

Об утверждении Инструкции об организации информационного процесса в деятельности участников системы формирования кредитных историй и их использования, формирования системы безопасности, установлении минимальных требований к их электронному оборудованию, сохранности базы данных кредитных историй и помещениям

Утративший силу

Постановление Председателя Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций от 18 июля 2008 года № 105. Зарегистрировано в Министерстве юстиции Республики Казахстан 25 сентября 2008 года № 5310. Утратило силу постановлением Правления Национального Банка Республики Казахстан от 27 мая 2015 года № 91

Сноска. Утратило силу постановлением Правления Национального Банка РК от 27.05.2015 № 91 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

В целях совершенствования нормативных правовых актов, регулирующих деятельность кредитных бюро, Правление Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций (далее - Агентство) **ПОСТАНОВЛЯЕТ:**

1. Утвердить прилагаемую Инструкцию об организации информационного процесса в деятельности участников системы формирования кредитных историй и их использования, формирования системы безопасности, установлении минимальных требований к их электронному оборудованию, сохранности базы данных кредитных историй и помещениям (далее - Инструкция).

2. Признать утратившими силу:

1) постановление Правления Агентства от 25 октября 2004 года № 303 "Об утверждении Инструкции об организации информационного процесса в деятельности участников системы формирования кредитных историй и их использования, защиты и сохранности базы данных кредитных историй, о минимальных требованиях к их информационным ресурсам, информационным системам, помещениям, электронному оборудованию" (зарегистрированное в Реестре государственной регистрации нормативных правовых актов под № 3318, опубликованное в Бюллетене нормативных правовых актов центральных исполнительных и иных государственных органов Республики Казахстан, № 3-8, 2 0 0 5 г . , с т . 1 8) ;

2) постановление Правления Агентства от 27 августа 2007 года № 221 "О внесении изменений и дополнения в постановление Правления Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций от 25 октября 2004 года № 303 "Об утверждении Инструкции об организации информационного процесса в деятельности участников системы формирования кредитных историй и их использования, защиты и сохранности базы данных кредитных историй, о минимальных требованиях к их информационным ресурсам, информационным системам, помещениям, электронному оборудованию" (зарегистрированное в Реестре государственной регистрации нормативных правовых актов под № 4966).

3. Настоящее постановление вводится в действие по истечении десяти календарных дней со дня первого официального опубликования.

4. Кредитным бюро в течение двух месяцев со дня введения в действие настоящего постановления привести свою деятельность в соответствие с И н с т р у к ц и е й .

5. Управлению информационных технологий (Тусупов К.А.):

1) совместно с Юридическим департаментом (Сарсенова Н.В.) 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 довести настоящее постановление до сведения кредитных бюро, Объединения юридических лиц "Ассоциация финансистов Казахстана" .

6. Службе Председателя Агентства (Кенже А.А.) обеспечить публикацию настоящего постановления в средствах массовой информации Республики К а з а х с т а н .

7. Контроль за исполнением настоящего постановления возложить на заместителя Председателя Агентства Байсынова М.Б.

Председатель

Е. Бахмутова

" С О Г Л А С О В А Н О "

Агентство Республики Казахстан
по информатизации и связи

25 августа 2008 года

П р е д с е д а т е л ь

Е с е к е е в К . Б .

(п о д п и с ь , д а т а ,

гербовая печать)

У т в е р ж д е н а
постановлением Правления
Агентства Республики Казахстан
по регулированию и надзору
финансового рынка и
финансовых организаций
от 18 июля 2008 года № 105

Инструкция

об организации информационного процесса в деятельности участников системы формирования кредитных историй и их использования, формирования системы безопасности, установлении минимальных требований к их электронному оборудованию, сохранности базы данных кредитных историй и помещениям

1. Общие положения

Сноска. Заголовок главы в редакции постановления Правления Национального Банка РК от 24.02.2012 № 89 (вводится в действие по истечении десяти календарных дней после дня его первого опубликования).

1. В настоящей Инструкции используются понятия, предусмотренные Законом Республики Казахстан от 6 июля 2004 года "О кредитных бюро и формировании кредитных историй в Республике Казахстан" (далее - Закон о кредитном бюро), а также следующие понятия:

1) администратор безопасности информационных систем (далее - администратор) - работник организации, обеспечивающий функционирование системы электронного получения и (или) передачи данных, реализацию мер по их защите, осуществляющий генерацию поступающей и (или) передаваемой информации с учетом ее функций и полномочий;

2) аутентификация - подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа и м е ю щ и м с я в с и с т е м е ;

3) ввод в эксплуатацию - процесс выполнения организационно- технических мероприятий по подготовке информационной системы и начало функционирования данной системы в промышленных условиях;

4) идентификатор - уникальные персональный код и (или) имя, присвоенные субъекту и (или) объекту системы, и предназначенные для регламентированного

историй), участвующие в обмене электронными документами и являющиеся сторонами договора о предоставлении информации и (или) получении кредитных отчетов;

16) помещение ограниченного доступа - помещение, в котором разрешается пребывание ограниченного круга лиц, и доступ других лиц в эти помещения может происходить только в сопровождении специально допущенных работников.

