Руководство администратора

Atlansys Software

Atlansys ESS

Atlansys Enterprise Security System
Руководство администратора

Версия 4.1.6

Содержание

Список иллюстраций

Введение

1. Назначение документа

Данное руководство администратора содержит сведения по установке и эксплуатации Atlansys Enterprise Security System и предназначено для администраторов системы.

2. Дополнительные сведения

Дополнительные сведения об использовании данного продукта и последнии версии документации можно получить на сайте компании www.atlansys.ru.

Глава 1. Установка и удаление программного обеспечения

Важно

Что следует помнить перед установкой Atlansys Enterprise Security System:

- Центр Управления в текущей версии продукта устанавливается только на Windows Server 2008.
- Консоль Администратора и дополнительные утилиты могут устанавливаться на Windows 7 и более поздние версии Windows.
- Для установки программы необходимо обладать правами Администратора операционной системы.

1.1. Установка программного обеспечения с помощью интерактивного инсталлятора

Для установки программного обеспечения на рабочую станцию необходимо выполнить следующие действия:

1. Запустить программу инсталлятора Atlansys Enterprise Security System для рабочих станций **Atlansys-ESS-CC-(номер версии)-setup.msi**.(Рисунок 1.1)

Рисунок 1.1. Установка Atlansys Enterprise Security System

2. Нажать кнопку «Далее», после чего появится диалоговое окно (Рисунок 1.2), в котором предлагается ознакомиться с лицензионным договором. В случае согласия необходимо выбрать пункт: «Я принимаю условия лицензионного договора». Для продолжения процедуры установки нажать кнопку «Далее».

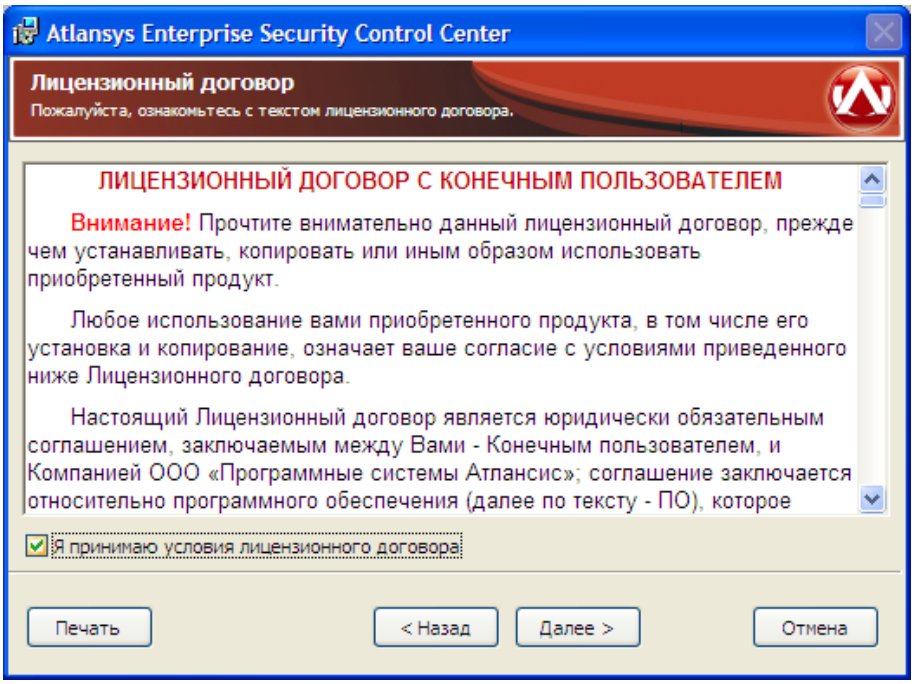

Рисунок 1.2. Лицензионный договор

3. Ввести имя пользователя, организацию, серийный номер, который поставляется с продуктом. Серийный номер содержит пять полей по пять символов, все буквы должны вводиться в верхнем регистре. Для продолжения нажать кнопку "Далее".

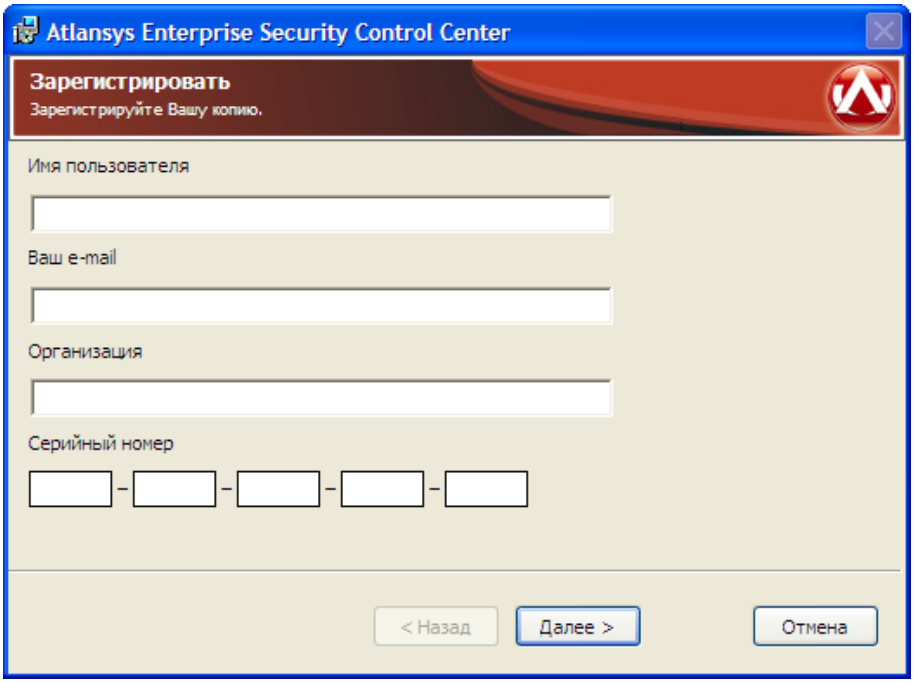

Рисунок 1.3. Регистрация

4. Выбрать компоненты программного обеспечения, которые необходимо установить. По умолчанию будут установлены все компоненты, обеспечивающие полную функциональность Atlansys Enterprise Security System. (Рисунок 1.4)

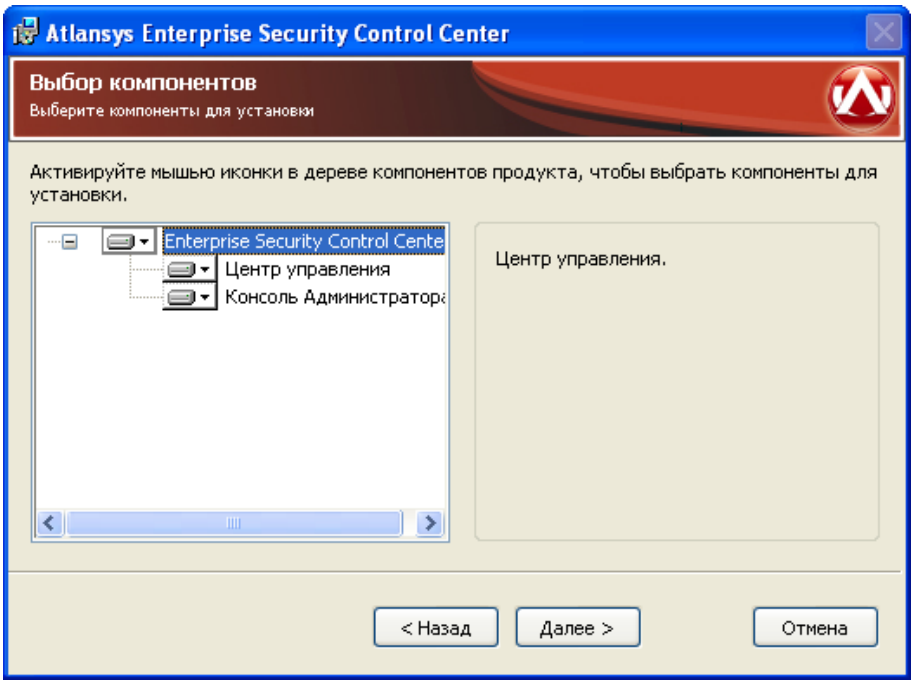

Рисунок 1.4. Выбор компонентов клиентского программного обеспечения

5. Указать имя каталога для установки программы (рекомендуется оставить значение по умолчанию). Имя каталога можно задать вручную или выбрать каталог, нажав на кнопку «Обзор». По умолчанию на Рабочий стол помещаются ярлыки программ, если в этом нет необходимости, то необходимо отключить чекбокс "Поместить ярлыки программ на рабочий стол". Для продолжения нажать кнопку «Далее». (Рисунок 1.5)

Рисунок 1.5. Выбор каталога для установки программы

6. Указать имя учетной записи и пароль администратора центра управления, в случае, если выбран компонент "Центр управления". (Рисунок 1.6)

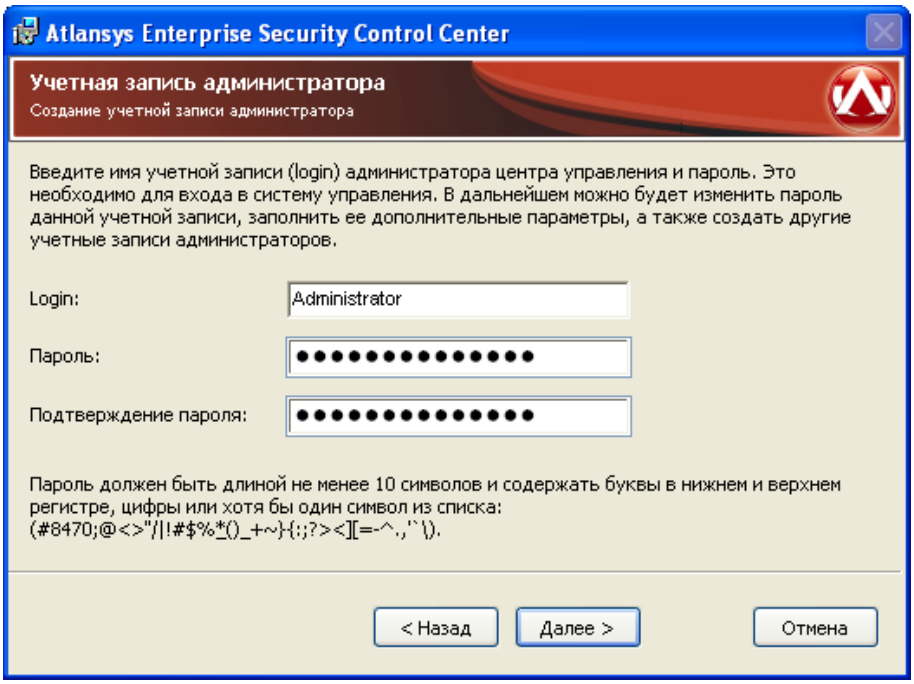

Рисунок 1.6. Ввод имени и пароля администратора

7. При необходимости, можно нажать на кнопку "Назад" и изменить ранее введеные параметры. Для запуска процесса установки необходимо нажать кнопку «Установить». (Рисунок 1.7)

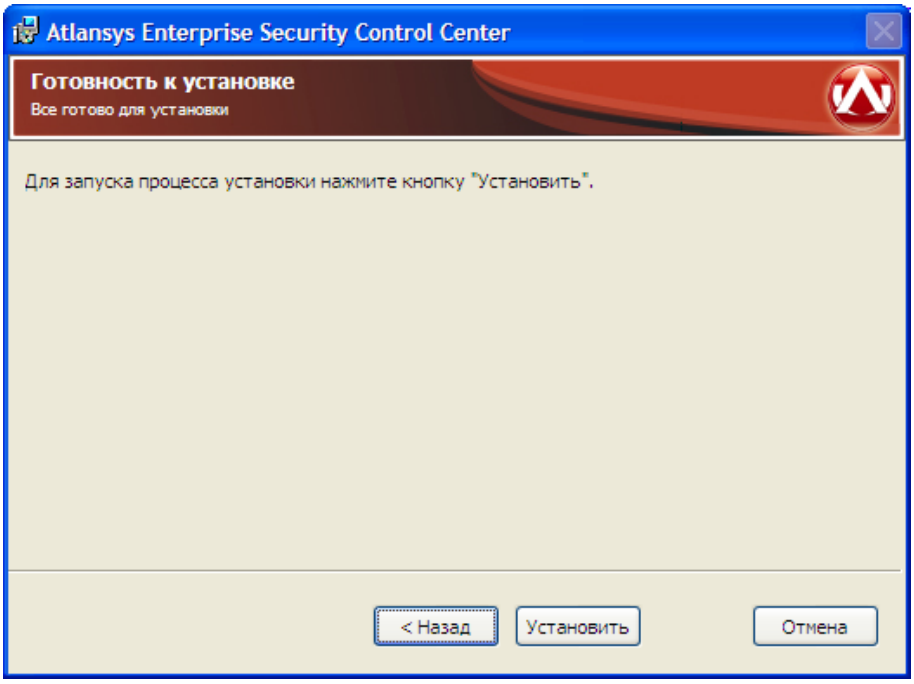

Рисунок 1.7. Запуск процесса установки

8. После этого появится окно, отображающее процесс установки программного обеспечения. (Рисунок 1.8)

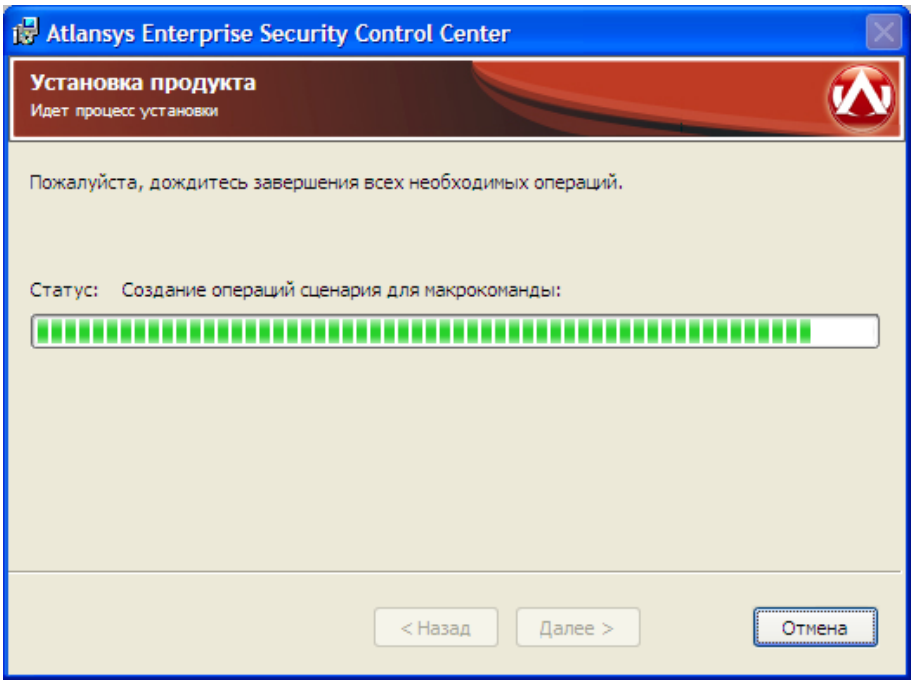

Рисунок 1.8. Процесс установки

9. Для окончания процесса установки необходимо нажать на кнопку «Завершить». (Рисунок 1.9)

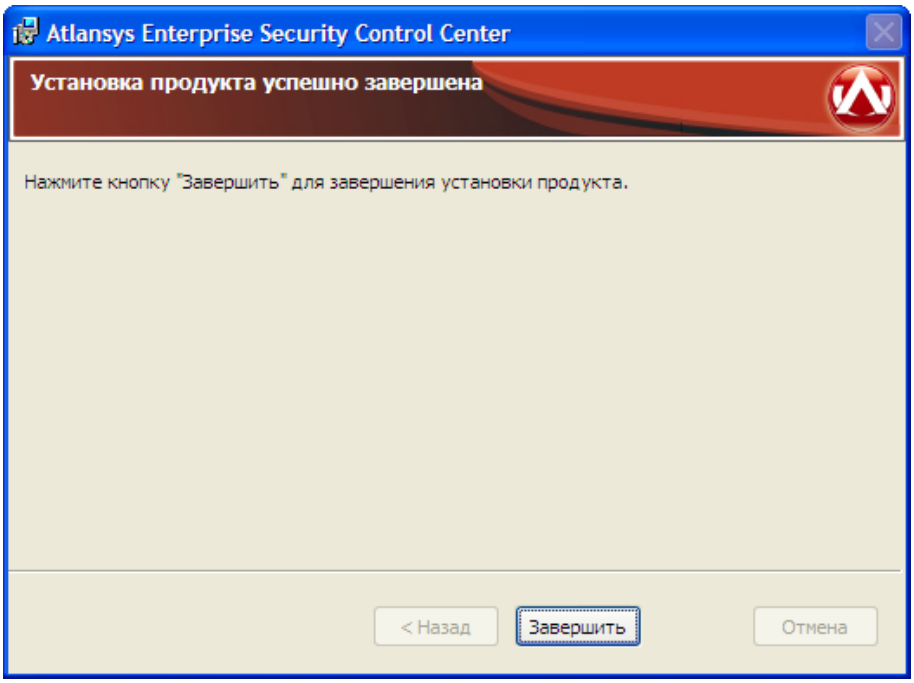

Рисунок 1.9. Завершение установки

1.2. Обновление программного обеспечения

Если на рабочей станции уже установлена более ранняя версия продукта, то при установке новой версии, совместимой с предыдущей, произведется ее автоматическое обновление. Описание совместимости версий программного обеспечения, для которых возможно обновление, смотрите в поставляемой с инстал-

лятором документации или на сайте производителя. Все конфигурационные файлы предыдущей версии продукта сохраняются и используются новой версией.

Для обновления программного обеспечения Atlansys Enterprise Security System необходимо:

1. Запустить программу инсталятора Atlansys Enterprise Security System **Atlansys-ESS-CC-(номер версии)-setup.msi**. Нажать кнопку "Далее". (Рисунок 1.10)

Рисунок 1.10. Обновление Atlansys Enterprise Security System

2. После этого появится окно, отображающее процесс обновления программного обеспечения. (Рисунок 1.11)

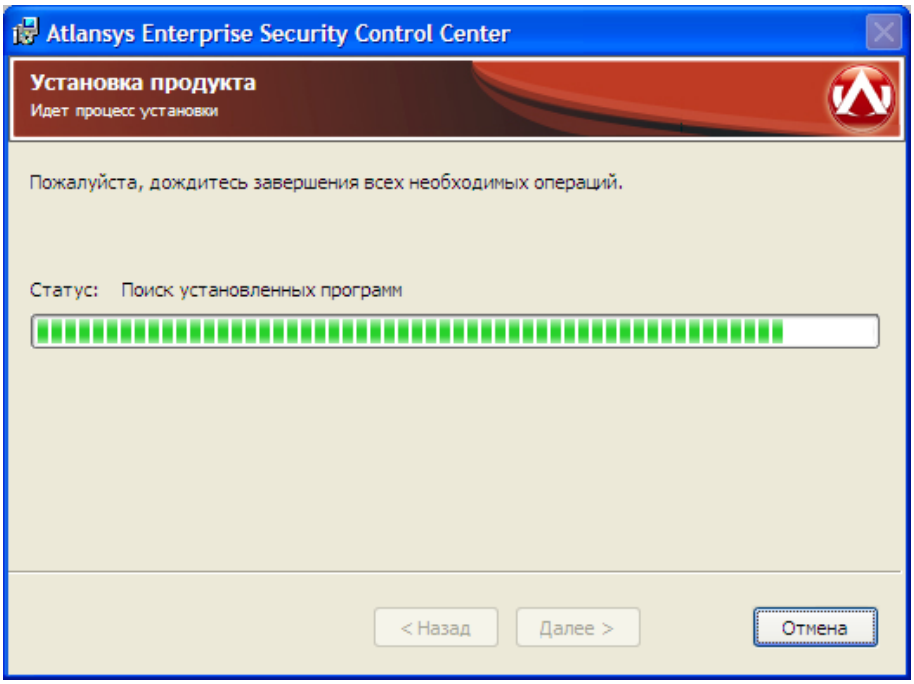

Рисунок 1.11. Процесс установки

3. Для окончания процесса установки необходимо нажать на кнопку «Завершить». (Рисунок 1.12)

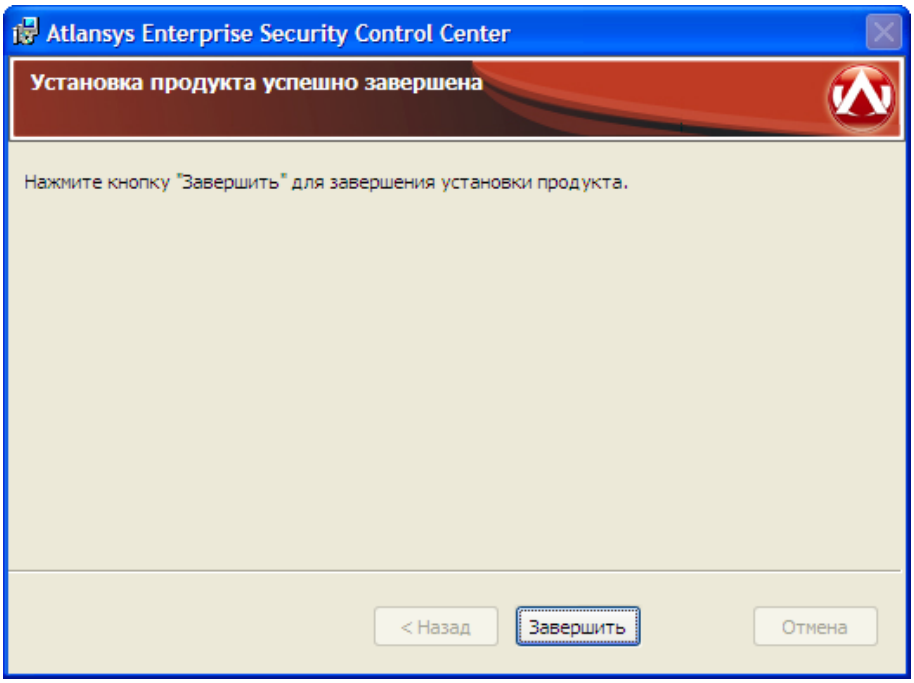

Рисунок 1.12. Завершение установки

1.3. Установка программного обеспечения с использованием конфигурационного файла

Чтобы автоматизировать установку Atlansys Enterprise Security System с заранее заданной конфигурацией, можно использовать конфигурационный файл, который содержит текст со списком опций и их значений. Файл должен быть написан в кодировке windows-1251. Каждая опция записывается в отдельной строке и

не должна быть больше 512 символов. Каждая опция записывается в отдельной строке. Строки, начинающиеся со знака решётки (#), считаются комментариями и игнорируются. Чтобы запустить инсталятор в неинтерактивном режиме необходимо выполнить в командной строке команду установки с флагом /qn:

msiexec /i Atlansys-ESS-CC-(номер версии)-setup.msi /qn

По умолчанию конфигурационный файл должен иметь имя **settings.cfg** и располагаться в том же каталоге, что и файл инсталлятора. Если необходимо задать другое имя файла, то его можно задать через командную строку:

msiexec /i Atlansys-ESS-CC-(номер версии)-setup.msi CONFIG="config.txt"

В конфигурационном файле можно задавать опции:

1. **COMPANYNAME=company** - наименование компании, на которую зарегистрирован продукт.
2. **USERNAME=user** - имя пользователя, на которого зарегистрирован продукт.
3. **PIDKEY=serial number** - серийный номер продукта, который поставляется вместе с продуктом. Содер-жит пять полей из пяти символов (букв в верхнем регистре и цифр), разделенных символом дефиса '-'.
4. **INSTALLDIR=path** - путь к каталогу установки.
5. **ADDDEFAULT=module1,module2,...** - позволяет выборочно включать установку компонентов. Значение – названия компонентов через запятую. Также можно написать ADDDEFAULT=ALL – это будет означать установку всех компонентов. Можно указывать следующие названия компонентов:
   - ControlCenter – центр управления Atlansys ESS (устанавливается только на Windows Server 2008);
   - ControlUtilites– консоль администратора центра управления, а также дополнительные утилиты;
6. **ADMINLOGIN=login** - имя учетной записи администратора Центра Управления. При инсталляции Центра Управления формируется база данных администраторов системы, в которую заносится данная учётная запись, используемая в дальнейшем при входе в Консоль Администратора.
7. **ADMINPASSWORD=password** - пароль учетной записи администратора.

