Приложение 2 к Приказу ОАО «ТГК-1»
от 25.06.2013 г. № 75-а

Инструкция

пользователя Удостоверяющего центра ОАО «ТГК-1»

Санкт-Петербург
2013

Термины и определения

Применительно к настоящей Инструкции используются следующие термины и определения:

владелец сертификата ключа проверки электронной подписи (владелец сертификата) – лицо, которому в порядке, установленном Федеральным законом от 06.04.2011 № 63-ФЗ, выдан сертификат ключа проверки электронной подписи;

инфраструктура открытых ключей – технологическая инфраструктура и сервисы, обеспечивающие выпуск и управление сертификатами ключей проверки электронной подписи;

сеть удостоверяющих центров Группы Газпром (СУЦ) – совокупность удостоверяющих центров Группы Газпром, а также иных организаций, объединенных на основе иерархической модели доверия и действующих на основании Положения о Сети удостоверяющих центров Группы Газпром;

репозиторий СУЦ – информационный ресурс Сети удостоверяющих центров Группы Газпром, на котором размещается технологическая информация для функционирования СУЦ (реестры выданных и аннулированных удостоверяющими центрами СУЦ сертификатов ключей проверки электронной подписей и т.д.);

сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

удостоверяющий центр СУЦ – удостоверяющий центр, зарегистрированный в СУЦ;

уполномоченное лицо удостоверяющего центра СУЦ – представитель удостоверяющего центра СУЦ, наделенный полномочиями по созданию и выдаче от имени удостоверяющего центра сертификатов ключей проверки электронной подписи;

электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связанная с такой информацией и которая используется для определения лица, подписывающего информацию;

электронная подпись в корпоративных информационных системах – усиленная неквалифицированная электронная подпись, применяемая в корпоративных информационных системах ОАО «ТГК-1» и Группы Газпром.

1. Общие положения

Настоящая Инструкция разработана в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и Распоряжением ОАО «Газпром» от 24.01.2013 № 18 «Об утверждении нормативных документов, регламентирующих деятельность Сети удостоверяющих центров Группы Газпром».

В соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» в настоящей инструкции под пользователем удостоверяющего центра понимается владелец сертификата – лицо, которому удостоверяющим центром выдан сертификат ключа проверки электронной подписи.

Настоящая инструкция определяет порядок действий, которые выполняет владелец сертификата в процессе регистрации, при получении и работе с сертификатами ключа проверки электронной подписи и ключевыми носителями.

Для обеспечения защиты информации от перехвата, искажения и модификации при её передаче по открытым каналам связи, включая сеть Интернет, требуется использовать шифрование и электронную подпись электронных документов. ЭП также позволяет подтвердить (определить) авторство электронного документа.

Функции по выдаче ключей ЭП и ключей проверки ЭП, сертификатов ключей проверки ЭП пользователям и управлению ключами проверки ЭП обеспечивает Удостоверяющий центр ОАО «ТГК-1» (далее УЦ-ТГК-1).

УЦ-ТГК-1 подключен к Сети удостоверяющих центров ОАО «Газпром» и имеет статус подчиненного. Корневым удостоверяющим центром является Корпоративный УЦ-ТГК-1 ОАО «Газпром».

Порядок функционирования УЦ-ТГК-1 установлен Регламентом УЦ-ТГК-1 ОАО «ТГК-1» (далее Регламент).

Регламент определяет условия предоставления и правила пользования услугами УЦ-ТГК-1, включая права, обязанности, ответственность УЦ-ТГК-1 и владельцев сертификата, форматы данных, основные организационно-технические мероприятия, направленные на обеспечение работы УЦ-ТГК-1.

Владельцы сертификата обязаны соблюдать требования Регламента, в части относящейся к ним.

2. Регистрация владельцев сертификата и получение сертификата ключа проверки электронной подписи

Процедура регистрации применяется в отношении физических лиц, обращающихся в УЦ-ТГК-1 с целью получения ключей ЭП и сертификатов ключей проверки подписи.

Регистрация владельца сертификата УЦ-ТГК-1 осуществляется оператором УЦ-ТГК-1 на основании заявления на регистрацию владельца сертификата, создание ключей ЭП и проверки ЭП и создание сертификата ключа проверки ЭП. Заявление может подаваться на бумажном носителе при личном прибытии лица, проходящего процедуру регистрации, либо доверенного лица по соответствующей доверенности.

