Об утверждении 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

Утративший силу

Постановление Правления Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций от 25 октября 2004 года N 303. Зарегистрировано Министерством юстиции Республики Казахстан от 29 декабря 2004 года N 3318. Утратило силу постановлением Правления Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций от 18 июля 2008 года N 105.

Сноска. Утратило силу постановлением Правления Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций от 18 июля 2008 года N 105 *(порядок введения в действие см.* п.3 *).*

Сноска. Наименование с изменениями, внесенными постановлением Правления Агентства РК по регулированию и надзору фин. рынка и фин. организаций от 27 августа 2007 г. N 221 *(вводится в действие по истечении 14 дней со дня гос. регистрации).*

В целях реализации Закона Республики Казахстан "О кредитных бюро и формировании кредитных историй в Республике Казахстан", Правление Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций (далее - Агентство) ПОСТАНОВЛЯЕТ:

1. Утвердить Инструкцию 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. Пункт 1 с изменениями, внесенными постановлением Правления Агентства РК по регулированию и надзору фин. рынка и фин. организаций от 27 августа 2007 г. N 221 *(вводится в действие по истечении 14 дней со дня гос. регистрации).*

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

3. Департаменту стратегии и анализа (Еденбаев Е.С.):

1) совместно с Юридическим департаментом (Байсынов М.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 довести настоящее постановление до сведения кредитных бюро и Объединения юридических лиц "Ассоциация финансистов Казахстана".

4. Департаменту по обеспечению деятельности Агентства (Несипбаев Р.Р.) в десятидневный срок со дня государственной регистрации в Министерстве юстиции Республики Казахстан обеспечить публикацию настоящего постановления в средствах массовой информации Республики Казахстан.

5. Контроль за исполнением настоящего постановления возложить на заместителя Председателя Агентства Досмукаметова К.М.

Председатель

Согласовано
Агентство Республики Казахстан
по информатизации и связи
19 ноября 2004 года

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

Инструкция 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. Правый верхний угол и наименование с изменениями, внесенными постановлением Правления Агентства РК по регулированию и надзору фин. рынка и фин. организаций от 27 августа 2007 г. N 221 *(вводится в действие по истечении 14 дней со дня гос. регистрации).*

Настоящая Инструкция разработана в соответствии с Законом Республики Казахстан от 4 июля 2004 года "О кредитных бюро и формировании кредитных историй в Республике Казахстан" (далее - Закон о кредитных бюро) и определяет требования к организации информационного процесса по формированию и использованию кредитных историй, основные условия формирования системы безопасности информационных систем, минимальные требования к электронному оборудованию, сохранности базы данных кредитных историй и помещениям участников системы формирования кредитных историй.

Сноска. Преамбула в редакции постановления Правления Агентства РК по регулированию и надзору фин. рынка и фин. организаций от 27 августа 2007 г. N 221 *(вводится в действие по истечении 14 дней со дня гос. регистрации).*

Глава 1. Общие положения

1. В настоящей Инструкции используются следующие понятия:

1) администратор безопасности информационных систем - 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 (далее - администратор);

2) аутентификация - подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа имеющимся в системе;

3) зловредное программное обеспечение (компьютерные вирусы, сетевые черви и аналогичное программное обеспечение) - совокупность выполняемого кода, способная создавать свои копии (частично или полностью совпадающие с оригиналом) и внедрять их в различные объекты/ресурсы компьютерных систем, сетей без ведома пользователя;

4) идентификатор - уникальные персональный код и/или имя, присвоенные субъекту и/или объекту системы, и предназначенные для регламентированного доступа в систему и/или к ресурсам системы;

5) идентификация - присвоение или определение соответствия предъявленного для получения доступа в систему и/или к ресурсу системы идентификатора перечню идентификаторов, имеющихся в системе;

6) информационная система участников системы формирования и использования кредитных историй - совокупность информационных технологий, информационных сетей и средств их программно-технического обеспечения, предназначенных для реализации поставщиками информации, кредитными бюро, получателями кредитных отчетов и субъектами кредитных историй информационных процессов (далее - информационная система формирования и использования кредитных историй);

7) ключевая информация - криптографические ключи и ключи электронной цифровой подписи;

8) комплекс мер по защите информационной системы формирования и использования кредитных историй - организационно-технические мероприятия, направленные на обеспечение безопасного функционирования информационной системы формирования и использования кредитных историй, в том числе программно-аппаратная защита электронных средств и компьютеров от несанкционированного доступа, обеспечивающая контроль доступа к установленному программному обеспечению и информации, предоставляющая средства разграничения полномочий зарегистрированных пользователей;

