование Плана).

21. Тестирование Плана проводится по разработанной и утвержденной банком программе, предусматривающей описание сценария возникновения нестандартной ситуации, восстанавливаемых рабочих процессов и объектов информационной системы, действий команды восстановления, требований по срокам и месту проведения работ.

22. По итогам тестирования Плана банком подготавливается документ о результатах тестирования (протокол) с указанием:

1) перечня информационных систем и их объектов, по которым проведено тестирование;

2) времени, затраченного на восстановление работы информационных систем и их объектов;

3) выявленных уязвимостей и предложений по их устранению.

Сведения о результатах тестирования представляются банком в Национальный Банк Республики Казахстан (далее - Национальный Банк) в течение десяти рабочих дней после утверждения документа о результатах тестирования уполномоченным органом банка.

Пункт 23 изложен в редакции постановления Правления Национального Банка РК от 22.12.17 г. № 248 (см. стар. ред.)

23. При возникновении сбоя (простоя) в работе информационной системы банк обеспечивает восстановление работы основного центра.

При отсутствии возможности восстановления работы основного центра в период минимально допустимого срока восстановления осуществляется перевод информационной системы на работу резервного центра.

Стандартный норматив времени по переводу информационной системы на резервный центр составляет не более четырех часов с момента возникновения сбоя (простоя).

При возникновении сбоя (простоя) в работе информационной системы банка, повлекшего прерывание доступа клиентов к электронным банковским услугам посредством систем удаленного доступа и (или) к сети электронных терминалов банка, продолжительностью более трех часов банк незамедлительно уведомляет Национальный Банк путем направления электронного сообщения. В случае возникновения сбоя (простоя) в нерабочее время, банк уведомляет Национальный Банк не позднее 10.00 часов времени города Астаны рабочего дня, следующего за днем возникновения сбоя (простоя).

24. Банк в направляемых в соответствии с Законом о банках клиентам уведомлениях о планируемом введении в действие изменений (обновлений), вносимых в технические, программные и другие средства, обеспечивающие работу информационной системы, и влияющих на доступность клиенту электронных банковских услуг, указывает вид электронных банковских услуг, на доступность которых повлияют планируемые изменения, а также время их предполагаемой недоступности. Минимальные требования по доведению до сведения клиентов уведомления о планируемых изменениях включают размещение оповещений на интернет-ресурсе банка.

25. Банк ежеквартально, не позднее десятого числа месяца, следующего за отчетным кварталом, направляет в Национальный Банк информацию о произошедших в течение отчетного периода плановых и внеплановых простоях (сбоях) не менее одного часа в работе информационной системы.

Сведения включают информацию о виде электронной банковской услуги, доступ к которой был приостановлен клиентам, периоде времени простоя (сбоя), предпринятых действиях и результатах работ по устранению простоя (сбоя).