2. Организация информационного процесса

Сноска. Заголовок главы в редакции постановления Правления Национального Банка РК от 24.02.2012 № 89 (вводится в действие по истечении десяти календарных дней после дня его первого опубликования).

2. Организация и функционирование информационной системы формирования и использования кредитных историй обеспечивают:

1) координацию и управляемость деятельности ее участников в рамках согласованных процедур и технологических параметров;

2) унификацию используемых программных и технических средств;

3) информационную безопасность, включая устранение возможности раскрытия информации;

4) внедрение высокоэффективных технологий;

5) гибкое и эффективное управление ресурсами;

6) рост качества услуг.

3. Организация обеспечивает:

1) контроль ввода данных;

2) возможность вычисления параметров документов (номеров документов, кода связи, номера договора);

3) генерацию сводной информации;

4) создание резервных копий, архивирование данных;

5) использование информационных систем, имеющих штатные средства защиты, с контролем за правами доступа;

6) наличие регламентированных процедур предоставления и получения электронных сообщений;

7) возможность подготовки аналитических и статистических отчетов.

4. Поставщики информации и получатели кредитного отчета обеспечивают выполнение организационных, технологических условий и требований кредитного бюро, вытекающие из заключенных с ним договоров о предоставлении информации и (или) получении кредитных отчетов и внутренних документов кредитного бюро, предусмотренных Законом о кредитном бюро.

5. Информация, представленная поставщиком информации, может быть возвращена кредитным бюро без ее использования в информационной системе формирования и использования кредитных историй, в связи с ее неправильным или неполным оформлением, несоответствием данных поставщика информации, получателя кредитного отчета, субъекта кредитной истории требованиям в используемой информационной системе.

3. Условия обмена информацией между поставщиками информации, получателями кредитных отчетов и кредитными бюро, а также условия проведения сверки информации, содержащейся в базах данных кредитного бюро с государственным участием и иных кредитных бюро

Сноска. Заголовок главы в редакции постановления Правления Национального Банка РК от 24.02.2012 № 89 (вводится в действие по истечении десяти календарных дней после дня его первого опубликования).

6. Обмен информацией между поставщиками информации, получателями кредитных отчетов и кредитными бюро осуществляется через информационную систему, условия использования которой определяются государственным уполномоченным органом, осуществляющим реализацию государственной политики и государственное регулирование в сфере информатизации и "электронного правительства" (далее - уполномоченный орган в сфере информатизации).

7. Кредитные бюро передают поставщикам информации и получателям кредитных отчетов специализированное программное обеспечение, необходимое для реализации информационных процессов либо устанавливают соответствующие требования к используемому ими программному обеспечению. В случае самостоятельной разработки специализированного программного обеспечения поставщиками информации и получателями кредитных отчетов оно согласуется с кредитными бюро.

8. Процесс разработки, внедрения и сопровождения информационных систем включает определение этапов разработки, порядка внесения изменений, приема, тестирования и ввода в эксплуатацию, требования к документированию всех этапов.

9. Разработка, внедрение и сопровождение информационных систем кредитными бюро выполняется в соответствии с их внутренними документами и действующими на территории Республики Казахстан стандартами.

10. Разработка информационных систем выполняется кредитными бюро на основании технического задания, утвержденного его первым руководителем.

11. В целях исключения несанкционированного изменения программного обеспечения и (или) данных информационной системы при необходимости внесения изменений (для устранения недостатков или доработки системы) в программное обеспечение, процесс внесения изменений осуществляется в соответствии с техническим заданием, стандартами, действующими на территории Республики Казахстан, и политикой информационной безопасности кредитных бюро.

12. При формировании и использовании информационных систем для размещения базы данных кредитных историй и средств защиты указанных информационных систем применяются сертифицированное оборудование и программное обеспечение.