При принятии УЦ-ТГК-1 положительного решения работник УЦ-ТГК-1 проводит процедуру идентификации владельца сертификата и выполняет регистрационные действия по занесению регистрационной информации в реестр УЦ-ТГК-1, а также изготавливает ключи ЭП и проверки ЭП и сертификат ключа проверки ЭП.

По окончании процедуры регистрации владельцу сертификата УЦ-ТГК-1 выдаются:

– ключевой носитель, содержащий ключевые файлы в контейнере и сертификат ключа проверки ЭП;

– сертификат ключа проверки ЭП владельца сертификата УЦ-ТГК-1 на бумажном носителе;

– копия заявления владельца сертификата УЦ-ТГК-1 на регистрацию владельца сертификата, создание ключей ЭП и проверки ЭП и создание сертификата ключа проверки ЭП с резолюцией уполномоченного лица УЦ-ТГК-1 (лица, временно его замещающего) и отметкой о произведенной регистрации владельца сертификата УЦ-ТГК-1, создании ключей ЭП и проверки ЭП и сертификата ключа проверки ЭП и их передачи заявителю;

– распечатанный на бумаге адрес в формате URL страницы WEB-сервера УЦ-ТГК-1, на которой владелец сертификата УЦ-ТГК-1 может получить электронные версии действующего сертификата УЦ-ТГК-1, а также списка аннулированных сертификатов УЦ-ТГК-1.

Факт выдачи сертификата и ключей фиксируется в заявлении на регистрацию владельца сертификата, создание ключей ЭП и проверки ЭП и создание сертификата ключа проверки ЭП и удостоверяется личной подписью владельца сертификата или его доверенного лица.

Факт выдачи ключевого носителя фиксируется в журнале регистрации, учета и выдачи ключевых документов и носителей.

На АРМ владельца сертификата должны быть выполнены работы по настройке аппаратно-программных средств АРМ владельца сертификата для работы со средствами шифрования и ЭП.

Порядок установки и настройки аппаратно-программных средств криптографической защиты приведен в Приложении № 1.

3. Порядок работы с ключевым носителем

Сертификат ключа проверки ЭП в электронной форме и ключ ЭП, хранятся на ключевом носителе (USB-ключ eToken), выданном владельцу сертификата.

Для получения доступа к защищённым данным, хранящимся в памяти ключевого носителя, требуется ввести PIN-код (Personal Identification Number), являющийся аналогом пароля.

Пользователь должен выполнять следующие требования:

– обеспечить сохранность ключевого носителя. Не передавать его другим лицам;

– изменить PIN-код сразу после получения ключевого носителя. PIN-код необходимо хранить в тайне;

– соблюдать требования к PIN-коду ключевого носителя, к его периодической смене;

Порядок смены пользователем PIN-кода приведен в Приложении № 2.

При последовательном вводе более пяти неправильных PIN-кодов ключевой носитель блокируется. Для разблокировки ключевого носителя необходимо обратиться в УЦ-ТГК-1.

По решению УЦ-ТГК-1 может быть предоставлен индивидуальный административный пароль для возможности самостоятельной разблокировки ключевого носителя.

В случае утраты ключевого носителя (USB-ключ eToken) ключ ЭП восстановить невозможно. Зашифрованная с помощью утерянного ключа ЭП информация восстановлению не подлежит!

При повторном получении сертификата ключа проверки ЭП информация, зашифрованная с использованием старого ключа ЭП в случае его уничтожения, восстановлению не подлежит.

4. Порядок работы с сертификатами ключа проверки электронной подписи

Для владельца сертификата порядок установки и работы с сертификатами ключа проверки ЭП, приведен в Приложении № 3.

На представительском веб-сайте ОАО «ТГК-1» (http://www.tgc1.ru/ca/) пользователям доступны:

– сертификат уполномоченного лица УЦ-ТГК-1 ОАО «ТГК-1» в электронной форме (TGC1 CA);

– список аннулированных сертификатов УЦ-ТГК-1 ОАО «ТГК-1».

Для обеспечения юридически значимого электронного обмена документами с ОАО «Газпром» пользователи имеют возможность получения с репозитория Сети удостоверяющих центров (СУЦ) ОАО «Газпром» (http://caweb.gazprom.ru/):

– сертификата уполномоченного лица корпоративного УЦ ОАО «Газпром» (Root Gazprom CA) в электронной форме;

– сертификатов уполномоченных лиц удостоверяющих центров СУЦ в электронной форме;

– списков отозванных сертификатов корпоративного УЦ-ТГК-1 ОАО «Газпром»;

– списков аннулированных сертификатов удостоверяющих центров СУЦ;

– сертификатов других зарегистрированных удостоверяющих центров СУЦ.