Пример файла settings.cfg:

```
# Конфигурация для Центра Управления
INSTALLDIR=C:\Program Files\AtlansysESS\
ADDDEFAULT=ControlUtilites
PIDKEY=527LD-2TEST-ONLY4-VOVAN-SFXFL
USERNAME=Василий Петров
COMPANYNAME=ООО Деревянная Скала
ADMINLOGIN=root
ADMINPASSWORD=1234@56Ff!
```

Эти же свойства можно задавать из командной строки. Например:

msiexec /i Atlansys-ESS-CC-4.1.6-setup.msi INSTALLDIR="c:\Program Files\AtlansysESS" ADDDEFAULT=ALL PIDKEY=527LD-4TEST-ONLY2-VOVAN-SFXFL USERNAME="Василий Петров" COMPANYNAME="ООО Деревянная Скала" ADMINLOGIN="root" ADMINPASSWORD="1234@56Ff!"

1.4. Удаление программного обеспечения

Для удаления программного обеспечения необходимо выполнить следующие действия:

1. Закрыть Консоль Администратора, если она была запущена.
2. Запустить приложение Установка и удаление программ (Пуск / Панель управления / Установка и удаление программ), из списка программ выбрать Atlansys Enterprise Control Center.

Для удаления Atlansys Enterprise Security System необходимо нажать на кнопку "Удалить". Появится окно для подтверждения запроса удаления, необходимо нажать на кнопку "Да", после чего начнется процесс удаления Atlansys Enterprise Security System.

1.5. Генерация файла мастер-сертификатов

Для инсталляции неуправляемых клиентов используется файл с мастер-сертификатами mcfc.dat, для генерации которого необходимо выбрать в главном меню консоли администратора пункт "Файл / Создание файла мастер-сертификатов". В диалоге необходимо добавить сертификаты в список и нажать кнопку "Сохранить". В появившемся диалоге выбрать каталог для сохранения файла msfc.dat.

Глава 2. Консоль Администратора

2.1. Назначение

Консоль Администратора - это приложение, предназначенное для управления Atlansys Enterprise Security System. Содержит такие разделы, как учетные записи администраторов, группы пользователей, хранилище ключей, удаленное управление, восстановление ключей.

2.2. Запуск программы

Запуск программы осуществляется либо через ярлык на рабочем столе Windows, либо через меню "**Пуск / Все программы / Atlansys / Enterprise Security Control Center/ Консоль администратора Atlansys ESS** ".

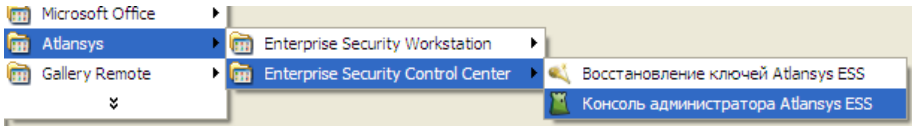

Рисунок 2.1. Запуск Atlansys Консоль администратора

2.3. Интерфейс

При запуске Консоли Администратора, появится окно аутентификации на центре управления.(Рисунок 2.2) В пустые поля необходимо ввести имя пользователя, пароль и адрес центра управления.

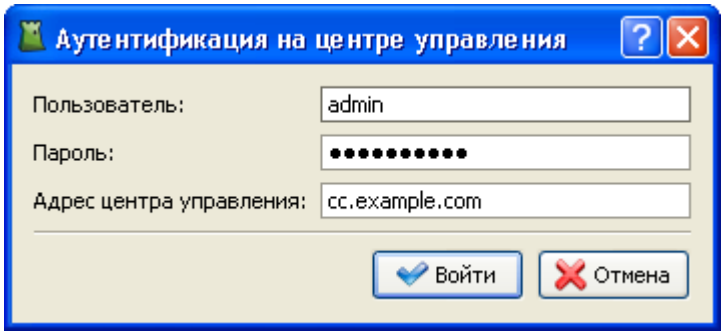

Рисунок 2.2. Аутентификация на центре управления

После успешной аутентификации открывается доступ к элементам управления консоли:

1. Кнопки быстрого перехода к соответствующими модулями Консоли.
2. Главное меню.
3. Адреса службы технической поддержки продукта.

Рисунок 2.3. Главное окно Atlansys Консоль администратора

1. Меню "Файл" содержит подменю:

   - "Создание файла мастер-сертификатов..." - вызов диалога создания файла мастер-сертификатов для инсталляции неуправляемых клиентов для рабочих станций.
   - "Утилита восстановления ключей" - запуск утилиты для восстановление поврежденных и уничтоженных ключей в криптообъектах.
   - "Обновить" - для обновления содержимого текущей страницы Консоли.
   - "Отключение" - позволяет закрыть текущую сессию администратора и зайти на Центр Управления под другим именем, либо на другой Центр Управления.
   - "Выход" - для выхода из Консоли Администратора.

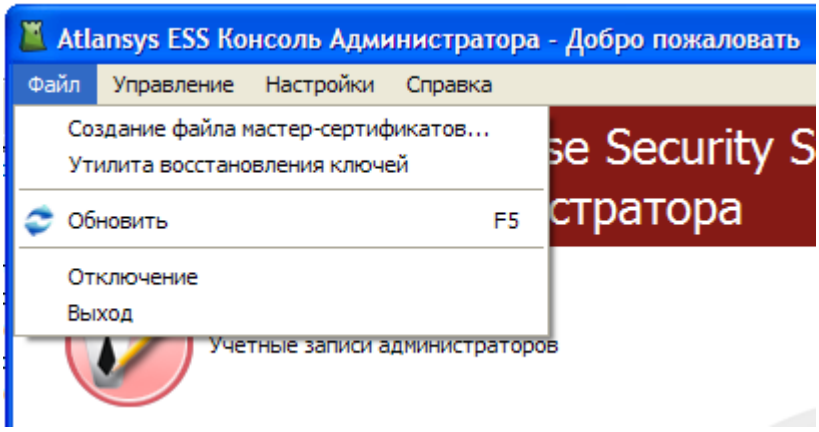

Рисунок 2.4. Меню "Файл"

2. Меню "Управление" содержит подменю для выполнения основных действий при работе с Центром Управления:

- "Учетные записи администраторов" - добавление, изменение, удаление учетных записей администраторов Центра Управления.
- "Группы пользователей" - добавление, удаление, назначение прав и мастер-сертификатов группам пользователей. Добавление пользователей в группы.
- "Группы компьютеров" - добавление, удаление, назначение прав и мастер-сертификатов группам компьютеров. Добавление компьютеров в группы.
- "Хранилище ключей" - просмотр списка сохраненных на Центре Управления ключей, созданных при работе клиентов на рабочих станциях.
- "Удаленное управление" - просмотр подключенных к Центру Управления клиентов. Оперативное закрытие криптообъектов пользователей.
- "Журнал регистрации событий" - просмотр журнала событий, зарегистрированных в системе.
- "Восстановление ключей" - запуск процедуры восстановления ключевого материала в криптообъектах пользователей.

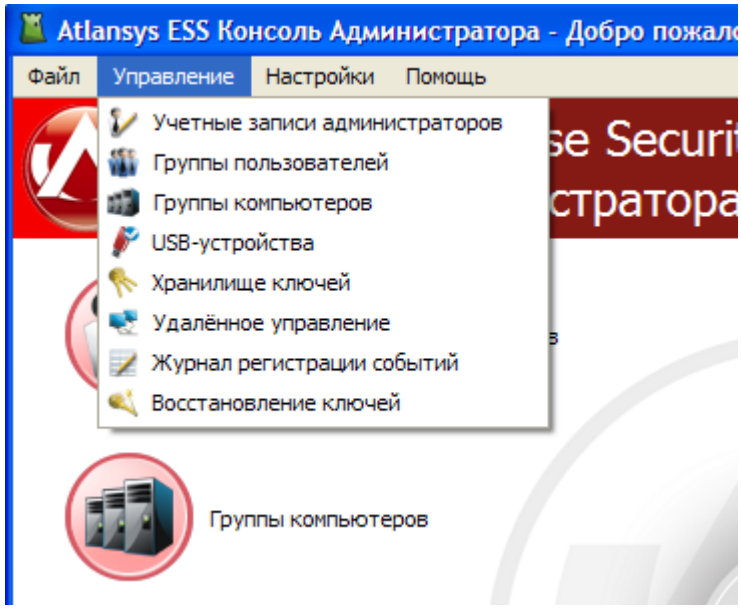

Рисунок 2.5. Меню "Управление"

3. Меню "Настройки" содержит подменю:
   - "Настройки..." - для запуска диалога настроек.

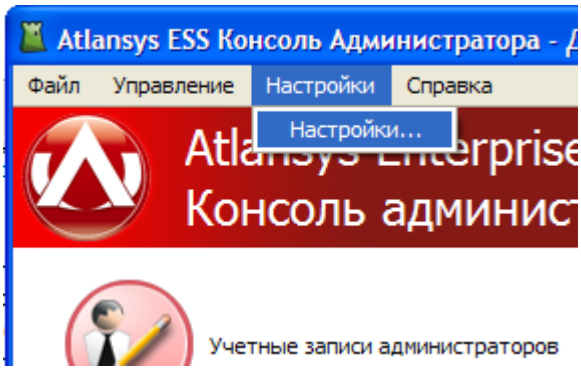

Рисунок 2.6. Меню "Настройки"

4. Меню "Справка" содержит подменю(Рисунок 2.7):

   - "Помощь" - для вызова справки по программе;

   - "О программе" - для вызова диалога "О программе", в котором содержится информация о версии программы, параметрах регистрации, и доступных лицензиях.

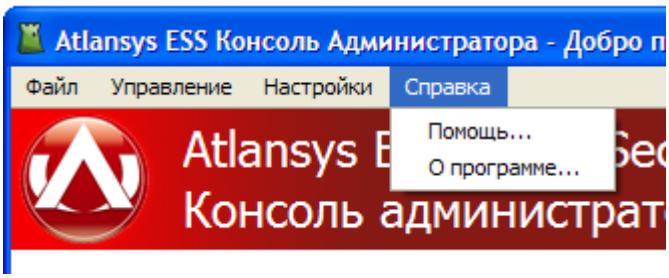

Рисунок 2.7. Меню "Справка"

2.4. Настройки продукта

Для уточнения параметров работы продукта используется диалог настроек, который вызывается через главное меню "Настройки / Настройки...". С левой стороны диалога расположена панель доступных для управления модулей, при выборе которых с правой стороны отображаются текущие параметры выбранного модуля.

Замечание

В зависимости от набора установленных дополнительных модулей список настроек может отличатся от приведённых в данном Руководстве.

1. "Общие" - общие настройки ЦУ. На этой вкладке можно время хранения записей о подключавшихся клиентах. Клиент, не подключавшийся к ЦУ дольше указанного срока, перестаёт отображаться во вкладке "Удалённое управление". Если указать срок в 0 дней, то записи клиентов будут удаляться сразу после их отключения от ЦУ.

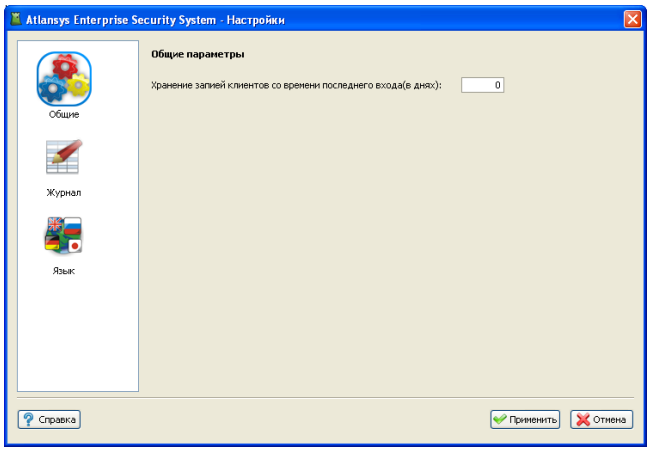

Рисунок 2.8. Язык

2. "Регистрация событий" - задаёт параметры регистрации сообщений в локальной базе и отправки лог-сообщений на внешний syslog-сервер.

   - "Файл журнала" - задаётся максимальный размер файла журнала. При превышении размера журнал архивируется.

   - "База данных лог-сообщений" - задаётся путь к файлу базы данных лог-сообщений. Рекомендуется оставить этот параметр по умолчанию. База данных состоит из одного файла, который создаётся автоматически при старте системы, если по указанному пути он не был найден.

   - "Отправлять сообщения на syslog сервер" - задаётся адрес syslog сервера, на который будут отсылаться лог-сообщения, а также уровень лога.

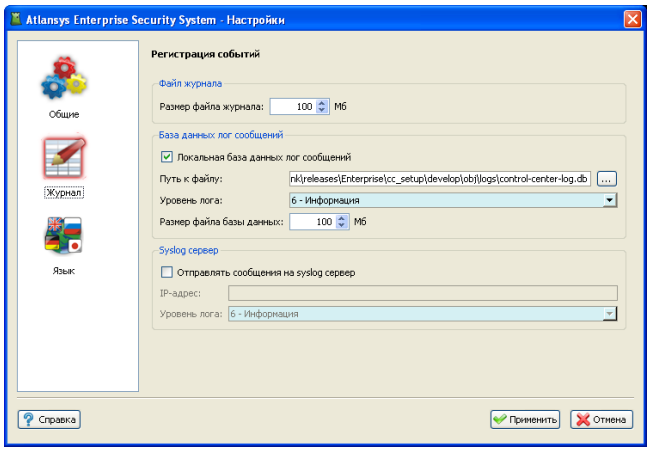

Рисунок 2.9. Регистрация событий

3. "Язык интерфейса" - выбор языка пользовательского интерфейса. Набор языков может отличаться в зависимости от локализации продукта.

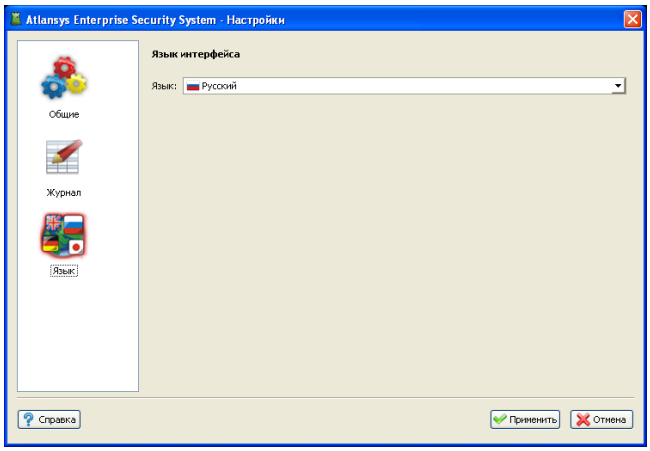

Рисунок 2.10. Язык

Глава 3. Учетные записи администраторов

3.1. Назначение

В данном разделе описывается работа с учетными записями администраторов, их создание, редактирование, удаление. Переход на панель учетных записей администраторов производится через главное меню "Управление / Учётные записи администраторов".

3.2. Создание учетной записи администратора Atlansys Enterprise Security System

Для создания новой учётной записи адмнинистратора необходимо нажать на кнопку "Добавить учетную запись администратора" на панели инструментов, или в контекстном меню выбрать пункт "Добавить учетную запись администратора".

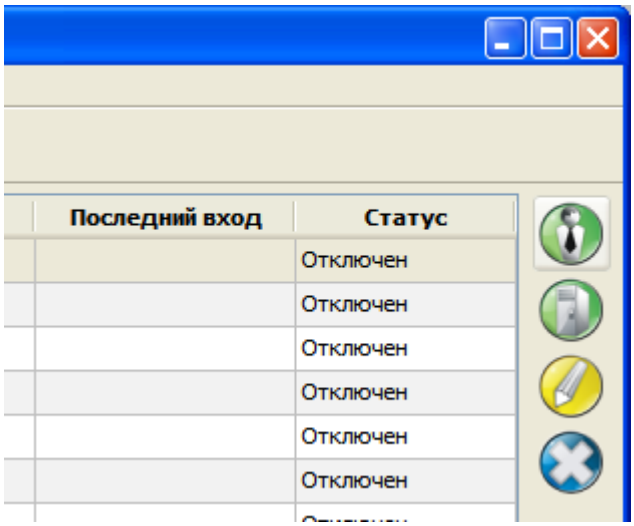

Рисунок 3.1. Добавление учетной записи администратора через панель инструментов

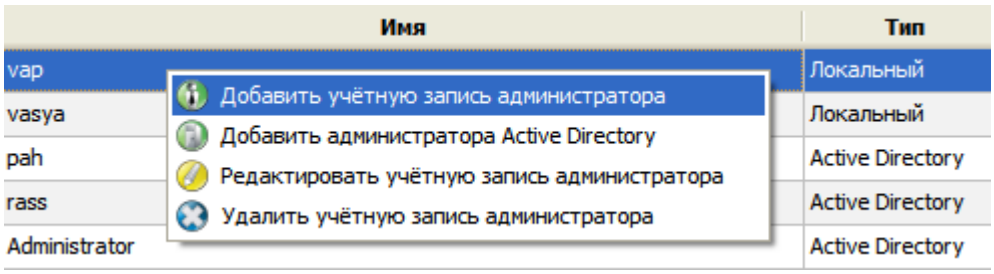

Рисунок 3.2. Добавление учетной записи администратора через контекстное меню

В появившемся диалоге необходимо заполнить поля:

- "Полное имя" - фамилия, имя администратора.
- "E-mail" - адрес электронной почты администратора.
- "Подразделение" - подразделение организации, к которому относится администратор.

- "Телефон" - телефонный номер для связи с администратором.
- "Пользователь" - идентификатор адмнинистратора, под которым он будет аутентифицироваться при входе в Консоль Администратора.
- "Пароль" - пароль администратора. Должен быть длиной не менее 10 символов в верхнем и нижнем регистре, хотя бы одной цифры и и спецсимвола.
- "Подтверждение пароля" - для повторного ввода пароля.

Поля, помеченные символом '*' обязательны для заполнения.

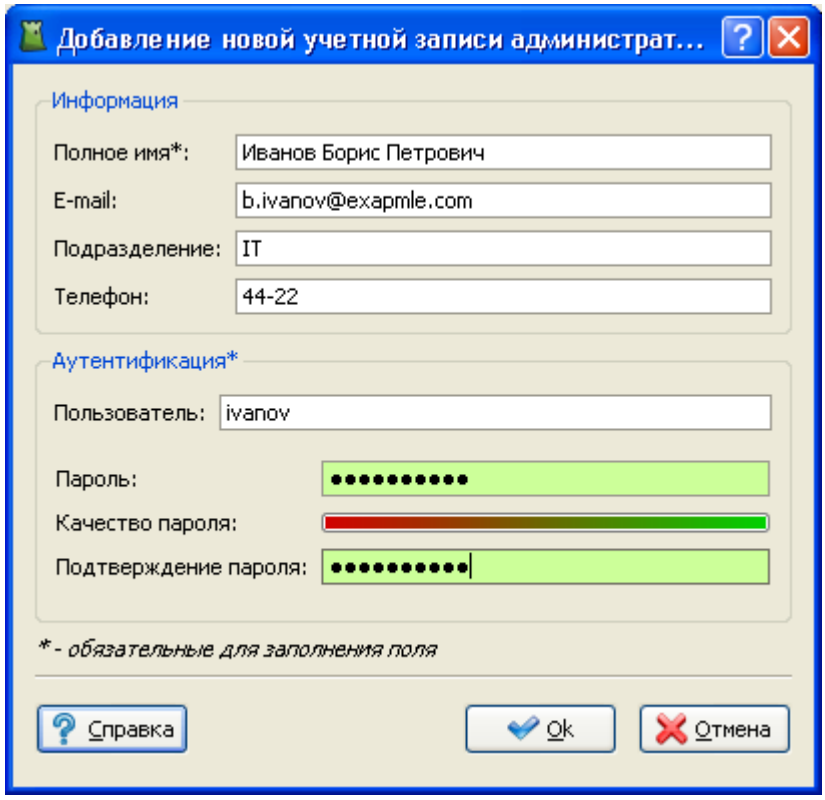

Рисунок 3.3. Внесение личных данных администратора

После заполнения необходимых полей необходимо нажать на кнопку "Ok".

3.3. Добавление учетной записи администратора Active Directory

Для создания новой учётной записи адмнинистратора необходимо нажать на кнопку "Добавить учетную запись администратора Active Directory" на панели инструментов, или в контекстном меню выбрать пункт "Добавить администратора Active Directory".

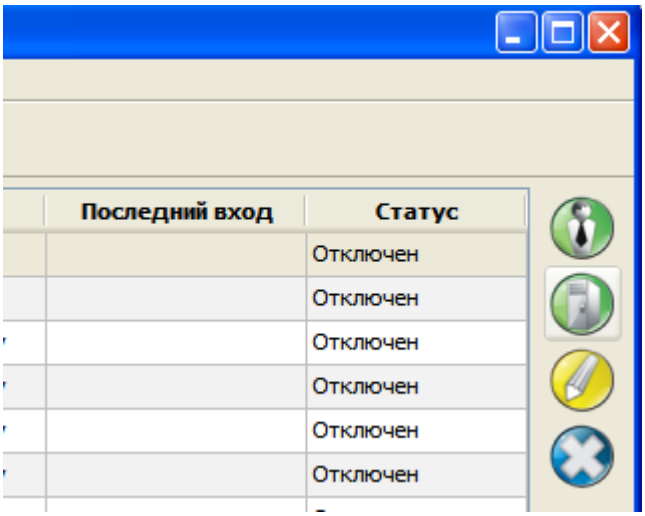

Рисунок 3.4. Добавление учетной записи администратора Active Directory через панель инструментов

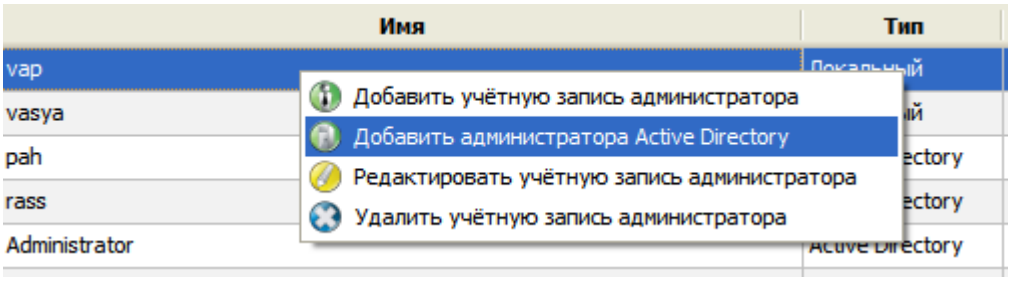

Рисунок 3.5. Добавление учетной записи администратора Active Directory через контекстное меню

В появившемся диалоге следует выбрать одного или нескольких администраторов Active Directory, после чего нажать кнопку "Добавить". После этого возможна аутентификация на центре управления при помощи учетной записи администратора Active Directory.

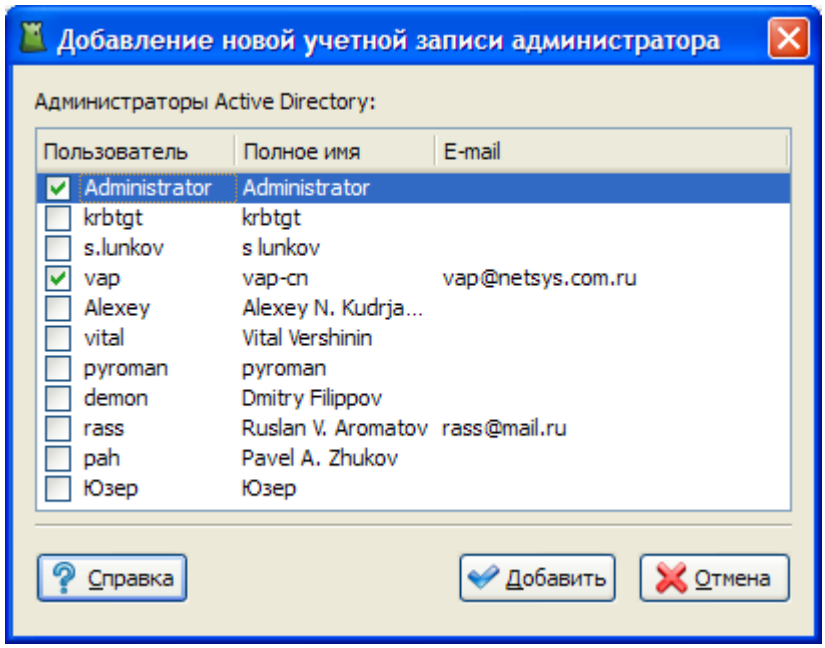

Рисунок 3.6. Добавление администратора Active Directory

3.4. Редактирование учетной записи администратора

Функция редактирования возможна только для учетной записи локального администратора Atlansys Enterprise Security System. Для редактирования учетной запись администратора, необходимо выделить необходимую учетную запись в списке адменистраторов, нажать нажать на кнопку "Редактировать" на панели инструментов, или в контекстном меню записи выбрать пункт "Редактировать учетную запись администратора".

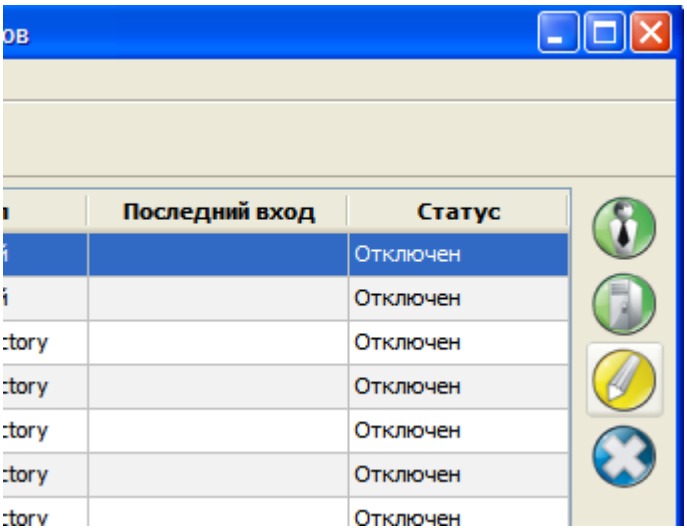

Рисунок 3.7. Редактирование учетной записи администратора через панель инструментов

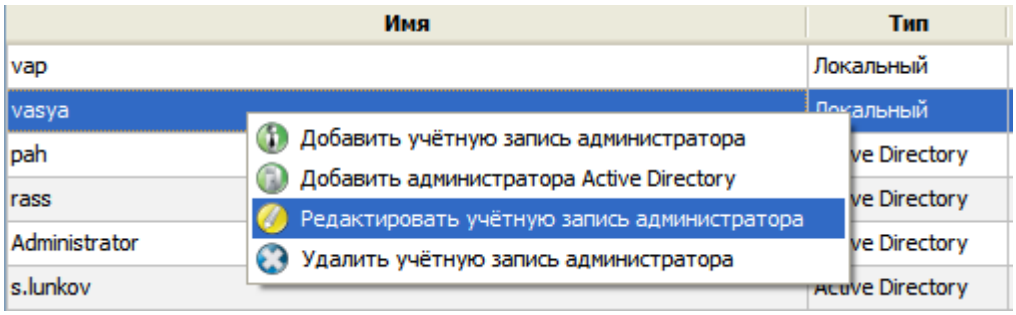

Рисунок 3.8. Редактирование учетной записи администратора через контекстное меню

В появившемся диалоге изменить необходимые данные, нажать кнопку "Ок".

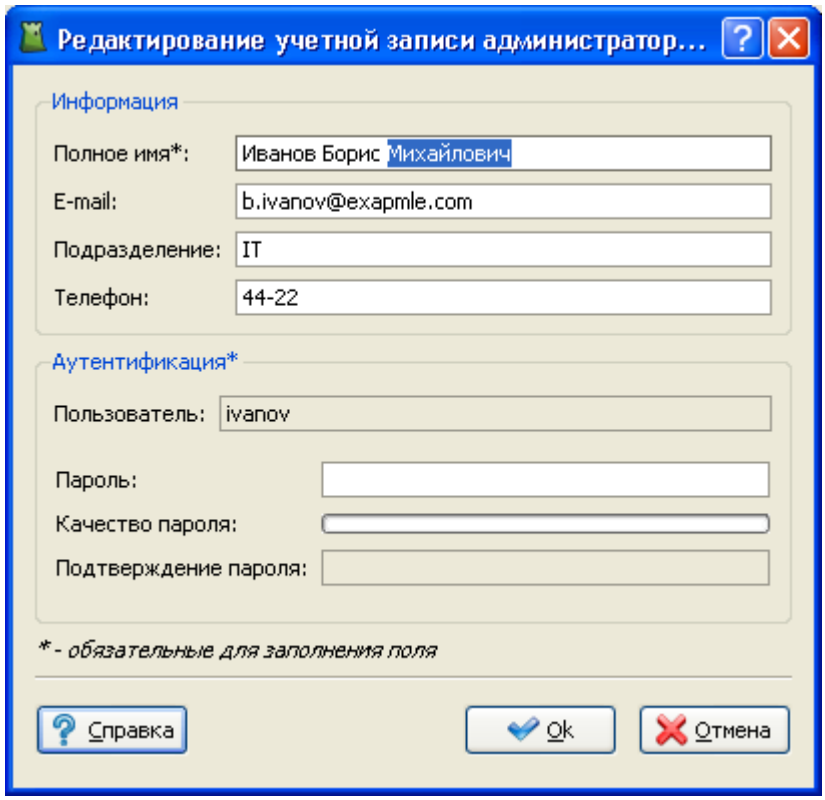

Рисунок 3.9. Редактирование личных данных администратора

3.5. Удаление учетной записи администратора

Для удаления учетной записи администратора, необходимо выделить учетную запись, нажать на кнопку "Удалить" на панели инструментов, или в контекстном меню записи выбрать пункт "Удалить учетную запись администратора".

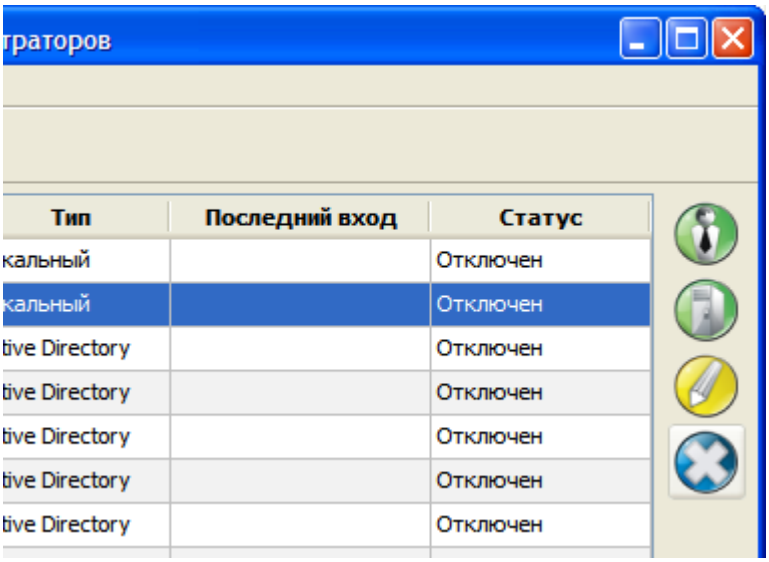

Рисунок 3.10. Удаление учетной записи администратора через панель инструментов

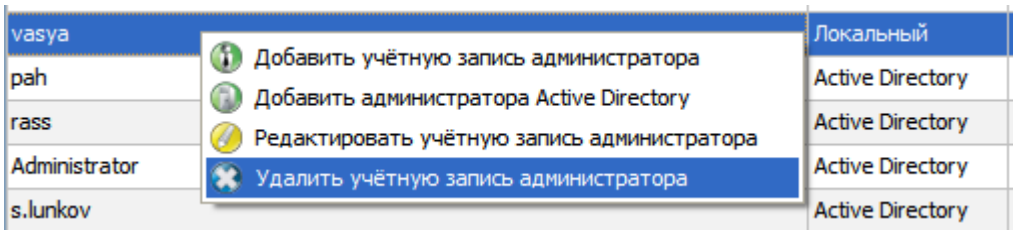

Рисунок 3.11. Удаление учетной записи администратора через контекстное меню

Появится окно с предупреждением о необходимости подтверждения удаления учетной записи администратора.

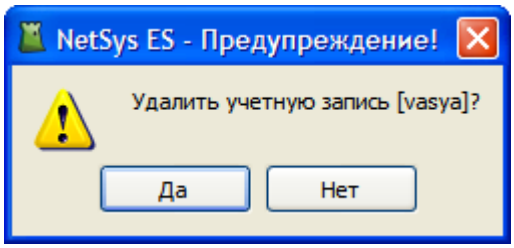

Рисунок 3.12. Подтверждение удаления учетной записи администратора

Глава 4. Группы пользователей

4.1. Назначение

В данном разделе описывается работа с группами пользователей, их создание, редактирование, удаление. Вызов панели для работы с пользователями осуществляется через главное меню "Управление / Группы пользователей". Каждый пользователь системы должен входить в одну из групп, каждой из которой присваиваются отдельные права на создание криптообъектов и набор мастер-сертификатов.

Мастер-сертифкаты служат для возможности восстановления ключевой информации в криптообъектах при утрате сертификатов или паролей пользователей. После восстановления ключевой информации доступ к криптообъекту будет осуществляться стандартными средствами с использованием новых сертификатов и/или паролей.

Важно

Закрытые ключи мастер-сертификатов должны охранятся особенно тщательно. Для защиты ценной информации должен использоваться набор мастер-сертификатов (не менее двух) для обеспечения наличия не менее двух участников в процедуре восстановления ключевой информации.

4.2. Создание группы пользователей

Для создания группы пользователей необходимо нажать на кнопку добавления группы на панели инструментов, или в контекстном меню списка групп выбрать пункт "Добавление группы пользователей".

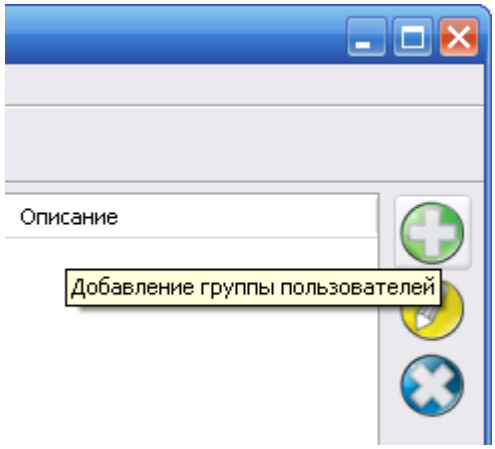

Рисунок 4.1. Добавление группы пользователей через панель инструментов

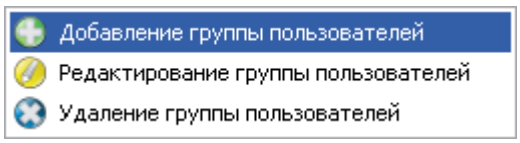

Рисунок 4.2. Добавление группы пользователей через контекстное меню

В появившемся диалоге, во вкладке "Информация", внести имя группы и её описание. Далее требуется задать набор мастер-сертификатов, для чего необходимо нажать на кнопку "Список мастер-сертификатов", которая вызывает диалог "Список сертификатов", в котором добавляются мастер-сертификаты.

Замечание

Закрытые ключи мастер-сертификатов необходимы только при восстановлении ключевой информации в криптообъектах, поэтому при создании группы достаточно наличия сертификатов без закрытых ключей.

После закрытия диалога со списком сертификатов на вкладке "Информация" отобразится количество выбранных сертификатов.

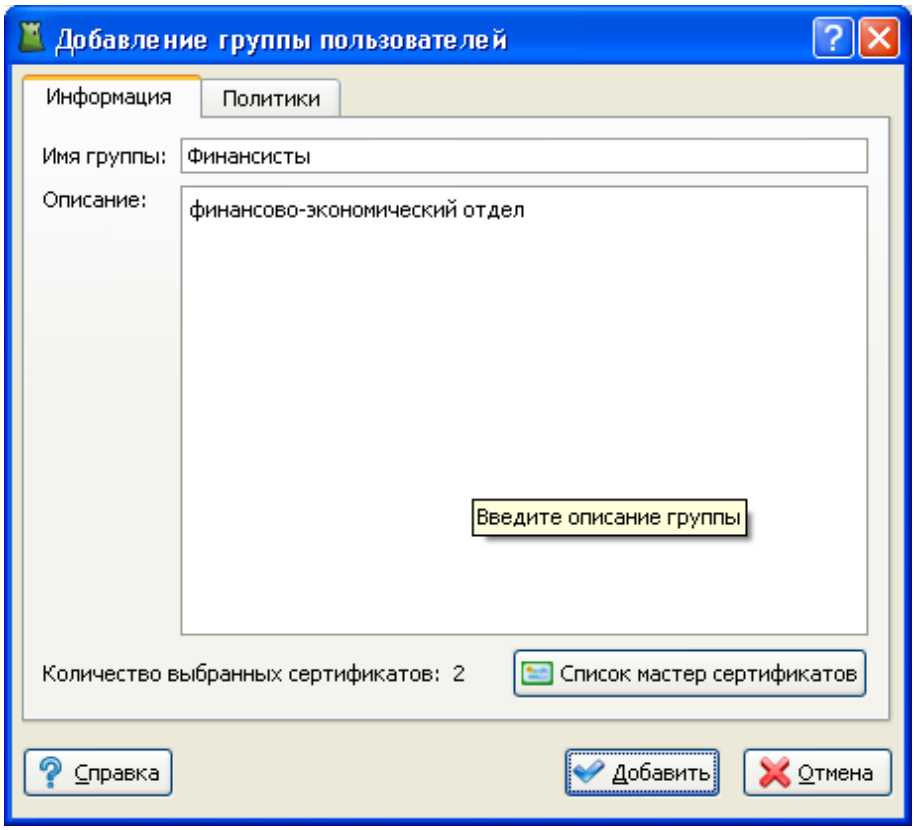

Рисунок 4.3. Внесение данных группы пользователей во вкладке "Информация"

Во вкладке "Политики" (Рисунок 4.4) выставить необходимые ограничения, для данной группы.

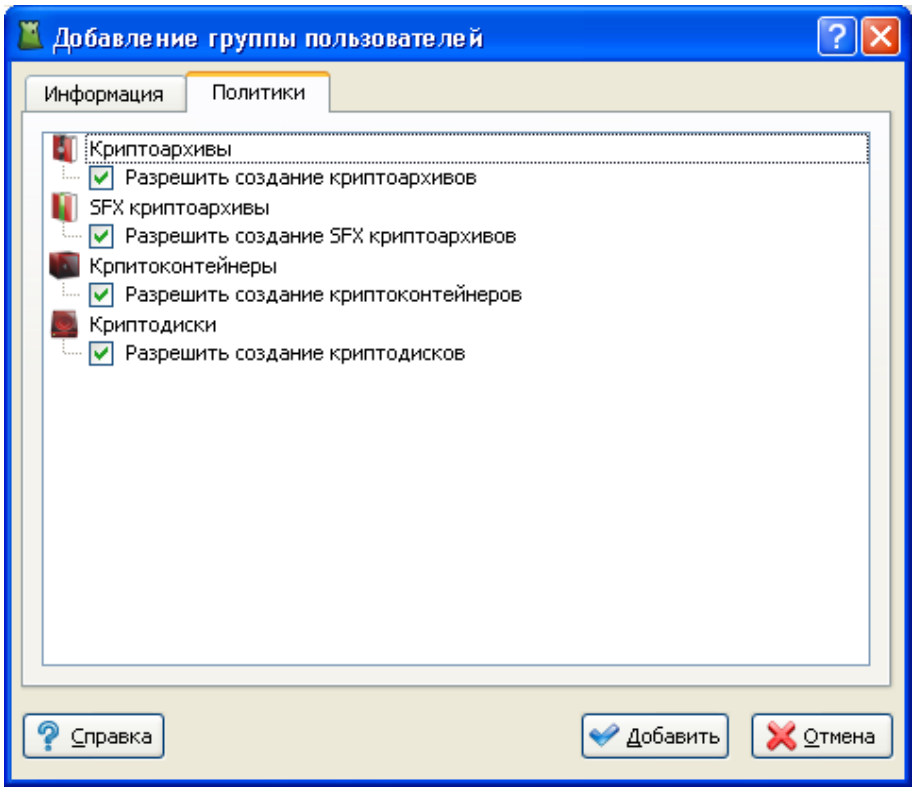

Рисунок 4.4. Выставление политик в группах пользователей

4.3. Редактирование группы пользователей

Для редактирования параметров группы пользователей, необходимо выделить в списке группу, нажать на кнопку "Редактировать" на панели инструментов, или в контекстном меню выбрать пункт "Редактирование группы пользователей".

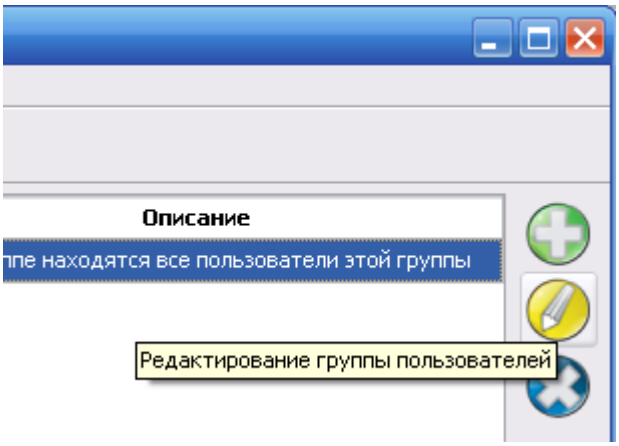

Рисунок 4.5. Редактирование группы пользователей через панель инструментов

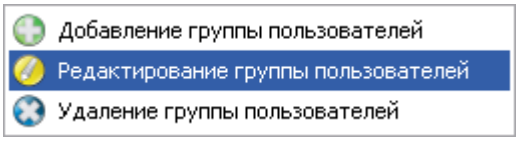

Рисунок 4.6. Редактирование группы пользователей через контекстное меню

В появившемся окне (Рисунок 4.7) изменить необходимые данные, после чего нажать на кнопку "Применить".

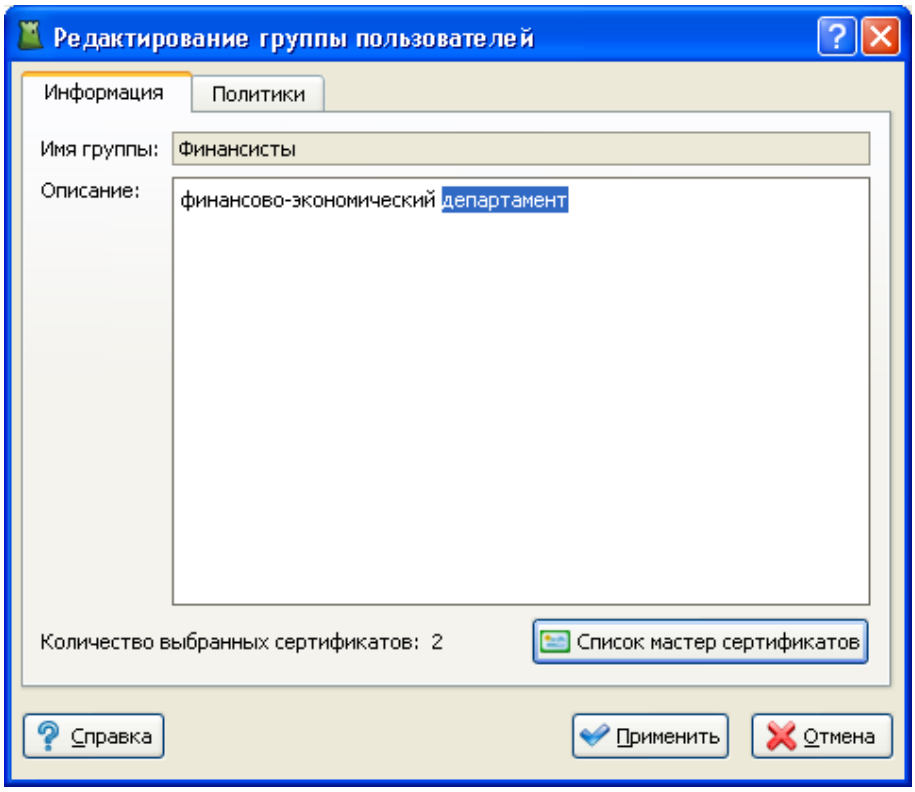

Рисунок 4.7. Редактирование группы пользователей

4.4. Удаление группы пользователей

Для удаления группы пользователей, необходимо выделить удаляемую группу, после чего нажать на кнопку "Удалить" на панели инструментов, или в контекстном меню выбрать пункт "Удаление группы пользователей".

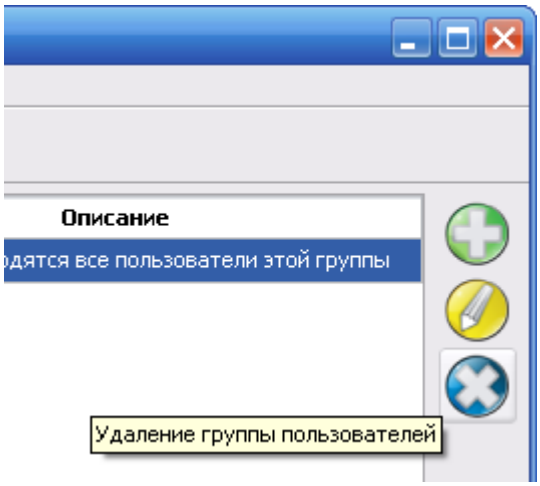

Рисунок 4.8. Удаление группы пользователей через панель инструментов

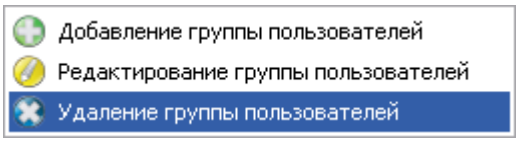

Рисунок 4.9. Удаление группы пользователей через контекстное меню

При удалении группы пользователей, появится окно-предупреждение подтверждения удаления учетной записи администратора. Для удаления группы необходимо нажать кнопку "Да".

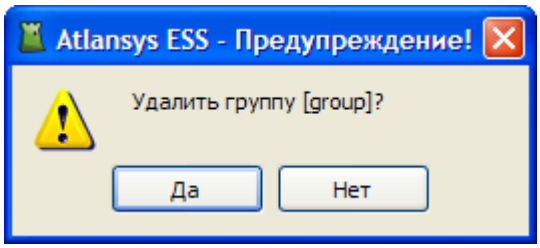

Рисунок 4.10. Подтверждение удаления группы пользователей

Глава 5. Группы компьютеров

5.1. Назначение

В данном разделе описывается работа с группами компьютеров, их создание и удаление. Вызов страницы для работы с пользователями осуществляется через главное меню "Управление / Группы компьютеров". Всем компьютерам в системе присваиваются определенные права на работу с криптообъектами.

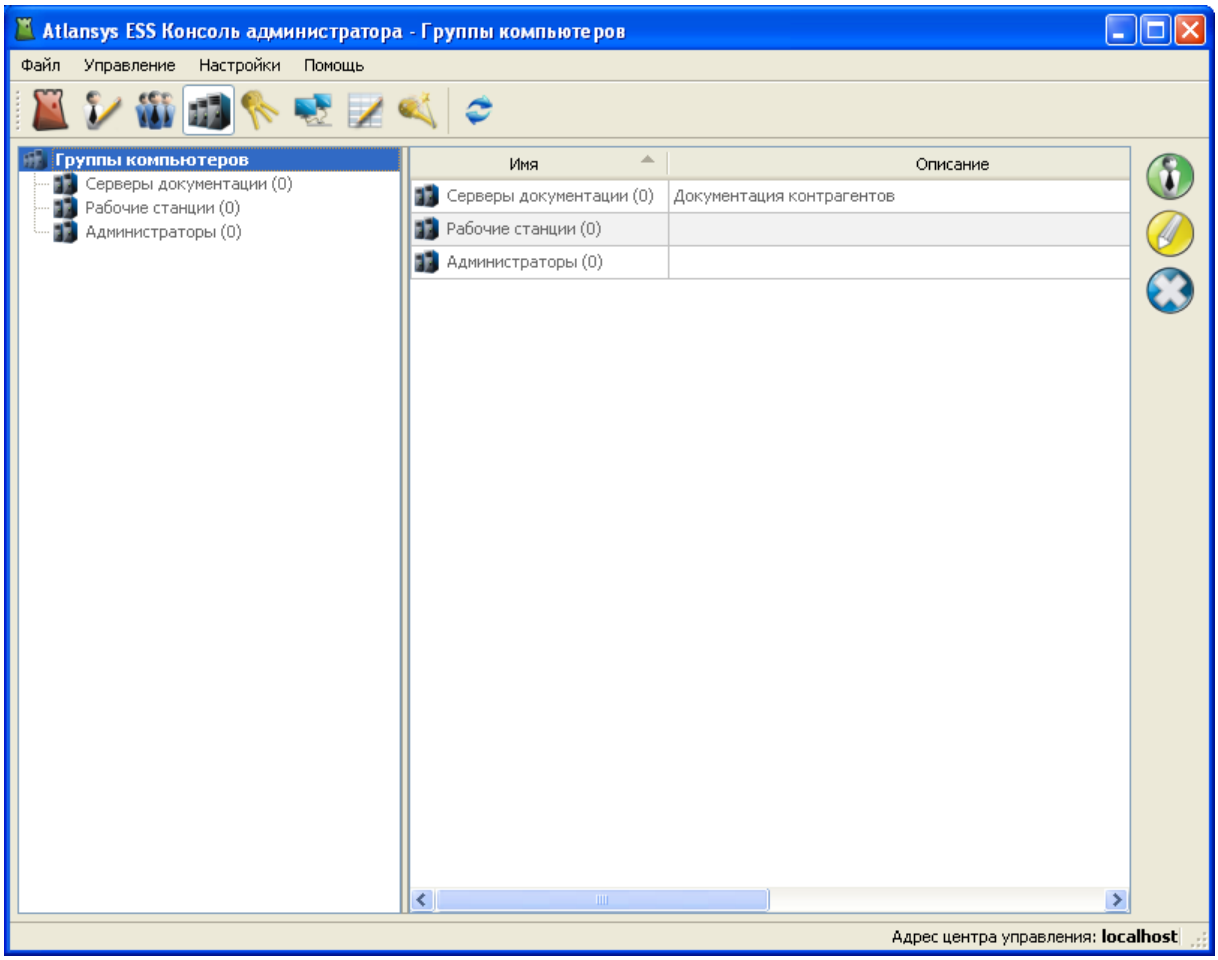

Рисунок 5.1. Страница "Группы компьютеров"

Мастер-сертифкаты служат для возможности восстановления ключевой информации в криптообъектах при утрате сертификатов или паролей пользователей. После восстановления ключевой информации доступ к криптообъекту будет осуществляться стандартными средствами с использованием новых сертификатов и/или паролей.

Важно

Закрытые ключи мастер-сертификатов должны охраняться особенно тщательно. Для защиты ценной информации должен использоваться набор мастер-сертификатов (не менее двух) для обеспечения наличия не менее двух участников в процедуре восстановления ключевой информации.

5.2. Создание группы компьютеров

Для создания группы компьютеров необходимо нажать на кнопку добавления группы на панели инструментов, или в контекстном меню списка серверов выбрать пункт "Добавить группу компьютеров".

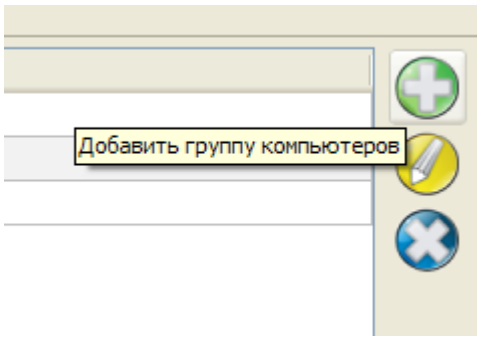

Рисунок 5.2. Добавление группы компьютеров через панель инструментов

В появившемся диалоге ввести имя группы и её описание. Далее требуется задать набор мастер-сертификатов, для чего необходимо нажать на кнопку "Список мастер-сертификатов", которая вызывает диалог "Список сертификатов", где добавляются мастер-сертификаты.

Замечание

Закрытые ключи мастер-сертификатов необходимы только при восстановлении ключевой информации в криптообъектах, поэтому при создании группы достаточно наличия сертификатов без закрытых ключей.

После закрытия диалога со списком сертификатов на вкладке "Информация" отобразится количество выбранных сертификатов.

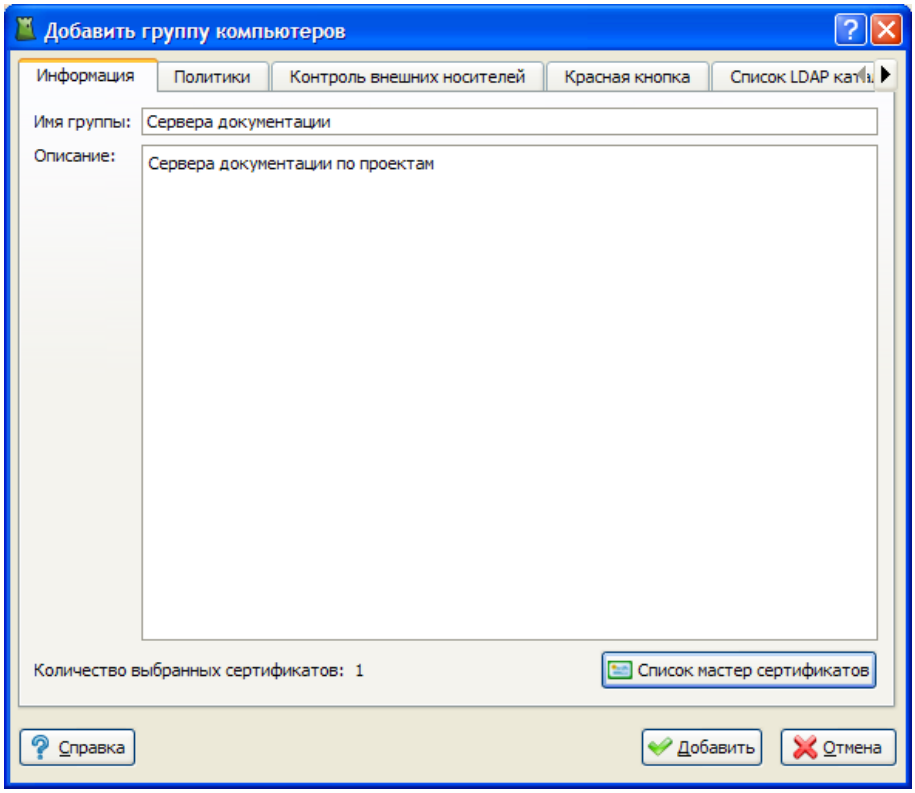

Рисунок 5.3. Внесение данных по группе компьютеров

На вкладке "Политики" можно назначить политики работы с криптообъектами для рабочих станций группы.

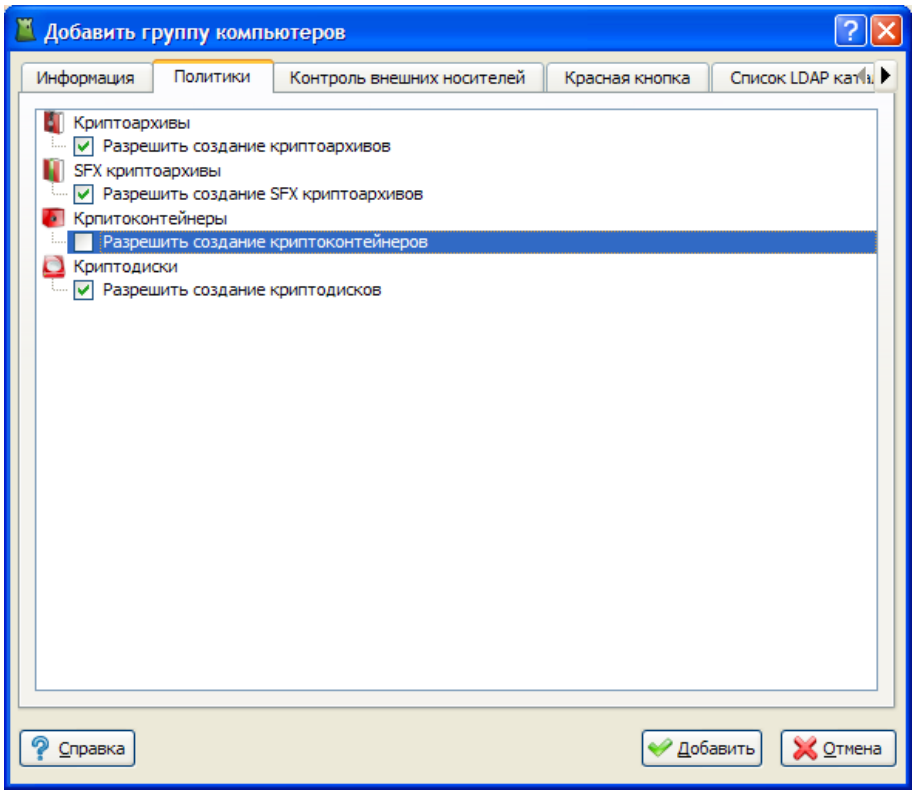

Рисунок 5.4. Настройка политик

На вкладке "Красная кнопка" настраиваются действия, выполняемые при активации Красной кнопки.

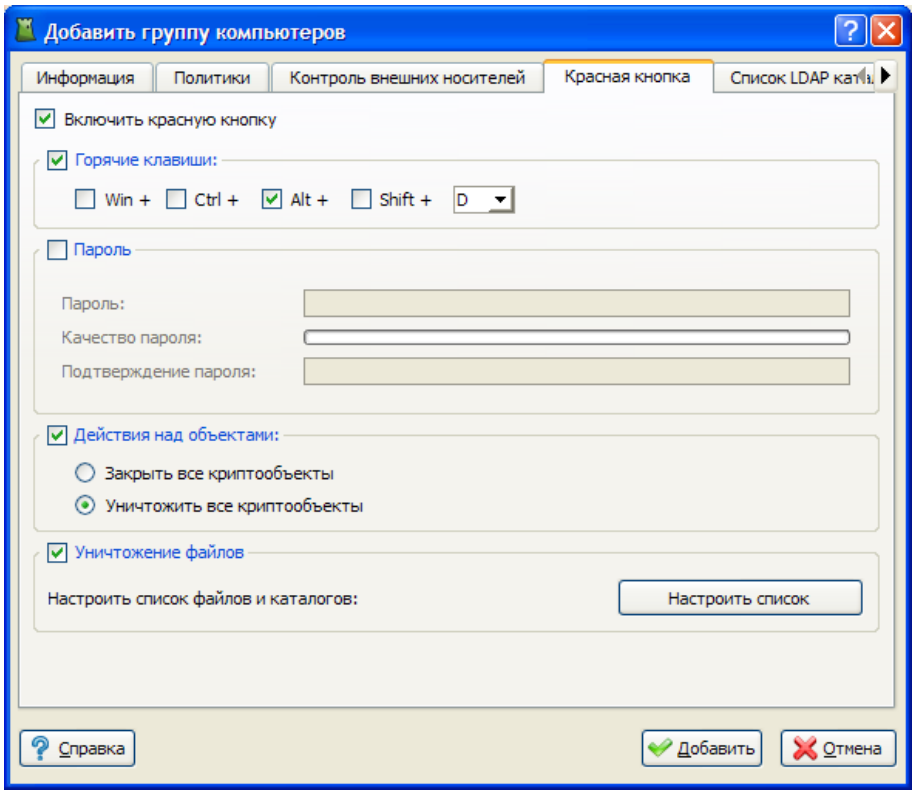

Рисунок 5.5. Настройка Красной кнопки

На вкладке "Список LDAP каталогов" настраивается список каталогов LDAP для поиска сертификатов при создании криптообъектов клиентами данной группы.

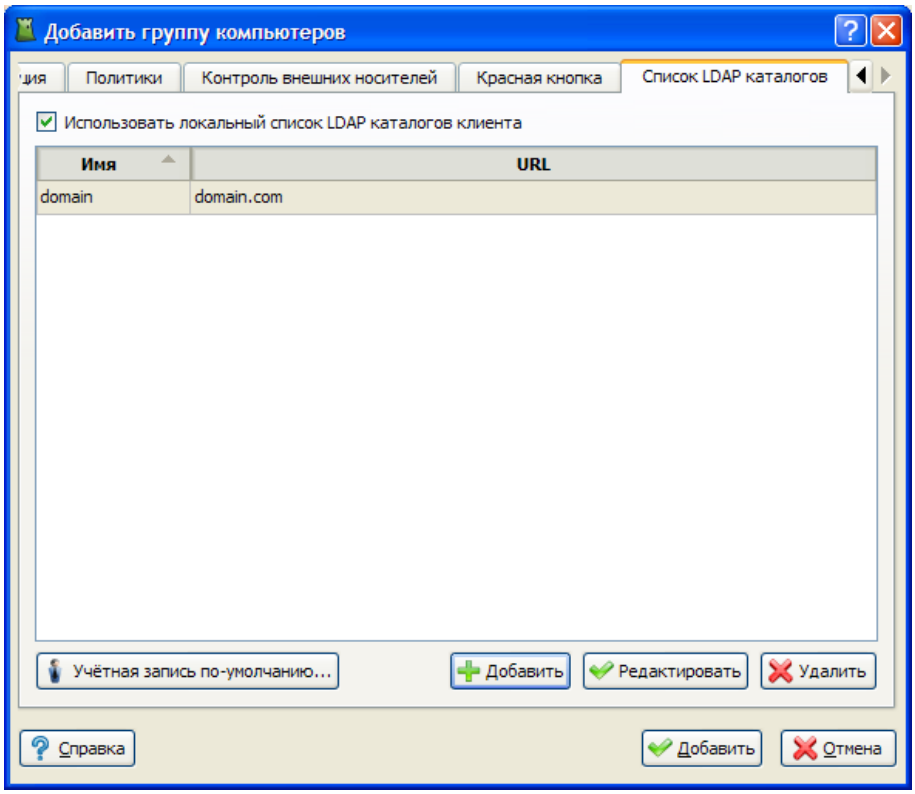

Рисунок 5.6. Настройка списка LDAP каталогов

На вкладке "Контроль внешних носителей" настраиваются политики доступа рабочих станций к съемным USB-устройствам.

Во вкладке "Права доступа по умолчанию" выбирается политика доступа к устройствам для списков устройств, где таковая не задана явным образом.

Во вкладке "Права доступа для списков USB-устройств" настраиваются политики доступа для каждого списка устройств, созданных на странице управления внешними USB-устройствами. Возможны следующие варианты прав доступа:

- DF - использовать значение по умолчанию;
- DN - запретить все устройства;
- RO - разрешить устройства только для чтения;
- RW - разрешить полный доступ к устройствам.

Первая строка в таблице списков устройств - настройка прав доступа для криптофлэш дисков, она присутствует всегда, даже когда не создано ни одного списка устройств.

Чекбокс "Логировать события" включает механизм логирования событий работы с USB-устройствами на рабочих станциях.