13. Кредитное бюро осуществляет обмен данными с поставщиками информации и получателями кредитных отчетов по выделенным каналам связи или через Интернет, при условии:

1) наличия основного канала, пропускной способностью не менее 10 мегабит в секунду;

2) наличия беспроводного резервного канала, пропускной способностью не менее 2 мегабит в секунду;

3) использования каналов разных провайдеров;

4) использования каналов исключительно для обмена информацией с поставщиками информации и получателями кредитных отчетов.

14. Для подтверждения соответствия требованиям, предъявляемым к участникам системы формирования кредитных историй и их использования (за исключением микрофинансовой организации и субъекта кредитной истории), поставщик информации или получатель кредитных отчетов направляет в уполномоченный орган в сфере информатизации заявление на бумажном носителе либо через веб-портал «электронного правительства»: www.e.gov.kz (далее – ПЭП) или веб-портал «Е лицензирование» www.elicense.kz (далее – Портал) в виде электронного документа, удостоверенного электронной цифровой подписью (далее – ЭЦП).

Соблюдение организацией (за исключением микрофинансовой организации) организационно-технических, технологических требований по защите программного обеспечения, соответствие используемых информационных систем установленным Инструкцией и законодательством Республики Казахстан условиям и требованиям, подтверждается комиссией уполномоченного органа в сфере информатизации, созданной совместно с уполномоченным органом по регулированию, контролю и надзору финансового рынка и финансовых организаций (далее - уполномоченный орган), путем составления акта о соответствии требованиям, предъявляемым к участникам системы формирования

кредитных историй и их использования (за исключением микрофинансовой организации и субъекта кредитной истории) по форме согласно приложению 1 к Инструкции (далее - акт о соответствии) в виде электронного документа, удостоверенного ЭЦП руководителя комиссии, созданной уполномоченным органом в сфере информатизации совместно с уполномоченным органом.

Акт о соответствии согласовывается всеми членами комиссии, после чего направляется на подписание представителю проверяемой организации. Если один из членов комиссии не согласен с принятым решением и не согласовывает акт о соответствии, он представляет в письменной форме информацию о причинах своего отказа комиссии и прилагает их к акту о соответствии через П Э П и л и П о р т а л .

Акт о соответствии считается принятым при наличии двух третей решений о согласовании членов комиссии уполномоченного органа в сфере информатизации и двух третей решений о согласовании членов комиссии уполномоченного органа.

Соблюдение микрофинансовой организацией организационно-технических, технологических требований по защите программного обеспечения, соответствие используемых информационных систем установленным Инструкцией и законодательством Республики Казахстан условиям и требованиям, подтверждается уполномоченным органом путем представления заключения о соответствии требованиям, предъявляемым к микрофинансовой организации по форме согласно приложению 2 к Инструкции (далее – заключение уполномоченного органа).

Сноска. Пункт 14 в редакции постановления Правления Национального Банка РК от 25.01.2013 № 9 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

15. Обмен информацией между поставщиками информации (за исключением микрофинансовых организаций), получателями кредитных отчетов и кредитными бюро осуществляется при наличии акта о соответствии с положительным заключением.

Обмен информацией между микрофинансовыми организациями, получателями кредитных отчетов и кредитными бюро осуществляется при наличии положительного заключения уполномоченного органа.

Сноска. Пункт 15 в редакции постановления Правления Национального Банка РК от 25.01.2013 № 9 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

16. Входящий и исходящий трафик должен быть обеспечен криптографической защитой.

16-1. Кредитное бюро с государственным участием утверждает внутренние

процедуры проведения сверки информации, содержащейся в базах данных кредитного бюро с государственным участием и иных кредитных бюро (далее - внутренние процедуры), которые подлежат согласованию с уполномоченным о р г а н о м .

Сноска. Инструкция дополнена пунктом 16-1 в соответствии с постановлением Правления Национального Банка РК от 24.02.2012 № 89 (вводится в действие по истечении десяти календарных дней после дня его первого о п у б л и к о в а н и я) .

16-2. Внутренние процедуры определяют: условия, порядок и сроки проведения сверки; параметры информации, подлежащей сверке; требование к программному обеспечению, необходимому для реализации информационных процессов, связанных со сверкой; порядок обеспечения защиты информации, подлежащей сверке; порядок возмещения кредитному бюро с государственным участием фактических расходов, понесенных в связи с проведением сверки.

Сноска. Инструкция дополнена пунктом 16-2 в соответствии с постановлением Правления Национального Банка РК от 24.02.2012 № 89 (вводится в действие по истечении десяти календарных дней после дня его первого о п у б л и к о в а н и я) .