5. Порядок шифрования и наложения ЭП

Для обеспечения защиты информации при организации электронной почтовой переписки (e-mail) используются функции по шифрованию и ЭП, встроенные в почтовые клиенты. Порядок работы пользователей при шифровании, наложении ЭП и выполнении обратных действий в почтовых клиентах приведен в Приложении № 4.

6. Список источников

1. КриптоПро УЦ. Регламентные задания.
2. КриптоПро УЦ. ЦС. Руководство по эксплуатации Windows 2008.
3. КриптоПро УЦ. ЦР. Руководство по эксплуатации.
4. КриптоПро УЦ. Руководство пользователя.
5. КриптоПро УЦ. Руководство по установке.
6. КриптоПро УЦ. Руководство по управлению системными ролями.
7. КриптоПро УЦ. Руководство по регистрации дополнительных объектных идентификаторов (OID).
8. КриптоПро УЦ. Руководство по восстановлению работоспособности компонент.
9. КриптоПро УЦ. Руководство по безопасности.
10. КриптоПро УЦ. Руководство администратора БД.
11. КриптоПро УЦ. Ошибки, возникающие при эксплуатации.
12. КриптоПро УЦ. Общее описание.
13. КриптоПро УЦ. Программный комплекс разбора конфликтных ситуаций.
14. КриптоПро УЦ. АРМ администратора ЦР. Руководство по эксплуатации.
15. КриптоПро УЦ. АРМ администратора ЦР. Практическая реализация регламентных процедур.

Приложение № 1 к Инструкции пользователя
Удостоверяющего центра ОАО «ТГК-1»

Установка и настройка аппаратно-программных средств криптографической защиты

Порядок установки программного обеспечения, необходимого для работы с сертификатом ключа проверки ЭП и ключевым носителем USB-ключ eToken:

1. Установить и настроить ПО eToken PKI Client.
2. Установить и настроить СКЗИ «КриптоПро CSP» версии 3.6.

1. Установка и настройка eToken PKI Client

1.1 USB-ключ/смарт-карта eToken

USB-ключ eToken – персональное средство аутентификации и хранения данных, аппаратно поддерживающее работу с сертификатами и ЭП.

USB-ключ eToken обладает защищенной энергонезависимой памятью и используется в качестве гарантированного хранилища ключей ЭП и сертификатов ключей проверки ЭП.

1.2 Программное обеспечение для USB-ключей eToken

eToken PKI Client — это среда функционирования USB-ключей eToken, включающая все необходимые драйверы.

1.3 Предупреждения

Запрещается подсоединять USB-ключ до установки и во время установки драйверов eToken PKI Client.

1.4 Установка

Для установки и удаления программного обеспечения для eToken необходимы полномочия локального администратора.

Для того чтобы установить eToken PKI Client, выполните следующую последовательность действий:

– Запустите программу установки eToken PKI Client PKIClientx32-5.1-SP1.msi или PKIClient-x64-5.1-SP1.msi.

– В окне приветствия программы установки eToken PKI Client нажмите **Next** (Далее).

– В окне **eToken PKI Client 5.1 Setup / End-User License Agreement** ознакомьтесь с лицензионным соглашением (на английском языке) и выберите **I accept the license agreement** (Я принимаю лицензионное соглашение), чтобы продолжить установку. Нажмите **Next** (Далее).

– В окне **eToken PKI Client 5.1 Setup / Ready to Install the Application** нажмите **Next** (Далее).

– Выполните необходимые действия, руководствуясь инструкциями в окне программы-мастера и, после того как установка будет завершена, нажмите кнопку Готово.

– Установка займёт некоторое время. Если на вашем компьютере был установлен **eToken PKI Client** одной из предыдущих версий, он будет удалён.

– По завершении процесса установки **eToken PKI Client** в окне **eToken PKI Client 5.1 Setup / eToken PKI Client 5.1 has been successfully installed** нажмите **Finish** (Готово).

– В конце процесса установки **eToken PKI Client 5.1** может потребоваться перезагрузка компьютера. Рекомендуется сразу после установки **eToken PKI Client** перейти к установке КриптоПро CSP и выполнить перезагрузку по завершении установки

КриптоПро CSP. В окне **Installer Information** нажмите **No** (Нет), если вы планируете перезагрузить компьютер позднее.

2. Установка и настройка СКЗИ «КриптоПро CSP» версии 3.6

Установка дистрибутива КриптоПро CSP должна производиться пользователем, имеющим права локального администратора. Для установки требуется программа установки КриптоПро CSP версии 3.6 R2 (csp-win32-kc1-rus.msi) или КриптоПро CSP 3.6.R3 (cspsetup.exe из папки дистрибутива).

Перед установкой дистрибутива удалите все ранее существующие версии устанавливаемого программного обеспечения. Если модуль криптографической поддержки не удален, новая версия не будет установлена. Для этого используйте пункты основного меню Windows **Пуск -> Настройка -> Панель управления -> Установка и удаление программ (Программы и компоненты).**

Для установки программного обеспечения запустите программу установки с дистрибутивного диска или из дистрибутивного комплекта. Последующая установка производится в интерактивном режиме. После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

При установке программного обеспечения КриптоПро CSP без ввода лицензии пользователю предоставляется лицензия с ограниченным сроком действия. Для использования КриптоПро CSP после окончания этого срока пользователь должен ввести серийный номер с бланка Лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (Дилера). Для ввода лицензии (под Windows 7 или 8) в меню выполните **Пуск>Все программы>Крипто-Про>Управление лицензиями КриптоПро PKI** >нажать правой кнопкой мыши на строке **КриптоПро CSP> Все задачи> Ввести серийный номер.**

Система отобразит окно «Сведения о пользователе», в котором необходимо указать сведения о пользователе, организации, а также ввести **серийный номер** с бланка **Лицензии** в соответствующие поля ввода.

После завершения программы установки рекомендуется зарегистрировать установленное программное обеспечение КриптоПро CSP у организации-разработчика.

Приложение № 2 к Инструкции пользователя
Удостоверяющего центра ОАО «ТГК-1»

Порядок смены PIN-кода USB-ключа eToken

1. Смена PIN-кода пользователем

Для того чтобы сменить PIN-код, необходимо выполнить следующие действия:

– подсоединить к АРМ ключевой носитель USB-ключ eToken, на котором требуется сменить PIN-код;

– если в системном трэе есть значок **eToken PKI Client,** то нажать на нём правой кнопкой мыши**.** В появившемся контекстном меню выбрать и нажать левой кнопкой строку **Изменить пароль eToken.** Если значка нет, то надо запустить утилиту eToken Properties, следующим образом: **Пуск** > **Все программы** > **eToken > eToken PKI Client> eToken Properties**, далее нажать строку **«Изменить пароль eToken»;**

– в появившемся окне ввести текущий PIN-код (если не меняли, то по умолчанию 1234567890) в поле **Текущий пароль для eToken**, а новый PIN-код — в поля **Новый пароль для eToken** и **Подтверждение**;

– нажать **ОК**;

– в случае успешной смены PIN-кода на экране появится окно **Изменить пароль** с сообщением: **Пароль успешно изменен**;

– нажать **ОК**;

– для выхода из программы закрыть основное окно **eToken Properties**.

2. **Требования к PIN-коду**

При назначении PIN-кода пользователь должен выполнять следующие требования:

– PIN-код должен состоять не менее чем из шести символов.

– В PIN-коде должны присутствовать символы из категорий:
  - строчные буквы английского алфавита от a до z;
  - прописные буквы английского алфавита от A до Z,
  - десятичные цифры от 0 до 9,

– Использование трёх и более подряд идущих на клавиатуре символов, набранных в одном регистре, недопустимо.

– Использование двух и более подряд идущих одинаковых символов недопустимо;

– Задание PIN-кода, совпадающего с любым из последних трёх PIN-кодов, недопустимо.

– PIN-код не должен содержать букв русского алфавита.

3. **Переименование USB-ключей eToken**

Для того чтобы изменить имя выбранного USB-ключа eToken:

– необходимо нажать **Переименовать;**

– при необходимости ввести PIN-код USB-ключа eToken и нажать **ОК;**

– в окне **Введите имя eToken** надо внести изменения в поле **Имя eToken**;

– нажать **ОК.**

Приложение № 3 к Инструкции пользователя
Удостоверяющего центра ОАО «ТГК-1»

Порядок установки и работы с сертификатами ключа проверки электронной подписи

1. Установка личного сертификата ключа проверки ЭП владельца сертификата

Установку личного сертификата ключа пользователя необходимо осуществлять, зарегистрировавшись в системе под личной учетной записью.

Последовательность установки:

– Установить выданный УЦ-ТГК-1 персональный ключевой носитель (USB-ключ eToken) в USB-разъем.

– Из панели управления запустить приложение КриптоПро CSP.

– Во вкладке **Сервис** нажать кнопку **Просмотреть сертификаты в контейнере**.

– Для выбора имени ключевого контейнера нажать **Обзор**.

– Выбрать ключевой контейнер, находящийся на считывателе AKS ifdh 0 (Aladdin Token JC 0), нажать **ОК**. Нажать **Далее**.

– Нажать кнопку **Свойства**.

– Нажать кнопку **Установить сертификат**.

– В окне приветствия мастера импорта сертификатов нажать **Далее**.

– Выбрать **Поместить все сертификаты в следующее хранилище**, нажать **Обзор**.

– В списке хранилищ сертификатов выбрать **Личные**, нажать **ОК**.

– Нажать **Далее**.

– В окне завершения мастера импорта сертификатов нажать **Готово**.

– Закрыть приложение КриптоПро CSP.

Для корректного построения цепочки доверия до сертификата ключа пользователя необходимо установить сертификаты корневого и подчиненного Удостоверяющих центров.

2. Установка сертификата корневого УЦ (Корпоративного УЦ ОАО «Газпром»)

Последовательность установки:

– Перейти по ссылке http://caweb.gazprom.ru/AIA/Root_Gazprom_CA.crt. При этом появится диалоговое окно:

– Нажать кнопку **Открыть**. При этом откроется сертификат.

– Нажать кнопку **Установить сертификат**.

– В окне приветствия мастера установки сертификатов нажать **Далее**.

– Выбрать **Поместить все сертификаты в следующее хранилище**, нажать **Обзор**.

– Выбрать хранилище **Доверенные корневые центры сертификации** и нажать **ОК**.

– Нажать **Далее**.

– В окне завершения мастера импорта сертификатов нажать **Готово**.

3. Установка сертификата подчиненного УЦ-ТГК-1 (УЦ-ТГК-1 ОАО «ТГК-1»)

Процедура аналогична процедуре установки сертификата корневого удостоверяющего центра, но на шаге 1 необходимо перейти по ссылке сертификата УЦ-ТГК-1 ОАО «ТГК-1» (http://www.tgc1.ru/ca/ TGC1_CA.crt или http://caweb.gazprom.ru/AIA/TGC1_CA.crt), а затем, в качестве хранилища выбрать **Промежуточные центры сертификации**.

4. Установка сертификатов других пользователей УЦ-ТГК-1

Для того чтобы пользователи УЦ-ТГК-1 имели возможность использовать средства шифрования и электронной подписи для обмена информацией с другими пользователями, им необходимо получить и установить сертификаты ключа проверки электронной подписи других пользователей.

Сертификаты пользователей УЦ-ТГК-1 являются открытой информацией. Их можно получить с помощью Сервиса поиска сертификатов, расположенного по адресу: http://caweb.gazprom.ru/Search.htm.

Сервис поиска сертификатов ключей подписей Сети удостоверяющих центров ОАО «Газпром» доступен только пользователям удостоверяющих центров Сети удостоверяющих центров ОАО «Газпром», дочерних обществ и организаций.

Для обеспечения поиска сертификатов ключей проверки ЭП на компьютере должны быть установлены и настроены средства криптографической защиты информации, реализующие протокол Transport Layer Security (TLS v.1.0, RFC 2246), с использованием российских криптографических стандартов (например, модуль поддержки сетевой аутентификации КриптоПро TLS, входящий в состав СКЗИ КриптоПро CSP).

Для успешной аутентификации и установления защищенного соединения с Сервисом поиска сертификатов ключей подписей должны быть обеспечены доверительные отношения с Корпоративным удостоверяющим центром ОАО «Газпром» и удостоверяющем центром, выдавшим сертификат.

С помощью вышеуказанной веб-страницы нужно выбрать удостоверяющие центры, где будет производиться поиск сертификатов, ввести шаблон поиска сертификата пользователя и нажать кнопку **Искать сертификаты**.

После того, как необходимый сертификат найден, его можно сохранить на компьютере в виде файла или установить в хранилище сертификатов.

5. Сохранение отдельного сертификата осуществляется следующим образом:

1. Для импорта сертификатов необходимо отметить поле выбора нужных сертификатов и нажать кнопку **Экспорт сертификатов**. При этом стандартный режим браузера MS IE предложит либо сохранить сертификат в файле на диске, либо открыть его при помощи встроенного в операционную систему режима просмотра сертификатов (В зависимости от версии браузера, возможно, потребуется при нажатии кнопки **Экспорт сертификатов** удерживать на клавиатуре кнопку **Ctrl**.)

2. Чтобы просмотреть сертификат нажмите кнопку **Открыть**. При этом сертификат будет отображен в стандартном окне просмотра сертификатов.

3. Для импорта сертификата в специальное хранилище операционной системы в данном окне нажмите кнопку **Установить сертифика**т. При этом запустится мастер установки (импорта) сертификатов в хранилище сертификатов пользователей. Сертификат следует установить в хранилище **Другие пользователи** с процедурами установки сертификатов, описанных выше.

Приложение № 4 к Инструкции пользователя
Удостоверяющего центра ОАО «ТГК-1»

Работа с почтовыми клиентами

Для шифрования и формирования ЭП почтовые клиенты должны быть предварительно настроены для работы с сертификатами ключа проверки ЭП. Порядок настройки приводится в документации на соответствующее программное обеспечение.

Отправка сообщений может производиться с использованием следующих функций:

- формирование ЭП сообщения;
- шифрование сообщения;
- формирование ЭП и шифрование сообщения.

В случае использования функций формирования ЭП, а также функции одновременного использования формирования ЭП и шифрования, необходимо использование ключевого носителя.

1. Шифрование и формирование ЭП в Microsoft Outlook 2010 (2013)

1.1 Проверить в OUTLOOK 2010 (2013) следующие настройки: Файл→Параметры→Центр управления безопасностью→Параметры Центра управления безопасностью→ Защита электронной почты→ в секции «Шифрованнная электронная почта» нажимаем Параметры... Откроется окно «Изменение настройки безопасности». Должны быть выбраны сертификаты подписи и шифрования этого пользователя и должна стоять галочка напротив «Передавать сертификаты с сообщением».

1.2 Отправка сообщений с цифровой подписью.

Для отправки сообщений с ЭП необходимо выполнить следующие действия:

- для создания и отправки подписанного сообщения на закладке **Главная** в области навигации выбрать **«Почта»** и нажать кнопку **Создать сообщение;**
- выберите получателя сообщения (поле **Кому**) и введите тему сообщения (**Тема**). Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить файл** в закладке **Вставка**;
- для того, чтобы подписать сообщение нажмите на кнопку **Подписать** в закладке **Параметры;**
- для отправки сообщения нажмите кнопку **Отправить.** Появится окно для ввода Pin-кода eToken.

1.3 Получение сертификата открытого ключа абонента для шифрования сообщений

Для шифрования сообщений в адрес других пользователей необходимо предварительно произвести обмен сертификатами. Для этого обычно достаточно переслать **подписанное** (не зашифрованное) сообщение в адрес требуемого абонента (сообщение посылается вместе с сертификатом отправителя при условии выбора чекбокса напротив «Передавать сертификаты с сообщением» - путь к нему указан в первом абзаце данной инструкции). После получения сообщения и проверки электронной цифровой подписи производится автоматическое добавление адреса отправителя и его сертификата в адресную книгу.

Для контроля добавления выполните следующие действия. Откройте полученное подписанное письмо. Установите курсор на адрес отправителя и, нажав правую кнопку мыши, выберите пункт **Добавить в контакты Outlook**. В отображаемом диалоге нажмите на закладку **Показать → Сертификаты** и убедитесь в наличии сертификата отправителя.

После этого нажмите на кнопку **Сохранить и Закрыть**. Если абонент с таким адресом уже существует, программа предложит, либо добавить новый контакт **Добавить новый контакт**, либо обновить сведения о выделенном контакте **Обновить информацию о выбранном контакте**. Выберите второй пункт. При этом в существующий контакт будет добавлен полученный сертификат, а резервная копия будет сохранена в папку **Удаленные**. В любой момент можно просмотреть сертификат другого абонента так: выбранный контакт → Вкладка Контакт → Показать → Сертификаты.

1.4 Отправка шифрованных сообщений.

Для создания и отправки шифрованного сообщения нажмите кнопку **Создать сообщение** в закладке **Главная**.

Выберите получателя сообщения (поле **Кому**) и введите тему сообщения (**Тема**). Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить файл** в закладке **Вставка**. Для отправки сообщения в зашифрованном виде нажмите кнопку **Шифровать** во вкладке **Параметры.**

После того, как сообщение подготовлено к отправке, нажмите кнопку **Отправить**. Появится окно для ввода Pin-кода eToken.

1.5 Для одновременного использования формирования ЭП и шифрования почтового сообщения необходимо выполнить пункты 1.2 и 1.4.