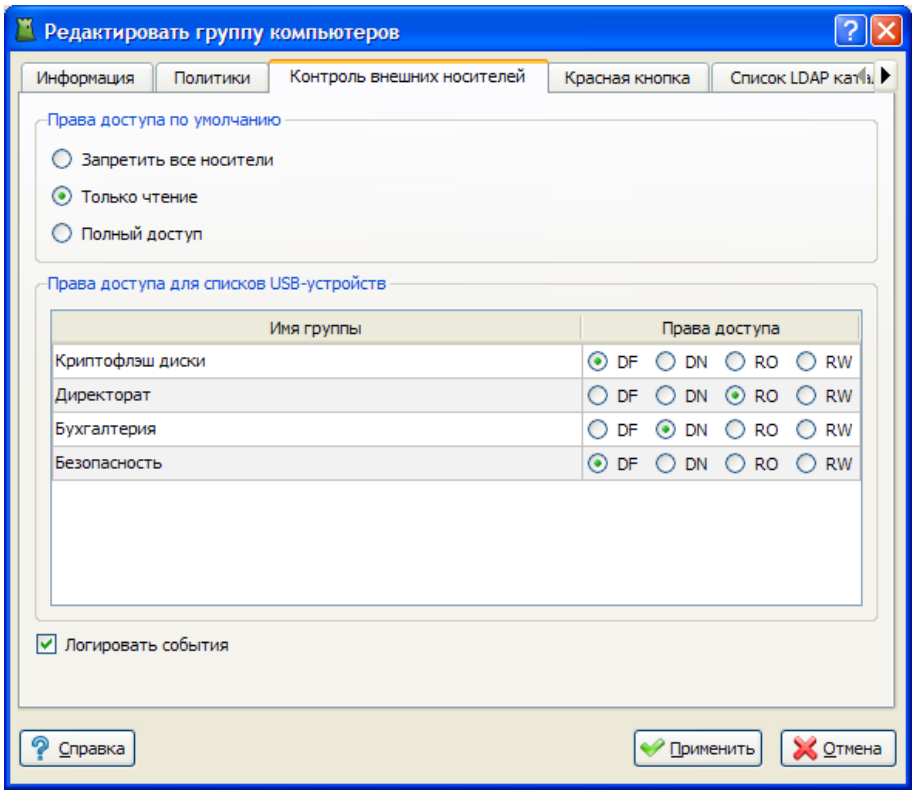

Рисунок 5.7. Настройка контроля внешних носителей

5.3. Редактирование группы компьютеров

Для редактирования параметров группы компьютеров необходимо выделить в списке группу, нажать на кнопку "Редактировать" на панели инструментов, или в контекстном меню выбрать пункт "Редактировать группу компьютеров".

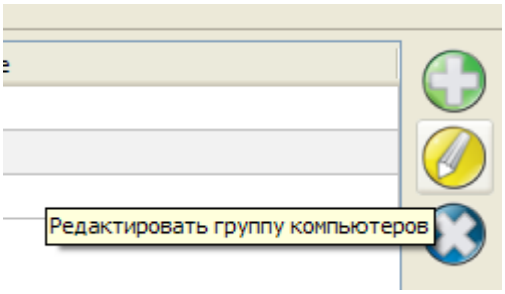

Рисунок 5.8. Редактирование группы компьютеров через панель инструментов

В появившемся окне изменить необходимые данные, после чего нажать кнопку "Применить".

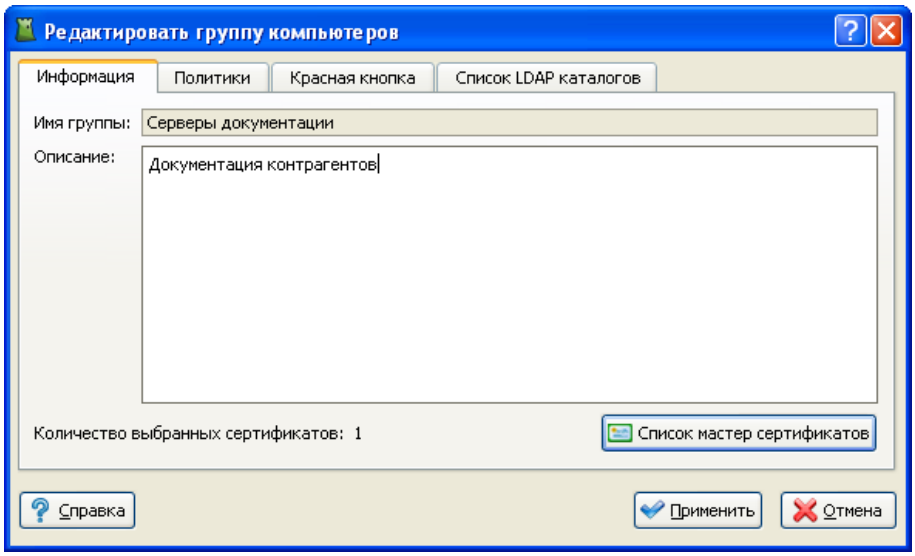

Рисунок 5.9. Редактирование группы компьютеров

Настройки Красной кнопки и LDAP-каталогов задаются также, как при добавлении группы компьютеров.

5.4. Удаление группы компьютеров

Для удаления группы компьютеров необходимо выделить удаляемую группу, после чего нажать кнопку "Удалить" на панели инструментов или в контекстном меню выбрать пункт "Удалить группу компьютеров".

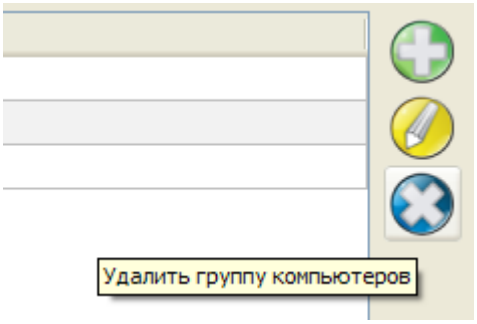

Рисунок 5.10. Удаление группы компьютеров через панель инструментов

При удалении группы компьютеров появится окно-предупреждение подтверждения удаления. Для удаления группы необходимо нажать кнопку "Да".

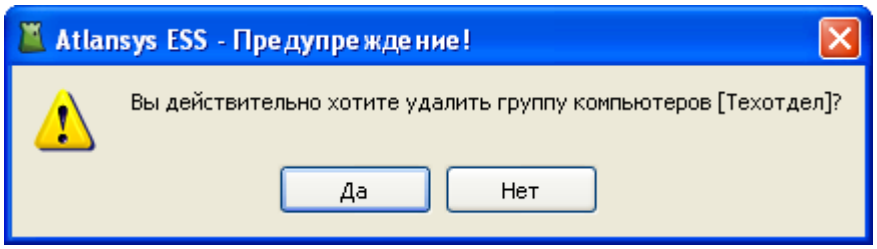

Рисунок 5.11. Подтверждение удаления группы компьютеров

Глава 6. Управление USB-устройствами

6.1. Назначение

В данном разделе описывается работа с внешними USB-устройствами: добавление, удаление устройств, создание списков устройств. Вызов страницы для работы с пользователями осуществляется через главное меню "Управление / USB-устройства".

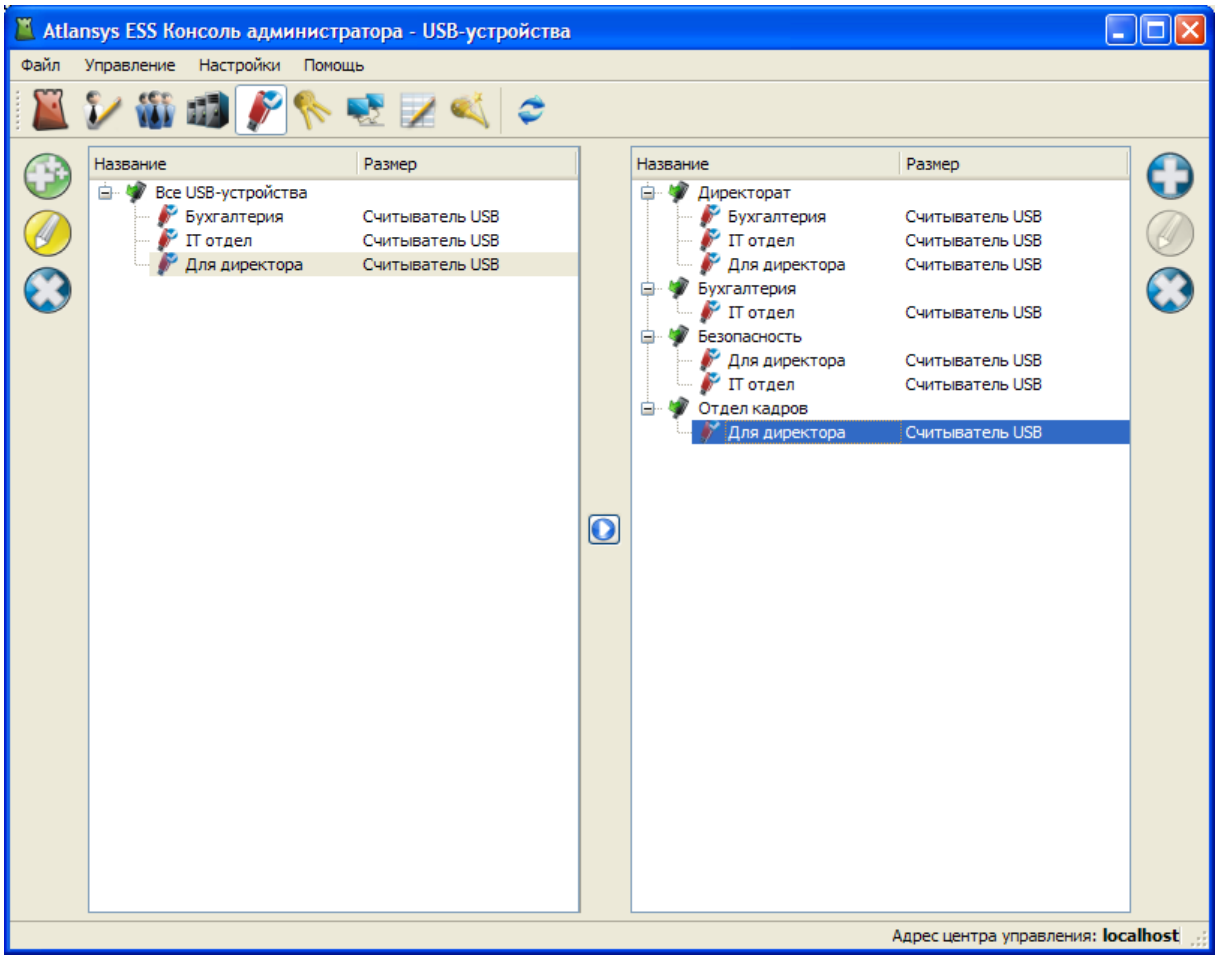

Рисунок 6.1. Страница "USB-устройства"

Механизм управления USB-устройствами предназначен для контроля доступа к ним на рабочих станциях пользователей. На данной странице осуществляется добавление устройств, используемых на рабочих станциях, в списки доступа, которым в дальнейшем можно назначить определенные политики доступа.

Принцип работы заключается в следующем: сначала создается общий список USB-устройств (окно слева), после чего устройства из этого списка добавляются в списки доступа, управление которыми происходит в окне справа.

6.2. Добавление USB-устройств в общий список

Диалог добавления USB-устройств в общий список (левое окно) вызывается кнопкой в левой панели инструментов у общего списка устройств.

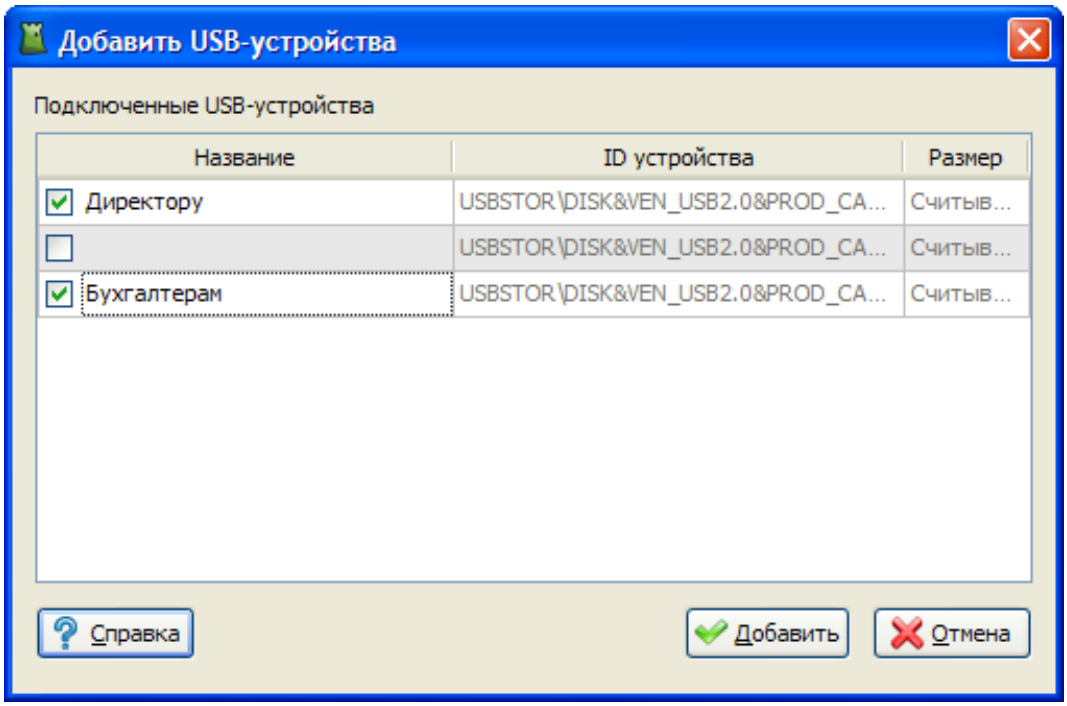

Рисунок 6.2. Диалог добавления USB-устройств

В диалоге отображаются все подключенные на данный момент к компьютеру USB-устройства, причем, если устройство отключить, а вместо него подключить другое, то первое не пропадет из списка, но в списке автоматически появится новое подключенное устройство. Таким образом, за один раз можно получить список всех необходимых устройств для добавления.

Те устройства, которые требуется добавить в общий список, следует отметить в соответствующих чекбоксах и указать название, которое будет в дальнейшем отображаться в общем списке, для удобства идентификации устройства. Редактирование названия осуществляется по двойному щелчку мышью на ячейке таблицы.

После нажатия на кнопку "Добавить", выбранные устройства помещаются в общий список в окне слева. Однако, если устройство с заданным идентификатором уже присутствует в списке, оно добавлено в него не будет.

После добавления устройства можно удалять (при этом они удалятся из всех списков, куда были включены) и редактировать - по кнопке "Редактировать" или двойному щелчку мышью на пункте.

6.3. Работа со списками USB-устройств

Диалог добавления списка USB-устройств (правое окно) вызывается кнопкой в правой панели инструментов у дерева списков. Там задается только его название.

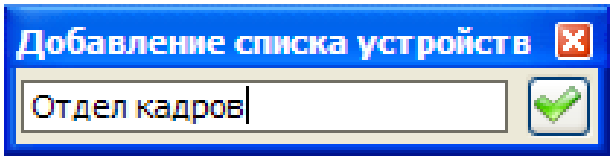

Рисунок 6.3. Диалог добавления списка USB-устройств

После создания списка, в него можно добавить USB-устройства из общего списка устройств (левое окно). Для этого используется кнопка добавления, расположенная посередине между окнами. Выделенные элементы в общем списке копируются к выделенному списку устройств в дереве справа. Одно устройство

одновременно может входить в несколько списков; в случае конфликтных ситуаций будет использоваться наиболее безопасная политика работы с устройством.

Чтобы отредактировать список устройств, следует нажать кнопку "Редактировать" в панели инструментов справа, либо выбрать соответствующий пункт в контекстном меню дерева.

Удаление списка или устройства из списка осуществляется нажатием на кнопку "Удалить" в панели инструментов справа. При удалении списка, также удаляются и все устройства из него. При удалении устройства, удаляется только запись об этом устройстве из списка, а само устройство остается в других списках и в общем списке устройств.

В дальнейшем, для каждого списка устройств можно назначить определенные политики доступа к устройствам для каждой группы копьютеров.

Глава 7. Хранилище ключей

7.1. Назначение

В хранилище ключей отображается список всех сохранённых на Центре Управления ключей. Ключи на Центр Управления передаются при создании криптодисков и могут использоваться при восстановлении ключевой информации на криптодисках. Переход на панель хранилища ключей осуществлятся через главное меню "Управление / Хранилище ключей".

7.2. Описание интерфейса

В списке хранилища ключей отображаются:

- "Пользователь" - имя пользователя, создавшего криптодиск.
- "Домен" - имя домена, в который входит пользователь.
- "Дата создания" - дата и время создания криптодиска.
- "GUID" - идентификатор криптодиска.
- "Описание" - описание криптодиска, которое пользователь вводил при его создании.

Для быстрого поиска необходимого ключа можно воспользоваться фильтром, в котором задаются поля фильтрации списка, после нажатия на кнопку "Применить" отобразится сокращенный список ключей в соответствии с заданными критериями фильтрации списка.

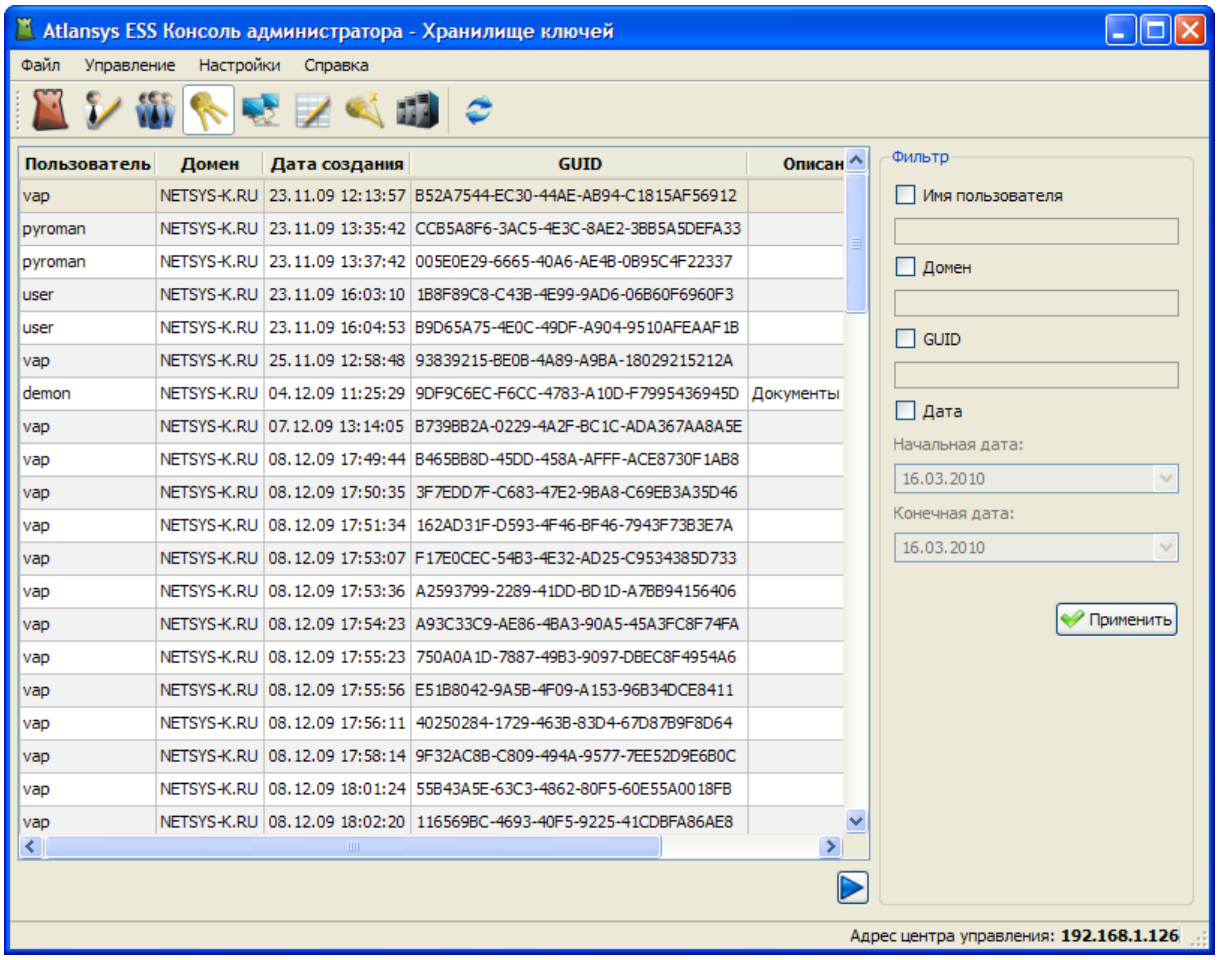

Рисунок 7.1. Хранилище ключей

Глава 8. Удалённое управление

8.1. Назначение

В данном разделе описывается удаленное управление криптообъектами на рабочих станциях пользователей через Консоль Администратора. Переход на панель удалённого управления осуществлятся через главное меню "Управление / Удалённое управление".

8.2. Описание интерфейса

С левой стороны панели отображается дерево групп пользователей и групп компьютеров. При открытии конкретной группы отображается список пользователей или компьютеров этой группы, подключеных в данный момент к Центру Управления. При выборе пользователя отображаются рабочие станции, на которых пользователь зарегистрирован. После выбора рабочей станции на правой стороне панели отображаются криптообъекты этого пользователя на данной рабочей станции. При выборе компьютера отображаются криптообъекты данного компьютера.

В списке криптообъектов отображаются:

- "Объект" - буква диска и метка криптообъекта.
- "Состояние" - текущее состояние криптообъекта: закрыт, открыт, недоступен.
- "Размещение" - путь к файлу криптоконтейнера или к устройству криптодиска.
- "Размер" - размер криптообъекта.
- "Действия" - кнопки действий, которые можно совершить над криптообъектом.

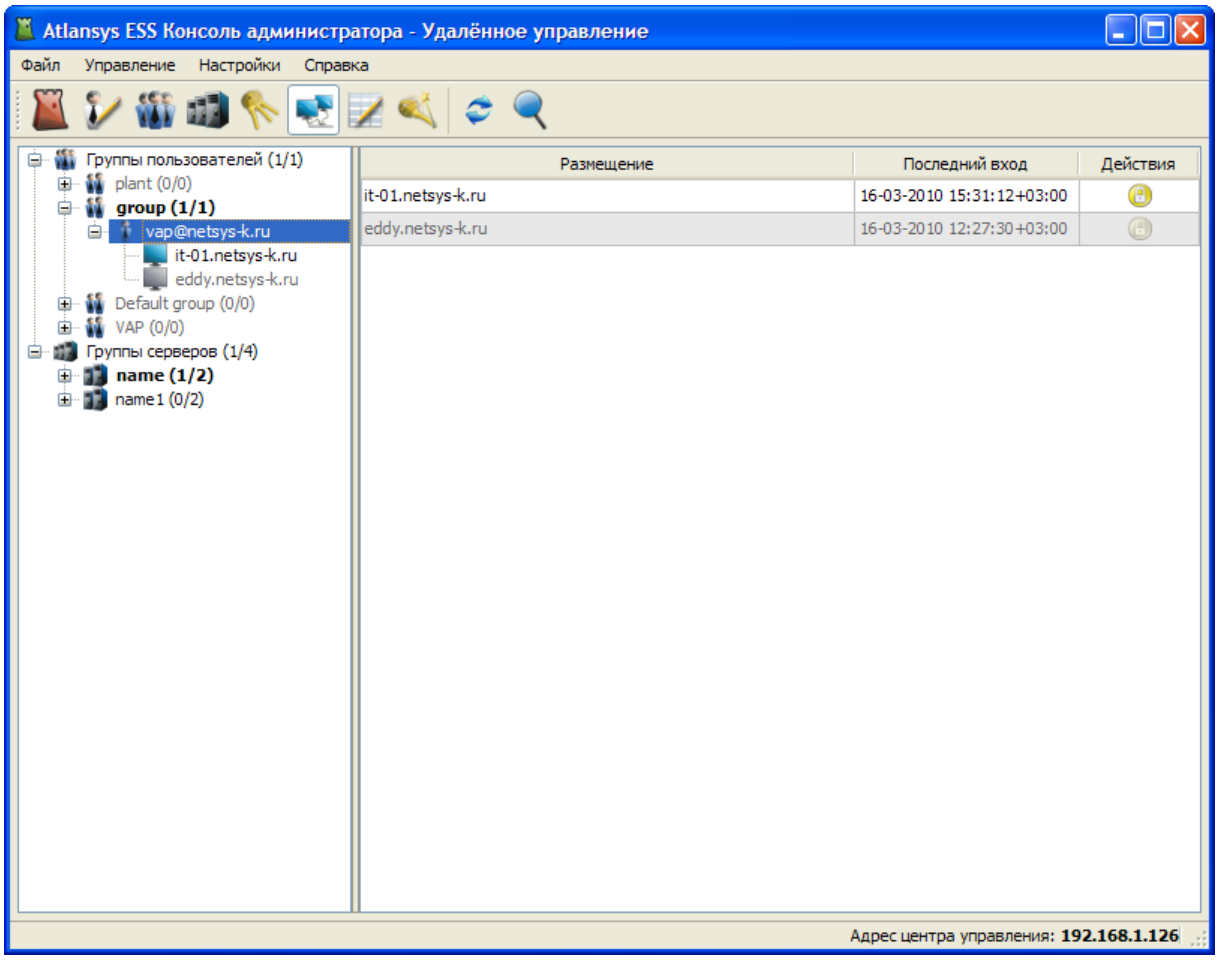

Рисунок 8.1. Удалённое управление

Для оперативного закрытия криптообъекта необходимо нажать на кнопку "Закрыть объект" в столбце "Действия".

Для удаления криптообъекта следует нажать кнопку "Удалить". Удаление возможно только в случае, если криптообъект предварительно был закрыт.

Подробную информацию о криптообъекте можно просмотреть после двойного щелчка на криптообъекте, либо через контекстное меню криптообъекта "Показать информацию о криптообъекте", либо нажав кнопку "Информация о криптообъекте".

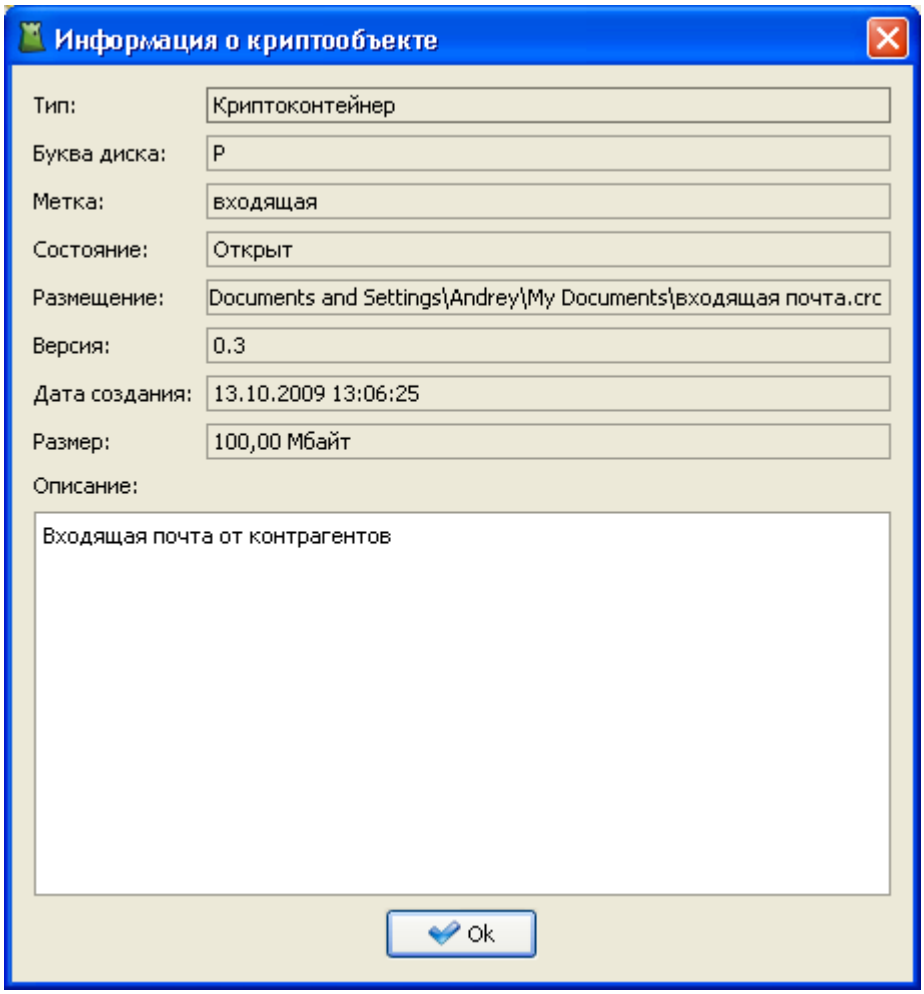

Рисунок 8.2. Информация о криптообъекте

Глава 9. Журнал событий

9.1. Назначение

Журнал событий служит для отоброжения лог-сообщений системы. Переход к журналу регистрации событий осуществляется через главное меню "Управление / Журнал регистрации событий".

9.2. Интерфейс

Окно просмотра журнала состоит из сиска сообщений, фильтра и кнопок навигации по журналу. Список сообщений является гибко настраиваемым и может отображать столбцы:

- "Дата/время" - дата и время возникновения события. Время отображается как локальное для рабочей станции (сервере), на которой возникло событие.
- "ID" - идентификатор события, однозначно определяющий тип и место возникновения события в системе.
- "Пользователь" - идентификатор пользователя, сгенерировавший событие. Для системных событий используется имя SYSTEM.
- "Хост" - адрес рабочей станции (сервера), на котором произошло событие.
- "Уровень" - уровень важности события.
- "Категория" - категория источника событий: система, администратор, пользователь.
- "Модуль" - подсистема, сгенерировшая событие.
- "Текст" - непосредственно сообщение.

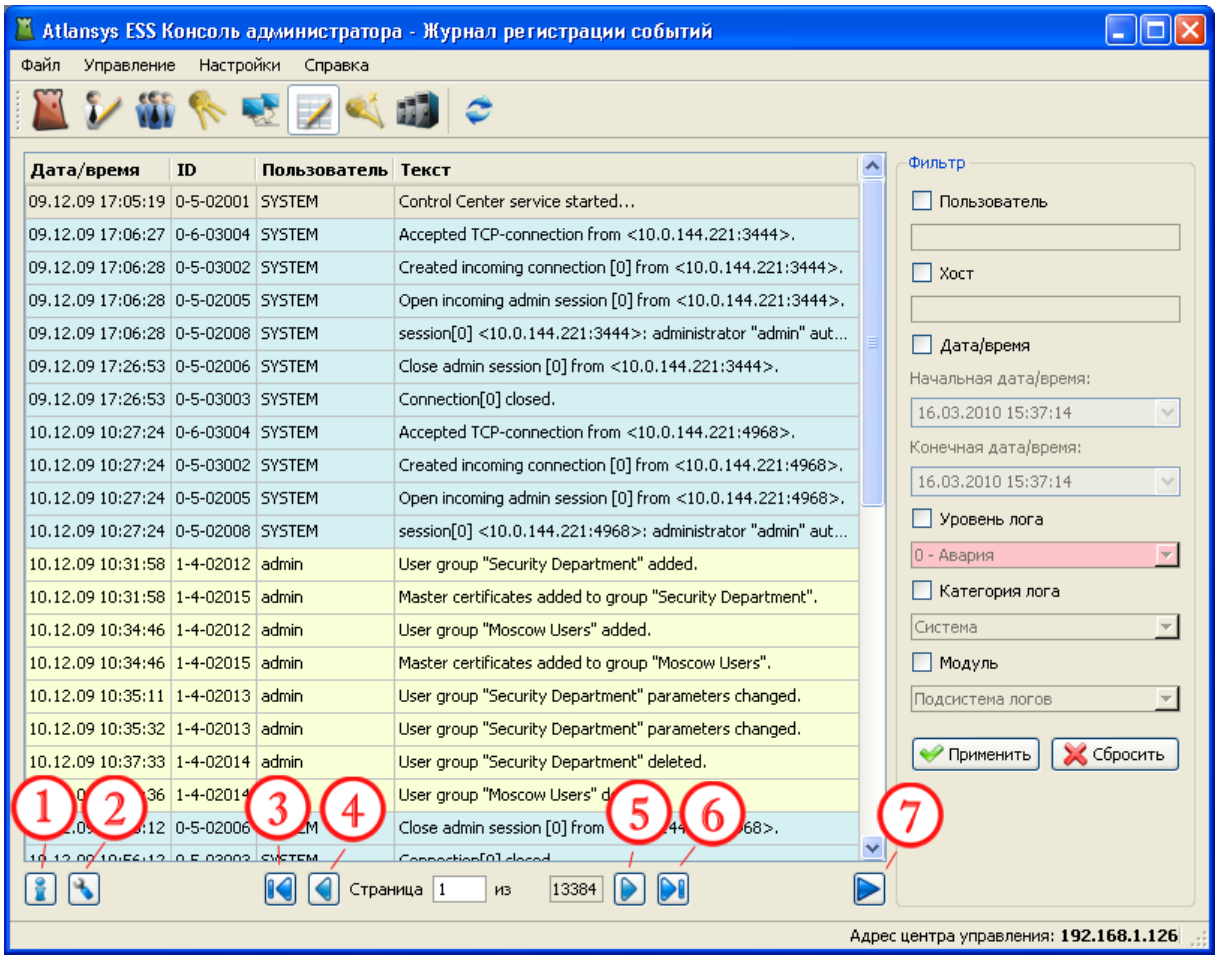

Рисунок 9.1. Журнал событий

Элементы управления и навигации:

1. Информация по выбранному сообщению.
2. Настройки журнала регистрации событий.
3. Перейти к первой странице.
4. Перейти к предыдущей странице.
5. Перейти к следующей странице.
6. Перейти к последней странице.
7. Показать/скрыть фильтр сообщений.

В диалоге информации по лог-сообщению отображается вся информация сообщения.

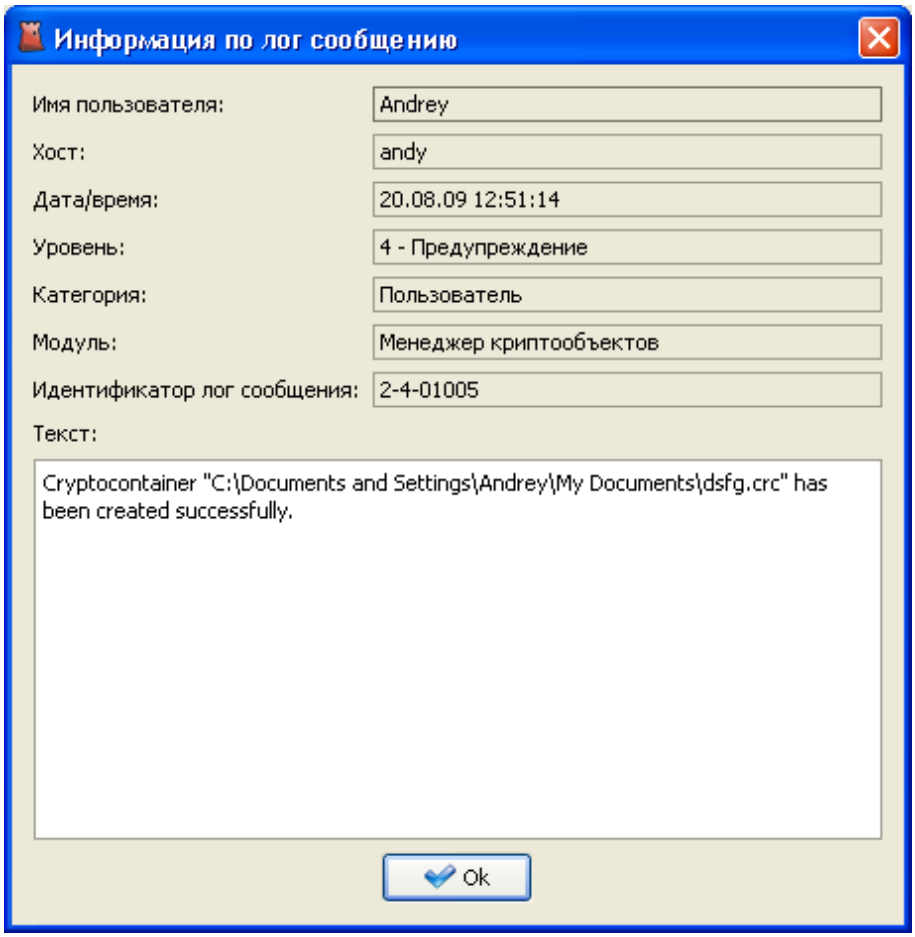

Рисунок 9.2. Информация по лог сообщению

В диалоге настройки журнала регистрации событий выбираются отображаемые столбцы списка и их порядок. Так же можно задать порядок отображения сообщений и выбрать цветовую гамму подсветки сообщений в журнале.

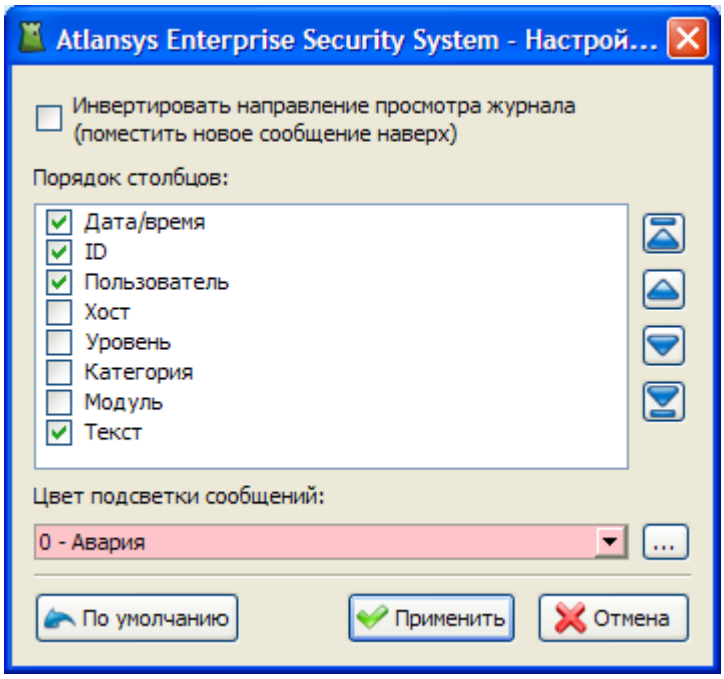

Рисунок 9.3. Настройки журнала регистрации событий

Для быстрого поиска необходимых сообщений в журнале реализована гибкая система фильтрации по таким критериям, как: имя пользователя, хост, дата, уровень лога, категория лога, модуль.

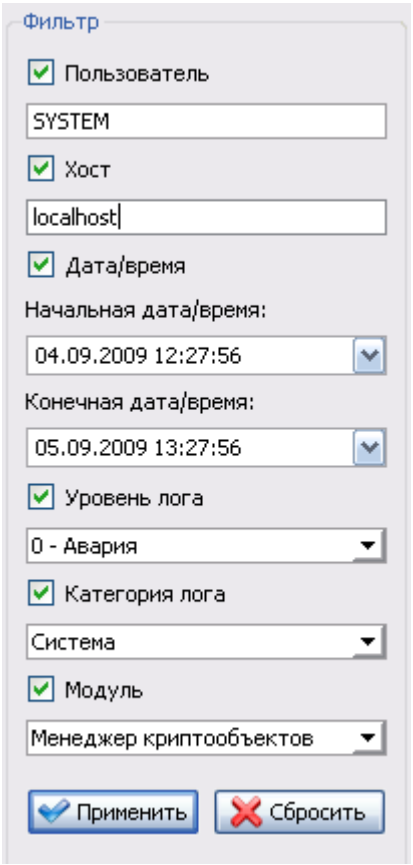

Рисунок 9.4. Фильтр журнала событий

После настройки фильтра необходимо нажать на кнопку "Применить", после чего отобразится отфильтрованный список сообщений.

Глава 10. Восстановление ключей

10.1. Введение

Процедура восстановления ключей применяется в случае невозможности открытия криптообъекта, в случае утраты пароля, либо сертификата с закрытым ключом. Также с помощью данной процедуры можно изменить схему защиты криптообъекта, заменить пароль, либо пользовательский сертификат.

Существует два способа получения ключевой информации для ее последующего восстановления:

1. Извлечение ключевой информации непосредственно из криптообъекта. Данный способ применим ко всем типам криптообъектов.

2. Извлечение ключевой информации из базы ключей, хранимой на Центре Управления. Данный способ применим только для восстановления ключей криптодисков на управляемых клиентах.

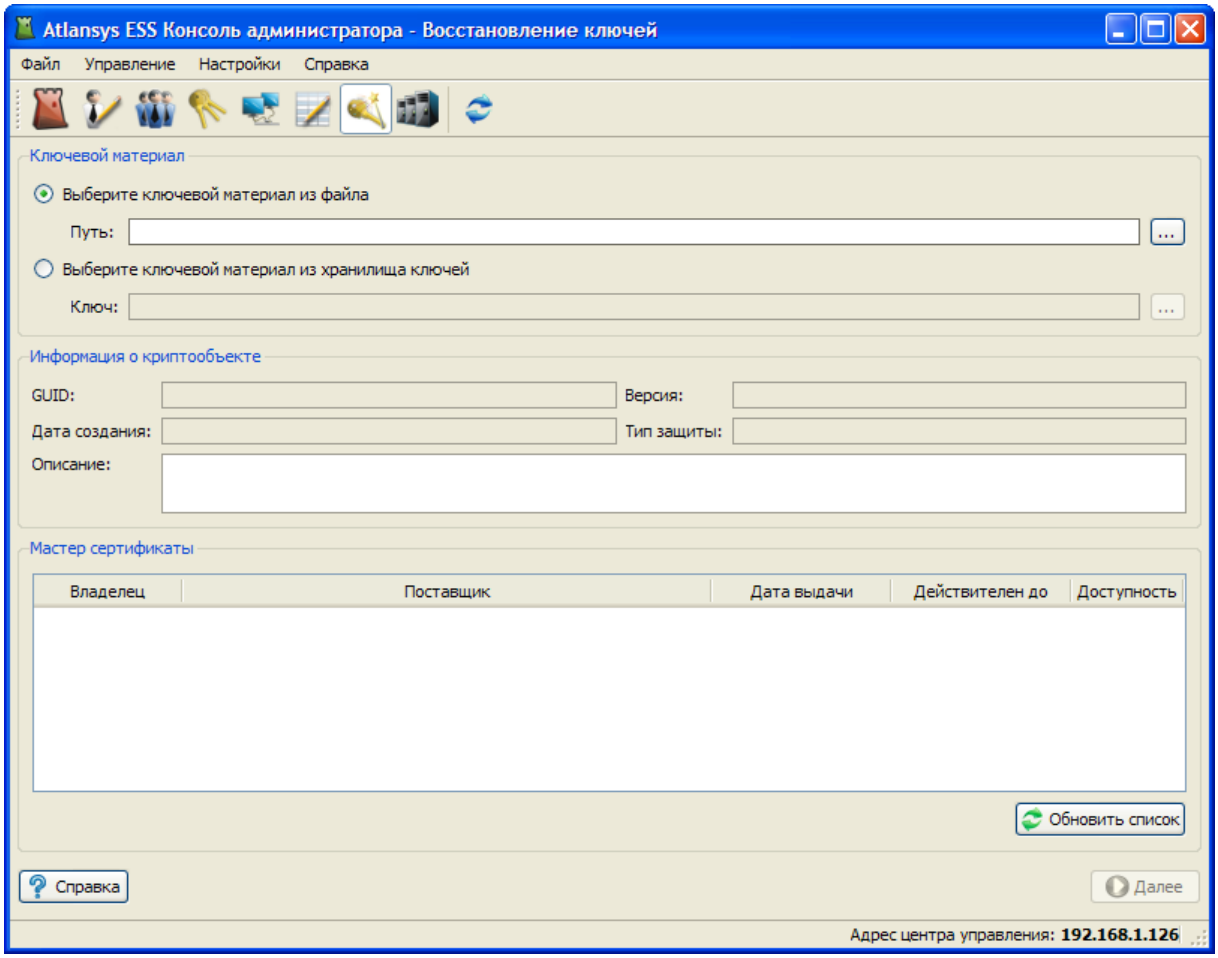

Рисунок 10.1. Страница восстановления ключей

10.2. Восстановление ключа с извлечением информации из криптообъекта

Процедура восстановления состоит из 3-х этапов.

10.2.1. Извлечение ключевой информации из криптообъекта

Извлечение ключевой информации из криптообъекта производится с помощью утилиты **key-recovery**. Она запускается отдельно из каталога инсталляции Консоли Администратора, либо через главное меню "Файл / Утилита восстановления ключей".

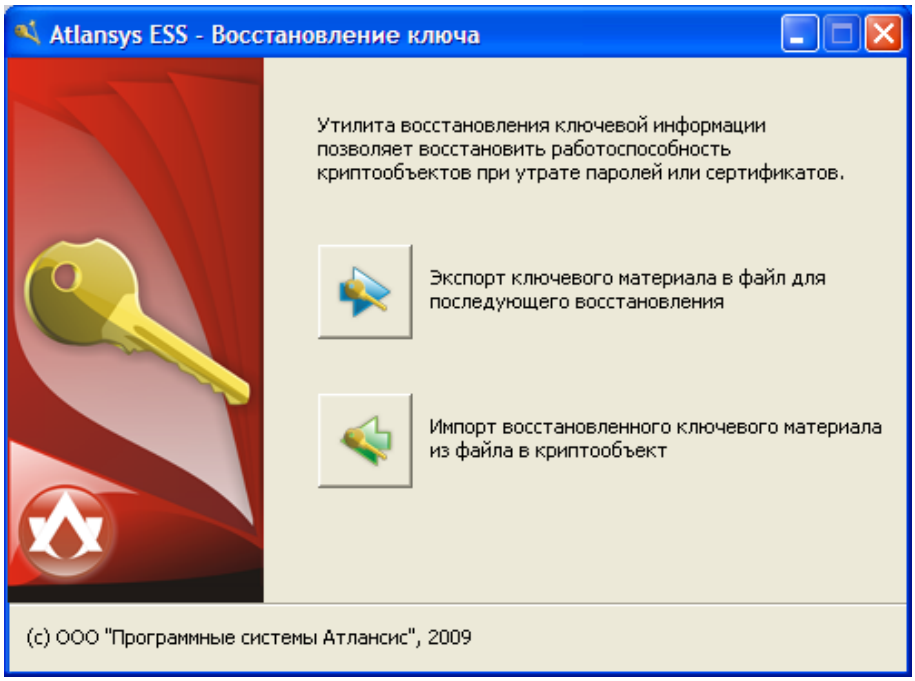

Рисунок 10.2. Утилита восстановления ключей

Для извлечения ключевой информации из криптообъекта необходимо нажать на кнопку экспорта ключевого материала в файл. Затем необходимо выбрать тип криптообъекта, для которого необходимо восстановить ключ и нажать на кнопку "Далее".

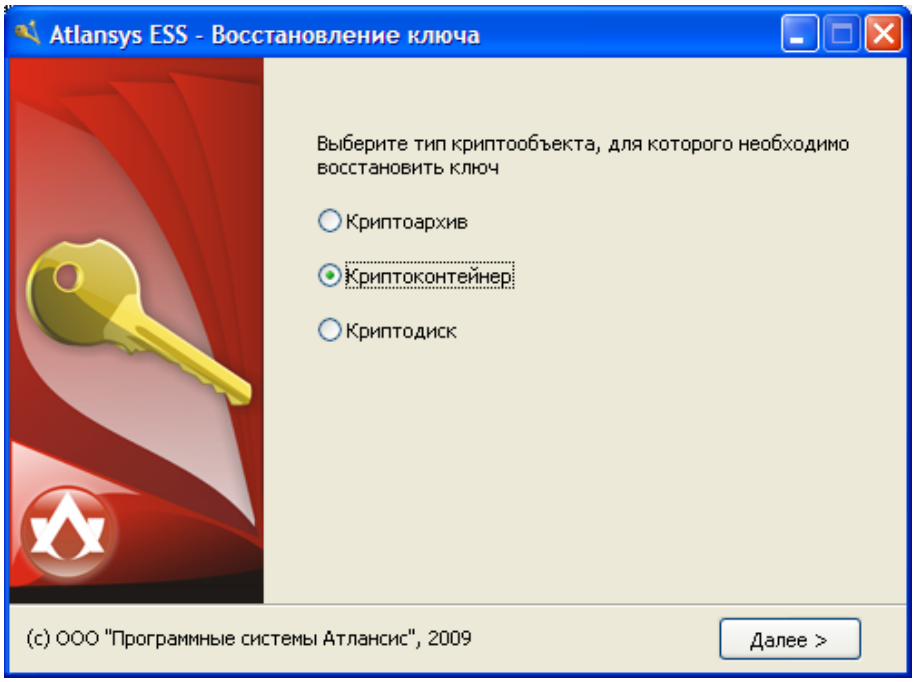

Рисунок 10.3. Утилита восстановления ключей - выбор типа крпитообъекта

После этого необходимо выбрать сам криптообъект. Для криптоархивов, самораспаковывающихся криптоархивов и криптоконтейнеров откроется стандартный диалог выбора файла. Для криптодиска откроется окно выбора криптодиска, в котором будут оторбажены все доступные в системе криптодиски.

Замечание

При восстановлении ключа для криптоконтейнера или криптодиска они должны быть закрыты, в противном случае приложение выдаст ошибку.

После выбора соответствующего криптообъекта появится окно с его описанием.

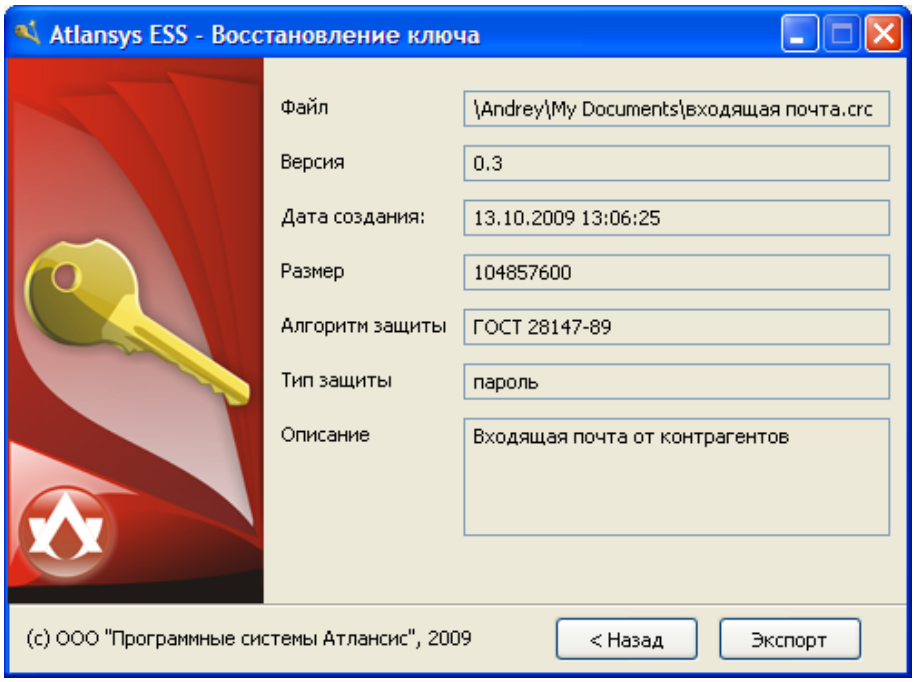

Рисунок 10.4. Утилита восстановления ключей - описание криптообъекта

Для завершения первого этапа восстановления ключа необходимо нажать на кнопку "Экспорт". В результате откроется стандартное диалоговое окно для сохранения ключевого материала в файл. В этом окне необходимо ввести имя файла ключевого материала и нажать на кнопку "Сохранить". После успешного сохранения ключевого материала в файл появится сообщение об успешном экспорте криптозаголовка.

10.2.2. Изменение схемы защиты ключевой информации криптообъекта.

В Консоли Администратора в главном меню необходимо выбрать пункт "Управление / Восстановление ключей". Далее выбрать пункт "Выберите ключевой материал из файла" и нажать на кнопку "…". В появившемся окне выбора файла с ключевым материалом необходимо выбрать соответствующий файл ключевого материала, созданный на первом этапе. После выбора файла с ключевым материалом на странице появится описание криптообъекта, для которого необходимо восстановить ключ, а в нижней части окна появится список мастер-сертификатов, которыми защищен ключевой материал.

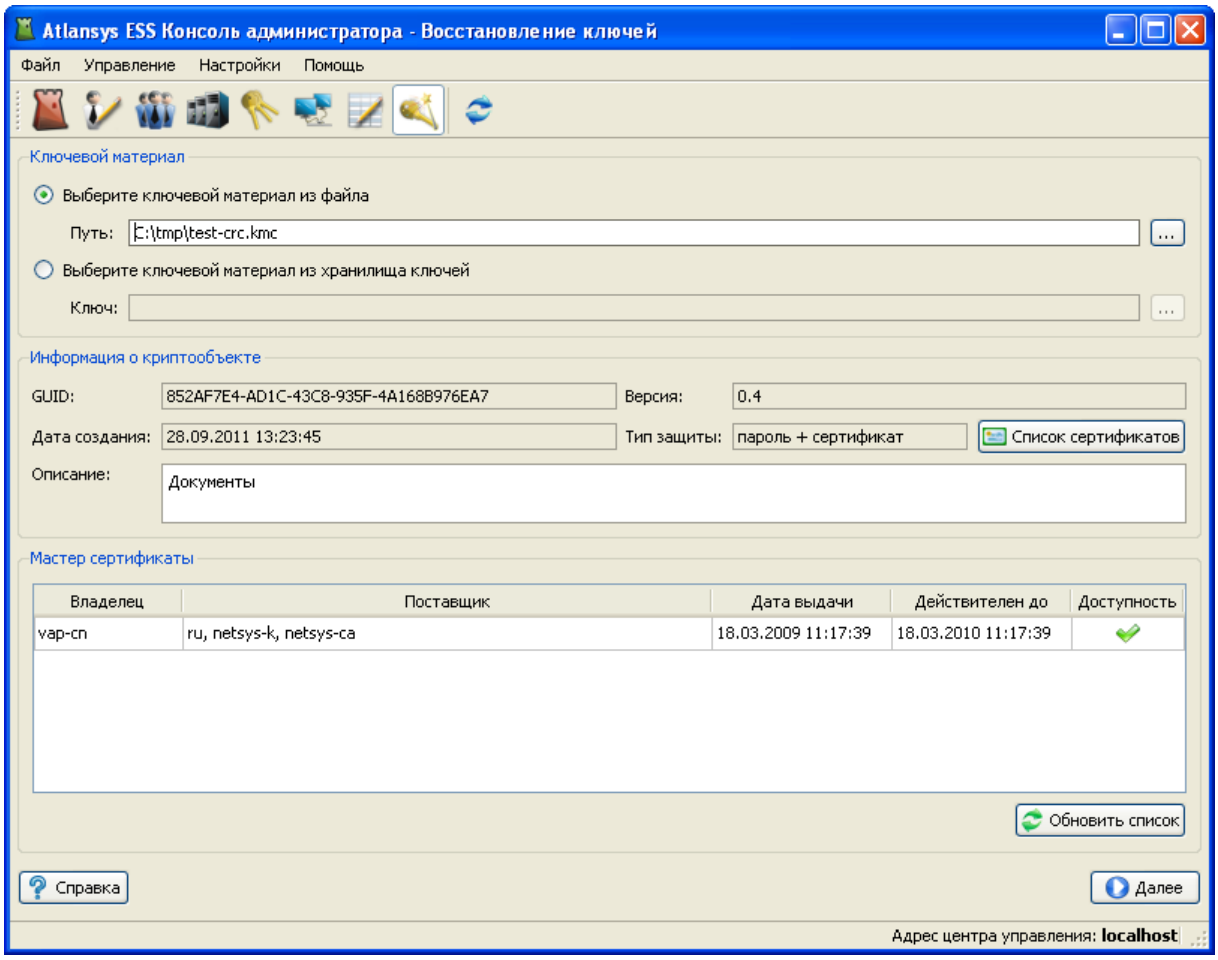

Рисунок 10.5. Восстановление ключей. Шаг 1.

Ключевой материал криптообъекта зашифрован мастер-сертификатами, для изменения схемы его защиты необходимо, чтобы в системе присутствовали все мастер-сертификаты со своими закрытыми ключами. После того как все мастер-сертификаты найдены, необходимо нажать кнопку «Далее». В результате откроется окно, в котором необходимо задать новую схему защиты ключа для криптообъекта.

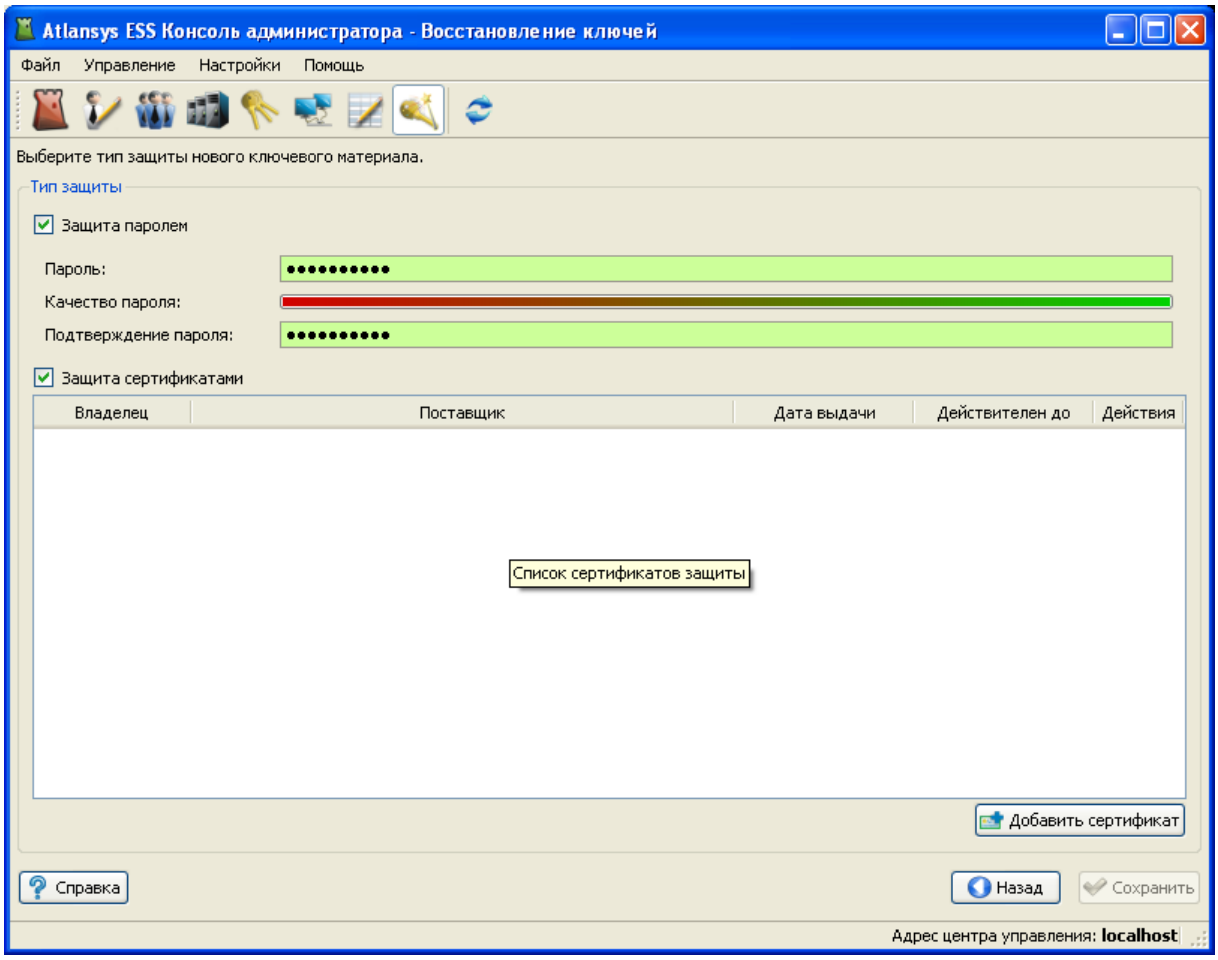

Рисунок 10.6. Восстановление ключей. Шаг 2.

После задания нового пароля и/или списка сертификатов защиты необходимо нажать на кнопку "Сохранить". Затем выбрать файл для сохранения нового ключевого материала.

10.2.3. Импорт новой ключевой информации в криптообъект.

Для импорта ключевого материала в криптообъект используется та же утилита **key-recovery**. После её запуска необходимо нажать на кнопку «Импорт восстановленного ключевого материала из файла в криптообъект». В результате откроется диалоговое окно выбора файла. В этом окне необходимо выбрать файл, созданный на этапе №2 и нажать на кнопку "Открыть". После этого необходимо выбрать тип криптообъекта, для которого восстанавливается ключ и нажать кнопку "Далее".

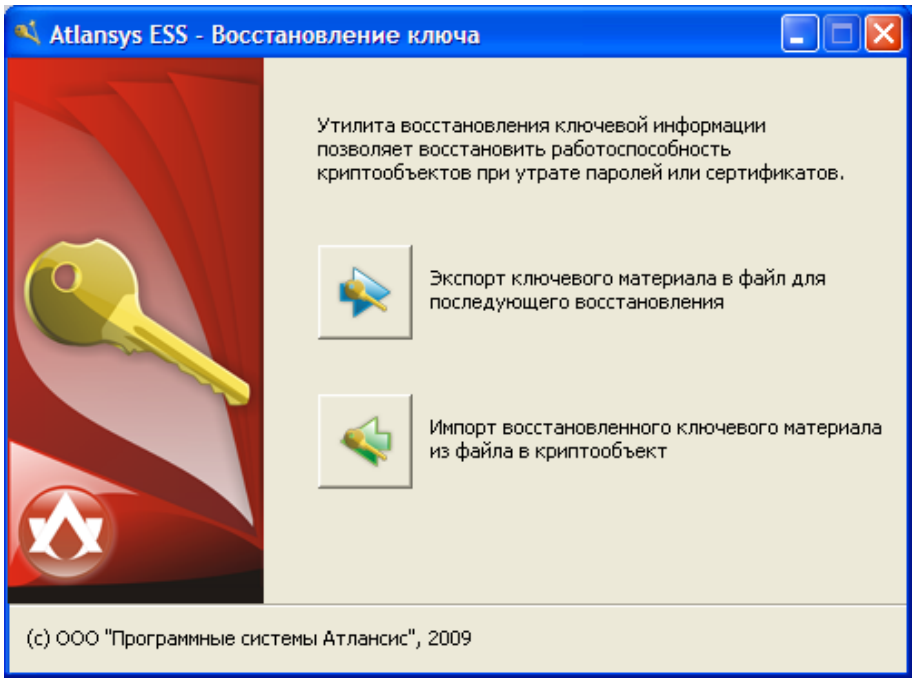

Рисунок 10.7. Утилита восстановления ключей

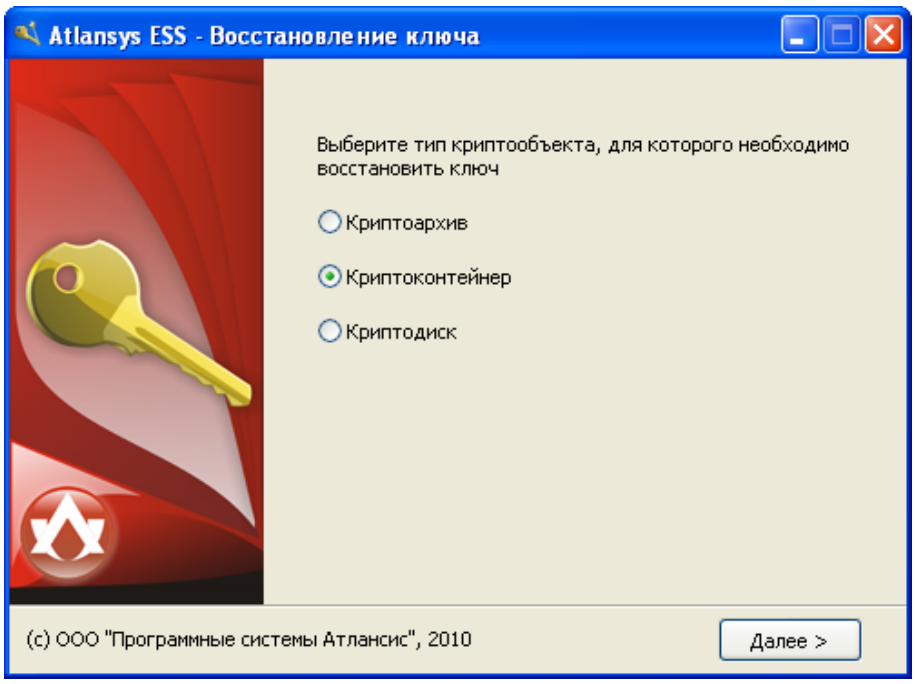

Рисунок 10.8. Выбор типа криптообъекта для импорта ключа

Затем необходимо выбрать сам криптообъект. Для криптоархивов, самораспаковывающихся криптоархивов и криптоконтейнеров откроется стандартный диалог выбора файла. Для криптодиска откроется окно выбора криптодиска, в котором будут оторбажены все криптодиски, доступные в системе.

Замечание

При восстановлении ключевой информации для криптоконтейнера и криптодиска они должны быть закрыты, в противном случае эта процедура невозможна. Также не-

обходимо убедиться, что был выбран тот же самый криптообъект, из которого был экспортирован ключевой материал (см. этап №1), в противном случае открыть криптообъект будет невозможно.

После выбора необходимого криптообъекта появится окно с его описанием. Для завершения процедуры восстановления ключа необходимо нажать на кнопку «Импорт». После этого можно будет открыть криптообъект, используя способы, заданные на этапе №2.

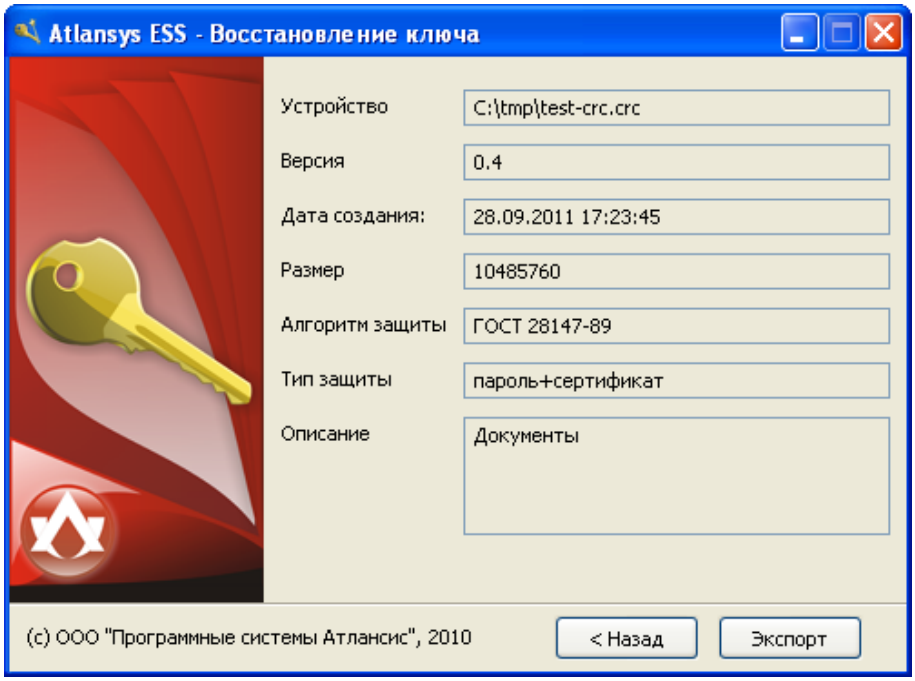

Рисунок 10.9. Проверка параметров перед импортом ключа в криптообъект

10.3. Восстановление ключа с извлечением информации из хранилища ключей Центра Управления

Данный способ применим только для восстановления ключа для криптодисков, созданных на управляемых клиентах.

На странице «Восстановление ключей» Консоли Администратора необходимо выбрать пункт «Выберите ключевой материал из хранилища ключей» и нажать на кнопку «…». В результате появится окно, в котором будет список всех ключей, доступных для восстановления. В этом окне необходимо выбрать ключ для восстановления и нажать на кнопку «Импорт».

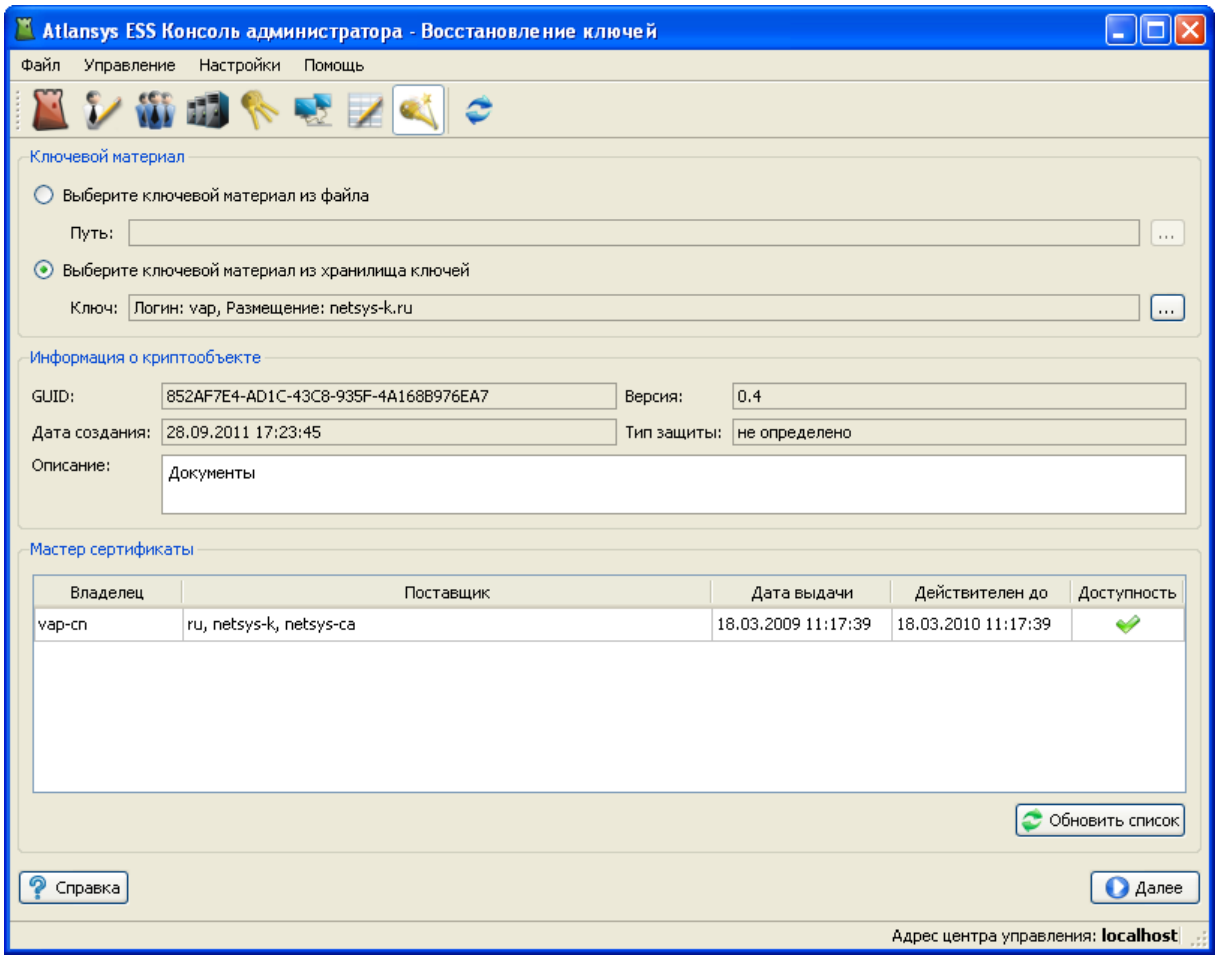

Рисунок 10.10. Восстановление ключей. Выбор ключа из хранилища ключей.

Второй и третий этапы этого способа восстановления ключевой информации аналогичны первому способу.

Глава 11. Сохранение и восстановление настроек Центра Управления

11.1. Сохранение настроек Центра Управления

Для сохранения настроек Центра Управления необходимо выполнить следюущие действия:

1. Открыть панель управления службами "**Администрирование/Службы**"
2. Остановить службу "**Control Center Service**"
3. Скопировать из корня каталога инсталяции Центра управления на резервный носитель следующие конфигурационные файлы:
   - admin.ini
   - keys.db
   - policy.db
   - tls-srv-cert.cer
   - tls-src-cert.pkey
   - logs/control-center-log.db
4. Запустить службу "**Control Center Service**"

11.2. Восстановление настроек Центра Управления

Для восстановления настроек Центра Управления необходимо выполнить следующие действия:

1. Открыть панель управления службами "**Администрирование/Службы**"
2. Остановить службу "**Control Center Service**"
3. Скопировать с резервного носителя в корень каталога инсталяции Центра управления следующие конфигурационные файлы, сохраненные ранее:
   - admin.ini
   - keys.db
   - policy.db
   - tls-srv-cert.cer
   - tls-src-cert.pkey
   - logs/control-center-log.db

   Если какие-либо из копируемых файлов уже существуют, то необходимо их заменить.
4. Запустить службу "**Control Center Service**"

Глава 12. Техническая поддержка

Техническая поддержка данного продукта осуществляется в рамках правил, опубликованых на сайте www.atlansys.ru. Обратиться в службу технической поддержки можно по телефонам, указанным на сайте, либо по электронной почте по адресу <support@atlansys.ru>. Для получения оперативного ответа при запросе в службу технической поддержке будьте готовы предоставить следующую информацию:

- Фамилию, имя, отчество контактного лица, адрес электронной почты, номер телефона.
- Полное наименование продукта.
- Версия продукта (отображается в диалоге «О программе»).
- Лицензионный ключ, либо серийный номер продукта.
- Версия операционной системы, описание конфигурации компьютера.
- Краткое описание возникшей проблемы и действий, которые к ней привели.
- По возможности, снимки экрана при возниконовении ошибки, код ошибки, лог-сообщения, которые предшествовали ошибке.
- При возникновении ошибок в сторонних программах, связанных с использованием данного продукта, наименование и номера версий этих программ.

Важно

Никогда не сообщайте кому-бы то ни было пароли и другую конфиденциальную информацию. Служба технической поддержки не запрашивает каких-либо паролей, ключей и пин-кодов.

Приложение A. Лицензионный договор

A.1. Лицензионный договор с конечным пользователем

Внимание! Прочтите внимательно данный лицензионный договор, прежде чем устанавливать, копировать или иным образом использовать приобретенный продукт. Любое использование вами приобретенного продукта, в том числе его установка и копирование, означает ваше согласие с условиями приведенного ниже Лицензионного договора. Настоящий Лицензионный договор является юридически обязательным соглашением, заключаемым между Вами - Конечным пользователем, и Компанией ООО "Программные системы Атлансис"; соглашение заключается относительно программного обеспечения (далее по тексту - ПО), которое поставляется вместе с данным Лицензионным договором. ПО, включая все носители, печатные материалы и электронную документацию, является объектом авторского права и охраняется законом. Если вы не согласны принять на себя условия настоящего Лицензионного договора, вы не имеете права устанавливать ПО и должны вернуть ПО организации, у которой вы приобрели ПО, в сроки, установленные законодательством страны его приобретения и правилами возврата, действующими в месте приобретения. Деньги вам будут возвращены полностью при условии, что вы отказались от использования ПО и вернули вместе с ПО всю относящуюся к ПО документацию, носители и упаковку.

1. **Предмет договора**

    1.1. Предметом настоящего Лицензионного договора является передача Компанией ООО "Программные системы Атлансис" (Правообладателем) Вам (Конечному пользователю) прав на использование ПО способами, указанными в настоящем Лицензионном договоре (неисключительных прав на использование ПО).

    1.2. Все условия, оговоренные далее, относятся как к ПО в целом, так и ко всем его компонентам в отдельности.

2. **Исключительное право**

    2.1. Компания ООО "Программные системы Атлансис" гарантирует, что имеет право на распоряжение ПО (в том числе любыми включенными в него графическими изображениями, фотографиями, текстами, дополнительными программами и другими объектами авторского права), а также права на распоряжение любыми копиями ПО и сопровождающими ПО печатными материалами. ПО защищается законодательством Российской Федерации и международными соглашениями об авторских правах страны приобретения ПО.

    2.2. ПО содержит коммерческую тайну и иную конфиденциальную информацию, которая защищена авторским правом, международными соглашениями и законодательством страны использования. Использование ПО в нарушение настоящего Лицензионного договора признается нарушением действующего законодательства об авторских правах и является достаточным основанием для лишения вас прав, предоставленных в отношении ПО.

    2.3. Вы имеете право один раз передать данный Лицензионный договор и само ПО непосредственно другому конечному пользователю. Такая передача должна распространяться на все ПО (включая все составные части, носители и печатные материалы, а также любые обновления). Указанная передача не может быть осуществлена косвенно или через какое-либо третье лицо. Лицо, получающее ПО в результате такой единовременной передачи, должно согласиться со всеми условиями настоящего Лицензионного договора, включая обязательство никому дальше не передавать настоящий Лицензионный договор и само ПО. Уступая свои права на ПО другому конечному пользователю, вы обязуетесь уничтожить все копии передаваемого ПО, установленные на вашем компьютере или сервере.

3. **Условия использования**

    3.1. В случае установки ПО на автономный (отдельный) компьютер разрешается установить ПО на один компьютер: либо на одном настольном компьютере или на одном переносном компьютере (ноутбуке); либо на одном офисном или одном домашнем. ПО не может одновременно использо-

ваться на настольном (офисном) компьютере и переносном (домашнем) компьютере. Вы не имеете права устанавливать ПО на каких-либо других компьютерах.

3.2. В случае сетевой установки ПО вы можете использовать ПО только в рамках одной локальной сети; вы можете установить ПО на один сервер. В любом случае одновременное использование ПО разрешается только на одной рабочей станции (если иное не оговорено в отдельном соглашении с Компанией ООО "Программные системы Атлансис").

4. **Поставка на двух типах носителей**

4.1. В случае если ПО поставляется на двух или нескольких видах носителей, включая поставку через Интернет, то, независимо от количества носителей, вы имеете право использовать только один из имеющихся у вас экземпляров ПО в соответствии с п.3 настоящего Лицензионного договора.

5. **Распространение программное обеспечение (ПО)**

5.1. Распространение ПО не допускается. Под распространением ПО понимается, в частности: предоставление доступа третьим лицам к воспроизведенным в любой форме компонентам ПО, в том числе путем продажи (за исключением случаев, указанных в п. 2.3 настоящего Лицензионного договора), проката, сдачи внаем или предоставления взаймы.

6. **Ограничения**

6.1. Регистрация. Вы согласны с тем, что ПО снабжается средствами защиты от копирования и неограниченного использования. Предоставленные вам настоящим Лицензионным договором права в отношении ПО могут не вступить в полную силу до тех пор, пока не будет произведена регистрация ПО в порядке, определенном в документации к ПО, либо на веб-сайте www.atlansys.ru , либо в иных поставляемых Компанией ООО "Программные системы Атлансис" открытых материалах. В процессе регистрации в ООО "Программные системы Атлансис" не передается никаких ваших персональных данных, за исключением указанных вами Имени Фамилии и Отчества и сохраняется полная анонимность.

6.2. Все условия и ограничения использования ПО указаны в пункте 3 настоящего Лицензионного договора, если иное не оговорено в отдельном соглашении между вами и Компанией ООО "Программные системы Атлансис".

6.3. Вы обязуетесь не осуществлять самостоятельно и не разрешать третьим лицам осуществлять следующие действия:

6.3.1. Дизассемблировать, декомпилировать (преобразовывать объектный код в исходный текст) программы, базы данных и другие компоненты ПО, за исключением случаев, когда возможность осуществления таких действий прямо предусмотрена действующим законодательством.

6.3.2. Модифицировать ПО, в том числе вносить изменения в объектный код программ или баз данных к ним, за исключением тех изменений, которые вносятся средствами, включенными в комплект ПО и описанными в документации.

6.3.3. Передавать права на использование ПО третьим лицам, за исключением случая, указанного в п. 2.3 настоящего Лицензионного договора.

6.3.4. Создавать условия для использования ПО лицами, не имеющими прав на использование данного ПО, в том числе работающими с вами в одной сети или многопользовательской системе.

7. **Техническая поддержка**

7.1. Компания ООО "Программные системы Атлансис" предоставляет вам услуги по технической поддержке ПО (далее - техническая поддержка) в соответствии с текущими правилами оказания технической поддержки Компании ООО "Программные системы Атлансис". Правила публикуются на

веб-сайте Компании ООО "Программные системы Атлансис" и могут быть изменены без предварительного уведомления.

7.2. Любое программное обеспечение, поставляемое в рамках технической поддержки, считается частью ПО и должно использоваться в соответствии с условиями настоящего Лицензионного договора.

7.3. Для осуществления технической поддержки Компания ООО "Программные системы Атлансис" вправе потребовать от вас предоставления информации, касающейся технических характеристик вашего оборудования, а также запросить стандартные анкетные данные, в том числе ваше имя, название компании (для юридических лиц), адрес, электронный адрес и номер телефона.

7.4. Компания ООО "Программные системы Атлансис" вправе использовать вышеуказанную информацию в целях развития бизнеса, в том числе (но не исключительно) для развития ПО и оказания технической поддержки, при условии что Компания ООО "Программные системы Атлансис" не использует эту информацию в какой-либо форме, позволяющей вас идентифицировать.

8. **Испытательные версии ПО**

8.1. Если версия ПО обозначена как «испытательная», «демонстрационная» или «облегченная» («Try&Buy», «Trial», «Demo» или «Lite»), далее «испытательная версия ПО», то, независимо от остальных условий настоящего Лицензионного договора, до тех пор, пока не будет приобретена лицензия на полнофункциональную версию ПО, применяется настоящий раздел.

8.2. Вы согласны с тем, что испытательная версия ПО имеет ограниченную функциональность и/или ограниченное время работы. ПО предоставляется таким, каково оно есть, предназначено исключительно для целей предварительного знакомства с возможностями полнофункционального ПО.

8.3. Компания ООО "Программные системы Атлансис" не несет ни какой ответственности за порчу или потерю данных на вашем компьютере или иных носителях информации при использовании испытательной версии ПО.

8.4. Если испытательное ПО является ограниченным по времени, то по истечении определенного периода времени, явно указанного в ПО, оно может прекратить работу. Если не была приобретена полнофункциональная версия ПО, настоящий Лицензионный договор прекращает свое действие по истечении испытательного периода.

9. **Программное обеспечение, предоставляемое как обновление**

9.1. Если ПО обозначено как «обновление» («Upgrade»), для его использования вы должны иметь действующую лицензию на использование программы, которая указана Компанией ООО "Программные системы Атлансис" как подлежащая обновлению.

9.2. ПО, обозначенное как «обновление», заменяет собой или дополняет программу, являющуюся основанием вашего права на обновление.

9.3. Устанавливая ПО, обозначенное как «обновление», на компьютер, вы лишаетесь лицензии на ранее используемую программу.

9.4. Вы имеете право использовать ПО, полученное в качестве обновления, только в соответствии с условиями Лицензионного договора, с которым оно поставляется.

9.5. Любые обязательства Компании ООО "Программные системы Атлансис" по технической поддержке ранее используемой программы прекращаются в момент передачи вам ПО, обозначенного как обновление.

10. **Расторжение договора**

10.1. Без ущерба для каких-либо своих прав Компания ООО "Программные системы Атлансис" может прекратить действие настоящего Лицензионного договора при несоблюдении вами его условий и/или ограничений.

10.2. При прекращении действия настоящего Лицензионного договора вы обязаны уничтожить все имеющиеся у вас копии ПО, а также деинсталлировать ПО.

11. Гарантии и возмещение

11.1. Компания ООО "Программные системы Атлансис" гарантирует качество данных на носителях, входящих в комплект ПО, и работоспособность поставляемых программ в течение гарантийного срока, установленного для ПО законодательством страны приобретения, и при условиях, оговоренных в документации (в том числе и электронной), а также гарантирует качественное оформление печатной документации. В случае приобретения ПО в пределах Российской Федерации гарантийный срок составляет 60 дней.

11.2. В остальном ПО поставляется «таким, каково оно есть». Компания ООО "Программные системы Атлансис" не гарантирует, что ПО не содержит ошибок, а также не несет никакой ответственности за прямые или косвенные убытки, включая упущенную выгоду, потерю конфиденциальной информации, возникшие в результате применения ПО, в том числе из-за возможных ошибок или опечаток в комплекте ПО.

11.3. Компания ООО "Программные системы Атлансис" не гарантирует, что ПО будет соответствовать вашим требованиям, а также не гарантирует работу ПО совместно с программным обеспечением и оборудованием других изготовителей.

11.4. За исключением случаев, прямо предусмотренных настоящей статьей, Компания ООО "Программные системы Атлансис" не дает никаких гарантий относительно ПО, его работоспособности, применимости для конкретного использования, даже если такие гарантии обычно предоставляются в соответствии с обычаями делового оборота.

11.5. Любая ответственность Компании ООО "Программные системы Атлансис", вне зависимости от оснований для ее возникновения, будет ограничена ценой, уплаченной вами при приобретении ПО.

12. Условия экспорта

12.1. Вы не должны экспортировать или реэкспортировать ПО в нарушение законодательства о совершении экспортных сделок, действующего в стране приобретения ПО, а также в нарушение любого другого применимого законодательства.

13. Прочие условия

13.1. В случае если вы приобрели или получили ПО, включая ПО «не для продажи», испытательные версии ПО и ПО, обозначенное как «обновление», через Интернет:

13.1.1. Компания ООО "Программные системы Атлансис" не предоставляет вам никаких гарантий в отношении каких бы то ни было потребительских качеств ПО, включая работоспособность ПО и пригодность для использования в каких-либо целях, даже если такие гарантии обычно предоставляются в соответствии с обычаями делового оборота;

13.1.2. Компания ООО "Программные системы Атлансис" не передает вам никаких печатных материалов, включая руководство пользователя.

13.2. Вознаграждением по настоящему Лицензионному договору признается стоимость ПО, установленная Компанией ООО "Программные системы Атлансис" или ее дистрибьюторами и подлежащая уплате в соответствии с определяемым ими порядком.

13.3. Настоящий Лицензионный договор считается заключенным с момента, когда вы примете его условия, а именно: отметите пункт «Я принимаю условия договора» на мониторе вашего компьютера и нажмете на кнопку «Далее»; настоящий Лицензионный договор сохраняет силу в течение всего периода действия исключительного права в отношении ПО.

13.4. В случае если вы не согласны с условиями Лицензионного договора, отметьте пункт «Я не принимаю условия договора» и нажмите на кнопку «Отмена» для выхода из программы установки.

13.5. Компания ООО "Программные системы Атлансис" гарантирует, что данные, сообщенные вами при установке и регистрации ПО, будут храниться и использоваться исключительно внутри Группы компаний ООО "Программные системы Атлансис".

13.6. Компания ООО "Программные системы Атлансис" гарантирует, что данные, сообщенные вами при активации ПО, будут храниться и использоваться исключительно внутри Компании ООО "Программные системы Атлансис".

13.7. Все права на наименования программных продуктов «Atlansys Enterprise Security Security», «Atlansys Server», «Atlansys Bastion», «Atlansys BastionPro», «Atlansys Bastion Ultimate», принадлежат исключительно ООО "Программные системы Атлансис".