16-3. Кредитное бюро для обеспечения достоверности информации, хранимой в базе данных кредитных историй кредитного бюро, не менее одного раза в год проводит ее сверку с информацией кредитного бюро с государственным участием на условиях, в порядке и сроки, определенными внутренними процедурами кредитного бюро с государственным участием.

Сверка информации, хранящейся в базе данных кредитных историй кредитного бюро, проводится не позднее двадцатого рабочего дня последнего м е с я ц а о т ч е т н о г о г о д а .

Объем информации, подлежащей сверке, определяется кредитным бюро самостоятельно, при условии соответствия параметров информации, подлежащих сверке, параметрам информации, определенным во внутренних процедурах кредитного бюро с государственным участием.

Сноска. Инструкция дополнена пунктом 16-3 в соответствии с постановлением Правления Национального Банка РК от 24.02.2012 № 89 (вводится в действие по истечении десяти календарных дней после дня его первого о п у б л и к о в а н и я) .

16-4. Кредитное бюро с государственным участием сверяет информацию, принятую от иного кредитного бюро, с информацией, содержащейся в базе данных кредитных историй кредитного бюро с государственным участием в срок

, установленный внутренними процедурами.

Сноска. Инструкция дополнена пунктом 16-4 в соответствии с постановлением Правления Национального Банка РК от 24.02.2012 № 89 (вводится в действие по истечении десяти календарных дней после дня его первого опубликования).

16-5. Уполномоченные представители кредитного бюро с государственным участием и иного кредитного бюро подтверждают соответствие или несоответствие информации, содержащейся в их базах данных кредитных историй, подлежащей сверке, путем составления в произвольной форме акта сверки или акта несоответствия.

При составлении акта несоответствия кредитное бюро с государственным участием в течение двух рабочих дней со дня составления представляет его копию в уполномоченный орган.

Сноска. Инструкция дополнена пунктом 16-5 в соответствии с постановлением Правления Национального Банка РК от 24.02.2012 № 89 (вводится в действие по истечении десяти календарных дней после дня его первого опубликования).

16-6. Акт сверки или акт несоответствия составляются в двух экземплярах, по одному для каждой из сторон, подписываются уполномоченными представителями сторон, осуществляющими сверку, и заверяются их печатями.

Сноска. Инструкция дополнена пунктом 16-6 в соответствии с постановлением Правления Национального Банка РК от 24.02.2012 № 89 (вводится в действие по истечении десяти календарных дней после дня его первого опубликования).

16-7. Акты сверки хранятся до проведения очередной сверки. Акты несоответствия подлежат хранению в течение пяти лет со дня их составления.

Сноска. Инструкция дополнена пунктом 16-7 в соответствии с постановлением Правления Национального Банка РК от 24.02.2012 № 89 (вводится в действие по истечении десяти календарных дней после дня его первого опубликования).

16-8. Кредитное бюро и кредитное бюро с государственным участием в течение десяти рабочих дней со дня составления акта несоответствия принимают меры по устранению выявленных несоответствий. О результатах принятых мер по устранению выявленных несоответствий кредитное бюро с государственным участием в течение трех рабочих дней уведомляет уполномоченный орган.

Сноска. Инструкция дополнена пунктом 16-8 в соответствии с постановлением Правления Национального Банка РК от 24.02.2012 № 89 (вводится в действие по истечении десяти календарных дней после дня его первого опубликования).

4. Формирование системы безопасности и минимальные требования к помещениям, электронному и иному оборудованию участников системы кредитных историй

Сноска. Заголовок главы в редакции постановления Правления Национального Банка РК от 24.02.2012 № 89 (вводится в действие по истечении десяти календарных дней после дня его первого опубликования).

17. Кредитное бюро размещается в нежилом здании, помещении с ограниченным доступом.

18. Система безопасности кредитного бюро должна отвечать требованиям, установленным настоящей Инструкцией:

- 1) к серверному помещению и помещению ограниченного доступа;
- 2) к системному программному обеспечению, используемому для автоматизации деятельности кредитного бюро;
- 3) к специализированному программному обеспечению (информационной системе), используемому для автоматизации деятельности кредитного бюро;
- 4) к техническим средствам (информационным ресурсам) кредитного бюро;
- 5) к обеспечению безопасности информации.

19. Оборудованное серверное помещение кредитного бюро содержит:

- 1) систему контроля доступа (индивидуальный электронный пропуск);
- 2) систему видеоконтроля входа в серверное помещение и кроссовые комнаты;
- 3) автоматическую систему газового пожаротушения с обязательным, полным резервом баллонов с газом, и подключенной к системе гарантированного питания;
- 4) систему охранной сигнализации дверей, окон и датчиками движения внутри гермозоны;
- 5) безотказную систему чистого питания находящуюся в гермозоне серверной комнаты;
- 6) систему гарантированного питания всей электрической сети серверной и кроссовых комнат, включая круглосуточное, дежурное освещение;
- 7) систему кондиционирования с полным резервом.