9) оператор - работник кредитного бюро, непосредственно осуществляющий подготовку, обработку, прием и передачу сообщений с использованием системы защиты;

10) организация - кредитное бюро, поставщик информации, получатель кредитного отчета (за исключением субъектов кредитных историй), обязанные принимать участие в информационной системе формирования и использования кредитных историй в соответствии с настоящей Инструкцией;

11) ответственное лицо - работник кредитного бюро, обеспечивающий функционирование и контроль средств защиты информации от несанкционированного доступа;

12) политика информационной безопасности - нормы и практические приемы, регулирующие управление, защиту и распределение информации ограниченного распространения;

13) пользователь - кредитное бюро и иные участники информационной системы кредитных историй, участвующие в обмене электронными документами и являющиеся сторонами договора о предоставлении информации и (или) получении кредитных отчетов.

Сноска. Пункт 1 с изменениями, внесенными постановлением Правления Агентства РК по регулированию и надзору фин. рынка и фин. организаций от 27 августа 2007 г. N 221 *(вводится в действие по истечении 14 дней со дня гос. регистрации).*

2. Поставщики информации и получатели кредитного отчета (за исключением

субъекта кредитной истории) 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 кредитных бюро.

Сноска. Пункт 2 с изменениями, внесенными постановлением Правления Агентства РК по регулированию и надзору фин. рынка и фин. организаций от 27 августа 2007 г. N 221 *(вводится в действие по истечении 14 дней со дня гос. регистрации).*

Глава 2. Организация информационного процесса

3. 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.

4. Кредитные бюро, поставщики информации и получатели кредитного отчета (за исключением субъектов кредитной истории) обеспечивают:

1) контроль ввода данных;

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

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.

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

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

7. Разработка информационных систем выполняется кредитными бюро на основании технического задания, утвержденного их первым руководителем.

Техническое задание, необходимое для разработки кредитными бюро информационных систем, взаимодействующих с государственными органами, осуществляющими регистрацию прав на недвижимое имущество и сделок с ним согласовывается с Комитетом регистрационной службы Министерства юстиции Республики Казахстан.

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

Сноска. Пункт 7 с изменениями, внесенными постановлением Правления Агентства РК по регулированию и надзору фин. рынка и фин. организаций от 27 августа 2007 г. N 221 *(вводится в действие по истечении 14 дней со дня гос. регистрации).*

8. 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 осуществляются в соответствии с техническим заданием, стандартами, действующими на территории Республики Казахстан, и внутренними документами кредитных бюро .

Глава 3. Условия обмена информацией между участниками системы формирования кредитных историй и их использования

9. Обмен информацией между поставщиками информации, получателями кредитных отчетов (за исключением субъекта кредитной истории) и кредитными бюро осуществляется через специальную автоматизированную систему, условия использования которой определяются центральным исполнительным органом, осуществляющим реализацию государственной политики и государственное регулирование деятельности в сфере информатизации и "электронного правительства" (далее - уполномоченный орган в сфере информатизации).

Сноска. Пункт 9 с изменениями, внесенными постановлением Правления Агентства РК по регулированию и надзору фин. рынка и фин. организаций от 27 августа 2007 г. N 221 *(вводится в действие по истечении 14 дней со дня гос. регистрации).*

10. Электронные документы используются в формате CMS (Cryptographic Message Syntax), с возможностью передачи в нем электронного сообщения в

любом формате.

Сноска. Пункт 10 с изменениями, внесенными постановлением Правления Агентства РК по регулированию и надзору фин. рынка и фин. организаций от 27 августа 2007 г. N 221 *(вводится в действие по истечении 14 дней со дня гос. регистрации).*

11. Формат электронного сообщения или файла (данные о субъекте кредитных историй, кредитный отчет и другие данные), передаваемого в электронном документе CMS, разрабатывают кредитные бюро по согласованию с уполномоченным органом в сфере информатизации.

Сноска. Пункт 11 с изменениями, внесенными постановлением Правления Агентства РК по регулированию и надзору фин. рынка и фин. организаций от 27 августа 2007 г. N 221 *(вводится в действие по истечении 14 дней со дня гос. регистрации).*

12. 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.

Глава 4. Основные вопросы формирования системы безопасности

13. Информационная система формирования и использования кредитных историй обеспечивает:

1) конфиденциальность информации - защиту от раскрытия информации в ходе ее хранения, обработки или при передаче по коммуникационным каналам;

2) сохранность информации - защиту от повреждений, целостность и защищенность от несанкционированного изменения, дополнения, копирования или удаления в ходе ее хранения, обработки или при передаче по коммуникационным каналам;

3) доступность - защиту от использования одним пользователем данных и иных ресурсов информационной системы, предназначенных для совместного использования, перехвата информационных сообщений и/или данных с последующей их задержкой, а также от перехвата информационных сообщений и /или данных с последующей их задержкой.

14. Базовым компонентом обязательных мер по обеспечению безопасности информационной системы формирования и использования кредитных историй является применение комплексного подхода к созданию системы информационной безопасности.

15. Комплексный подход к созданию системы информационной безопасности включает анализ и оценку рисков, в том числе по техническим каналам утечки

информации, учет характера и важности защищаемой информации, контроль за обеспечением безопасности технологии обработки электронных документов.

16. Участники информационной системы формирования и использования кредитных историй проводят действия по оперативному выявлению подозрительных действий в реальном масштабе времени и включающие мероприятия, направленные на установление:

1) нетипичного поведения (пользователей, программ или аппаратуры);

2) начала активности несанкционированных вторжений или использования зловредного программного обеспечения (компьютерных вирусов, сетевых червей и аналогичного программного обеспечения).

17. Основными направлениями, обеспечивающими комплексный подход к информационной безопасности на программно-техническом уровне являются:

1) контур безопасности;

2) внутрикорпоративная безопасность;

3) управление корпоративной безопасностью.

18. Контур безопасности предназначен для обеспечения защиты информационной системы формирования и использования кредитных историй (далее - Контур безопасности) кредитного бюро или поставщиков информации. Контур безопасности реализует защиту центрального и дополнительных офисов (филиалов, представительств, удаленных офисов), информационных потоков между ними, а также информационных ресурсов, хранящихся на серверах и рабочих станциях внешних соединений информационной системы с другими сетями.

19. Процедуры безопасности участников информационной системы формирования и использования кредитных историй предназначены для контроля несанкционированных вторжений и антивирусной защиты, обеспечения их внутренней информационной безопасности и предполагает необходимость построения и поддержания системы, обеспечивающей разделение пользователей на группы в соответствии с их статусом и правами, а также разделение ресурсов по уровню их конфиденциальности.

20. Управление корпоративной безопасностью, в рамках комплексной системы безопасности участников информационной системы формирования и использования кредитных историй, обеспечивается постоянным контролем за выполнением общих требований политики информационной безопасности, оперативным внесением в нее корректировок и повышения ее уровня.

21. Повышение уровня безопасности предусматривает:

1) определение политики информационной безопасности;

2) установление границ, в которых предполагается поддерживать режим информационной безопасности;

3) проведение оценки рисков;

4) выбор мер противодействия и управления рисками;

5) выбор средств и управления, обеспечивающих режим информационной безопасности.

22. Политика информационной безопасности содержит описание состава используемой информационной системы, список пользователей информационной системы организации, их права (в зависимости от их служебного положения и характера выполняемых функций) на доступ к информации, программным и техническим средствам и определяет:

1) общие направления работы в области информационной безопасности;

2) цель и задачи защиты информационной системы;

3) основные принципы и способы достижения необходимого уровня безопасности;

4) определение должностных лиц организаций, ответственных за разработку необходимых требований, определяющих политику информационной безопасности;

5) определение подразделений организаций, ответственных за создание и поддержание работоспособности информационных систем и системы их защиты;

6) меры, предотвращающие нарушения режима безопасности информационных систем в случае возникновения обстоятельств непреодолимой силы, к которым относятся стихийные бедствия, аварии, пожары, отключение электроэнергии, повреждение линий связи, массовые беспорядки, забастовки, военные действия.

23. Участники информационной системы формирования и использования кредитных историй (за исключением субъектов кредитных историй) обеспечивают:

1) соответствие используемых управленческих решений, технологий, подходов и конкретных программно-аппаратных средств действующему законодательству Республики Казахстан;

2) принятие внутренних документов об организации безопасности информационной системы.

24. Процедурный уровень защиты информации включает мероприятия по обеспечению безопасности, предпринимаемые организациями по следующим направлениям:

1) управление персоналом;

2) физическая защита;

3) реагирование на нарушения режима безопасности;

4) планирование восстановительных работ.

25. Средства идентификации/аутентификации участников информационной системы формирования и использования кредитных историй (за исключением субъектов кредитных историй) должны соответствовать условиям:

1) устойчивости к сетевым угрозам;

2) обеспечения единого входа в используемую информационную сеть.

26. План защиты информации включает следующие меры:

1) организационные;

2) программно-технические.

27. К организационным мерам обеспечения безопасности относятся:

1) физическая защита информационных систем;

2) поддержание работоспособности информационных систем, имеющих отношение к информационной безопасности;

3) установление каждому пользователю соответствующего права доступа, необходимого для выполнения им возложенных должностных обязанностей и обеспечения взаимозаменяемости;

4) планирование восстановительных работ.

28. Физическая защита подразделяется на:

1) физическое управление доступом;

2) меры противопожарной безопасности;

3) защита поддерживающей инфраструктуры;

4) защита от перехвата данных, защита мобильных систем.

29. Мероприятия по поддержанию работоспособности информационных систем подразделяются на:

1) поддержку пользователей - предоставление консультаций по вопросам информационной безопасности, выявление их типичных ошибок и обеспечение памятками с рекомендациями для распространенных ситуаций;

2) поддержку программного обеспечения - контроль лицензионной (сертифицированной) чистоты программного обеспечения;

3) конфигурационное управление - контроль и фиксирование изменений, вносимых в программную и техническую конфигурацию;

4) резервное копирование для восстановления информационной системы и данных в случае аварии и других обстоятельств непреодолимой силы;

5) управление носителями данных - порядок учета, обращения и хранения;

6) документирование - актуальное отражение текущего состояния дел.

30. В случае нарушения режима безопасности информационных систем ответственные лица, администратор осуществляют:

1) выполнение оперативных мероприятий с целью уменьшения наносимого вреда;

2) анализ и оценку имеющихся сведений о нарушениях - изучение инцидента,

выявление повторных нарушений, разработка мер по усовершенствованию системы защиты.

31. Резервное копирование и восстановление после потери работоспособности информационной системы определяются требованиями, установленными в организации.

Глава 5. Минимальные требования к электронному оборудованию, сохранности базы данных кредитных историй и помещениям

32. Программное обеспечение пользователя устанавливается на специально выделенном персональном компьютере, имеющем паспорт - описание рабочего места с подробными данными по его месторасположению, конфигурации, а также аппаратным и программным средствам, установленным на нем.

33. Не допускается эксплуатация персонального компьютера пользователя и установка на нем программных средств, не связанных с целями подготовки, обработки, передачи или ведения электронных документов в рамках участия в информационной системе формирования и использования кредитных историй.

34. Персональный компьютер пользователя 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.

35. Одному системному имени пользователя, по которому идентифицируется пользователь, при входе в информационные системы должно соответствовать одно физическое лицо.

36. Паспорт - описание рабочего места оформляется за подписью руководителя организации и хранится у ответственного лица, администратора.

37. Персональный компьютер пользователя должен иметь средства обеспечения целостности программного обеспечения.

38. Системный блок персонального компьютера пользователя опечатывается либо пломбируется ответственным лицом (администратором). В случае необходимости, допуск к системному блоку осуществляется в присутствии ответственного лица (администратора). По окончании работ системный блок опечатывается либо пломбируется ответственным лицом (администратором).

39. Порядок доступа к ресурсам (дисковое пространство, директории, сетевые ресурсы, базы данных и другие), 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.

40. Проведение и контроль работ по криптографической защите ведется ответственным лицом (администратором), который выполняет:

1) учет, хранение и сопровождение программных средств криптографической защиты;

2) генерацию криптографических ключей, получение, учет, хранение и выдачу информационных носителей, содержащих ключи;

3) ведение списка владельцев криптографических ключей;

4) обеспечение владельцев криптографических ключей необходимыми инструкциями.

41. Рабочее место системы защиты размещается в отдельном помещении.

42. Местонахождение, в котором находится рабочее место пользователя и технические средства охраны помещения (контроль доступа и охранно-пожарная сигнализация) должны исключать возможность неконтролируемого проникновения в это помещение лиц, не допущенных к рабочему месту пользователя.

43. Помещение организации должно находиться в охраняемой зоне, иметь кодовые замки и средства регистрации доступа.

При расположении помещения кредитного бюро на первых или последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц, окна помещений оборудуются металлическими решетками.

44. Средства технической защиты помещения организации (контроль доступа), должны исключать возможность неконтролируемого проникновения в это помещение лиц, не допущенных к рабочему месту пользователя. Допуск к работе в организации осуществляется в соответствии с ее регламентом и должностными обязанностями работников.

Глава 6. Иные вопросы деятельности организации

45. Внутренним актом организации определяется порядок работы с системой защиты, включающий:

1) порядок назначения сотрудников, на которых возлагаются обязанности ответственного лица, администратора, оператора;

2) режим работы;

3) права и обязанности ответственного лица, администратора и оператора, включая их должностные инструкции;

4) список сотрудников, допущенных к рабочему месту пользователя;

5) список сотрудников, допускаемых к рабочему месту пользователя в особых случаях.

46. Ответственные лица, администратор и оператор:

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) обеспечивают работоспособность средств защиты от утечки информации через съемные носители (гибкие диски, flash-карты, внешние накопители на жестких дисках и прочие);

8) регулярно просматривают журнал событий, проводят анализ с записями, где были попытки несанкционированного доступа к информации.

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

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

49. Ключевая информация должна находиться на внешнем носителе (дискета, пластиковая карточка).

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

51. При формировании и передаче электронного сообщения организации осуществляют защитные действия, в соответствии с установленным ими порядком использования программно-криптографической защиты и электронной цифровой подписи.

52. В случае нарушения порядка защитных действий или его разглашения, сторона, установившая данное нарушение, немедленно уведомляет об этом другую организацию и принимает меры к ликвидации последствий.

53. Проверка выполнения (соблюдения) участником информационной системы кредитных историй организационно-технических, технологических требований по защите программного обеспечения, соответствия используемых им информационных систем установленным настоящей Инструкцией и законодательством Республики Казахстан условиям и требованиям,

осуществляется комиссией уполномоченного органа в сфере информатизации, которая составляет акт о соответствии по форме согласно Приложению к настоящей Инструкции.

Сноска. Пункт 53 с изменениями, внесенными постановлением Правления Агентства РК по регулированию и надзору фин. рынка и фин. организаций от 27 августа 2007 г. N 221 *(вводится в действие по истечении 14 дней со дня гос. регистрации).*

Глава 7. Заключительные положения

54. Вопросы, не урегулированные настоящей Инструкцией, разрешаются в порядке, определенном законодательством Республики Казахстан.

Приложение
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. Приложение в редакции постановления Правления Агентства РК по регулированию и надзору фин. рынка и фин. организаций от 27 августа 2007 г . N 221 *(вводится в действие по истечении 14 дней со дня гос. регистрации).*

А К Т

о соответствии _____
(наименование участника)
требованиям, предъявляемым к участникам системы формирования кредитных историй и их использования (за исключением субъекта кредитной истории)

_____ _____
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 государственного органа по регулированию и надзору финансового рынка и финансовых организаций:

_____

_ _ _ _ _ _

_____

_ _ _ _ _ _

_____

_____

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

_____

_ _ _ _ _ _

_____

_ _ _ _ _ _

_____

_____

Подробное описание обследованных объектов и изученных комиссией документов:

конкретная деятельность участника системы формирования и использования кредитных историй;

охрана помещения;

описание рабочего места (программное обеспечение пользователя установлено на специально выделенным компьютере, имеющем паспорт с подробными данными по его месторасположению, конфигурации, а также аппаратным и программным средствам, установленным на нем);

обеспечение физической защиты в соответствии с пунктом 28 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, утвержденной постановлением Правления Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций от 25 октября 2004 года N 303 (далее - Инструкция), возможности резервного копирования и восстановления после потери работоспособности информационной системы, порядок работы с системой защиты, который определен внутренним актом организации, включающим подпункты 1)-5) пункта 45 Инструкции; описание программных продуктов, используемых в деятельности.

_____

_ _ _ _ _ _

_____

_ _ _ _ _ _

_____

_____

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/несоответствие 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:

_____

_ _ _ _ _ _

_____

_ _ _ _ _ _

_____

_____

Акт составлен в трех экземплярах и по одному экземпляру передан:

уполномоченному органу в сфере информатизации;

государственному органу по регулированию и надзору финансового рынка и финансовых организаций;

участнику информационной системы формирования и использования кредитных историй.

Члены комиссии:

_____

_ _ _ _ _ _

_____

_ _ _ _ _ _

_____

_____

Представитель проверяемой организации:

_____

_ _ _ _ _ _

_____

_ _ _ _ _ _

_____

_____