13 ноября 2007 г. 370-р

О вводе в эксплуатацию системы предоставления отчетности в ФСТ России по телекоммуникационным каналам связи с электронной цифровой подписью

Во исполнение требований комитета по тарифам и ценовой политике Правительства Ленинградской области от 15.05.2007 № 22-1-308/070, об обмене данными между региональными регулирующими органами и органами тарифного регулирования муниципальных образований в формате единой информационно-аналитической системы (ЕИАС) Федеральной службы по тарифам (ФСТ) России:

1. Установить абонентский комплект программного обеспечения средств криптографической защиты информации (СКЗИ) полученный от ЗАО «ПФ «СКБ Контур» по договору №3250022/07 от 1 августа 2007 года на автоматизированное рабочее место (АРМ) - компьютер главного специалиста отдела транспорта, связи и ЖКХ Мироновой А.Н..

2. Назначить пользователем электронной цифровой подписи (ЭЦП) главного специалиста отдела транспорта, связи и ЖКХ Миронову А.Н..

3. Допустить к ключевой информации (ЭЦП), информации обрабатываемой на АРМ следующих должностных лиц:

- заведующего отделом информационных технологий Покровского А.В.;
- заведующего отделом транспорта, связи и ЖКХ Харламову Т.П.;
- главного специалиста отдела транспорта, связи и ЖКХ Миронову А.Н.;
- ведущего специалиста отдела информационных технологий Алушина А.А.

4. Назначить ответственным за обеспечение информационной безопасности при эксплуатации СКЗИ (администратором безопасности) ведущего специалиста отдела информационных технологий Алушина А.А.

5. Утвердить Положение о порядке учета, хранения и использования носителей ключевой информации с закрытыми ключами ЭЦП и шифрования, согласно приложению 1.

Глава администрации
Лужского муниципального района С.Н.Тимофеев

Разослано: отд.ЖКХ, отд.информ.технологий, прокуратура.

Приложение 1
к распоряжению главы администрации
от 13.11.2007 № 370-р

Положение о порядке учета, хранения и использования носителей ключевой информации с закрытыми ключами ЭЦП и шифрования.

1. Общие положения

1.1 Настоящее положение определяет порядок учета, хранения и использования носителей ключевой информации, применяемых в системах установки/проверки ЭЦП и шифрования администрации Лужского муниципального района.
1.2 Термины, используемые в Положении, имеют следующие значения (перечисляются в алфавитном порядке):
1.2.1 Администратор безопасности средств криптографической защиты информации (СКЗИ) - полномочное лицо, назначенное в администрации для обеспечения безопасности конфиденциальной связи.
1.2.2 Владелец ЭЦП - администрация Лужского муниципального района
1.2.3 Ключ ЭЦП - цифровая последовательность, формируемая Владельцем ЭЦП с использованием программно-аппаратных средств и состоящая из закрытой (далее- секретный ключ) и публичной (далее- открытый ключ) частей, предназначенных для формирования и проверки ЭЦП, где:
• секретный ключ - цифровая последовательность, предназначенная для подписания отчетов в виде электронных документов ЭЦП;
• открытый ключ - цифровая последовательность, однозначно связанная с секретным ключом и позволяющая проверить правильность ЭЦП, которой подписан передаваемый документ.
1.2.4 Компрометация секретного ключа ЭЦП - событие, определенное Владельцем ЭЦП как ознакомление неуполномоченным лицом (лицами) с его секретным ключом ЭЦП.
1.2.5 Пользователь ЭЦП - лицо, назначенное Владельцем и уполномоченное им использовать ЭЦП для подписания передаваемых документов от имени Владельца ЭЦП.

1.3 Администрация Лужского муниципального района утверждает список лиц - ответственных исполнителей, имеющих доступ к ключевой информации.

2. Учет носителей ключевой информации

2.1 В качестве носителей ключевой информации используются накопители на гибком магнитном диске 3,5" (ГМД).
2.2 На этикетку ключевого ГМД абонента наносится следующую информация:
• название организации изготовителя ключевого документа;
• надпись "ключевая дискета пользователя";
• номер экземпляра (при наличии копии).

2.3 Администратор безопасности ведет "Журнал учета и движения ключевых документов" (Приложение 1), в котором фиксируется выработка ключей шифрования и ЭЦП и выдача пользователям ключевых документов
2.4 Администратор безопасности ведет "Журнал абонента сети" (Приложение 2), где записывают данные о полученной исходной ключевой информации, подготовленных ключевых носителях, нештатных ситуациях, произошедших на АРМ с СКЗИ.

3 Хранение носителей ключевой информации

3.1 Для хранения носителей секретных ключей ЭЦП и шифрования в помещениях отделов должны устанавливаться сейфы, оборудованные надежными запирающими устройствами с двумя экземплярами ключей (один у исполнителя, другой в отделе информационных технологий). Хранение носителей секретных ключей шифрования и ЭЦП допускается в одном хранилище с другими документами, но при этом отдельно от них в отдельном контейнере, опечатываемом ответственным исполнителем.
3.2 Доступ неуполномоченных лиц к носителям ключевой информации должен быть исключен.
3.3 По окончании рабочего дня, а также вне времени составления и передачи документов требующих подписания с помощью ЭЦП носители секретных ключей шифрования и ЭЦП должны хранится в штатном месте хранения.
3.4 Хранение носителей секретных ключей шифрования допускается только в сейфе администратора безопасности отдела информационных технологий.
3.5 Во избежание потери ключевой информации рекомендуется хранить рабочую копию ключевой дискеты.

4 Использование носителей ключевой информации

4.1 Для пользователя системы администратор безопасности формирует рабочие ключевые носители на основе исходной информации (лицензионного диска).
4.2 Диск с исходной информацией (лицензионный диск) хранится у администратора службы безопасности и предназначен для выработки ключей шифрования и электронной цифровой подписи пользователей. В качестве носителей с исходной информацией используются только дискеты в формате MS DOS. Носители с исходной информацией необходимо использовать только для формирования ключевых носителей. Для предотвращения внесения несанкционированных изменений дискету с исходной информацией для АРМ, ее необходимо использовать только в абонентском комплекте программного обеспечения средств криптографической защиты информации (СКЗИ) ЗАО «ПФ «СКБ Контур».
4.3 При компрометации секретных ключей шифрования и ЭЦП администрация предпринимает все меры для прекращения передачи документов с использованием этих ключей шифрования и ЭЦП, и информирует другую сторону в установленном порядке.

НЕ ДОПУСКАЕТСЯ:
• Осуществлять несанкционированное копирование ключевых носителей.
• Разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер (за исключением случаев, предусмотренных данными правилами).
• Вставлять ключевой ГМД (или другой ключевой носитель) в дисковод ПЭВМ (или другое устройство считывания) в режимах, не предусмотренных штатным режимом, а также в дисководы других ПЭВМ.
• Записывать на ГМД с ключами постороннюю информацию.
• Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем их переформатирования.

5 Уничтожение ключевых документов

5.1 Пользователь уничтожают выведенные из действия (после плановой смены или компрометации) ключи ЭЦП с магнитного носителя не позднее, чем через одни сутки после момента вывода ключа из действия.
5.2 С ЖМД ЭВМ ключи уничтожаются стиранием ключевого файла.

5.3 Ключевая информация на носителях уничтожается администратором безопасности с использованием опции форматирования ключевого носителя на абонентский комплекте программного обеспечения средств криптографической защиты информации (СКЗИ) ЗАО «ПФ «СКБ Контур».
Данные носители могут быть использованы в дальнейшем участниками расчетов при условии записи на них новой ключевой информации.
5.4 Об уничтожении ключей делается соответствующая запись в "Журнале учета и движения ключевых документов".

6 Ответственность должностных лиц

6.1 Администрация Лужского муниципального района назначает специальное должностное лицо - администратора безопасности ведущего специалиста отдела информационных технологий. В случае его отсутствия его обязанности выполняет начальник отдела информационных технологий. Функции администратора безопасности должны заключаться в выполнении процедур установки ПО, настройки системного окружения, установки, настройки, обслуживании и обеспечении функционирования средств защиты СКЗИ. Администратор безопасности должен иметь возможность доступа ко всей информации, обрабатываемой на рабочем месте.
6.2 Администратор безопасности, заведующий отделом информационных технологий несут персональную ответственность за сохранность установленного программного обеспечения, а также ключей шифрования и ЭЦП.

Приложение 1

Журнал учета и движения ключевых документов

Журнал разбит на разделы.
п/п
Серия и номер ключевого носителя
Полное название организации,
Ф.И.О. лица, получившего ключевой комплект
Расписка в получении ключевого комплекта
Дата и время получения

Примечание

Приложение 2

Журнал абонента сети

В журнале отражается следующая информация:
• дата, время;
• дата компрометации ключа;
• запись об изготовлении личного ключевого ГМД администратора безопасности;
• запись об изготовлении личного ключевого ГМД пользователя, полный номер (с личным кодом) ГМД пользователя с ключом подписи, дата регистрации (сертификации) открытого ключа ЭЦП, дата компрометации ключа;
• записи, отражающие выдачу на руки ответственным исполнителям и сдачу ими на хранение личных ключевых ГМД, включая резервные ключевые ГМД;
• события, происходившие на АРМ абонента с указанием причин и предпринятых действий;
• примечание.