20. Серверное помещение должно располагаться в местах, где возможно впоследствии расширение пространства и есть возможность размещения крупногабаритной аппаратуры, и отвечать следующим требованиям:

- 1) минимальный допустимый размер серверной комнаты - 20 квадратных метров;
- 2) серверная комната должна быть соединена с главным электродом системы

заземления здания кондуитом размером 1,5;

3) требуемая минимальная высота потолка серверной комнаты должна составлять 2,44 метра.

21. Помещение ограниченного доступа кредитного бюро должно соответствовать следующим требованиям:

1) наличие системы контроля доступа (индивидуальный электронный пропуск), которая исключает возможность неконтролируемого проникновения в это помещение лиц, не допущенных к рабочему месту ответственного лица;

2) наличие системы видеоконтроля входа (видеокамера с постоянной записью)

3) наличие системы пожарной сигнализации;

4) наличие системы охранной сигнализации;

5) запрещается располагать в помещении рабочие места, не имеющие отношения к деятельности кредитного бюро;

6) при расположении помещения ограниченного доступа на первых или последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц, окна помещений оборудуются металлическими решетками;

7) в помещении ограниченного доступа размещаются рабочие места ответственных лиц.

22. К помещению ограниченного доступа поставщиков информации (за исключением микрофинансовой организации) и получателей кредитных отчетов предъявляются требования, установленные подпунктами 1), 3), 4), 5) и 6) пункта 21 Инструкции, а также доступ в помещение ограничивается списком ответственных лиц, каждое посещение которых регистрируется в журнале посещений с указанием фамилии, имени, при наличии - отчества, должности, даты, времени и цели посещения.

К помещению ограниченного доступа микрофинансовой организации предъявляются требования, установленные в подпунктах 1), 3), 4) и 5) пункта 21 Инструкции, а также доступ в помещение ограничивается списком ответственных лиц, каждое посещение которых регистрируется в журнале посещений с указанием фамилии, имени, при наличии - отчества, должности, даты, времени и цели посещения.

При наличии общей системы охранной сигнализации в здании, в котором расположена микрофинансовая организация, отдельная охранная сигнализация на помещение ограниченного доступа микрофинансовой организации не требуется.

Сноска. Пункт 22 в редакции постановления Правления Национального Банка РК от 25.01.2013 № 9 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

23. Рабочее место ответственного лица должно соответствовать следующим требованиям :

1) программное обеспечение устанавливается на специально выделенном персональном компьютере, имеющем паспорт, в котором указано его месторасположение, конфигурация, а также аппаратные и программные средства, установленные на нем. Паспорт оформляется за подписью руководителя организации и хранится у ответственного лица;

2) не допускается эксплуатация персонального компьютера ответственного лица и установка на нем программных средств, не связанных с целями подготовки, обработки, передачи или ведения электронных документов в рамках участия в информационной системе;

3) персональный компьютер ответственного лица должен иметь комплекс защиты, включающий в себя:

средства идентификации и аутентификации пользователей;
возможность ведения электронных журналов в течение срока хранения электронных документов, с целью контроля деятельности, связанной с доступом к компьютеру и действиями пользователей;

4) наличие одного системного имени пользователя (ответственного лица), по которому идентифицируется пользователь, при входе в информационную систему должно соответствовать одному физическому лицу;

5) персональный компьютер должен иметь средства обеспечения целостности и конфиденциальности программного обеспечения;

6) доступ к сетевым ресурсам и внешним носителям, а также к портам ввода-вывода информации с персонального компьютера оператора должен быть отключен, в том числе и в настройках базовой системы ввода-вывода;

7) системный блок, порты ввода-вывода информации персонального компьютера опечатываются либо пломбируются администратором. Процесс опечатывания (пломбирования) фиксируется в специальном журнале с указанием фамилии, имени, при наличии - отчества, должности, даты, времени и цели нанесения пломбы (печати). Для ноутбуков разрешается использовать только отключение устройств в базовой системе ввода-вывода без опечатывания портов. Выносить из здания компьютеры и ноутбуки не допускается, за исключением случаев проведения профилактических и ремонтных работ, которые проводятся на основании заявки ответственного лица руководителю службы информационной безопасности;

8) порядок доступа к иным ресурсам (дисковое пространство, директории, базы данных и резервные копии базы данных), выделенным для накопления в них информации для передачи в информационную среду с использованием системы защиты, получения информации из информационной среды, хранения,

архивирования либо другой обработки информации, должен исключать возможность несанкционированного доступа к этим ресурсам;

9) доступ к рабочему месту ответственного лица и в помещение ограниченного доступа осуществляется в соответствии с его должностными обязанностями.

