Об утверждении Инструкции по определению особенностей организации деятельности поставщиков информации, кредитных бюро и получателей кредитных отчетов (за исключением субъектов кредитных историй) на рынке информационных услуг

Утративший силу

Приказ Председателя Агентства Республики Казахстан по информатизации и связи от 23 марта 2005 года N 72-п. Зарегистрирован в Министерстве юстиции Республики Казахстан 28 апреля 2005 года N 3605. Утратил силу приказом и.о. Министра по инвестициям и развитию Республики Казахстан от 17 марта 2016 года № 275

Сноска. Утратил силу приказом и.о. Министра по инвестициям и развитию РК от 17.03.2016 № 275 (вводится в действие со дня его официального опубликования).

В целях реализации пункта 3 статьи 4 Закона Республики Казахстан "О кредитных бюро и формировании кредитных историй в Республике Казахстан"

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую Инструкцию по определению особенностей организации деятельности поставщиков информации, кредитных бюро и получателей кредитных отчетов (за исключением субъектов кредитных историй) на рынке информационных услуг.

2. Департаменту информатизации и юридической службы Агентства Республики Казахстан по информатизации и связи (далее - Агентство) (Жайлаубаевой А.) обеспечить в установленном порядке государственную регистрацию настоящего приказа в Министерстве юстиции Республики Казахстан.

3. Управлению финансового регулирования Агентства (Арпабаев Б.К.) после государственной регистрации настоящего приказа, в установленном порядке, обеспечить его официальное опубликование в средствах массовой информации.

4. Настоящий приказ вводится в действие со дня официального опубликования.

Председатель

Согласовано:

Председатель Правления Агентства Республики Казахстан по регулированию и надзору

финансового рынка и финансовых организаций
4 апреля 2005 г.

Утверждена
приказом Председателя Агентства Республики Казахстан по информатизации и связи
от 23 марта 2005 года N 72-п

Инструкция
по определению особенностей организации деятельности поставщиков информации, кредитных бюро и получателей кредитных отчетов (за исключением субъектов кредитных историй) на рынке информационных услуг

Настоящая Инструкция разработана в соответствии с Законами Республики Казахстан "О кредитных бюро и формировании кредитных историй в Республике Казахстан" (далее - Закон о кредитных бюро), " Об информатизации" , " Об электронном документе и электронной цифровой подписи" и определяет особенности организации деятельности поставщиков информации, кредитных бюро и получателей кредитных отчетов (за исключением субъектов кредитных историй) на рынке информационных услуг.

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) идентификация - процесс присвоения или определения соответствия предъявленного для получения доступа в систему и (или) к ресурсу системы идентификатора перечню идентификаторов, имеющихся в системе;

4) 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);

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

6) оператор - работник кредитного бюро, непосредственно осуществляющий прием, сбор, обработку и передачу информации с использованием системы защиты;

7) 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;

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

9) 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;

10) электронная цифровая подпись - набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания;

11) электронный документ - документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи.

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 внутренних документов кредитного бюро, предусмотренных Законом о кредитных бюро.

2. Техническое обеспечение деятельности участников в системе формирования кредитных историй

3. Порядок технического обеспечения деятельности организации в системе формирования кредитных историй определяется актом участника в системе формирования кредитных историй (приказ, распоряжение) включающим:

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

2) список сотрудников, допущенных к рабочему месту пользователя;

3) режим работы.

4. Ключевая информация находится на машинном носителе. Машинные носители после окончания работы хранятся в специально выделенных для этих целей сейфах.

5. Хранение и использование машинных носителей с ключевой информацией исключают возможность несанкционированного доступа к ним. 6. Сотрудникам организации не допускается:

1) снимать несанкционированные копии с носителей ключевой информации;

2) разглашать данные в отношении носителей ключевой информации, порядка их хранения, а также передавать носители ключевой информации посторонним лицам;

3) записывать постороннюю информацию на носители ключевой информации.

3. Технические требования к рабочему месту системы защиты, компьютерному оборудованию и программному обеспечению

7. Программные и аппаратные меры защиты основаны на использовании специальных программ и аппаратуры, входящих в состав информационной системы и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты:

1) идентификацию и аутентификацию пользователей;

2) разграничение доступа к ресурсам;

3) регистрацию событий;

4) криптографические преобразования;

5) проверку целостности системы;

6) проверку отсутствия вредоносных программ;

7) программную защиту передаваемой информации и каналов связи;

8) защиту системы от наличия и появления нежелательной информации;

9) создание физических препятствий на путях проникновения нарушителей;

10) мониторинг и сигнализацию соблюдения правильности работы системы;

11) создание резервных копий ценной информации.

8. Рабочее место системы защиты размещается в специально выделенном изолированном помещении. Местонахождение, контроль доступа и охранно-пожарная сигнализация исключают возможность неконтролируемого проникновения в помещение лиц, не допущенных к рабочему месту пользователя .

9. Программное обеспечение пользователя устанавливается на специально выделенных программно-аппаратных средствах, имеющих паспорт рабочего места с подробными данными по его месторасположению, конфигурации.

10. Не допускается эксплуатация программно-аппаратных средств пользователя и установка на них программных средств, не связанных с целью подготовки, обработки, передачи или ведения электронных документов в рамках участия в информационной системе участников системы формирования и использования кредитных историй.

11. Программно-аппаратные средства пользователя сертифицируются в соответствии с законодательством Республики Казахстан о сертификации и включают следующий комплекс защиты:

1) средства идентификации и аутентификации пользователей,

2) возможность ведения электронных журналов в течение срока хранения электронных документов, с целью контроля деятельности, связанной с доступом к компьютеру и действиями пользователей.

12. Одному системному имени пользователя соответствует один идентификационный код для входа в информационные системы.

13. Системный блок программно-аппаратных средств пользователя опечатывается или пломбируется ответственным лицом. В случае необходимости допуск к системному блоку осуществляется в присутствии ответственного лица. По окончании работ системный блок опечатывается или пломбируется ответственным лицом.

14. Подготовка электронных документов, предназначенных для передачи в зашифрованном виде, происходит исключительно на рабочем месте системы защиты и исключает возможность несанкционированного доступа.

15. Доступ к ресурсам (дисковое пространство, директории, сетевые ресурсы, базы данных), выделенным для накопления в них информации для передачи в информационную среду с использованием системы защиты, получение

информации из информационной среды, хранение, архивирование и другая обработка информации исключают возможность несанкционированного доступа к этим ресурсам.

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

4. Выявление технических каналов утечки информации

17. Технические каналы утечки информации делятся на:

1) радиоканалы (электромагнитные излучения радиодиапазона);

2) электрические (напряжения и токи в различных токопроводящих коммуникациях);

3) акустические (распространение звуковых колебаний в любом звукопроводящем материале);

4) оптические (электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра).

18. Источниками излучений в технических каналах являются разнообразные технические средства, особенно те, в которых циркулирует конфиденциальная информация. К их числу относятся:

1) сети электропитания и линии заземления;

2) автоматические сети телефонной связи;

3) системы факсимильной, телекодовой и телеграфной связи;

4) средства громкоговорящей связи;

5) средства звуко- и видеозаписи;

6) системы звукоусиления речи;

7) электронно-вычислительная техника;

8) электронные средства оргтехники.

19. Для создания системы защиты объекта от утечки информации по техническим каналам необходимо осуществить ряд мероприятий. Необходимо проанализировать специфические особенности расположения зданий, помещений в зданиях, территорию вокруг них и подведенные коммуникации. Затем необходимо выделить те помещения, внутри которых циркулирует конфиденциальная информация и инвентаризировать используемые в них технические средства.

20. Технические мероприятия:

1) проверить используемую технику на соответствие величины побочных излучений допустимым уровням;

2) экранировать помещения с техникой или эту технику в помещениях;

3) перемонтировать отдельные цепи, линии, кабели;

4) использовать специальные устройства и средства пассивной и активной защиты.

5. Особенности использования электронной цифровой подписи в системе формирования кредитных историй

21. Применение электронной цифровой подписи в системе формирования кредитных историй регулируется в соответствии с Законом Республики Казахстан "Об электронном документе и электронной цифровой подписи".

6. Заключительные положения

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