24. Рабочее место оператора поставщиков информации и получателей кредитных отчетов должно размещаться в помещении ограниченного доступа и отвечать требованиям, установленным пунктом 23 настоящей Инструкции.

25. Использование кредитным бюро системных программных обеспечений (операционные системы, системы управления базами данных, офисные программы, антивирусные программы) должны подтверждаться лицензиями, сертификатами.

26. Для накопления и хранения данных по кредитным историям должна использоваться промышленная система управления базами данных, разработчик которой должен иметь официальное представительство и центр технической поддержки на территории Республики Казахстан.

27. Внедрение и ввод в эксплуатацию (разработка или адаптация готового продукта) программного обеспечения кредитным бюро выполняется на основании технического задания, утвержденного его первым руководителем, при этом необходимо наличие соответствующих сертификатов на механизмы безопасности. Разработчики информационной системы кредитного бюро должны иметь опыт разработки аналогичных систем не менее двух лет.

28. Программное обеспечение кредитного бюро должно обеспечивать два и более способа получения (передачи) информации:

интерактивный интерфейс с подготовкой файла в стандартном формате с использованием программного обеспечения формирования отчетов в доступных форматах;

сетевой доступ с использованием стандартного формата передачи в режиме реального времени, ввод данных с помощью функционала ручного ввода, заполнение экранных форм на сайте, с использованием веб-браузера.

29. В целях информационной безопасности программное обеспечение кредитного бюро должно обеспечивать следующее:

1) идентификацию и аутентификацию с криптографическим преобразованием;

2) разграничение прав пользователей;

3) работу на уровне ядра программного обеспечения таким образом, чтобы ни одно значимое действие в рамках системы (будь то действие пользователя или процесса) не происходило без участия механизма безопасности;

4) схема безопасности, реализованная в программном обеспечении, должна

быть отделена от средств безопасности самой операционной системы, на которой будет реализовано программное обеспечение, в том смысле, что уязвимость средств безопасности операционной системы не должна влиять на работу безопасности программного обеспечения;

5) замкнутое сохранение данных в программном обеспечении должно быть организовано способом, обеспечивающим:

невозможность получения логического доступа к указанным данным вне рамок работы приложения программного обеспечения;

любые перемещения данных в/из базу данных программного обеспечения под контролем механизмов безопасности;

б) фиксирование информации, необходимой для идентификации факта, объекта и субъекта процесса удаления, изменение и возможность восстановления удаленных данных;

7) возможность устойчивой работы при появлении сбоев;

8) трехуровневую архитектуру "клиент-сервер" с тем, чтобы вывод из строя рабочего места пользователя или получение злоумышленником несанкционированного доступа к нему не сказывался на работе серверной части системы, а сбой сервера приложений не влиял на состояние данных системы;

9) аудит системно-значимых событий с фиксированием в регистрационный журнал, а также с возможностью защиты со стороны любого субъекта;

10) аудит действий пользователей и администраторов, как успешных, так и неудачных, начиная от попытки установления связи;

11) контроль экспортируемых и импортируемых данных;

12) возможность разработки (доработки) модулей и механизмов безопасности ;

13) в договоре с разработчиком информационной системы должна быть предусмотрена обязанность:

регулярного информирования кредитного бюро об обнаруженных ошибках и уязвимостях системы, а также своевременного предоставления изменений и обновлений к системе;

организовать службу оперативной поддержки, в том числе по вопросам безопасности для консультирования работников кредитного бюро и оказания им практической помощи в вопросах информационной безопасности.

29-1. Программное обеспечение кредитного бюро должно обеспечивать хранение информации в отношении субъекта кредитной истории в течение срока, установленного Законом о кредитном бюро, а также возможность формирования в течение одного рабочего дня кредитных отчетов по состоянию на любой момент времени с начала формирования кредитных историй.

Сноска. Инструкция дополнена пунктом 29-1 в соответствии с

постановлением Правления Национального Банка РК от 26.08.2011 № 97 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

30. Требования к техническим средствам кредитного бюро:

1) наличие собственного аппаратного обеспечения (компьютерное оборудование, серверы, аппаратные средства защиты, комплектующие и другое оборудование), также наличие документов, подтверждающих принадлежность аппаратного обеспечения кредитному бюро;

2) наличие сертификатов соответствия аппаратного обеспечения на соответствие требованиям безопасности, выданных органом подтверждения соответствия;

3) наличие системы гарантированного питания - щита автоматического включения резерва, дизельного генерирующего устройства, работающих от сигнала с двух источников бесперебойного питания (далее - ИБП) и непрерывно поддерживающей электричество в сети чистого питания во всей организации. При этом, нагрузка каждого ИБП должна быть не более сорока процентов в штатном режиме.

31. Серверы кредитного бюро должны составлять отказоустойчивую завершённую систему и представлять собой кластер со стопроцентным дублированием аппаратной части. Резервные серверы базы данных кредитного бюро должны быть расположены от основных серверов на расстоянии не менее десяти километров, и обеспечивать бесперебойную работу базы данных кредитного бюро таким образом, чтобы в случае прекращения работы основных серверов базы данных, кредитное бюро могло обеспечить восстановление работы базы данных на резервных серверах в срок не более 6 (шести) часов с момента прекращения работы основного сервера.

Сноска. Пункт 31 редакции постановления Правления Национального Банка РК от 26.08.2011 № 97 (вводится в действие по истечении десяти календарных дней со дня первого официального опубликования).

32. Требования к организации (за исключением микрофинансовой организации) по обеспечению безопасности информации:

1) наличие защищенного канала передачи данных с шифрованием трафика с помощью аппаратных граничных маршрутизаторов;

2) наличие системы обнаружения (предотвращения) атак из сети Интернет в компьютерную сеть организации с помощью межсетевого экрана;

3) наличие системы криптографической защиты компьютеров с помощью криптоключей и систем идентификации пользователя;

4) наличие аппаратного сетевого анализатора трафика по идентификатору управления доступом к носителю сетевых карт пользователей;

5) наличие системы резервного копирования - библиотеки на внешние носители информации.

Для реализации вышеуказанных требований кредитное бюро проводит анализ и оценку рисков, уязвимостей и угроз для обеспечения безопасности информации.

На микрофинансовую организацию распространяются требования по обеспечению безопасности информации, предусмотренные в подпунктах 2) и 5) настоящего пункта.

Сноска. Пункт 32 в редакции постановления Правления Национального Банка РК от 25.01.2013 № 9 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

33. Организация (за исключением микрофинансовой организации) в процессе своей деятельности выполняет следующие требования:

- 1) наличие службы информационной безопасности;
 - 2) наличие ответственных лиц по кредитным историям;
 - 3) наличие политики информационной безопасности;
 - 4) наличие политики формирования и использования паролей;
 - 5) наличие политики резервного копирования (архивирования);
- б) наличие документации с описанием процедур по ограничению доступа и обязанностей пользователей, администраторов безопасности, системных администраторов.

Микрофинансовая организация в процессе своей деятельности выполняет требование, установленное в подпункте 2) настоящего пункта.

Сноска. Пункт 33 в редакции постановления Правления Национального Банка РК от 25.01.2013 № 9 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

34. Организация (за исключением микрофинансовой организации) принимает внутренний документ, который определяет порядок работы с информационной системой, включающий:

- 1) порядок назначения сотрудников, на которых возлагаются обязанности ответственных лиц;
- 2) режим работы;
- 3) права и обязанности ответственных лиц, включая должностные инструкции;
- 4) список сотрудников, допущенных к рабочему месту оператора;
- 5) список сотрудников, допускаемых к рабочему месту оператора в особых случаях (в кризисных ситуациях, а также в случаях замещения сотрудника).

На микрофинансовую организацию распространяются требования, предусмотренные в подпунктах 3), 4), 5) настоящего пункта.

Сноска. Пункт 34 в редакции постановления Правления Национального Банка РК от 25.01.2013 № 9 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

35. Ответственные лица:

- 1) обеспечивают обязательность процедуры идентификации и аутентификации для доступа к ресурсам информационных систем;
- 2) не допускают получения права доступа к информационным ресурсам неавторизованными пользователями;
- 3) контролируют регулярность выполнения резервного копирования информации, обрабатываемой информационной системой;
- 4) проводят плановую и внеплановую проверку надежности защиты ресурсов системы;
- 5) обеспечивают защиту оборудования корпоративной сети, в том числе специальных межсетевых программных средств;
- 6) принимают меры по отражению угрозы и выявлению нарушителей;
- 7) регулярно просматривают журнал событий, проводят анализ с записями, где были попытки несанкционированного доступа к информации.

36. Сотрудники организации (ответственное лицо, администратор, оператор) дают письменное обязательство о неразглашении и нераспространении информации, ставшей им известной в процессе исполнения ими служебных обязанностей.

37. При увольнении ответственного лица производится внеплановая смена ключевой информации организации, о чем уведомляется кредитное бюро. Новая ключевая информация вводится в действие со дня их увольнения.

38. Порядок хранения и использования внешних носителей с ключевой информацией в организации должен исключать возможность несанкционированного доступа к ним.

Глава 6. Заключительные положения

Сноска. Глава 6 исключена постановлением Правления Национального Банка РК от 24.02.2012 № 89 (вводится в действие по истечении десяти календарных дней после дня его первого опубликования).

П р и л о ж е н и е 1
к Инструкции об организации
информационного процесса в
деятельности участников системы
формирования кредитных историй и
их использования, формирования

системы безопасности, установления
минимальных требований к их
электронному оборудованию,
сохранности базы данных кредитных
историй и помещениям

Форма

А К Т

о соответствии _____

(наименование участника)

требованиям, предъявляемым к участникам
системы формирования кредитных историй и
их использования (за исключением микрофинансовой
организации и субъекта кредитной истории)

Сноска. Приложение 1 в редакции постановления Правления Национального
Банка РК от 25.01.2013 № 9 (вводится в действие по истечении десяти
календарных дней после дня его первого официального опубликования).

_____ место составления

_____ дата составления

Настоящий акт о готовности участника системы формирования
кредитных историй и их использования к началу своей деятельности на
рынке информационных услуг и выполнении им требований по организации
информационного процесса в деятельности участников системы
формирования кредитных историй и их использования, формирования
системы безопасности, выполнении минимальных требований к их
электронному оборудованию, сохранности базы данных кредитных историй
и помещениям составлен комиссией в следующем составе:
представители уполномоченного органа в сфере информатизации:

представители уполномоченного органа:

В работе комиссии участвуют представители участника системы
формирования кредитных историй и их использования:

Подробное описание обследованных объектов и изученных комиссией документов :

Краткое содержание пояснений представителей участника системы формирования кредитных историй и их использования:

Проверкой комиссией технических и иных документов участника системы формирования кредитных историй и их использования _____, обследованием его технических помещений, электронно-компьютерного оборудования, систем связи и защитных устройств и иных объектов, предназначенных для работы в системе формирования кредитных историй и их использования установлено

(соответствие (не соответствие) предъявляемым требованиям и достаточность (недостаточность) для начала (продолжения) деятельности организации на рынке информационных услуг). Участником системы формирования кредитных историй и их использования предъявлена следующая техническая документация и иные документы, которые приложены к акту комиссии:

Ч л е н ы к о м и с с и и :

(должность)	(ФИО)	согласовано/не согласовано
-------------	-------	----------------------------

(должность)	(ФИО)	согласовано/не согласовано
-------------	-------	----------------------------

(должность)	(ФИО)	согласовано/не согласовано
-------------	-------	----------------------------

Руководитель к о м и с с и и :

(ЭЦП)

П р и л о ж е н и е 2
к Инструкции об организации
информационного процесса в
деятельности участников системы
формирования кредитных историй и
их использования, формирования
системы безопасности, установления
минимальных требований к их
электронному оборудованию,
сохранности базы данных кредитных
историй и помещениям

Сноска. Инструкция дополнена приложением 2 в соответствии с постановлением Правления Национального Банка РК от 25.01.2013 № 9 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Форма

Заключение

о соответствии _____

(наименование микрофинансовой организации)

требованиям, предъявляемым к микрофинансовой организации

место составления дата составления

Заключение о готовности микрофинансовой организации к началу своей деятельности на рынке информационных услуг и выполнении ею требований по организации информационного процесса в деятельности участников системы формирования кредитных историй и их использования, формирования системы безопасности, выполнении минимальных требований к их электронному оборудованию, сохранности базы данных кредитных историй и помещениям составлено представителями уполномоченного органа в следующем составе:

Подробное описание обследованных объектов и изученных документов:

Проверкой технических и иных документов микрофинансовой организации _____, обследованием ее технических помещений, электронно-компьютерного оборудования, систем связи и защитных устройств и иных объектов, предназначенных для работы в системе формирования кредитных историй и их использования _____ установлено

(соответствие (не соответствие) предъявляемым требованиям и достаточность (недостаточность) для начала (продолжения) деятельности организации на рынке информационных услуг).
Представители уполномоченного органа:
