Руководство пользователя

Atlansys Software

Atlansys ESS

Atlansys Enterprise Security System
Руководство пользователя

Версия 7.0.3

Информация, касающаяся описания продукта в данном руководстве, может быть изменена без предварительного уведомления. Все утверждения, информация и рекомендации в настоящем руководстве полагаются корректными, но приведены без гарантий любого рода, явных или подразумеваемых. Пользователи должны принять на себя полную ответственность за их применение. Лицензия на программное обеспечение изложена в документации, поставляющейся вместе с продуктом, а также включена в настоящее руководство. Если по каким-либо причинам вы не можете найти текста лицензионного соглашения, свяжитесь с представителем ООО «Программные системы Атлансис» для получения ее копии.

Компания ООО «Программные системы Атлансис» не несет ответственности за любой косвенный, специальный или побочный ущерб, включая, без ограничений, упущенную прибыль, убыток или повреждение данных, вытекающие из использования или невозможности использования данного руководства, даже если ООО «Программные системы Атлансис», ее поставщики, партнеры или дистрибьюторы были заранее извещены о возможности такого ущерба.

Содержание

Введение viii
1. Назначение документа viii
2. Сведения о продукте viii
3. Лицензионный договор viii
1. Установка и удаление программного обеспечения 1
1.1. Установка программного обеспечения с помощью интерактивного инсталлятора 1
1.2. Обновление программного обеспечения 9
1.3. Установка программного обеспечения с использованием конфигурационного файла 12
1.4. Удаление программного обеспечения 13
2. Atlansys Enterprise Security System Навигатор 15
2.1. Назначение 15
2.2. Запуск программы 15
2.3. Интерфейс 15
2.4. Настройки продукта 18
2.5. Автоматическое открытие криптоконтейнеров и криптодисков 26
2.6. Подключаемые модули 28
3. Работа с криптоконтейнерами 29
3.1. Введение 29
3.2. Создание криптоконтейнера 29
3.3. Добавление криптоконтейнера 32
3.4. Работа с криптоконтейнерами 33
3.5. Удаление криптоконтейнера 36
4. Работа с криптодисками 38
4.1. Введение 38
4.2. Создание криптодиска 38
4.3. Добавление криптодиска 44
4.4. Работа с криптодисками 45
4.5. Удаление криптодиска 47
5. Шифрование системного раздела 49
5.1. Введение 49
5.2. Шифрование системного раздела 49
5.3. Работа с зашифрованным системным разделом 52
5.4. Дешифрация системного раздела 52
5.5. Восстановления пароля зашифрованного системного раздела 52
6. Работа с автономными криптофлэш дисками 56
6.1. Введение 56
6.2. Создание автономного криптофлэш диска 56
6.3. Работа с автономным криптофлэш диском 58
7. Свойства криптообъекта 61
7.1. Диалог свойств криптообъекта 61
7.2. Изменение пароля и сертификатов 61
7.3. Дополнительно 63
8. Работа с криптоархивами 65
8.1. Создание криптоархивов 65
8.2. Извлечение данных из криптоархива 69
9. Работа с самораспаковывающимися криптоархивами 71
9.1. Создание самораспаковывающегося криптоархива 71
9.2. Извлечение данных из самораспаковывающегося криптоархива 73
10. Гарантированное удаление файлов 76
10.1. Гарантированное удаление 76
11. Журнал событий 78
11.1. Журнал событий 78
12. Электронно-цифровая подпись 82
12.1. Назначение электронно-цифровой подписи (ЭЦП) 82
12.2. Подписывание файлов 82

12.3. Проверка ЭЦП 83
13. Техническая поддержка 85
A. Лицензионный договор 86
A.1. Лицензионный договор с конечным пользователем 86

Список иллюстраций

1.1. Установка Atlansys Enterprise Security System 1
1.2. Лицензионный договор 2
1.3. Регистрация 3
1.4. Тип клиента 4
1.5. Установка управляемого клиента 5
1.6. Выбор компонентов клиентского программного обеспечения 6
1.7. Выбор каталога для установки программы 7
1.8. Запуск процесса установки 8
1.9. Процесс установки 8
1.10. Завершение установки 9
1.11. Обновление Atlansys Enterprise Security System 10
1.12. Процесс установки 11
1.13. Завершение установки 12
1.14. Окно Панели управления «Установка и удаление программ» 14
1.15. Окно запроса на удаление 14
2.1. Запуск Atlansys Enterprise Security System Навигатор через меню Пуск 15
2.2. Главное окно Навигатора 16
2.3. Меню «Файл» 17
2.4. Меню «Действия» 17
2.5. Меню «Настройки» 18
2.6. Меню «Помощь» 18
2.7. Язык 19
2.8. Настройки создания криптоархива - Формат криптоархива Atlansys 20
2.9. Настройки создания криптоархива - Формат PKCS7 20
2.10. Диалог «Добавлнение сертификата» 21
2.11. Настройки ЭЦП - Формат файла подписи Atlansys 21
2.12. Настройки ЭЦП - Формат файла подписи PKCS7 22
2.13. Регистрация событий 23
2.14. Уничтожение данных 23
2.15. Настройка Красной кнопки 24
2.16. Настройка списка файлов и каталогов для удаления 25
2.17. Настройка LDAP каталогов 25
2.18. Добавление LDAP каталога 26
2.19. Автооткрытие криптоконтейнера 27
2.20. Автооткрытие криптодиска 27
2.21. Диалог автооткрытия криптообъектов 28
3.1. Меню «Файл» / «Создать» 29
3.2. Мастер создания криптоконтейнеров. 30
3.3. Мастер создания криптоконтейнеров. Способы защиты. 31
3.4. Мастер создания криптоконтейнеров. Прогресс создания. 32
3.5. Меню «Файл» / «Добавить» 32
3.6. Мастер добавления криптоконтейнеров 33
3.7. Диалог открытия криптоконтейнера 33
3.8. Список криптоконтейнеров и криптодисков 34
3.9. Меню «Действия» 35
3.10. Контекстное меню криптоконтейнера 35
3.11. Панель инструментов, кнопка «Открыть» 35
3.12. Панель инструментов, кнопка «Удалить» 36
3.13. Мастер удаления криптоконтейнеров 37
4.1. Меню «Файл» / «Создать» 38
4.2. Мастер создания криптодисков. Выбор раздела. 39
4.3. Мастер создания криптодисков. Метка диска и описание. 40
4.4. Мастер создания криптодисков. Способы защиты. 41
4.5. Мастер создания криптодисков. Сводная информация. 42
4.6. Мастер создания криптодисков. Предупреждение. 42

4.7. Мастер создания криптодисков. Прогресс создания. 43
4.8. Процесс преобразования криптодиска. 43
4.9. Мастер создания криптодисков. Заполнение случайными данными. 44
4.10. Меню «Файл» / «Добавить» 44
4.11. Мастер добавления криптодисков. Выбор раздела. 45
4.12. Мастер добавления криптодисков. Сводная информация о криптодиске. 45
4.13. Меню «Действия» 46
4.14. Контекстное меню криптодиска 46
4.15. Панель инструментов 46
4.16. Диалог открытия криптодиска 47
4.17. Панель инструментов, кнопка «Удалить» 47
4.18. Мастер удаления криптодисков 48
5.1. Меню шифрования системного раздела 49
5.2. Мастер шифрования системного раздела. Предупреждение. 50
5.3. Мастер шифрования системного раздела. Параметры криптодиска. 50
5.4. Мастер шифрования системного раздела. Защита. 51
5.5. Мастер шифрования системного раздела. Сводная информация. 51
5.6. Мастер расшифрования системного раздела 52
5.7. Начальный экран загрузки диска восстановления 53
5.8. Главное окно программы. 53
5.9. Показать информацию о системном диске Atlansys. 54
5.10. Восстановление пароля. 54
5.11. Восстановление пароля. 55
6.1. Меню «Файл» / «Создать» 56
6.2. Мастер создания автономного криптофлэш диска. Выбор раздела. 57
6.3. Мастер создания автономного криптофлэш диска. Способы защиты. 57
6.4. Мастер создания автономного криптофлэш диска. Прогресс создания. 58
6.5. Стандартный диалог открытия криптодиска. 59
6.6. Сообщение об успешном открытии криптофлэш диска. 59
6.7. Меню программы в системном трее. 59
7.1. Кнопка вызова диалога свойств криптообъекта 61
7.2. Диалог свойств криптообъекта - Информация 61
7.3. Диалог свойств криптообъекта - Защита 62
7.4. Диалог изменения пароля 62
7.5. Диалог изменения списка существующих сертификатов 63
7.6. Диалог «Список сертификатов» 63
7.7. Диалог свойств криптообъекта - Дополнительно 64
8.1. Запуск Atlansys ESS / Криптоархив 65
8.2. Окно «Atlansys Enterprise Security System / Криптоархив» 66
8.3. Окно «Список сертификатов» 67
8.4. Окно «Выбор личного сертификата» 68
8.5. Окно «Список сертификатов» 68
8.6. Прогресс создания криптоархива 69
8.7. Завершение создания криптоархива 69
8.8. Окно извлечения данных из криптоархива 70
8.9. Завершение извлечения данных из криптоархива 70
9.1. Создание самораспаковывающегося криптоархива 71
9.2. Окно списка файлов самораспаковывающегося криптоархива 72
9.3. Прогресс создания самораспаковывающегося криптоархива 73
9.4. Самораспаковывающийся криптоархив. Окно ввода пароля. 74
9.5. Самораспаковывающийся криптоархив. Выбор файлов и пути распаковки. 75
10.1. Контекстное меню Гарантированно удалить. 76
10.2. Диалог удаления файлов 77
11.1. Запуск журнала событий 78
11.2. Окно журнала событий 78
11.3. Информация по лог сообщению 79
11.4. Настройки журнала регистрации событий 80
11.5. Фильтр журнала событий 81

12.1. Выбор файлов для подписывания 82
12.2. Вопрос о перезаписи файла ЭЦП 82
12.3. Список файлов после подписывания 83
12.4. Выбор файла для проверки ЭЦП 84
12.5. Диалог проверки ЭЦП 84
12.6. Предупреждение о невалидном сертификате 84

Введение

1. Назначение документа

Данное руководство пользователя содержит сведения по установке и эксплуатации Atlansys Enterprise Security System и предназначено для конечных пользователей системы.

2. Сведения о продукте

Программный продукт Atlansys Enterprise Security System предназначен для криптографической защиты конфиденциальной информации на рабочих станциях и серверах. Защита информации осуществляется с помощью шифрования криптостойкими алгоритмами, гарантирующими надежную защиту от несанкционированного доступа к конфиденциальной информации. Atlansys Enterprise Security System содержит следующие подсистемы:

- *Криптоконтейнеры*, которые являются файлами, содержащими полностью зашифрованный образ файловой системы раздела, подключаемого в систему в виде диска. Открытый криптоконтейнер выглядит в системе как диск, на котором можно сохранять любые файлы, устанавливать приложения, использовать системные утилиты для работы с диском. Закрытый криптоконтейнер представляет собой обычный файл, который можно безопасно копировать, архивировать, передавать по сети, так как все содержимое криптоконтейнера зашифровано. (подробнее см. Глава 3)

- *Криптодиски*, представляющие собой полностью зашифрованные разделы жестких дисков или флешнакопителей. (подробнее см. Глава 4)

- *Криптоархивы*, позволяющие создавать зашифрованные архивы файлов и каталогов. Используются для защищенной передачи файлов внутри компании или контрагентам. (подробнее см. Глава 8)

- *Самораспаковывающиеся криптокархивы* - это криптоархивы, которые можно распаковывать без установки Atlansys Enterprise Security System. Используются для защищенной передачи файлов контрагентам, у которых не установлен продукт. (подробнее см. Глава 9)

- *Электронная цифровая подпись* - криптографические файлы, подтверждающие целостность подписанных данных. (подробнее см. Глава 12)

- *Гарантированное удаление* файлов, обеспечивающее полное уничтожение данных в файлах и невозможность восстановления информации из них программными средствами. (подробнее см. Глава 10)

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

3. Лицензионный договор

Приложение А данного руководства содержит текст Лицензионного договора, с которым необходимо ознакомиться перед установкой, копированием или каким-либо другим использованием данного продукта. Любое использование продукта, в том числе его установка и копирование, означает согласие с условиями Лицензионного договора.

Глава 1. Установка и удаление программного обеспечения

Важно

Что следует помнить перед установкой ПО Atlansys Enterprise Security System:

- Если у вас была установлена демонстрационная версия или предыдущая полнофункциональная версия, не совместимая с новой, закройте все открытые криптоконтейнеры и криптодиски, деинсталлируйте предыдущую версию программы и перезагрузите компьютер. Только после этого производите новую установку.
- Перед установкой программы закройте все работающие приложения.
- 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-WS-(номер версии)-setup.msi**.(Рисунок 1.1)

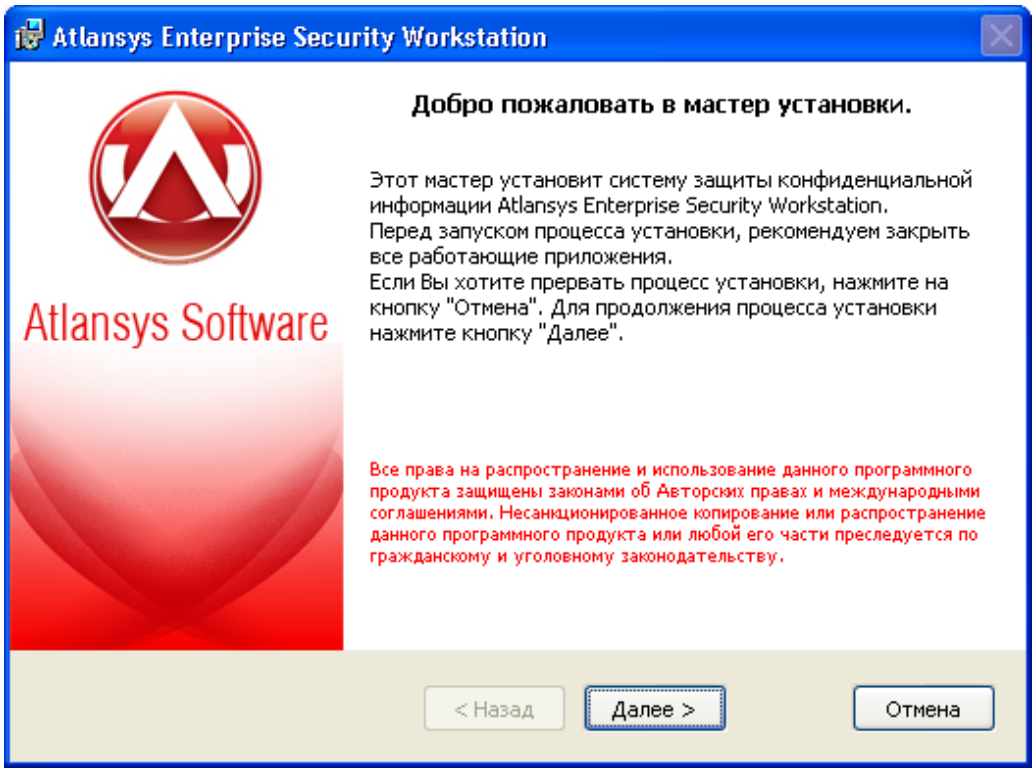

Рисунок 1.1. Установка Atlansys Enterprise Security System

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».

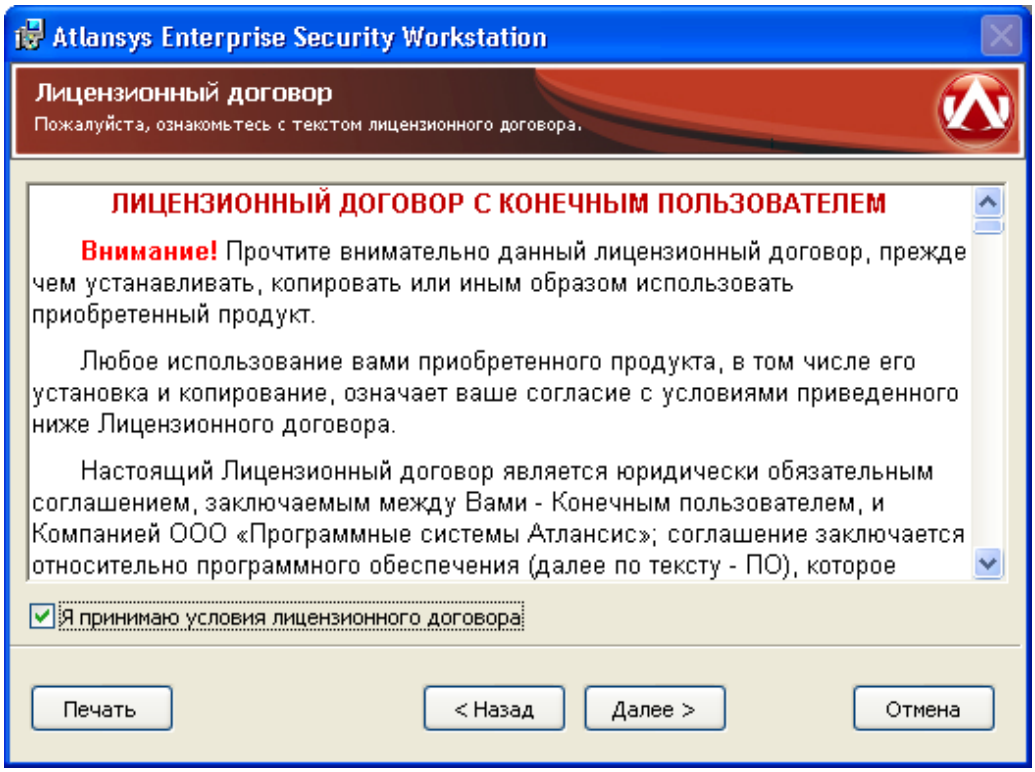

Рисунок 1.2. Лицензионный договор

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».

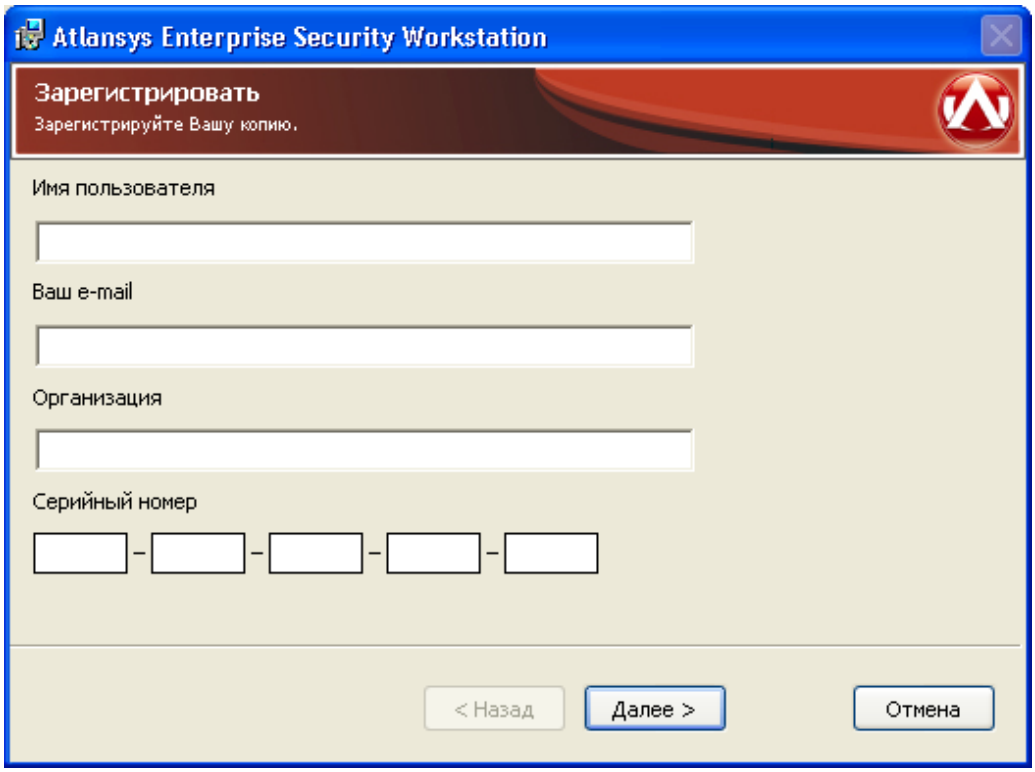

Рисунок 1.3. Регистрация

4. Выбрать тип клиента. Управляемый клиент рекомендуется для работы в корпоративной сети, все настройки продукта клиент получает от Центра Управления, что позволяет централизованно управлять политиками безопасности всех клиентов. Неуправляемый клиент может работать автономно и ему разрешено создание любых криптообъектов. Данный тип рекомендуется для тех рабочих станций и ноутбуков, которые не входят в корпоративную сеть. После выбора типа клиента нажать кнопку «Далее».

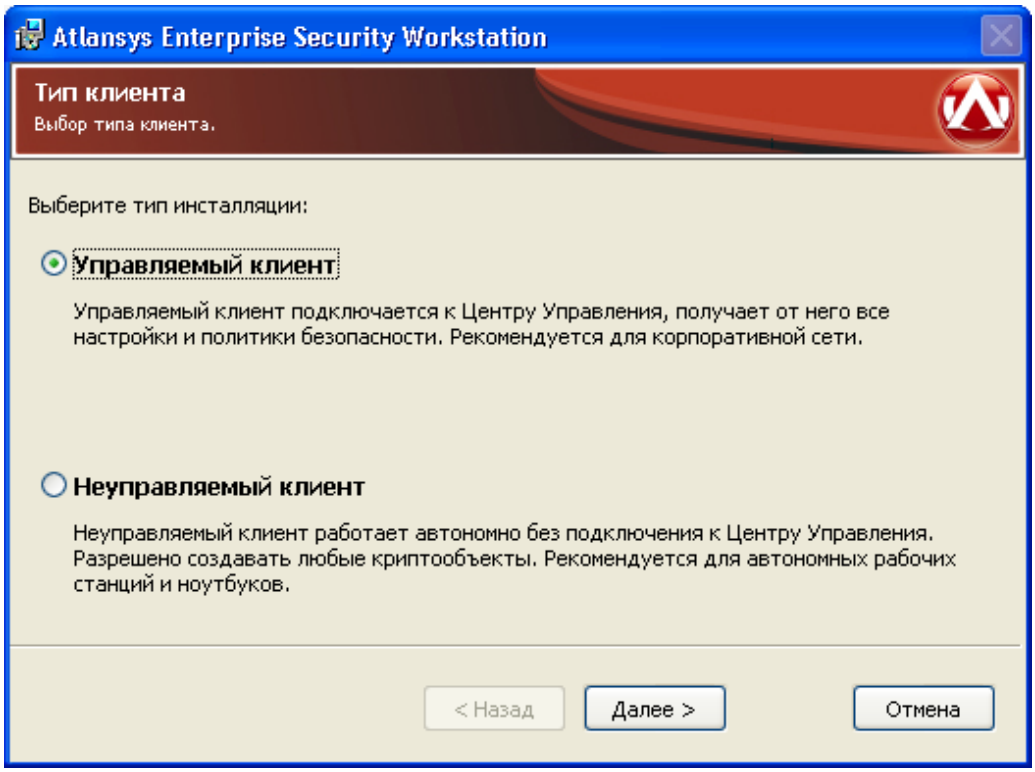

Рисунок 1.4. Тип клиента

5. Если выбран «Управляемый клиент», необходимо для продолжения инсталляции ввести IP-адрес Центра Управления и группу пользователей данного компьютера по умолчанию. Данная группа будет использоваться для получения политик безопасности клиента, если пользователь не задан явно на Центре Управления. Если группа по умолчанию не задаётся, то это поле необходимо оставить пустым. После задания параметров необходимо нажать кнопку «Далее».

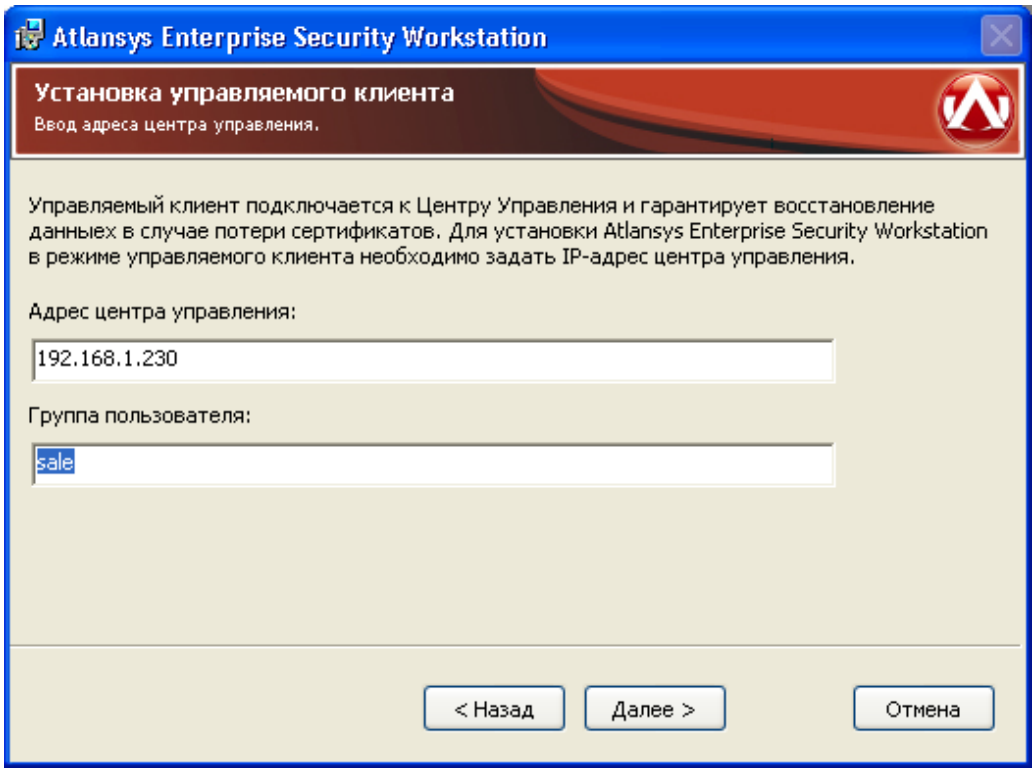

Рисунок 1.5. Установка управляемого клиента

6. Выбрать компоненты программного обеспечения, которые необходимо установить. По умолчанию будут установлены все компоненты, обеспечивающие полную функциональность Atlansys Enterprise Security System. (Рисунок 1.5)

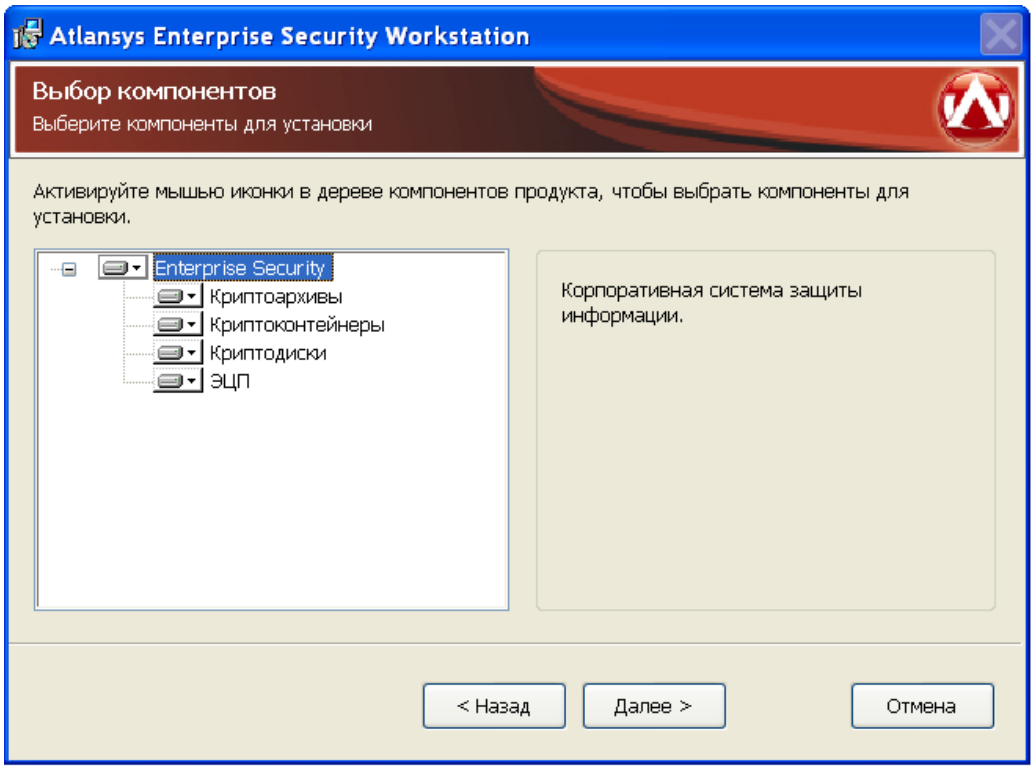

Рисунок 1.6. Выбор компонентов клиентского программного обеспечения

7. 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 1.7)

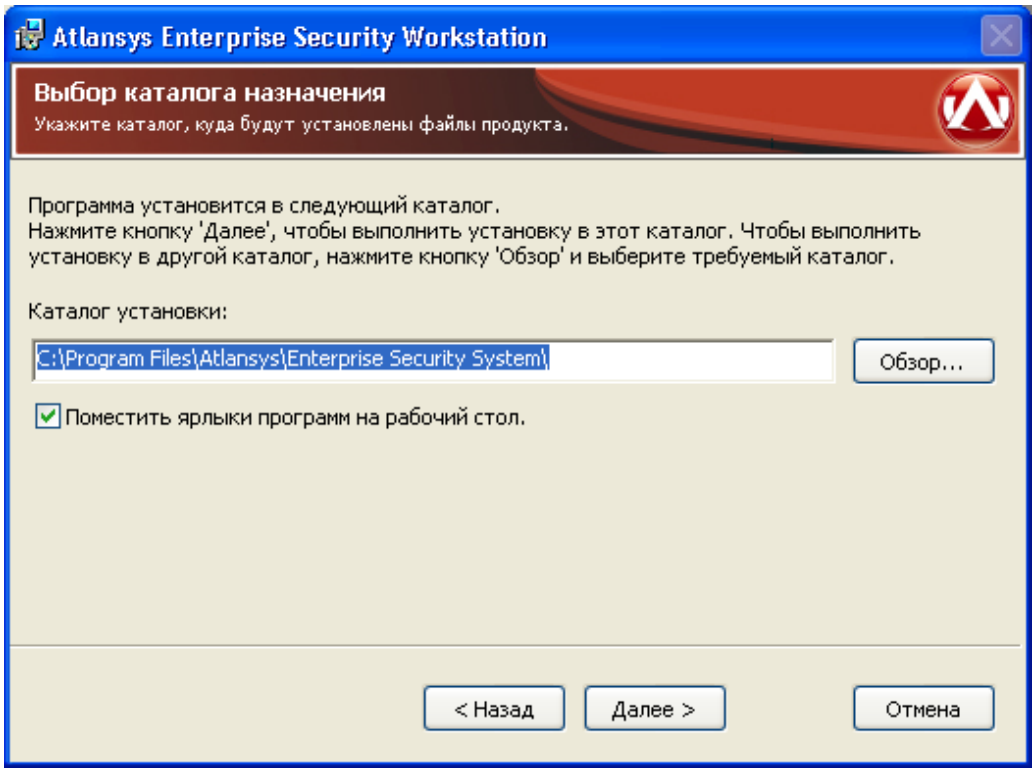

Рисунок 1.7. Выбор каталога для установки программы

8. При необходимости, можно нажать на кнопку «Назад» и изменить ранее введеные параметры. Для запуска процесса установки необходимо нажать кнопку «Установить». (Рисунок 1.8)

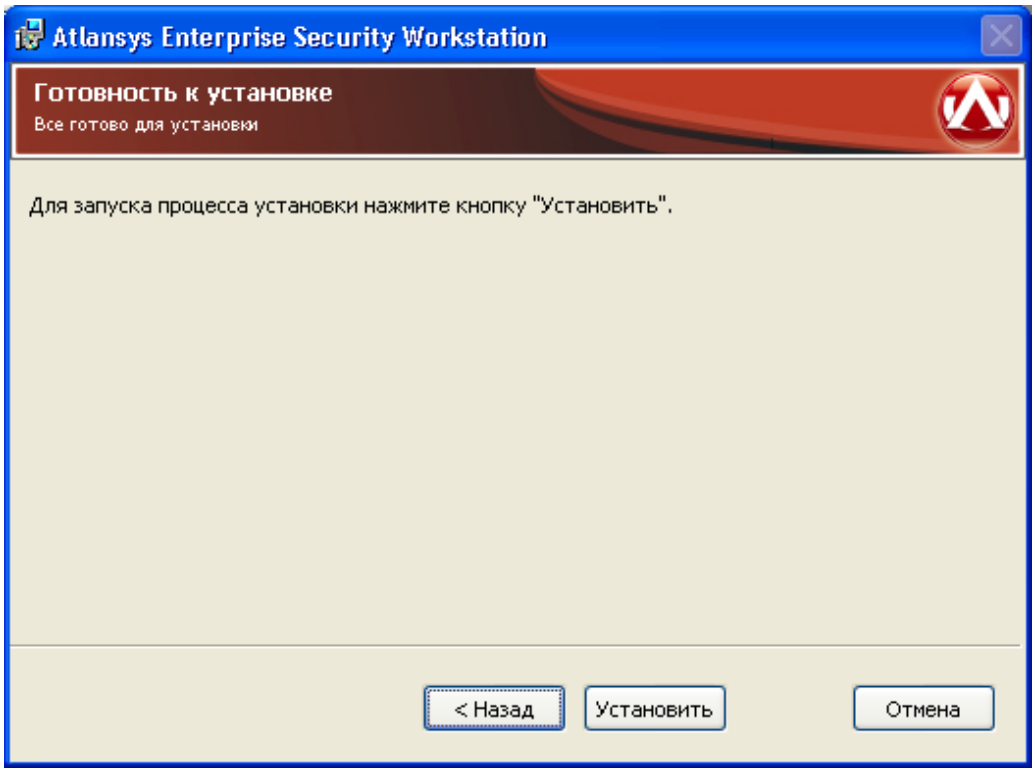

Рисунок 1.8. Запуск процесса установки

9. После этого появится окно, отображающее процесс установки программного обеспечения. (Рисунок 1.9)

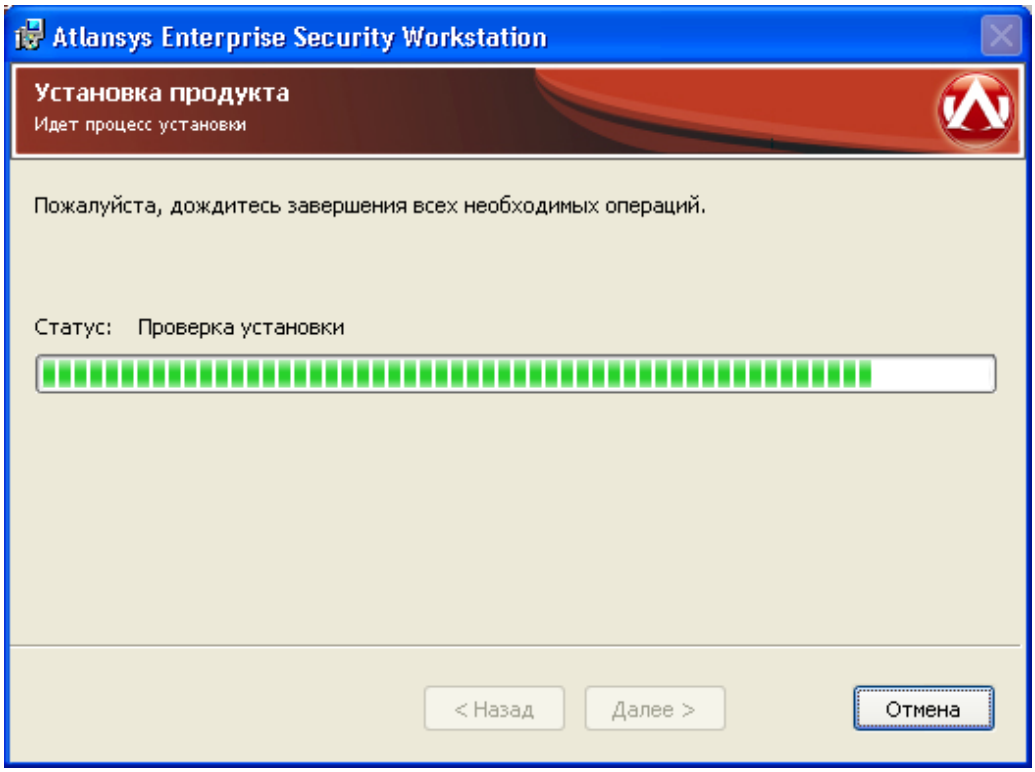

Рисунок 1.9. Процесс установки

10. Для окончания процесса установки необходимо нажать на кнопку «Завершить». (Рисунок 1.10)

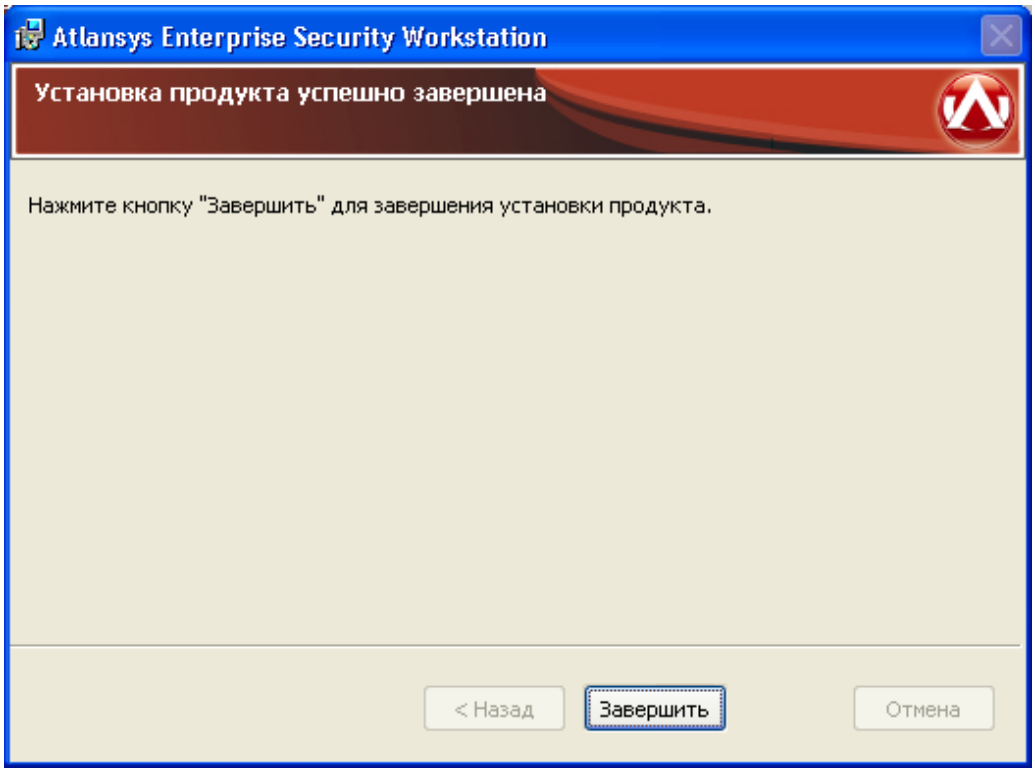

Рисунок 1.10. Завершение установки

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

Важно

Перед обновлением программного обеспечения закройте все открытые криптоконтейнеры и криптодиски, закройте все работающие приложения, и только после этого производите обновление.

Для обновления программного обеспечения Atlansys Enterprise Security System необходимо:

1. Запустить программу инсталятора Atlansys Enterprise Security System для рабочих станций **Atlansys-ESS-WS-(номер версии)-setup.msi**. Нажать кнопку «Далее». (Рисунок 1.11)

Рисунок 1.11. Обновление Atlansys Enterprise Security System

2. После этого появится окно, отображающее процесс обновления программного обеспечения. (Рисунок 1.12)

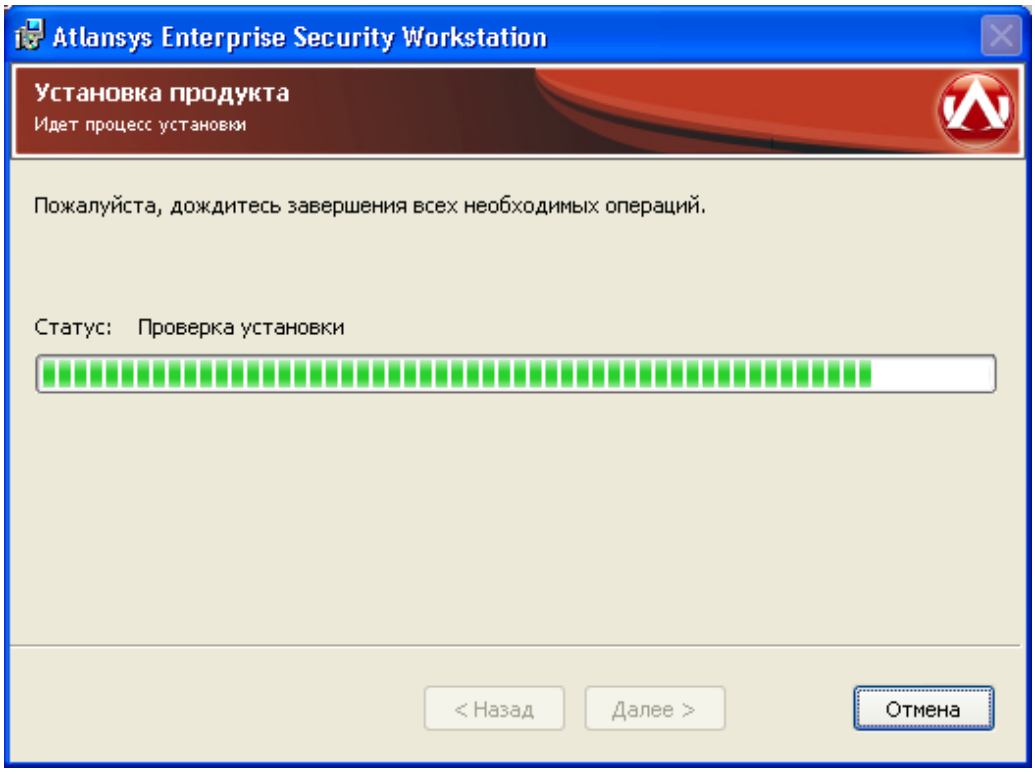

Рисунок 1.12. Процесс установки

3. Для окончания процесса установки необходимо нажать на кнопку «Завершить». (Рисунок 1.13)

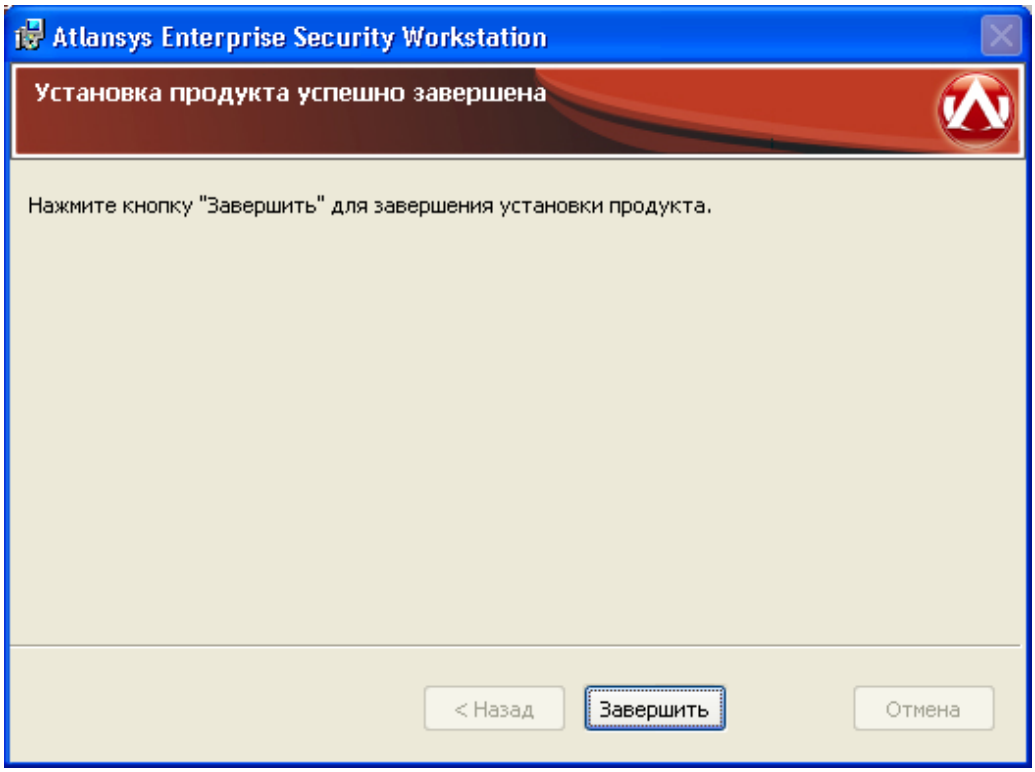

Рисунок 1.13. Завершение установки

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. 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-WS-(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-WS-(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. "**GROUP=group**" - имя группы пользователя по умолчанию. Данная группа будет использоваться для получения политик безопасности клиента, если пользователь не задан явно на Центре Управления.
4. "**PIDKEY=serial number**" - серийный номер продукта, который поставляется вместе с продуктом. Содержит пять полей из пяти символов (букв в верхнем регистре и цифр), разделенных символом дефиса '-'.

5. "**INSTALLDIR = path**" - путь к каталогу установки.

6. "**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:

   - CryptoArchive – криптоархивы (в том числе самораспаковывающиеся);
   - CryptoCont – криптоконтейнеры;
   - CryptoDisk – криптодиски.

7. "**CONTROL_CENTER = address**" - IP-адрес или доменное имя центра управления. Если этот параметр указан, то производится установка управляемого клиента.

Пример файла settings.cfg:

```
# Конфигурация для рабочей станции INSTALLDIR=C:\Program
    Files\Atlansys ESS\ CONTROL_CENTER=192.168.66.33
    ADDDEFAULT=CryptoArchive,CryptoCont PIDKEY=527LD-2TEST-ONLY4-VOVAN-SFXFL
    USERNAME=Василий Петров GROUP=sale COMPANYNAME=ООО Деревянная
    Скала
```

Эти же свойства можно задавать из командной строки. Например:

msiexec /i Atlansys-ESS-WS-(номер версии)-setup.msi INSTALLDIR = "c:\Program Files\Atlansys ESS" ADDDEFAULT = ALL PIDKEY = 527LD-4TEST-ONLY2-VOVAN-SFXFL USERNAME = "Василий Петров" GROUP = sale COMPANYNAME = "ООО Деревянная Скала"

1.4. Удаление программного обеспечения

Для удаления программного обеспечения необходимо выполнить следующие действия:

1. Закрыть все программы, использующие криптоконтейнеры и криптодиски.

2. С помощью Навигатора закрыть все открытые криптоконтейнеры и криптодиски.

Важно

После удаления программного обеспечения все криптоконтейнеры и криптодиски на данной рабочей станции будут недоступны. Криптоконтейнеры и криптодиски можно будет использовать на других рабочих станциях, где установлен продукт.

3. Запустить приложение Установка и удаление программ (Пуск / Панель управления / Установка и удаление программ), из списка программ выбрать Atlanasys Enterprise Security Workstation. (Рисунок 1.14)

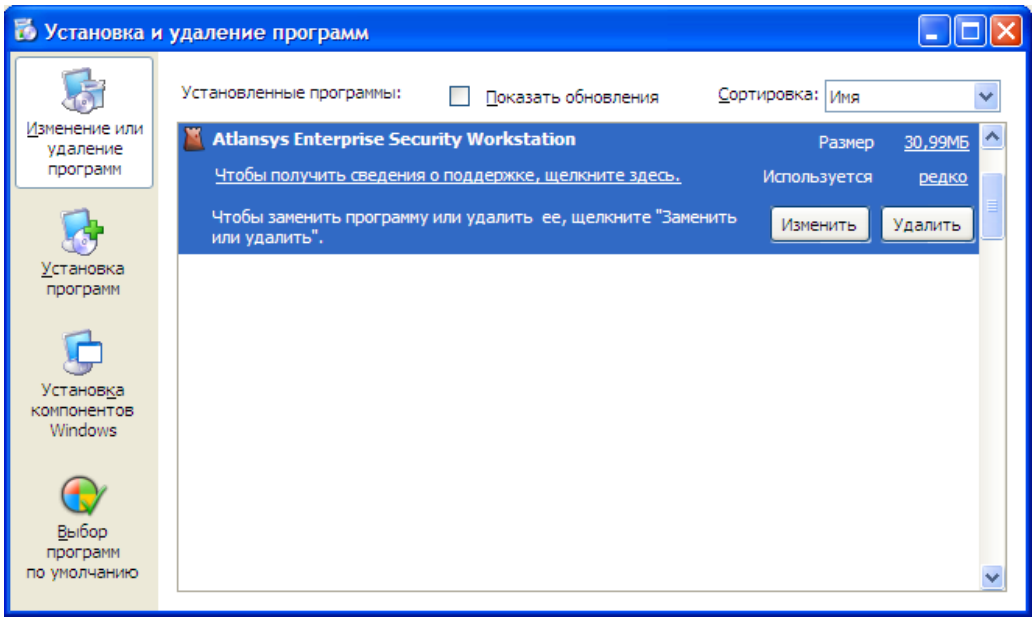

Рисунок 1.14. Окно Панели управления «Установка и удаление программ»

Для удаления Atlansys Enterprise Security System необходимо нажать на кнопку «Удалить». Появится окно для подтверждения запроса удаления. (Рисунок 1.15)

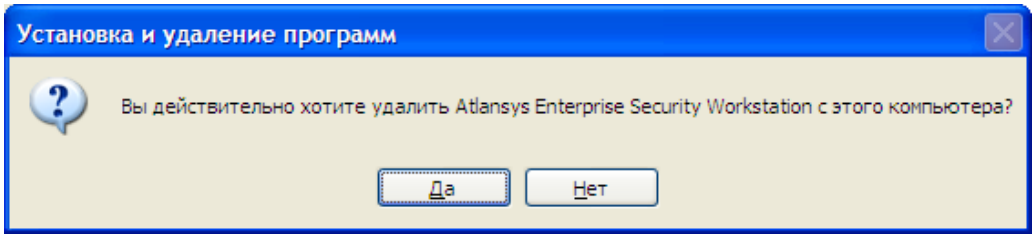

Рисунок 1.15. Окно запроса на удаление

Необходимо нажать на кнопку «Да», после чего начнется процесс удаления Atlansys Enterprise Security System с рабочей станции.

Глава 2. Atlansys Enterprise Security System Навигатор

2.1. Назначение

Atlansys Enterprise Security System Навигатор - это графический пользовательский интерфейс Atlansys Enterprise Security System. В нем сосредоточено управление над всем комплексом программ и подключаемых модулей, включенных в состав Atlansys Enterprise Security System.

2.2. Запуск программы

Запуск программы осуществляется либо через ярлык на рабочем столе компьютера, либо через выбор соответствующего пунта меню «**Пуск / Все программы / Atlansys / Enterprise Securiry Workstation / Atlansys Enterprise Security System Навигатор**»(Рисунок 2.1).

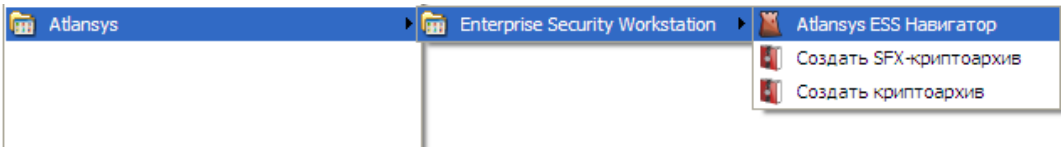

Рисунок 2.1. Запуск Atlansys Enterprise Security System Навигатор через меню Пуск

2.3. Интерфейс

После запуска Навигатора на экране появится главное окно программы. Главное окно состоит из следующих разделов:

1. Главное меню.

2. Кнопки для работы с соответствующими модулями Навигатора.

3. Техническая поддержка, содержащая ссылки и адрес электронной почты для обращения в службу технической поддержки.

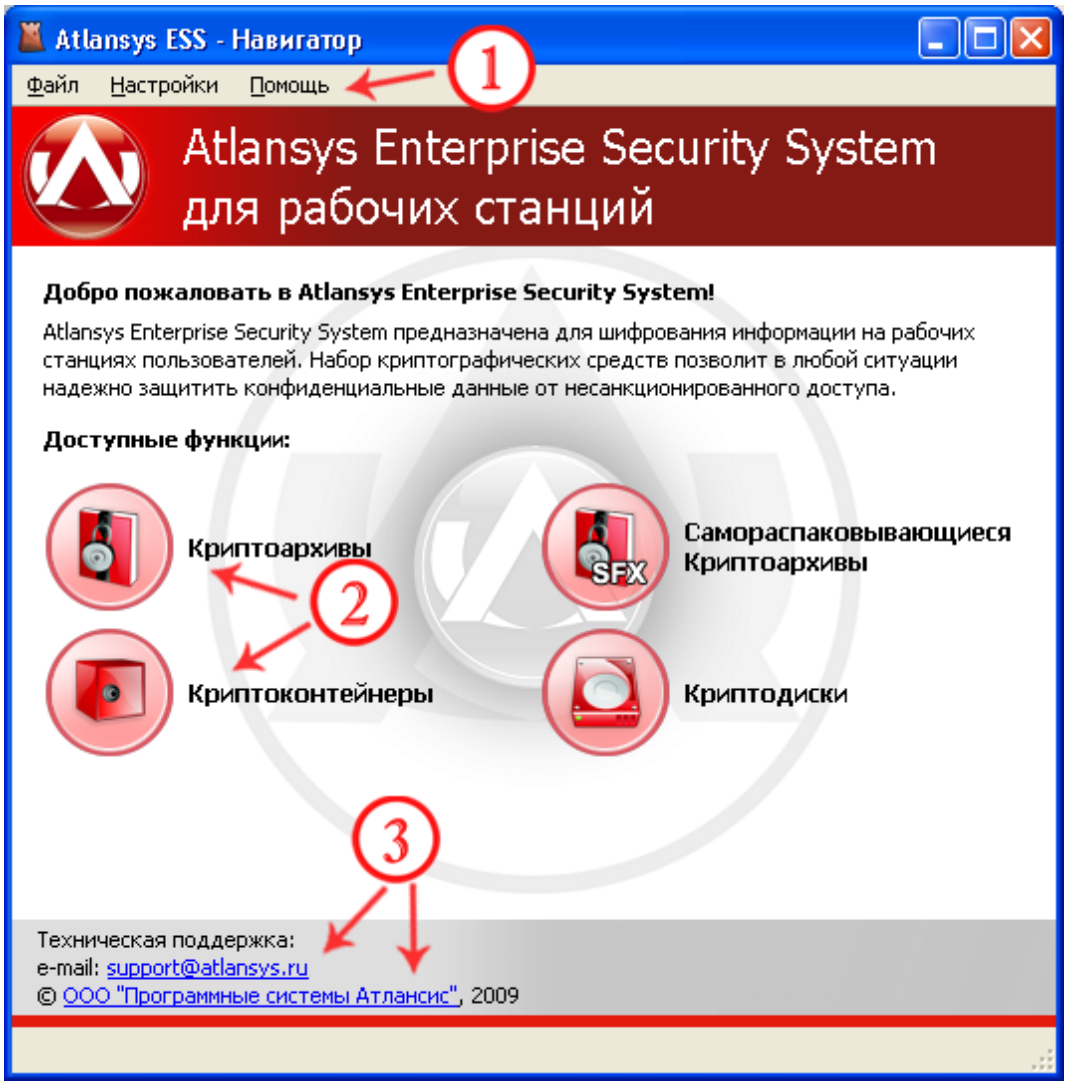

Рисунок 2.2. Главное окно Навигатора

1. Меню «Файл» содержит подменю:

   - «Создать» - для создания новых криптоконтейнеров, криптодисков, криптоархивов и самораспаковывающихся криптоархивов.
   - «Добавить» - для добавления существующих криптоконтейнеров и криптодисков, которые были созданы на других рабочих станциях.
   - «Шифровать» - для шифрования системного раздела.
   - «Закрыть все криптообъекты» - быстрое закрытие всех открытых криптоконтейнеров и криптодисков.
   - «Активировать красную кнопку» - для активации красной кнопки.
   - «Журнал событий» - окно для просмотра журнала регистрации событий, происходящих в системе.
   - «Выход» - для выхода из Навигатора.

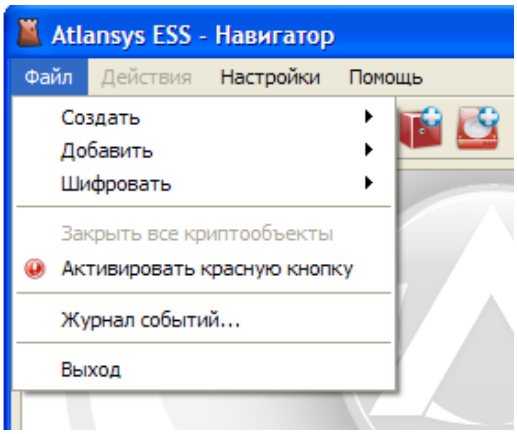

Рисунок 2.3. Меню «Файл»

2. Меню «Действия» активно, когда отображается список криптоконтейнеров и криптодисков, и содержит действия, которые можно осуществлять над текущим критообъектом.

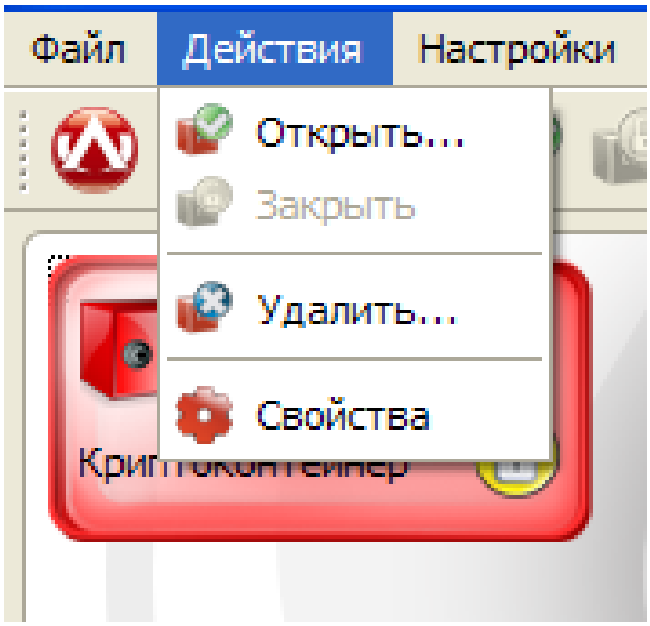

Рисунок 2.4. Меню «Действия»

3. Меню «Настройки» содержит подменю:

   - «Настройки...» - для вызова диалога настройки параметров работы приложения.
   - «Список плагинов...» - для отображания списка загруженных модулей (плагинов) Навигатора.
   - «Сворачивать в трей» - для сворачивания окна Навигатора в системный трей, при нажатии на кнопки закрытия или минимизации окна Навигатора, что позволяет обеспечить быстрый доступ к Навигатору без его повторной загрузки.
   - «Запускать при старте» - для запуска Навигатора при старте системы, при этом Навигатор сворачивается в системный трей.

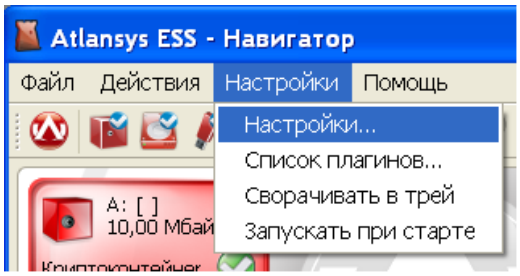

Рисунок 2.5. Меню «Настройки»

4. Меню «Справка» содержит пункты:

   - «Главное меню» - для перехода на главную страницу.
   - «Справка...» - для вызова справки по программе.
   - «Обновить лицензию...» - для ввода параметров новой лицензии.
   - «Зарегистрировать...» - для ввода регистрационных данных.
   - «О программе...» - для вызова диалога «О программе», в котором содержится информация о версии программы, параметрах регистрации, и доступных лицензиях.

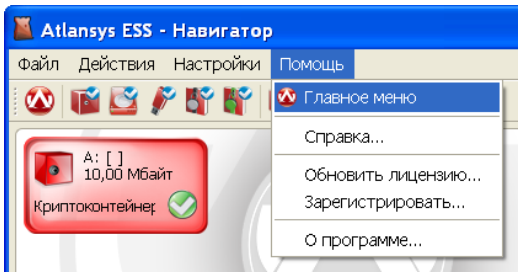

Рисунок 2.6. Меню «Помощь»

2.4. Настройки продукта

Для управления параметрами работы продукта используется диалог настроек, который вызывается через главное меню «Настройки / Настройки...». С левой стороны диалога расположена панель доступных для управления модулей, 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. «Язык интерфейса» - выбор языка пользовательского интерфейса. Набор языков может отличаться в зависимости от локализации продукта.

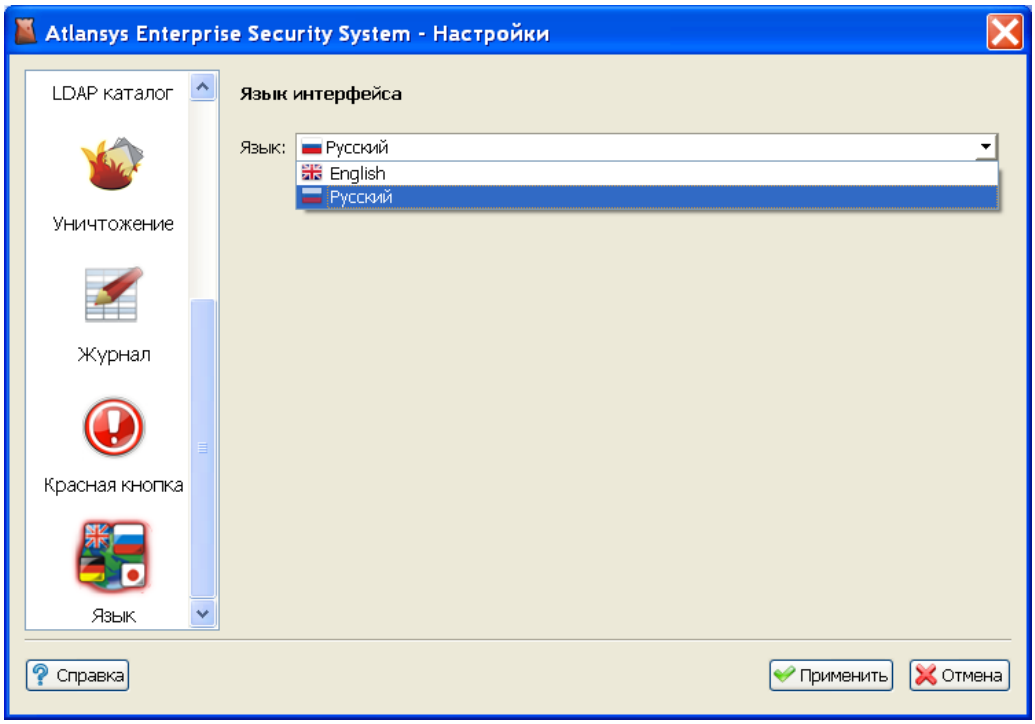

Рисунок 2.7. Язык

2. «Создание криптоархива» - задаёт формат создаваемого криптоархива. Возможны следующие форматы криптоархива:

   - «Формат криптоархива Atlansys» - создание криптоархива в формате Atlansys. Доступны следующие криптосхемы: «ГОСТ 28147-89», «Blowfish», «AES 256».

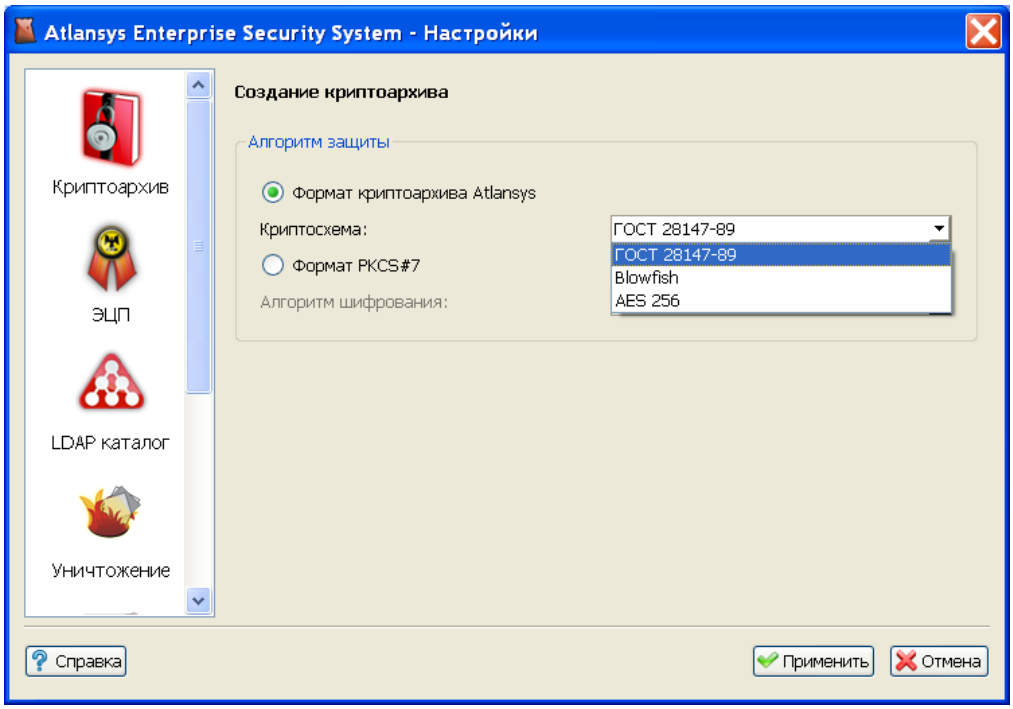

Рисунок 2.8. Настройки создания криптоархива - Формат криптоархива Atlansys

- «Формат PKCS7» - создание криптоархива по криптографическому стандарту PKCS7. Список алгоритмов шифрования содержит алгоритмы, поддерживаемые установленными в системе криптопровайдерами.

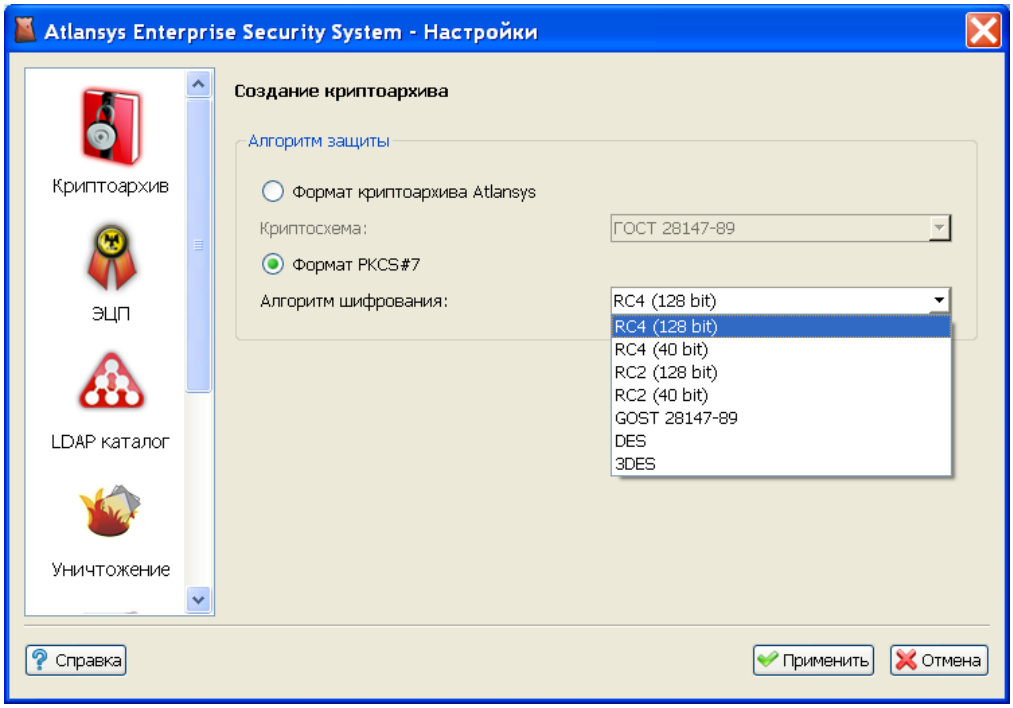

Рисунок 2.9. Настройки создания криптоархива - Формат PKCS7

3. «Настройка ЭЦП» - настройка электронной цифровой подписи. На странице «Электронная цифровая подпись» необходимо выбрать сертификат ЭЦП, формат файла ЭЦП и алгоритм хеширования. Выбор сертификата ЭЦП осуществляется по нажатии на кнопку «...».

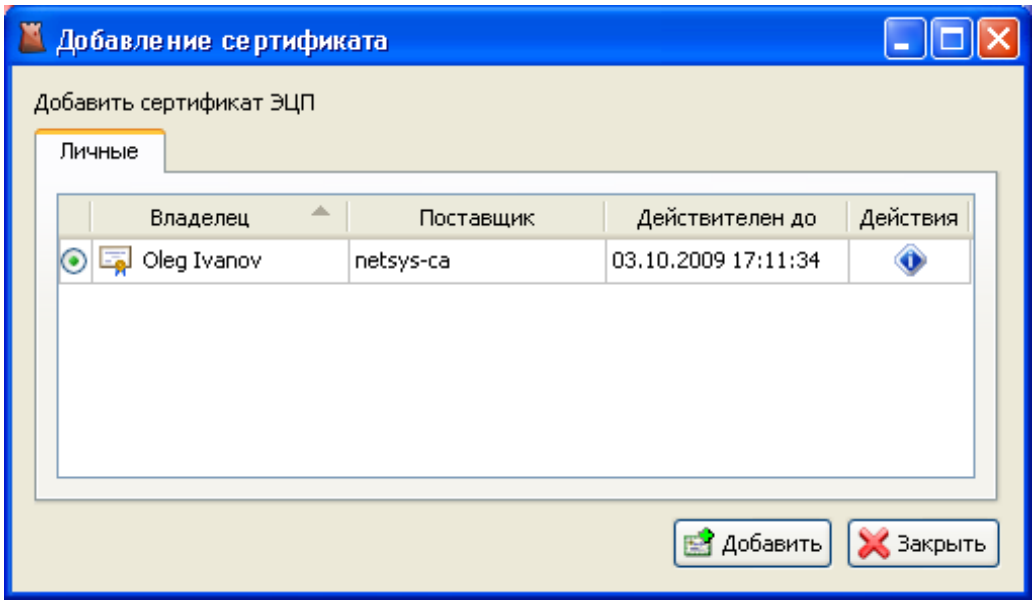

Рисунок 2.10. Диалог «Добавлнение сертификата»

Доступны следующие форматы файла ЭЦП:

- «Формат файла подписи Atlansys» - создание файла ЭЦП в формате Atlansys.

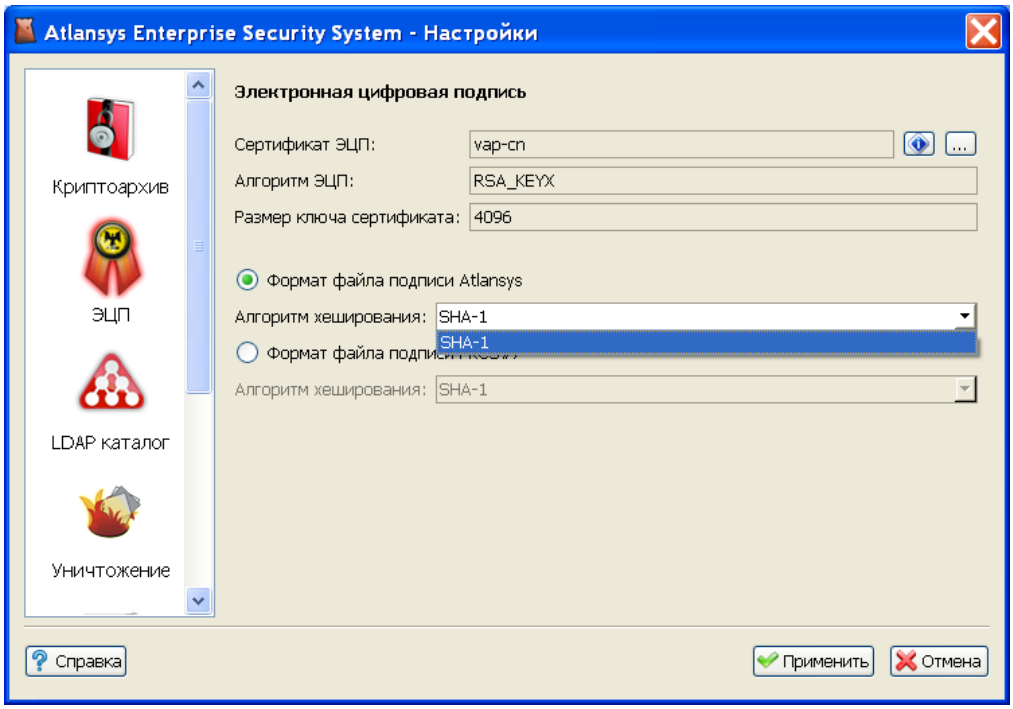

Рисунок 2.11. Настройки ЭЦП - Формат файла подписи Atlansys

- «Формат файла подписи PKCS7» - создание файла подписи по криптографическому стандарту PKCS7. Список алгоритов хеширования берётся у криптопровайдера, который поддерживает сертификат ЭЦП.

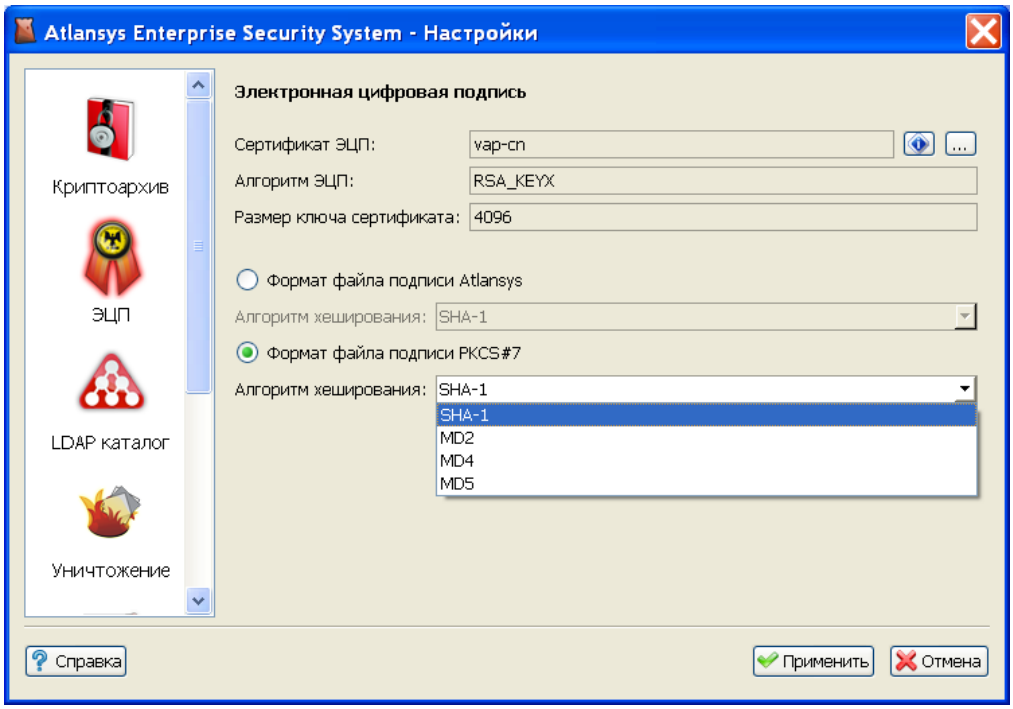

Рисунок 2.12. Настройки ЭЦП - Формат файла подписи PKCS7

4. «Регистрация событий» - задаёт параметры регистрации сообщений в локальный файл журнала и в локальной базе данных.

   - «Файл журнала» - задаётся размер файла журнала.

   - «Локальная база данных лог-сообщений» - задаётся путь к файлу базы данных, уровень лога и размер файла базы данных. Рекомендуется оставить параметр «Путь к файлу» по умолчанию. База данных состоит из одного файла, который создаётся автоматически при старте системы, если по указанному пути он не был найден.

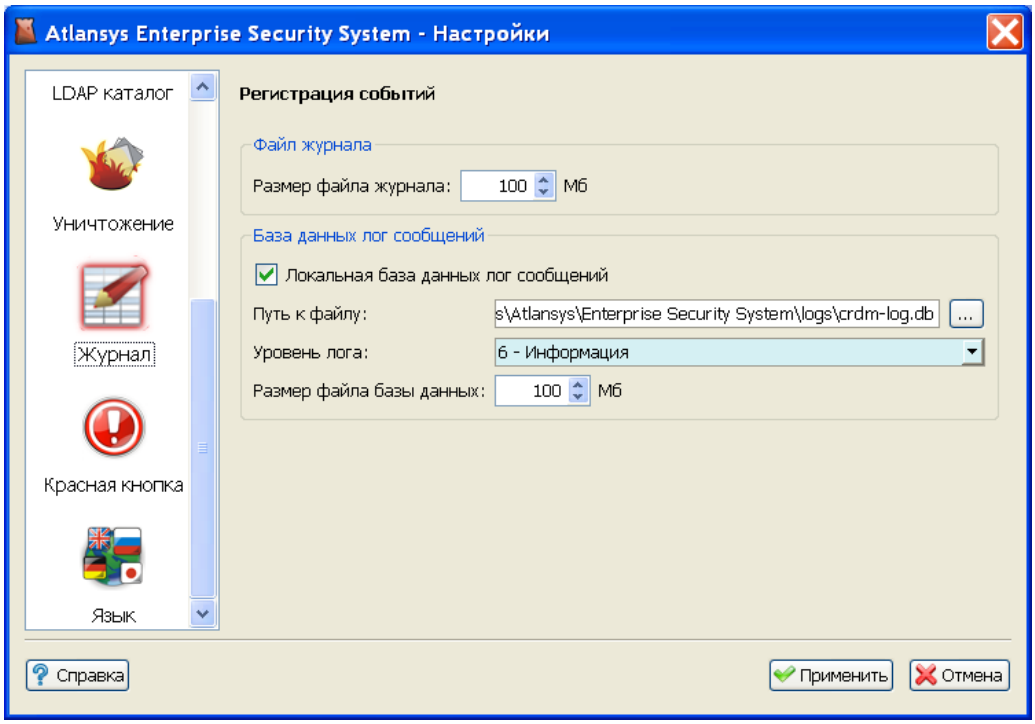

Рисунок 2.13. Регистрация событий

5. «Уничтожение данных» - задаёт предпочитаемый алгоритм гарантированного удаления данных без возможности последующего восстановления. Выбранный алгоритм будет применяется для уничтожения файлов через контекстное меню Проводника Windows.

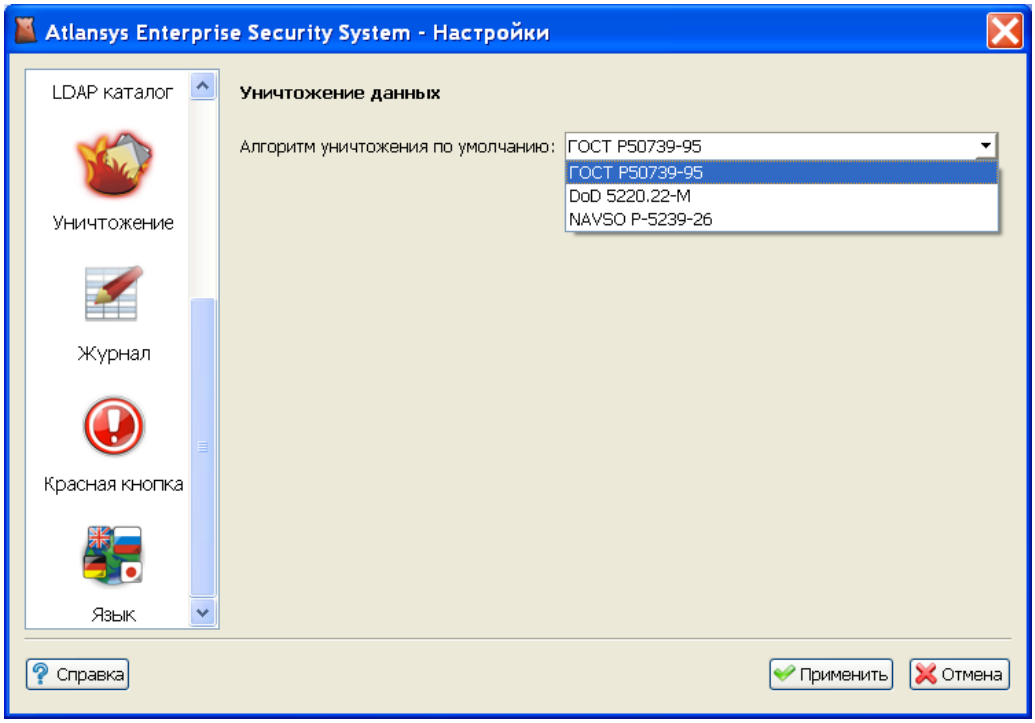

Рисунок 2.14. Уничтожение данных

6. Механизм «Красная кнопка» подразумевает выполнение ряда действий как над криптообъектами, так и над обычными файлами и каталогами файловой системы, предназначенное прежде всего для предот-

вращения несанкционированного доступа к важной (секретной) информации в случае форс-мажорных обстоятельств. Настройки красной кнопки позволяют гибко управлять этим механизмом.

Включение механизма «Красная кнопка» осуществляется выбором пункта «Включить красную кнопку». После этого появляется возможность выбрать способы активации - при помощи горячих клавиш или при вводе специально заданного пароля при открытии криптообъектов (для этого необходимо, чтобы хотя бы один криптообъект имел защиту паролем).

Замечание

Если компьютер подключен к Центру управления, и настройки красной кнопки неактивны, значит, что они заданы администратором Центра управления. В этом случае изменить их невозможно.

Кроме способа активации, также можно настроить действия, выполняемые при активации красной кнопки. «Закрыть все криптообъекты» - все открытые криптообъекты будут немедленно закрыты. «Уничтожить все криптообъекты» - уничтожает все криптообъекты, находящиеся в списке Навигатора.

Важно

После уничтожения криптообъектов, информацию с них восстановить будет невозможно.

Также можно выбрать уничтожение произвольных файлов. Для этого следует на вкладке «Уничтожение файлов» нажать кнопку «Настроить список», и в появившемся диалоге выбрать список файлов и каталогов для уничтожения.

Важно

Уничтожение файлов - необратимая операция, восстановить их будет невозможно.

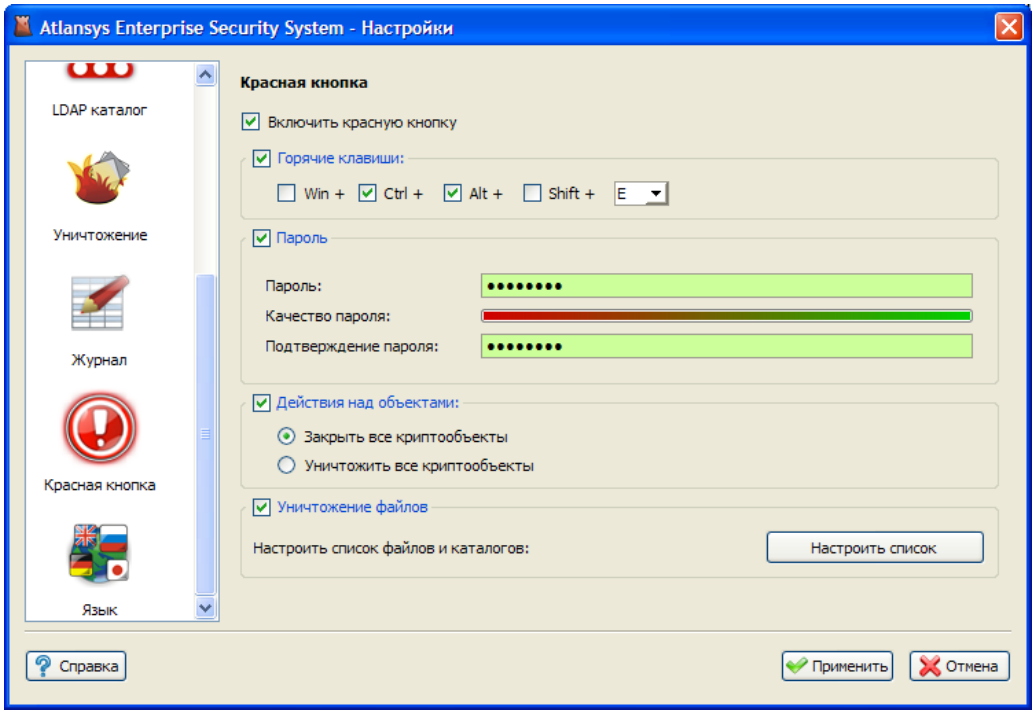

Рисунок 2.15. Настройка Красной кнопки

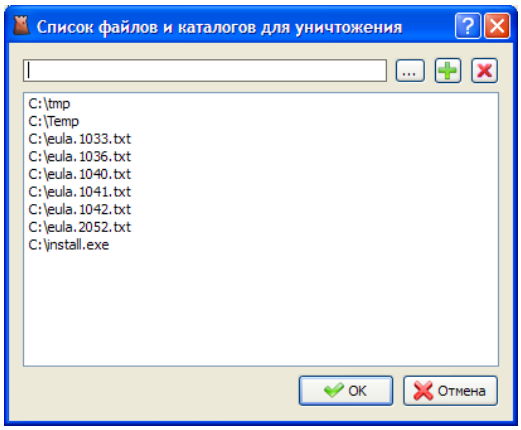

Рисунок 2.16. Настройка списка файлов и каталогов для удаления

После сохранения настроек, активировать красную кнопку можно при помощи горячих клавиш (для этого необходимо, чтобы Навигатор был запущен) или при помощи ввода специального пароля на открытие криптообъекта (в этом случае механизм активируется без дополнительного вопроса).

7. «LDAP каталог» - позволяет задавать список каталогов LDAP для поиска сертификатов защиты при создании криптообъектов. Редактируемый список LDAP каталогов на странице настроек позволяет добавлять, удалять и редактировать LDAP каталоги, используемые для поиска сертификатов.

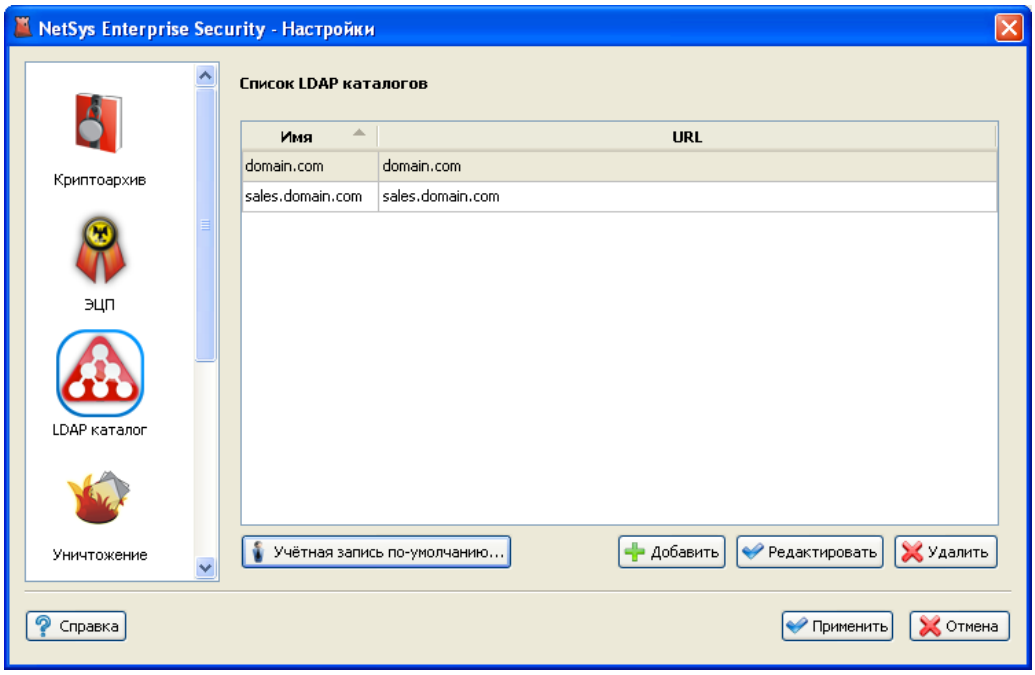

Рисунок 2.17. Настройка LDAP каталогов

Для добавления нового LDAP каталога нажмите кнопку «Добавить» и введите параметры в диалоге.

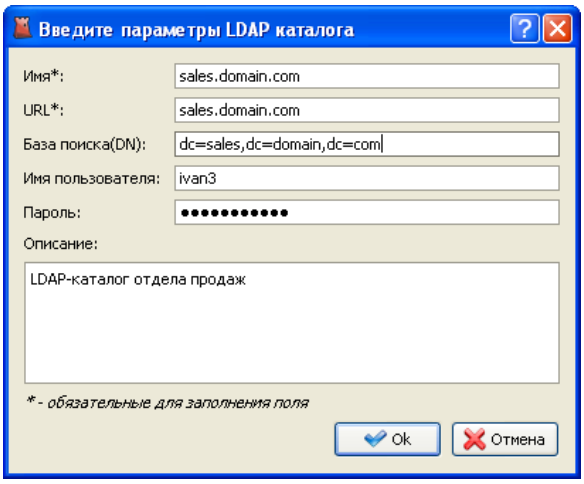

Рисунок 2.18. Добавление LDAP каталога

Необходимо указать условное имя каталога и его URL. Кроме того можно указать базовый путь в каталоге для поиска сертификатов, аккаунт для доступа к каталогу и произвольное описание. Если не указывать логин и пароль для доступа к каталогу, то будет взят общий для всех каталогов аккаунт по умолчанию, заданный на странице настроек. Если аккаунт по умолчанию не задан, будет происходить аутентификация по системной учётной записи текущего пользователя.

Если клиент подключён к Центру Управления, то могут применяться настройки LDAP каталогов, указанные администратором. Так же, администратор может разрешить использование локальных настроек LDAP каталогов.

2.5. Автоматическое открытие криптоконтейнеров и криптодисков

Автоматическое открытие криптообъектов служит для максимально удобного использования криптоконтейнеров и криптодисков. При каждом входе пользователя в операционную систему будет производиться автоматическое открытие всех доступных криптодисков и криптоконтейнеров, у которых установлен признак автоматического открытия.

При защите криптоконтейнера или криптодиска сертификатом, автоматическое открытие будет работать только, если в системе имеется хотя бы один закрытый ключ для сертификатов, которыми он защищен. При защите с помощью пароля при автоматическом открытии криптоконтейнера или криптодиска откроется диалог, в котором необходимо ввести пароль и, при необходимости, выбрать букву диска.

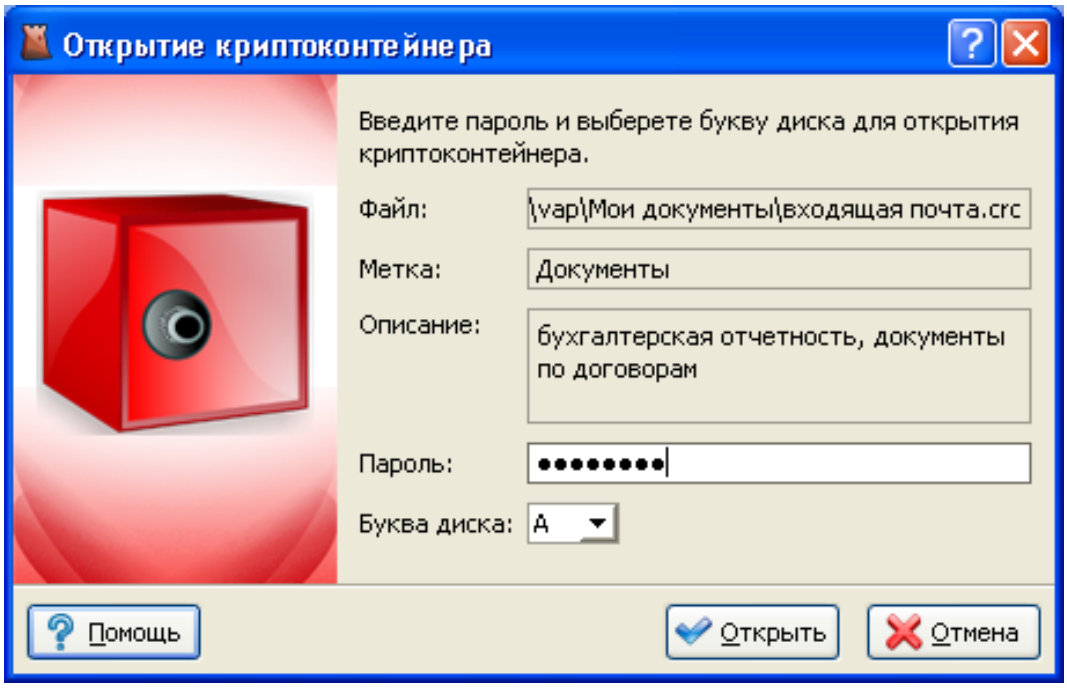

Рисунок 2.19. Автооткрытие криптоконтейнера

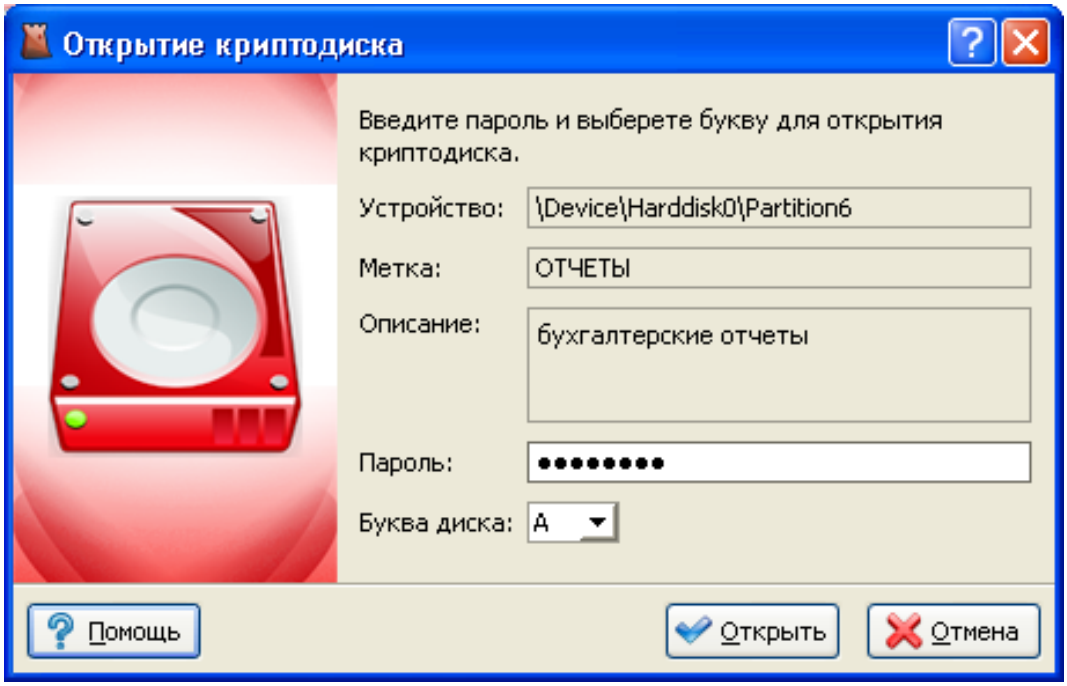

Рисунок 2.20. Автооткрытие криптодиска

В процессе автоматического открытия криптообъектов в системном трее появится значок диалога автооткрытия, в котором отображаются все криптообъекты, подлежащие автооткрытию с отображением их состояния.

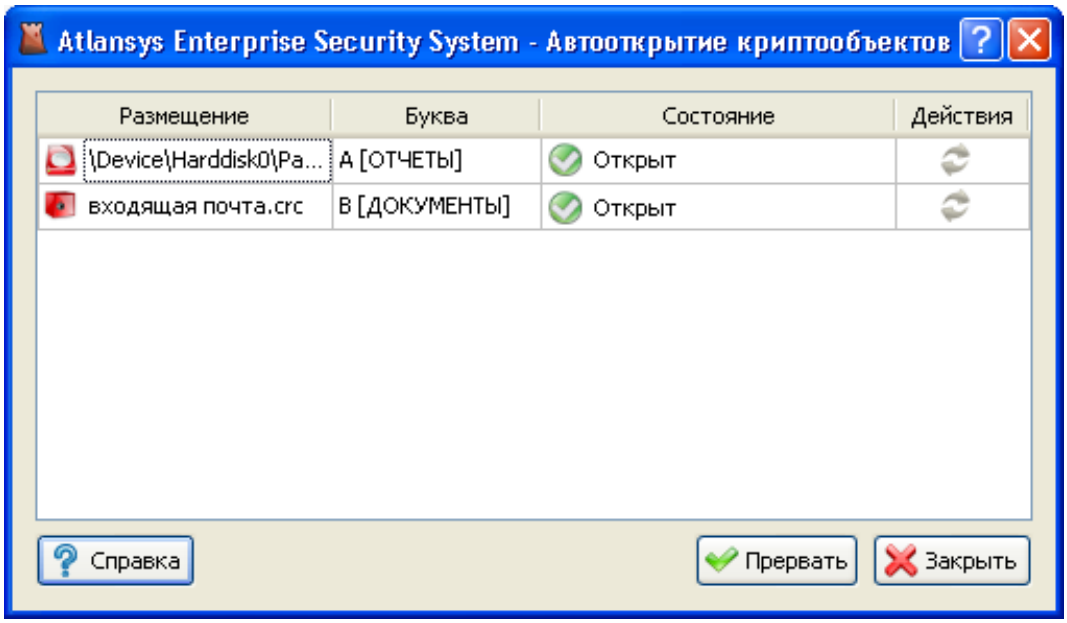

Рисунок 2.21. Диалог автооткрытия криптообъектов

Замечание

Криптообъекты, которые не имеют свойств автоматического открытия, в дальнейшем можно открыть стандартными средствами Навигатора, как описано в разделах по работе с криптоконтейнерами и криптодисками.

2.6. Подключаемые модули

В зависимости от комплекта поставки, Atlansys Enterprise Security System может поддерживать разный набор функций. Таким образом, при необходимости включения новой функциональности не требуется приобретать и переустанавливать все программное обеспечение, а нужно лишь добавить новый модуль (о вопросах приобретения дополнительных подключаемых модулей смотрите пункт «Техническая поддержка»).

Подключаемый модуль представляет собой отдельный файл (динамическую бибилиотеку), который необходимо поместить в каталог **plugins** в рабочем каталоге программы. Также вместе с подключаемым модулем поставляется файл перевода интерфейса на русский язык, который следует поместить в каталог **tr** рабочего каталога программы.

В настоящее время поддерживаются следующие подключаемые модули:

- Модуль работы с криптоконтейнерами (смотрите главу «Работа с криптоконтейнерами»).
- Модуль работы с криптодисками (смотрите главу «Работа с криптодисками»).

Глава 3. Работа с криптоконтейнерами

3.1. Введение

В данном разделе описывается работа с защищенными криптоконтейнерами, их создание, добавление, удаление и основные действия над ними. Криптоконтейнер представляет собой файл, содержащий полностью зашифрованный образ файловой системы раздела, который можно подключить (подмонтировать) в систему в виде диска. При этом все приложения и служебные программы Windows будут воспринимать его как полноценное дисковое устройство. Пока криптоконтейнер не открыт, его содержимое невозможно прочитать, так как оно зашифровано криптостойким алгоритмом, поэтому файл криптоконтейнера можно безопасно копировать на различные носители, передавать по сети.

Доступ к криптоконтейнеру может быть защищен с помощью пароля и/или набора сертификатов. Выбор типа защиты делается исходя из необходимости использования криптоконтейнера несколькими пользователями, наличия в организации центра сертификатов.

3.2. Создание криптоконтейнера

Чтобы создать криптоконтейнер, необходимо в Atlansys Enterprise Security System Навигаторе выбрать в главном меню пункты «Файл» / «Создать» / «Криптоконтейнер...»

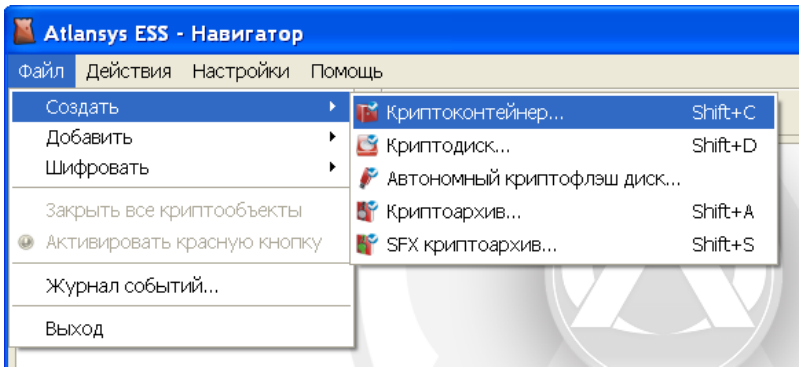

Рисунок 3.1. Меню «Файл» / «Создать»

После чего запустится Мастер создания криптоконтейнеров. В появившемся окне необходимо задать имя файла криптоконтейнера, либо выбрать файл через диалог выбора файла, который вызывается при нажатии на кнопку «...».

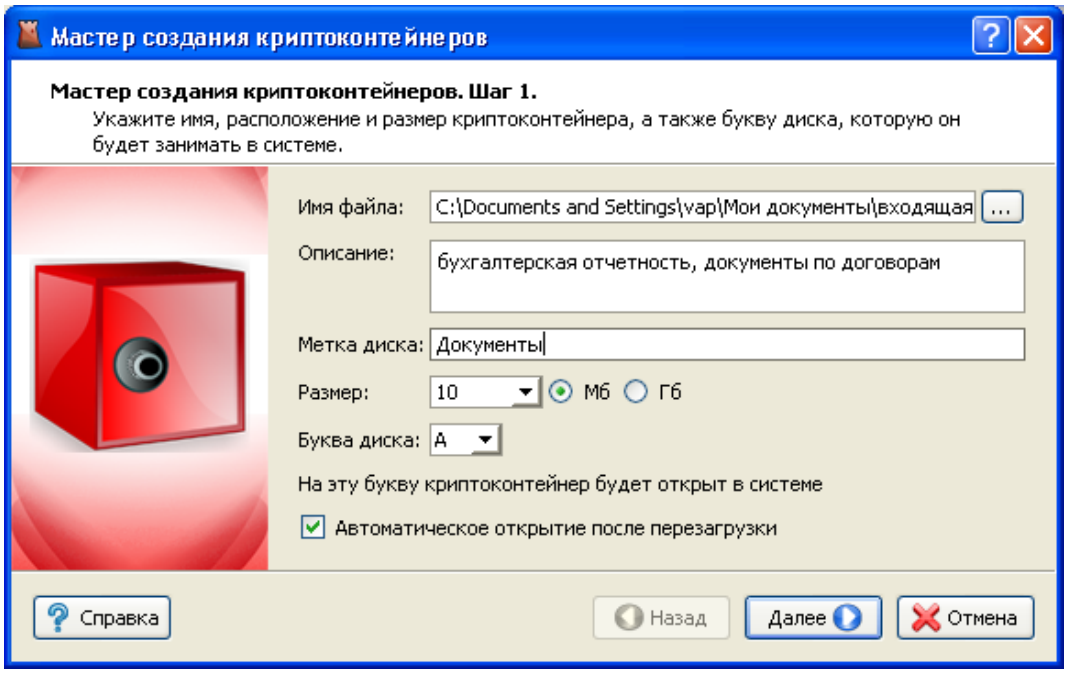

Рисунок 3.2. Мастер создания криптоконтейнеров.

Рекомендуется заполнить поле описания криптоконтейнера, в котором записывается назначение или краткое описание содержимого. Рекомендуется задать метку диска, которая в дальнейшем будет отображаться в системе, по ней можно будет легко отличать данный криптоконтейнер от других дисков.

Необходимо задать размер создаваемого криптоконтейнера. Его можно ввести вручную, либо выбрать из предложенного списка. Переключатель Мб/Гб переключает выбор размера криптоконтейнера в мегабайтах или гигабайтах. Максимальный размер криптоконтейнера ограничен размером свободного места носителя, на котором он создается.

Необходимо выбрать букву диска из списка свободных, на которую будет подмонтирован создаваемый криптоконтейнер.

При необходимости автоматического открытия криптоконтейнера при старте системы следует оставить выбранным чекбокс автоматического открытия.

После того, как необходимые поля будут заполнены, разблокируется кнопка «Далее», после нажатия которой Мастер создания криптоконтейнеров перейдет на шаг выбора типа защиты.

На данном шаге необходимо выбрать способы защиты криптоконтейнера. Возможны различные комбинации защиты:

- с помощью пароля;
- с помощью одного сертификата или набора сертификатов;
- с помощью пароля и сертификатов одновременно, в этом случае, при отсутствии необходимого сертификата, для открытия криптоконтейнера можно будет использовать пароль.

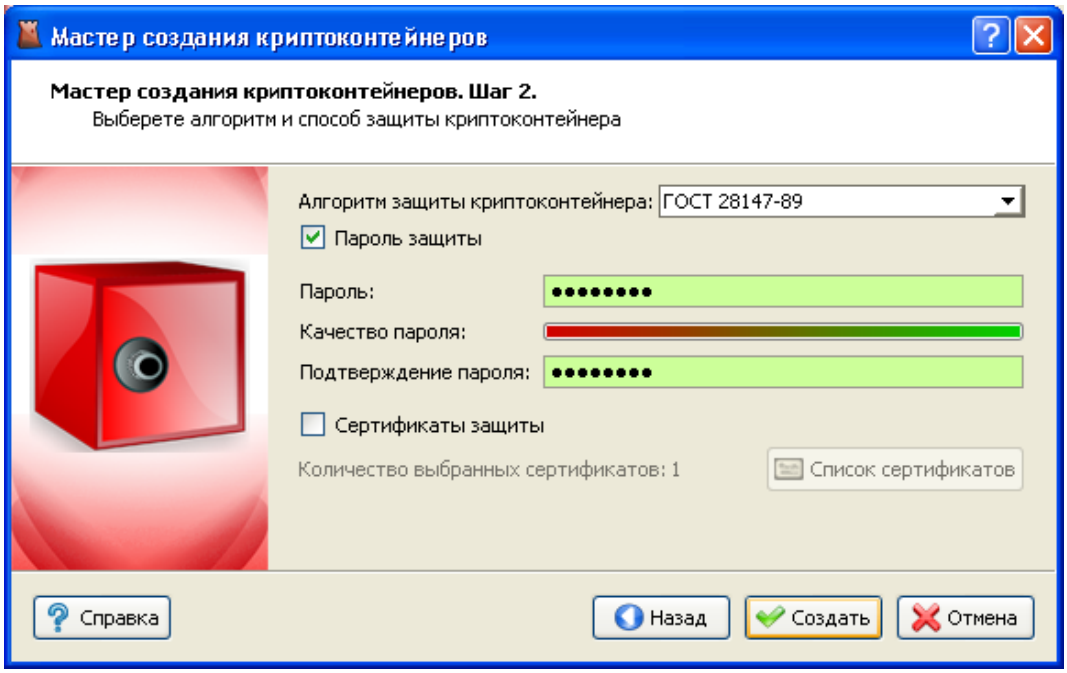

Рисунок 3.3. Мастер создания криптоконтейнеров. Способы защиты.

Для защиты с помощью пароля необходимо выбрать чекбокс «Пароль защиты» и ввести пароль в поля «Пароль» и «Подтверждение пароля». При вводе пароля в поле «Качество пароля» будет отображаться его качественные характеристики по стойкости к подбору. Качественный пароль должен содержать не менее восьми символов из букв в верхнем и нижнем регистре, минимум одну цифру и минимум один спецсимвол. При достижении необходимого качества пароля поле ввода окрашивается в зеленый цвет, после чего необходимо повторить ввод пароля в поле «Подтверждение пароля». Когда оба пароля совпадут, оба поля ввода пароля окрасятся в зеленый цвет.

При использовании сертификатов для защиты данных необходимо выбрать чекбокс "Сертификаты защиты" и нажать кнопку "Список сертификатов". В появившемся диалоге выбираются сертификаты для защиты криптоконтейнера. Доступ к данным криптоконтейнера будет возможен только при наличии у пользователя одного из сертификатов защиты с закрытым ключом. После закрытия диалога со списком сертификатов в окне Мастера создания криптоконтейнеров отобразится количество выбранных сертификатов.

Замечание

Как минимум один из выбранных сертификатов должен содержать закрытый ключ, с помощью которого расшифровывается содержимое криптоконтейнера. В противном случае доступ к содержимому криптоконтейнера на данной рабочей станции будет невозможен.

После выбора способов защиты необходимо нажать кнопку «Создать», после чего появится окно создания криптоконтейнера, в котором отображается прогресс создания, количество прошедшего времени с начала создания криптоконтейнера, прогноз оставшегося времени. После успешного завершения создания криптоконтейнера появится сообщение «Криптоконтейнер успешно создан». Затем необходимо нажать на кнопку «Готово», после чего созданный криптоконтейнер появится в окне Навигатора и запустится Проводник Windows на открытом криптоконтейнере.

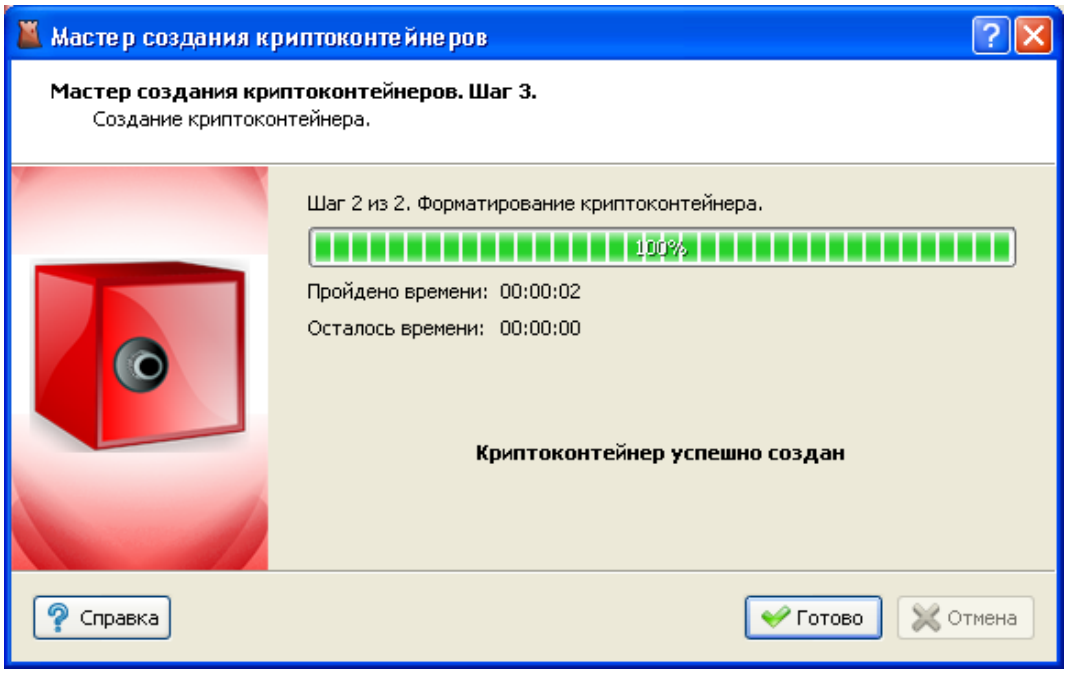

Рисунок 3.4. Мастер создания криптоконтейнеров. Прогресс создания.

3.3. Добавление криптоконтейнера

Для добавления криптоконтейнера, созданного на другой рабочей станции в список Навигатора, необходимо выбрать в Главном меню пункт «Файл» / «Добавить» / «Криптоконтейнер».

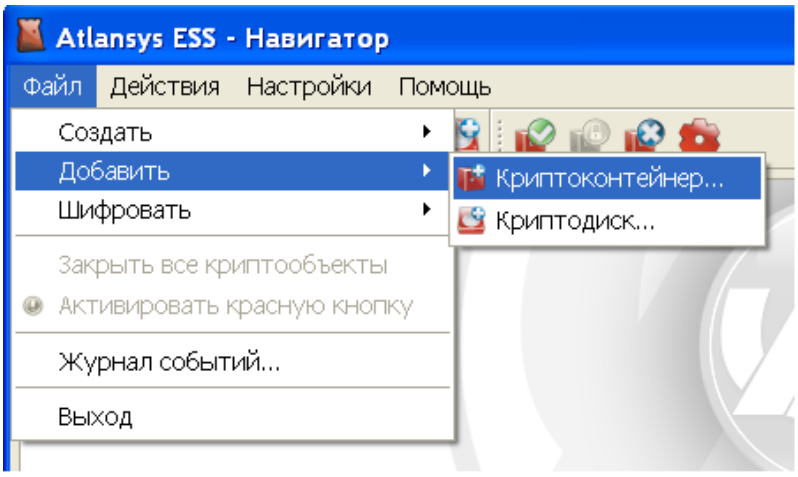

Рисунок 3.5. Меню «Файл» / «Добавить»

В появившемся окне Мастера добавления криптоконтейнеров выбрать файл криптоконтейнера, после чего его параметры отобразятся в окне Мастера. Необходимо выбрать букву диска, под которой криптоконтейнер будет монтироваться в систему. При необходимости автоматического открытия криптоконтейнера после перезагрузки системы, следует оставить выбранным чекбокс автоматического открытия. Затем нажать кнопку «Добавить», после чего криптоконтейнер добавится в список Навигатора. Если криптоконтейнер защищен сертификатом и его закрытый ключ имеется в системе, криптоконтейнер автоматически откроется и запустится Проводник Windows, открытый на соответствующем диске.

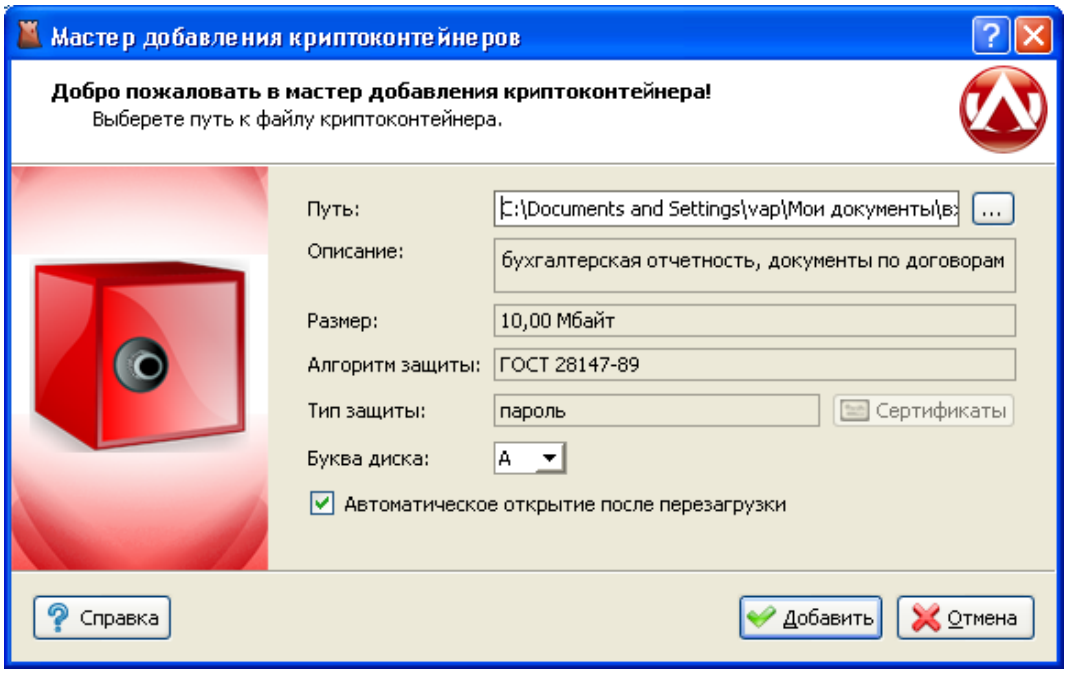

Рисунок 3.6. Мастер добавления криптоконтейнеров

Если криптоконтейнер защищен паролем, то автоматически откроется новое окно «Открытие криптоконтейнера», в котором необходимо ввести пароль для доступа к криптоконтейнеру, который использовался при его создании. При необходимости можно изменить букву диска.

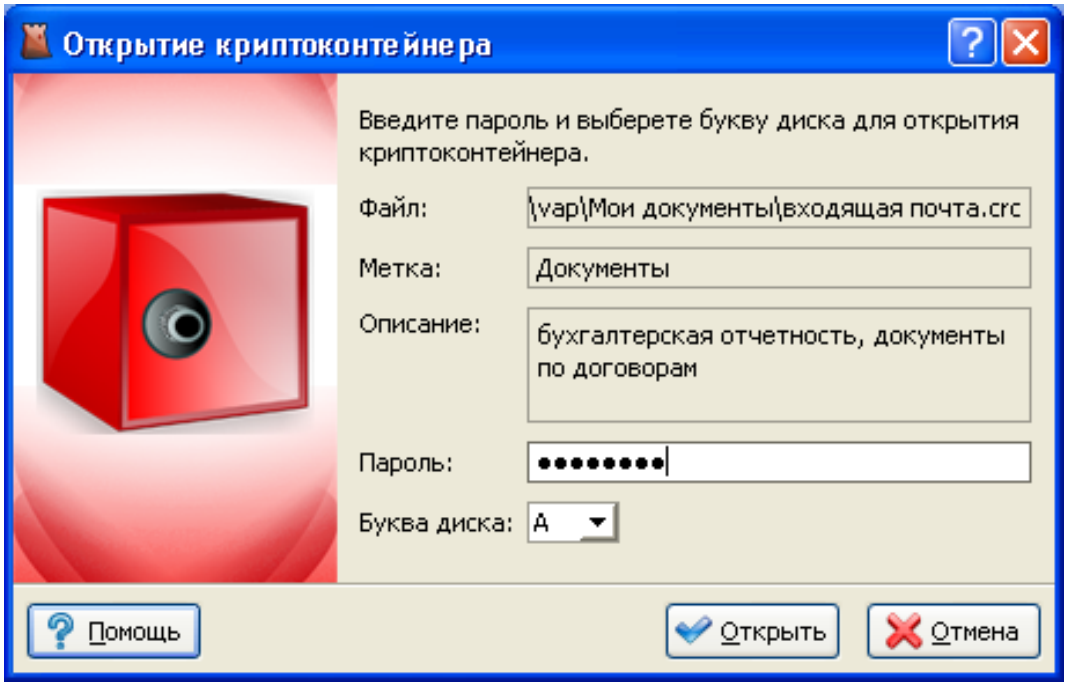

Рисунок 3.7. Диалог открытия криптоконтейнера

3.4. Работа с криптоконтейнерами

Все криптоконтейнеры и криптодиски отображаются в списке криптообъектов Навигатора. Текущий активный криптообъект выделяется рамкой, при этом его параметры выводятся в нижней части окна Навигатора. Для криптоконтейнеров отображается следующая информация:

- имя файла криптоконтейнера;
- дата создания;
- версия криптоконтейнера;
- алгоритм защиты данных;
- тип защиты: пароль, сертификат, либо пароль + сертификат. Если криптоконтейнер защищен сертификатами, то список сертификатов можно просмотреть, нажав на кнопку списка сертификатов. В списке сертификатов криптообъекта отображаются все сертификаты, которым защищен криптоконтейнер, для каждого сертификата отображается состояние доступности. Криптоконтейнер может быть открыт, если доступен хотя бы один сертификат, имеющий закрытый ключ.

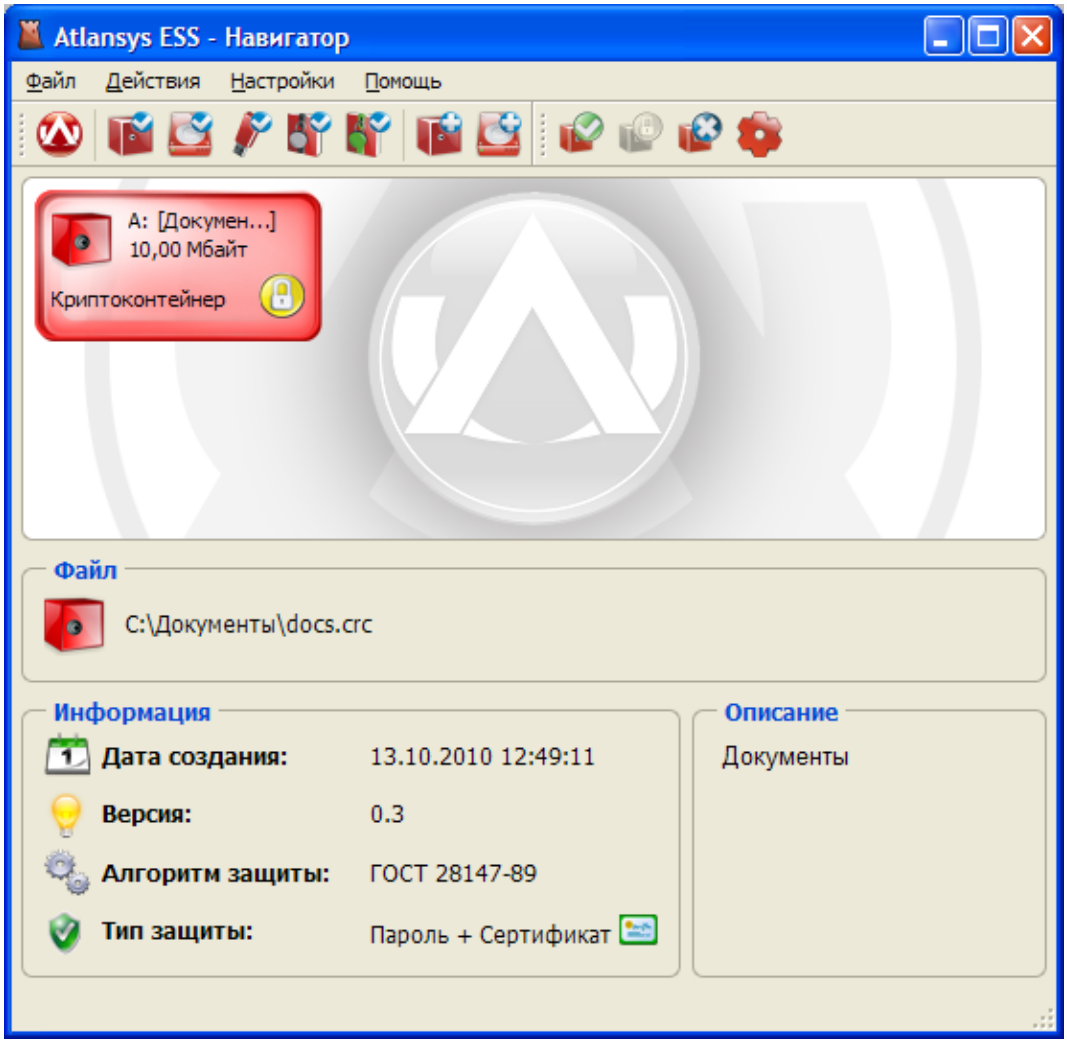

Рисунок 3.8. Список криптоконтейнеров и криптодисков

Для того, чтобы закрыть криптоконтейнер, необходимо закрыть все работающие с ним приложения, выделить его в списке Навигатора, затем в главном меню выбрать пункт «Действия» / «Закрыть». Либо в контекстном меню криптоконтейнера выбрать пункт «Закрыть». Либо нажать кнопку «Закрыть» на панели инструментов.

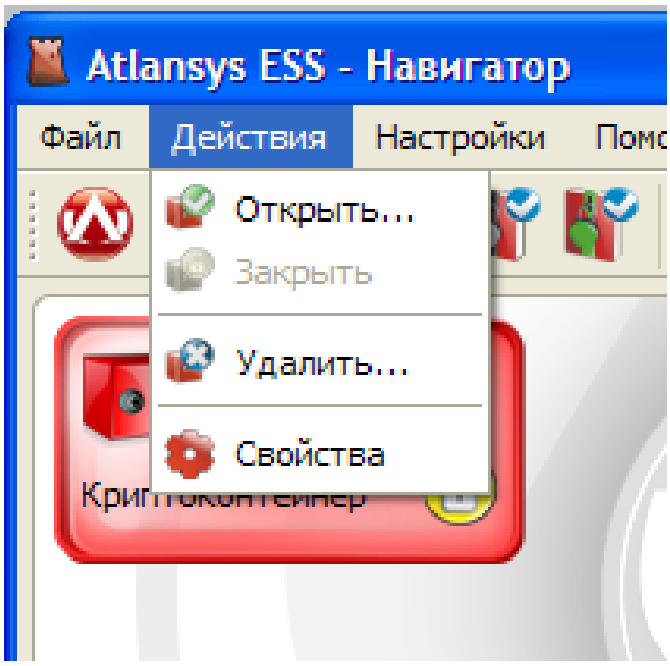

Рисунок 3.9. Меню «Действия»

Чтобы открыть закрытый криптоконтейнер, необходимо выделить криптоконтейнер в списке, в главном меню выбрать пункт «Действия»/«Открыть». Либо в контекстном меню выбрать пункт «Открыть».

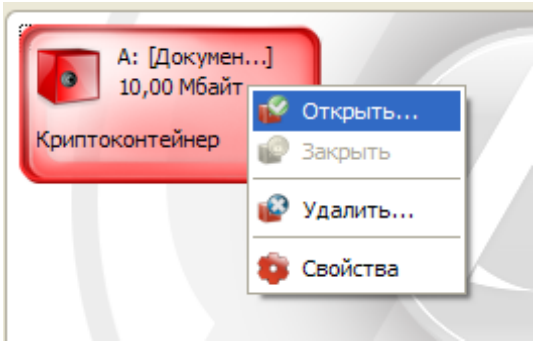

Рисунок 3.10. Контекстное меню криптоконтейнера

Либо нажать кнопку «Открыть» на панели инструментов. Двойной щелчок мыши на криптоконтейнере также открывает и запускает Проводник.

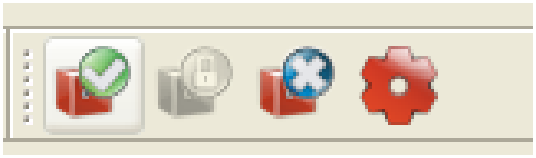

Рисунок 3.11. Панель инструментов, кнопка «Открыть»

Если криптоконтейнер защищен сертификатами, и в системе имеется закрытый ключ хотя бы к одному сертификату, криптоконтейнер откроется, и на нем автоматически запустится Проводник Windows. Если криптоконтейнер защищен паролем, то откроется диалог открытия криптоконтейнера, в поле «Пароль» которого необходимо ввести пароль, который использовался при создании криптоконтейнера, при необходимости можно поменять букву диска, под которой криптоконтейнер будет виден в системе, и нажать кнопку «Открыть».

3.5. Удаление криптоконтейнера

При удалении криптоконтейнера сначала необходимо закрыть все приложения, которые с ним работают, затем закрыть криптоконтейнер. Далее, в главном меню выбрать пункт «Действия» / «Удалить», либо выбрать в контекстном меню пункт «Удалить», либо в панели инструментов нажать на кнопку «Удалить».

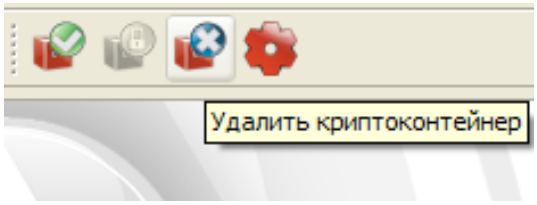

Рисунок 3.12. Панель инструментов, кнопка «Удалить»

После этого появится окно Мастера удаления криптоконтейнеров, в котором необходимо выбрать один из способов удаления криптоконтейнера:

- *Удалить криптоконтейнер из списка.* Удаляет криптоконтейнер только из списка Навигатора. При этом файл криптоконтейнера и все данные, содержащиеся в нем, не удаляются. Данный способ может использоваться при переносе криптоконтейнера на другую рабочую станцию.

- *Удалить криптоконтейнер.* В файле криптоконтейнера стирается ключевая информация и заголовок, затем файл удаляется. Так как вся информация в криптоконтейнере зашифрована, то удаление ключевой информации полностью блокирует доступ к данным, содержащимся в криптоконтейнере. Это самый быстрый способ удаления криптоконтейнера, но он не защищает от дешифрования данных с помощью прямого перебора ключей.

- *Уничтожить криптоконтейнер.* Для гарантированного уничтожения данных помимо удаления ключевой информации, все данные в криптоконтейнере уничтожаются одним из алгоритмов гарантированного удаления данных.

  - Алгоритм по стандарту ГОСТ Р 50739-95 имеет два цикла записи псевдослучайных значений.

  - Алгоритм по стандарту DoD 5220.22M имеет два цикла записи псевдослучайных значений и один цикл записи фиксированных значений.

  - Алгоритм по стандарту NAVSO P-5239-26 имеет два цикла записи фиксированных значений и один цикл записи псевдослучайных значений.

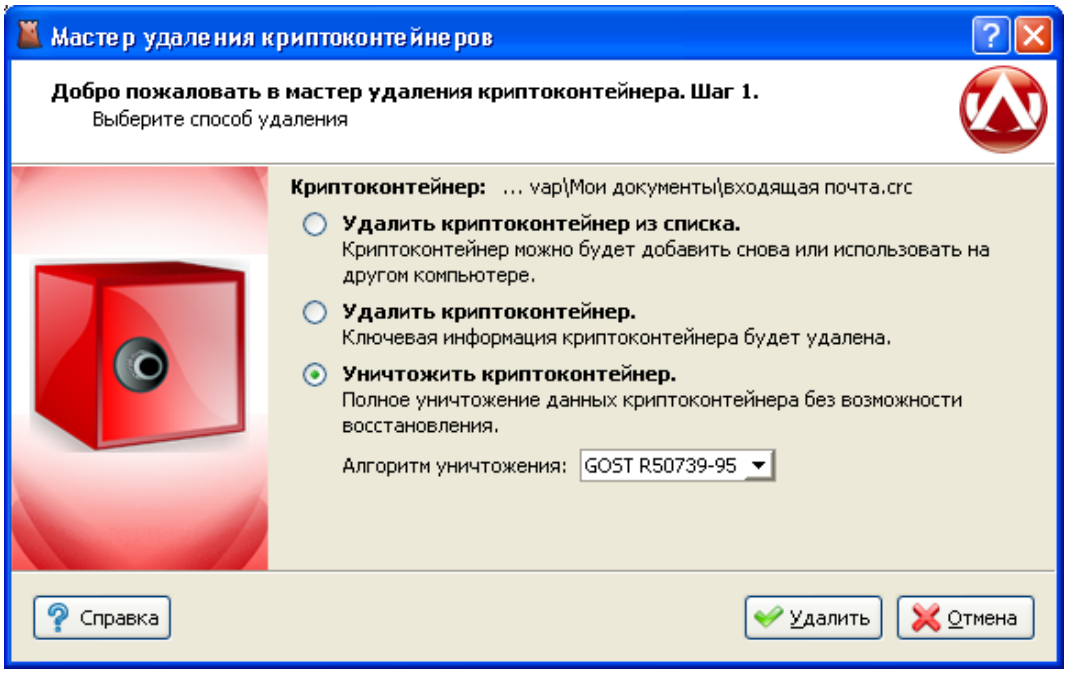

Рисунок 3.13. Мастер удаления криптоконтейнеров

Важно

Любой из алгоритмов уничтожения полностью удаляет всю информацию, содержащуюся в криптоконтейнере.

Не гарантируется полное удаление информации на некоторых типах флеш-накопителей, содержащих механизмы нивелирования износа (wear levelling).

Глава 4. Работа с криптодисками

4.1. Введение

В данном разделе описывается работа с защищенными криптодисками, их создание, добавление, удаление и основные действия над ними. Криптодиск представляет собой полностью зашифрованный раздел диска, либо флэш-накопитель. Пока криптодиск закрыт, его содержимое невозможно прочитать, так как оно зашифровано криптостойким алгоритмом шифрации, при этом зашифровываются не отдельные файлы, а вся файловая система целиком, что позволяет предотвратить несанкционированный доступ ко всей информации на диске.

4.2. Создание криптодиска

Для того, чтобы создать криптодиск, необходимо выбрать в главном меню Навигатора пункт «Файл» / «Создать» / «Криптодиск».

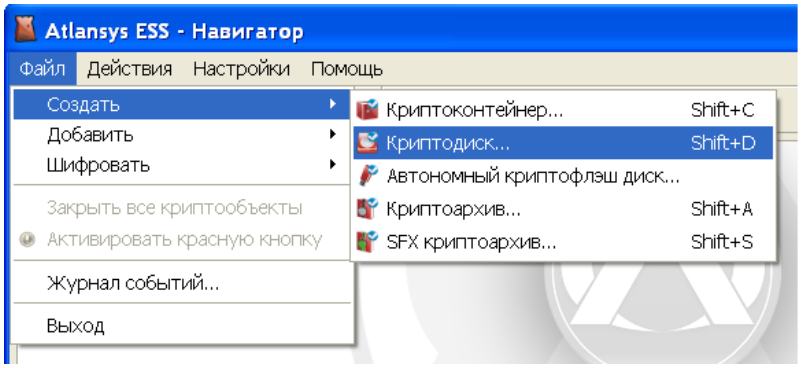

Рисунок 4.1. Меню «Файл» / «Создать»

В появившемся окне выбрать необходимый раздел жесткого диска или флэш-накопителя, на котором будет создаваться криптодиск и нажать кнопку «Далее».

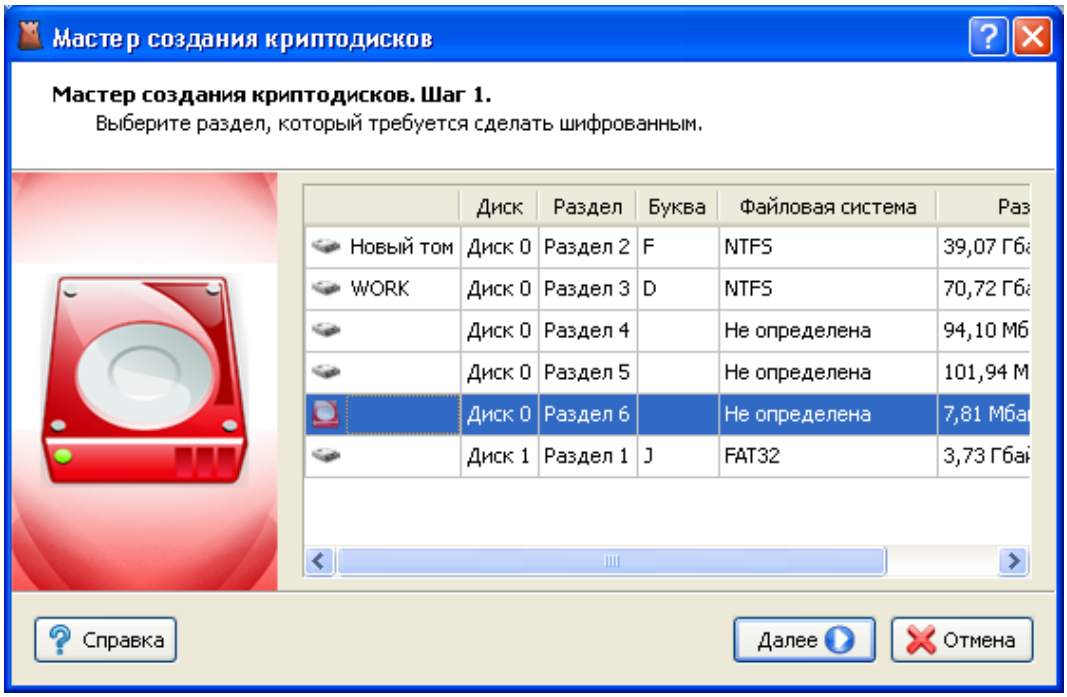

Рисунок 4.2. Мастер создания криптодисков. Выбор раздела.

Замечание

Будьте внимательны при выборе необходимого раздела. После создания криптодиска он не будет отображаться в системе как дисковое устройство и невозможно будет получить доступ к данным стандартными системными средствами.

Важно

В текущей версии Atlansys Enterprise Security System не поддерживается шифрация системных дисков. Если на разделе, который используется для создания криптодиска, находится профиль пользователя, то возможны ситуации недоступности профиля при последующей загрузке операционной системы и невозможности входа пользователя в систему.

Шифрация динамических дисков в текущей версии не поддерживается.

В следующем окне предлагается ввести метку диска, описание криптодиска и букву диска, под которой криптодиск будет отображаться в системе. Если нет необходимости сохранять данные на выбранном разделе, следует снять отметку выбора с чекбокса «Сохранить существующие данные». Процедура создания криптодиска без сохранения данных на нем занимает гораздо меньше времени.

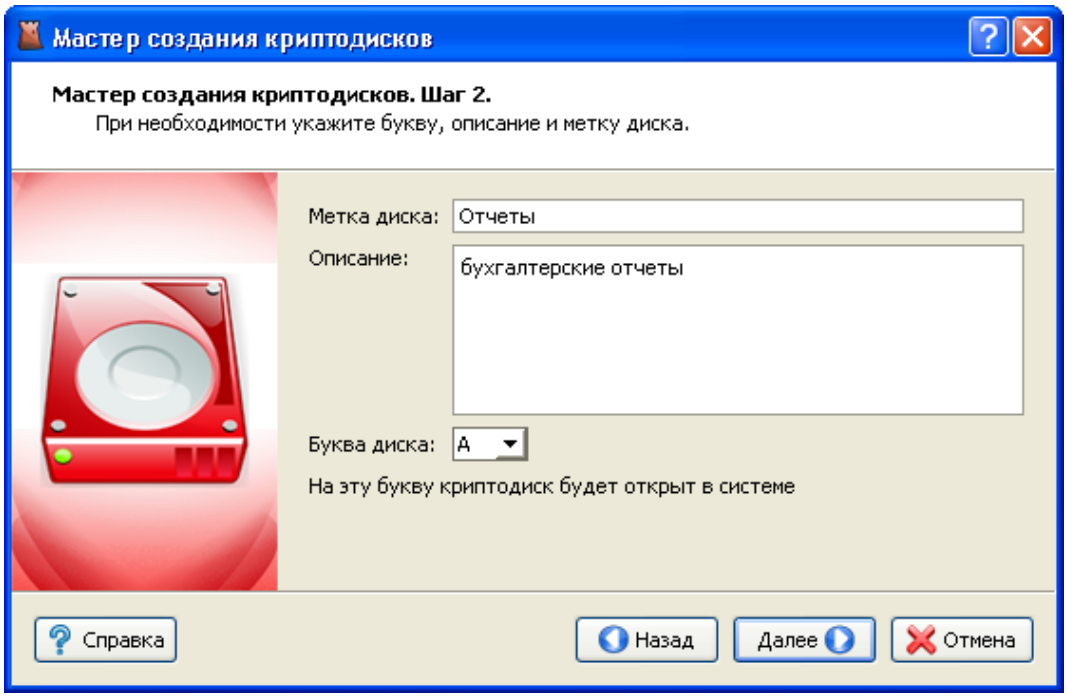

Рисунок 4.3. Мастер создания криптодисков. Метка диска и описание.

Важно

При создании криптодиска без сохранения существующих данных все данные на диске будут полностью уничтожены.

Замечание

Преобразование файловой системы NTFS с зашифрованными файлами и каталогами не поддерживается. При наличии зашифрованных файлов и каталогов на диске необходимо до создания криптодиска снять у данных файлов и каталогов атрибут «Шифровать содержимое для защиты данных».

После нажатия на кнопку «Далее» Мастер перейдет на окно выбора типа защиты криптодиска. На данном шаге необходимо выбрать способы защиты криптодиска. Возможны различные комбинации защиты:

- с помощью пароля;
- с помощью сертификата или набора сертификатов;
- с помощью пароля и сертификатов одновременно, в этом случае при отсутствии необходимого сертификата для открытия криптодиска можно будет использовать пароль.

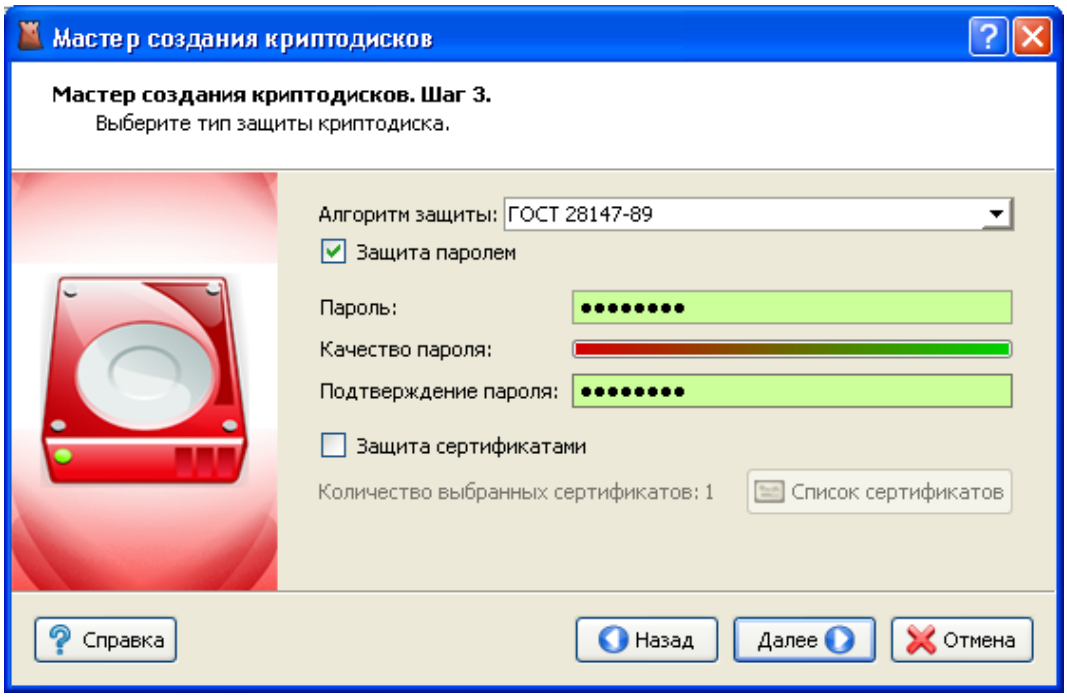

Рисунок 4.4. Мастер создания криптодисков. Способы защиты.

Для защиты с помощью пароля необходимо выбрать чекбокс «Пароль защиты» и ввести пароль в поля «Пароль» и «Подтверждение пароля». При вводе пароля в поле «Качество пароля» будет отображаться его качественные характеристики по стойкости к подбору. Качественный пароль должен содержать не менее восьми символов из букв в верхнем и нижнем регистре, минимум одну цифру и минимум один спецсимвол. При достижении необходимого качества пароля поле ввода окрашивается в зеленый цвет, после чего необходимо повторить ввод пароля в поле «Подтверждение пароля». Когда оба пароля совпадут, оба поля ввода пароля окрасятся в зеленый цвет.

При использовании сертификатов для защиты данных необходимо выбрать чекбокс "Сертификаты защиты" и нажать кнопку "Список сертификатов". В появившемся диалоге выбираются сертификаты для защиты криптоконтейнера. Доступ к данным криптоконтейнера будет возможен только при наличии у пользователя одного из сертификатов защиты с закрытым ключом. После закрытия диалога со списком сертификатов в окне Мастера создания криптоконтейнеров отобразится количество выбранных сертификатов.

Замечание

Как минимум один из выбранных сертификатов должен содержать закрытый ключ, с помощью которого расшифровывается содержимое криптодиска. В противном случае доступ к содержимому криптодиска на данной рабочей станции будет невозможен.

После выбора способов защиты необходимо нажать кнопку «Далее», после чего появится окно с информацией о создаваемом криптодиске. Необходимо проверить данные и нажать кнопку «Далее».

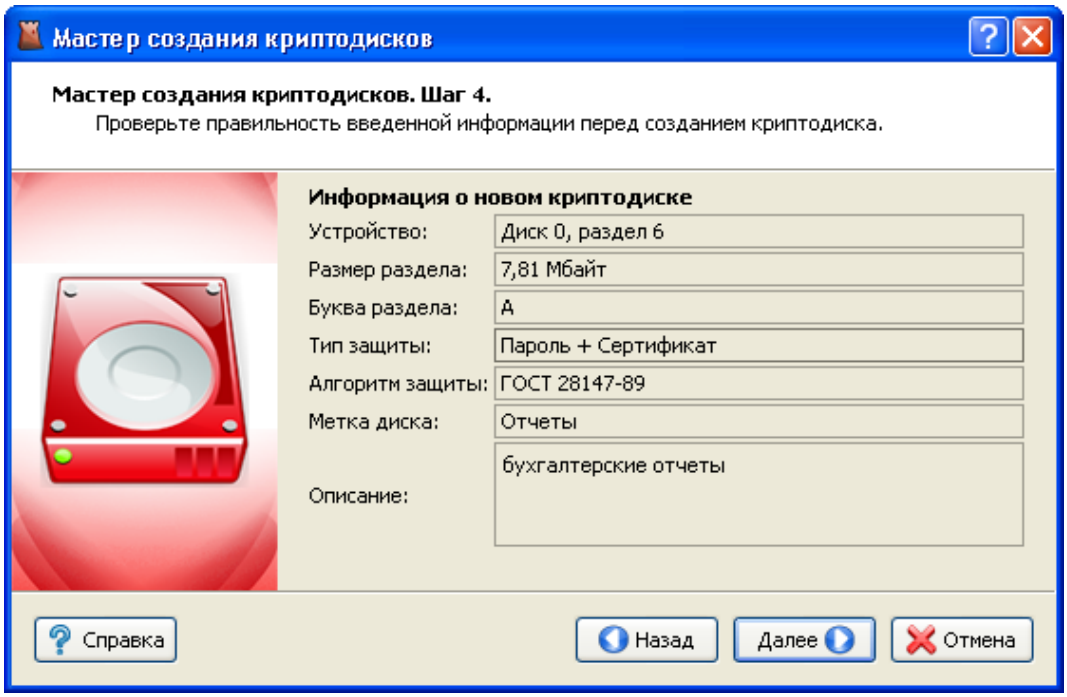

Рисунок 4.5. Мастер создания криптодисков. Сводная информация.

Если на Шаге 2 был выбран режим создания криптодиска с сохранением существующих данных, то появится окно предупреждения о выбранном режиме преобразования существующего раздела в криптодиск. Необходимо ознакомится с предупреждением и нажать кнопку «Создать».

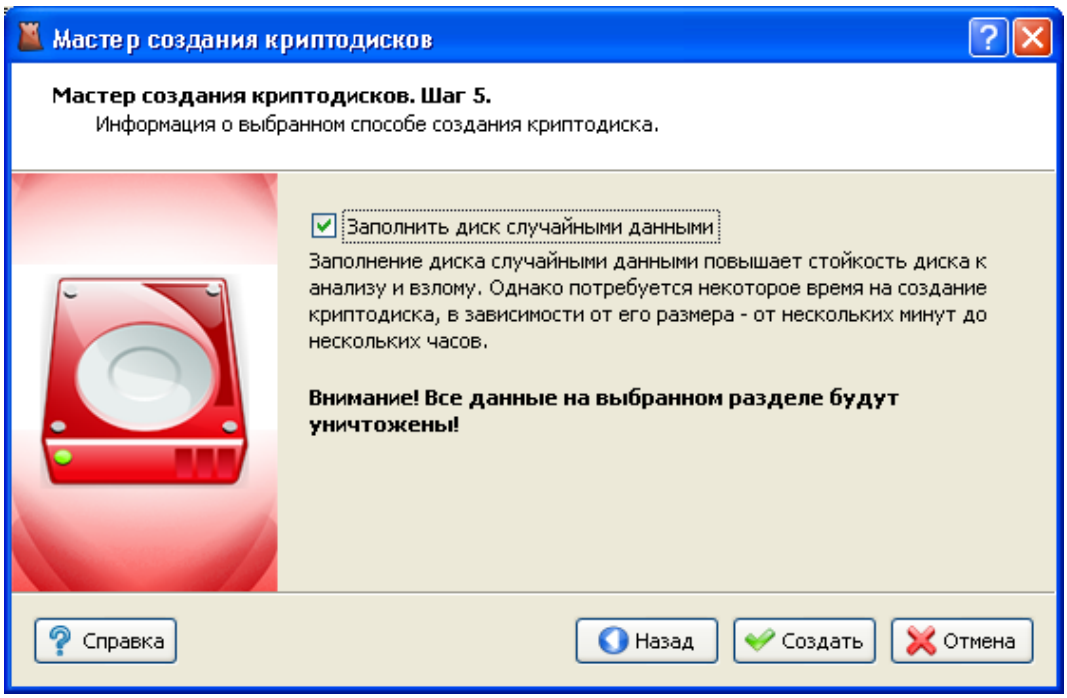

Рисунок 4.6. Мастер создания криптодисков. Предупреждение.

После этого появится окно с прогрессом создания криптодиска, в котором отображается прогресс создания, количество прошедшего времени с начала создания криптодиска, прогноз оставшегося времени.

Важно

В процессе создания криптодиска не выключайте компьютер и не извлекайте носитель до окончания процесса создания криптодиска.

После успешного завершения создания криптодиска появится сообщение «Криптодиск создан успешно». Затем необходимо нажать на кнопку «Готово», после чего созданный криптодиск добавится в список Навигатора и запустится Проводник Windows на открытом криптодиске.

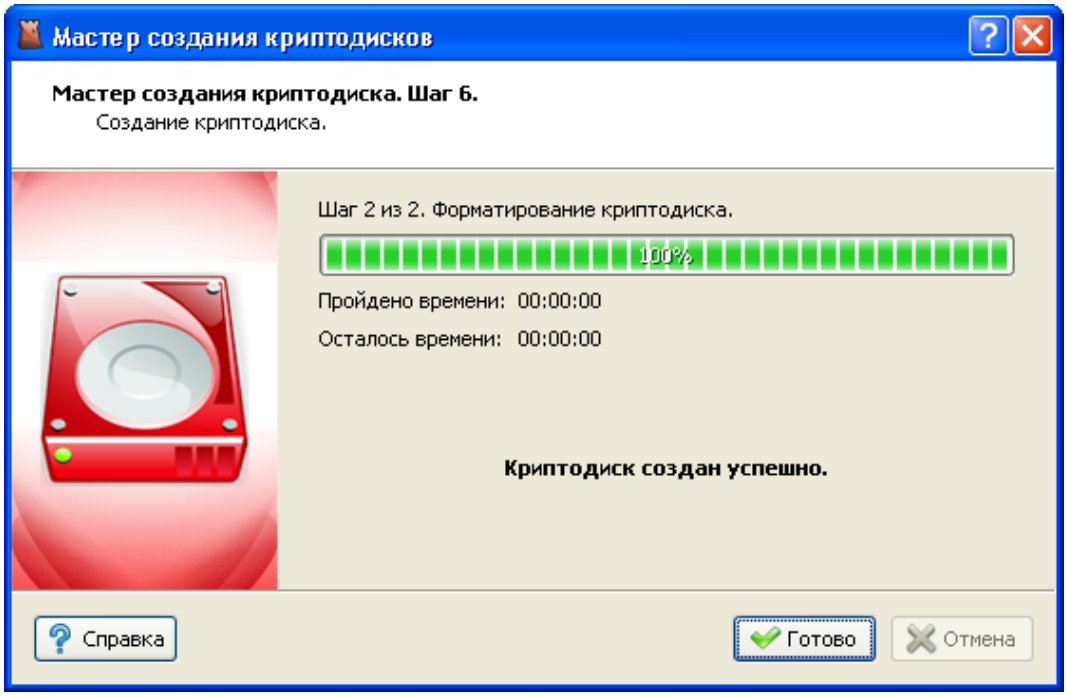

Рисунок 4.7. Мастер создания криптодисков. Прогресс создания.

Для криптодисков, созданных с сохранением существующих данных, в списке Навигатора будут отображаться проценты количества зашифрованных данных на диске. При достижении 100% все данные на диске будут полностью зашифрованы.

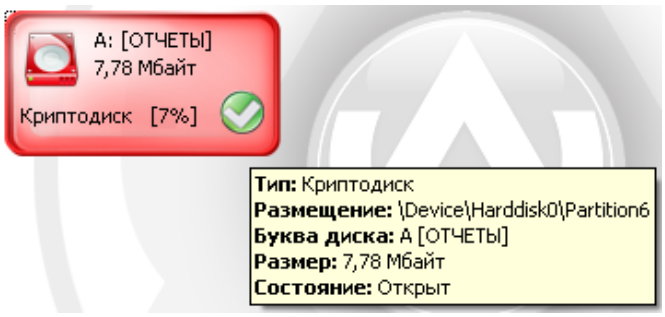

Рисунок 4.8. Процесс преобразования криптодиска.

Важно

Криптодиски на извлекаемых устройствах должны закрываться стандартными средствами Навигатора перед извлечением устройства.

Если на Шаге 2 Мастера был выбран режим создания без сохранения данных, или этот режим не доступен для текущей файловой системы раздела, то появится окно с чекбоксом «Заполнить диск случайными

данными». Если нет необходимости заполнения диска случайными данными, то можно отключить этот чекбокс, при этом скорость создания криптодиска многократно возрастет. Однако в целях увеличения безопасности использования криптодиска рекомендуется оставить этот чекбокс включенным.

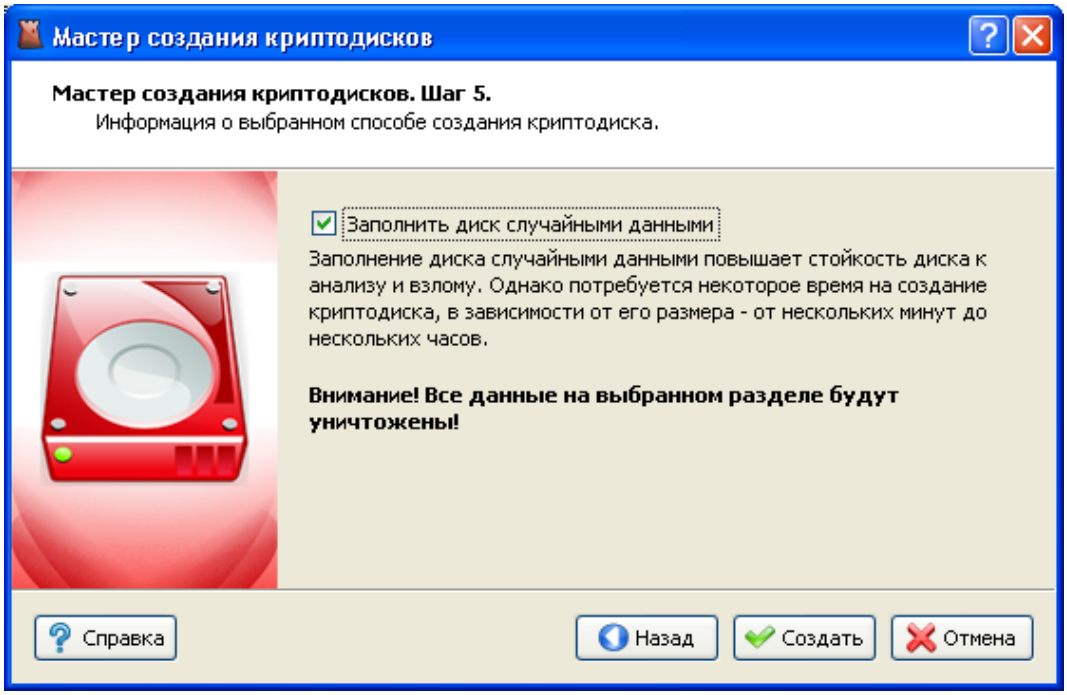

Рисунок 4.9. Мастер создания криптодисков. Заполнение случайными данными.

Важно

При создании криптодиска без сохранения существующих данных вся информация на разделе будет полностью уничтожена без возможности восстановления.

4.3. Добавление криптодиска

Для добавления криптодиска, созданного на другой рабочей станции, необходимо выбрать в главном меню Навигатора пункт «Файл» / «Добавить» / «Криптодиск...».

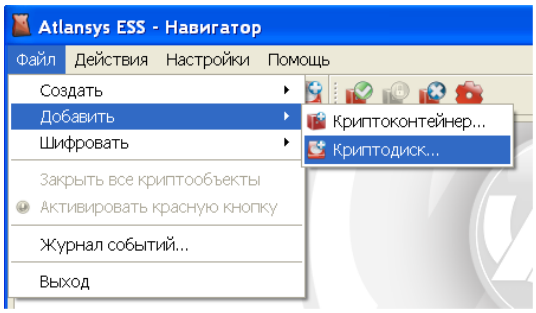

Рисунок 4.10. Меню «Файл» / «Добавить»

В списке разделов выбрать необходимый раздел и нажать кнопку «Далее». В списке добавляемых криптодисков отображаются только те разделы, которые опознаются как криптодиски и еще не добавлены в список Навигатора.

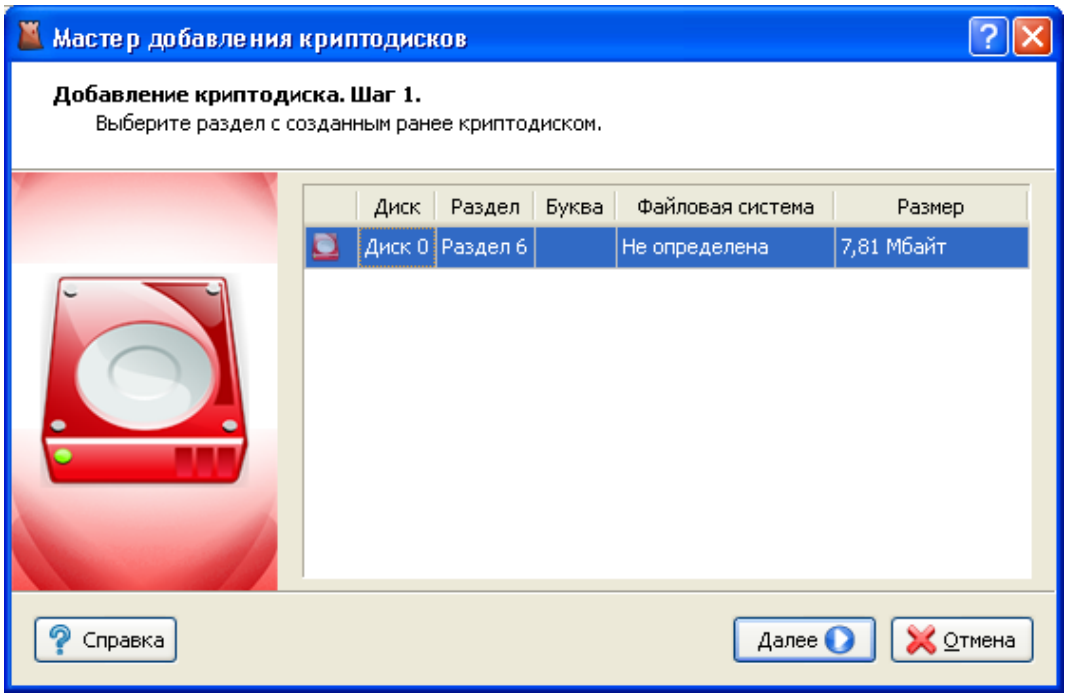

Рисунок 4.11. Мастер добавления криптодисков. Выбор раздела.

На втором шаге Мастера отобразится информация по добавляемому криптодиску. Необходимо выбрать букву диска, под которой криптодиск будет отображаться в системе. Для добавления криптодиска необходимо нажать на кнопку «Добавить». Криптодиск добавится в список Навигатора, автоматически откроется и на нем запустится Проводник Windows.

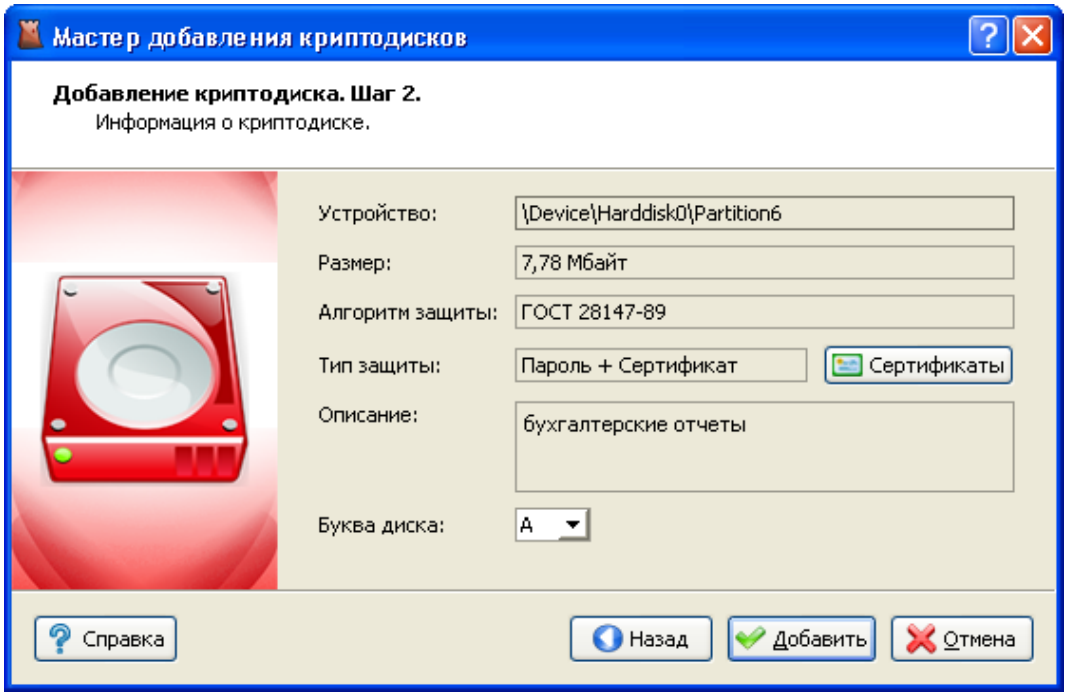

Рисунок 4.12. Мастер добавления криптодисков. Сводная информация о криптодиске.

4.4. Работа с криптодисками

По умолчанию созданный или добавленный диск имеет состояние «Открыт», что отображается на его иконке. Все криптоконтейнеры и криптодиски отображаются в списке Навигатора. Текущий активный

элемент выделяется рамкой, при этом его параметры выводятся в нижней части окна Навигатора. Для криптодисков отображается следующая информация:

- устройство, на котором создан криптодиск;
- дата создания;
- версия криптоконтейнера;
- алгоритм защиты данных;
- тип защиты: пароль, сертификат, либо пароль + сертификат. Если криптодиск защищен сертификатами, то список сертификатов можно просмотреть, нажав на кнопку списка сертификатов. В списке сертификатов отображаются все сертификаты, которым защищен криптодиск, для каждого сертификата отображается состояние доступности. Криптодиск может быть открыт, если хотя бы один сертификат, имеющий закрытый ключ, доступен.

Для того, чтобы закрыть криптодиск, необходимо закрыть все работающие с ним приложения, выделить его в списке Навигатора, затем в главном меню выбрать пункт «Действия» / «Закрыть». Либо в контекстном меню криптодиска выбрать пункт «Закрыть». Либо нажать кнопку «Закрыть» на панели инструментов.

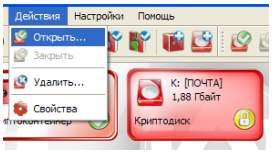

Рисунок 4.13. Меню «Действия»

Чтобы открыть закрытый криптодиск, необходимо выделить его в списке Навигатора, в главном меню выбрать пункт «Действия» / «Открыть». Либо в контекстном меню выбрать пункт «Открыть».

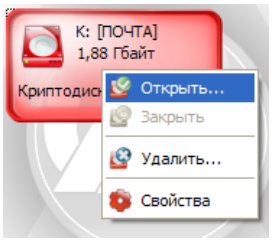

Рисунок 4.14. Контекстное меню криптодиска

Либо нажать кнопку «Открыть» на панели инструментов. Двойной щелчок мыши на иконке криптодиска в списке Навигатора также его открывает и запускает Проводник.

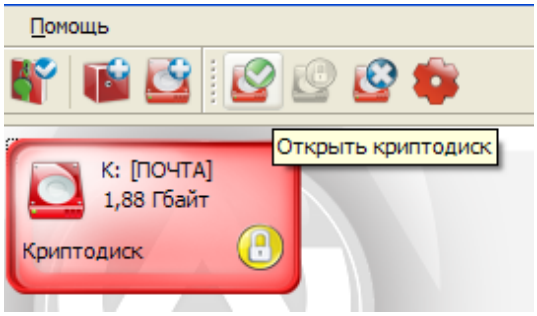

Рисунок 4.15. Панель инструментов

Если криптодиск защищен сертификатами, и в системе имеется закрытый ключ хотя бы к одному сертификату, криптодиск откроется, и на нем автоматически запустится Проводник Windows. Если криптодиск защищен паролем, то откроется диалог открытия криптодиска, в поле «Пароль» которого необходимо вве-

сти пароль, который использовался при создании криптодиска, при необходимости можно поменять букву диска, под которой криптодиск будет виден в системе, и нажать кнопку «Открыть».

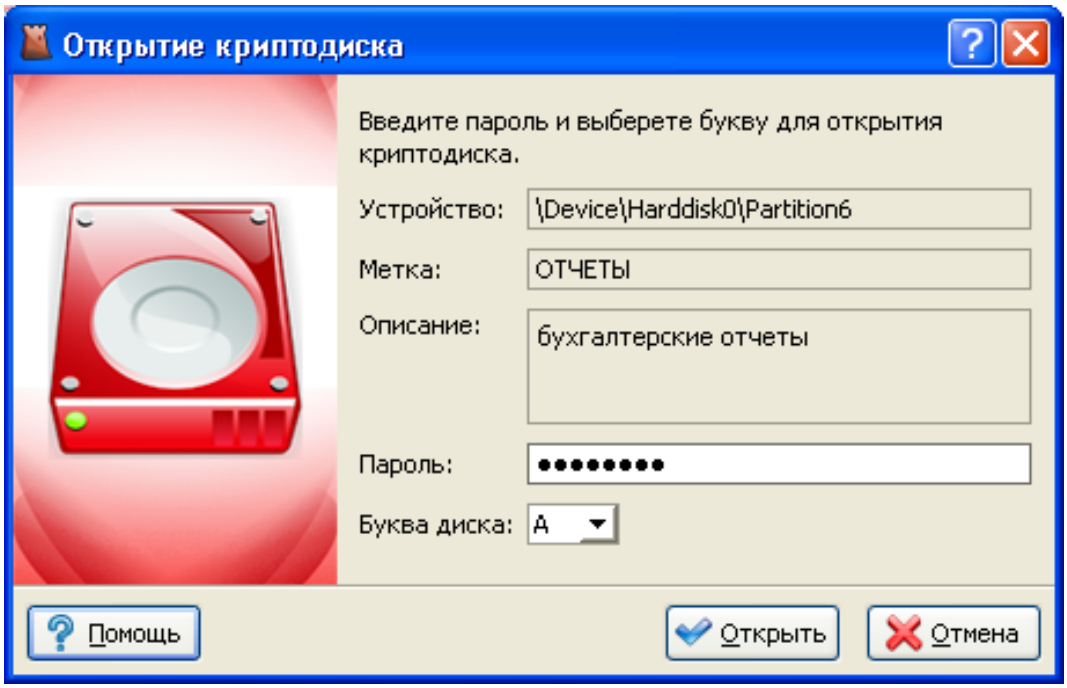

Рисунок 4.16. Диалог открытия криптодиска

4.5. Удаление криптодиска

При удалении криптодиска сначала необходимо закрыть все приложения, которые с ним работают, затем закрыть криптодиск, далее в главном меню выбрать пункт «Действия» / «Удалить», либо выбрать в контекстном меню пункт «Удалить», либо в панели инструментов нажать на кнопку «Удалить».

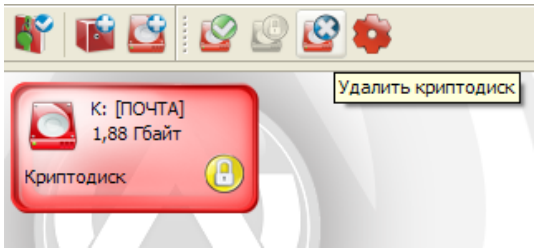

Рисунок 4.17. Панель инструментов, кнопка «Удалить»

После этого появится окно Мастера удаления криптоконтейнеров, в котором необходимо выбрать один из способов удаления криптоконтейнера:

- *Удалить криптодиск из списка.* Удаляет криптодиск только из списка Навигатора. При этом криптодиск и все данные, содержащиеся в нем не удаляются. Данный способ может использоваться при переносе криптодиска на другую рабочую станцию.

- *Удалить криптодиск.* В криптодиске стирается ключевая информация и заголовок. Так как вся информация в криптодиске зашифрована, то удаление ключевой информации полностью блокирует доступ к данным, содержащимся на криптодиске. Это самый быстрый способ удаления диска, но он не защищает от дешифрования данных с помощью прямого перебора ключей.

- *Уничтожить криптодиск.* Для гарантированного уничтожения данных помимо удаления ключевой информации, все данные на криптодиске уничтожаются одним из алгоритмов уничтожения.

- Алгоритм по стандарту ГОСТ Р 50739-95 имеет два цикла записи псевдослучайных значений.
- Алгоритм по стандарту DoD 5220.22M имеет два цикла записи псевдослучайных значений и один цикл записи фиксированных значений.
- Алгоритм по стандарту NAVSO P-5239-26 имеет два цикла записи фиксированных значений и один цикл записи псевдослучайных значений.

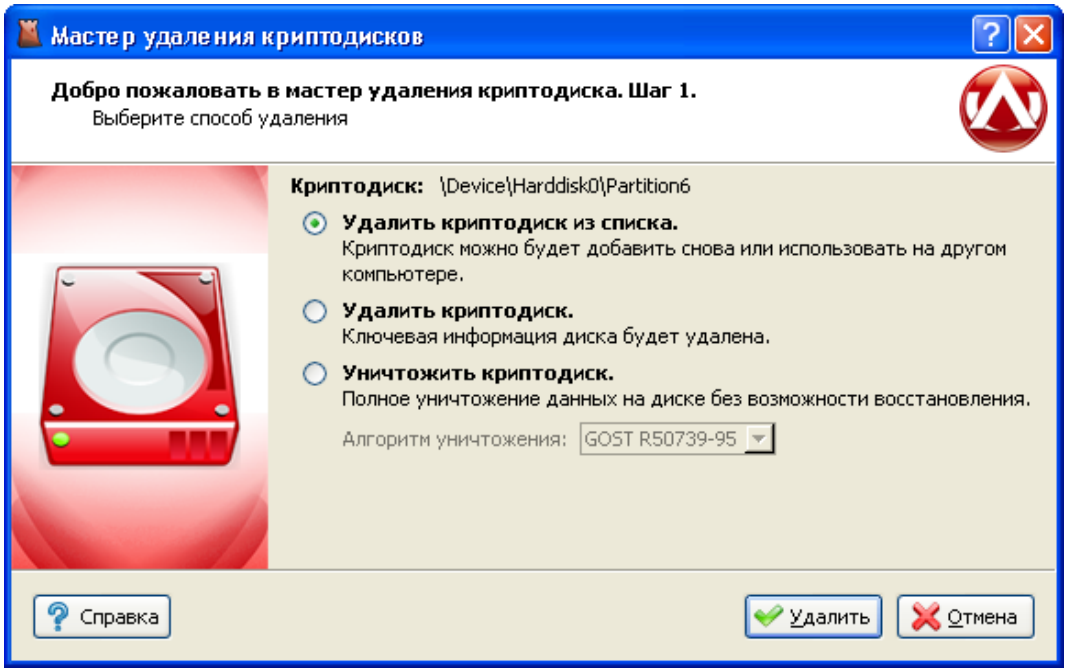

Рисунок 4.18. Мастер удаления криптодисков

Важно

Форматирование раздела, на котором был криптодиск, стандартными средствами Windows не удаляет всю служебную информацию криптодиска, поэтому криптодиски должны удаляться средствами Навигатора и только затем форматироваться.

Глава 5. Шифрование системного раздела

5.1. Введение

В данном разделе описывается работа с защищенным системным разделом: его создание, особенности загрузки операционной системы, восстановление в случае повреждения.

Защищенный системный раздел представляет собой полностью зашифрованный раздел диска или весь жесткий диск, на котором установлена операционная система. В этом случае невозможно прочитать зашифрованные данные, не зная пароля, даже если получить доступ к жесткому диску из другой операционной системы или на другом компьютере. При этом шифруется вся файловая система раздела или диска целиком.

Важно

В настоящее время Atlansys Enterprise Security System не поддерживает шифрование системного раздела, если операционная система установлена не в активный раздел жесткого диска.

5.2. Шифрование системного раздела

Для того, чтобы зашифровать системный диск, необходимо выбрать в главном меню Навигатора пункт "Шифровать" / "Системный раздел".

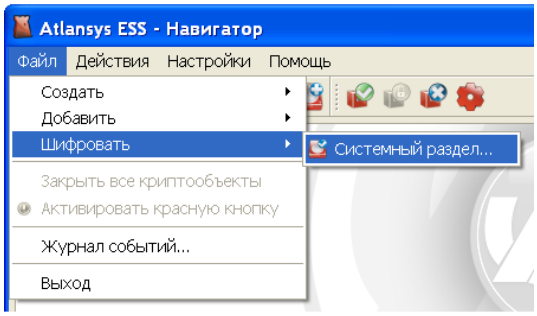

Рисунок 5.1. Меню шифрования системного раздела

Появится Мастер шифрования системного раздела, первая страница которого содержит предупреждение и краткое описание процесса шифрования системного раздела.

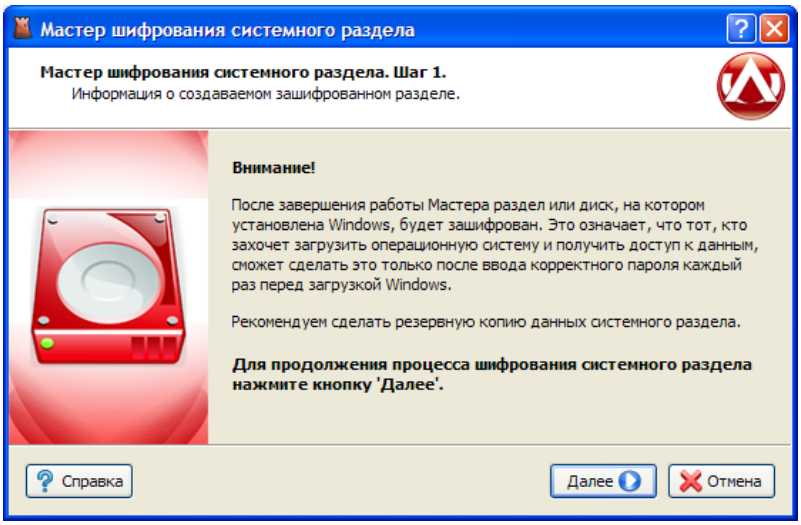

Рисунок 5.2. Мастер шифрования системного раздела. Предупреждение.

На следующей странице Мастера следует указать метку диска и его описание, если это необходимо.

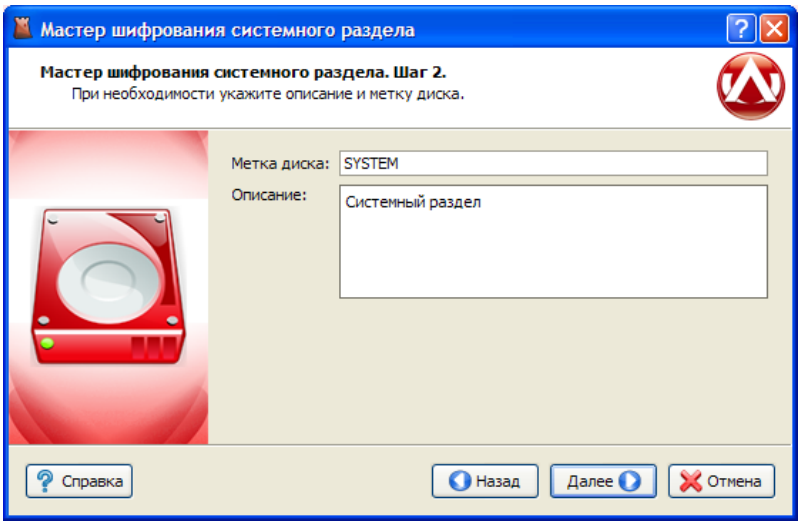

Рисунок 5.3. Мастер шифрования системного раздела. Параметры криптодиска.

Перейдя на следующую страницу Мастера, выберите алгоритм защиты создаваемого криптодиска и задайте пароль, заполнив поля "Пароль" и "Подтверждение пароля". При вводе пароля в поле "Качество пароля" будут отображаться его качественные характеристики по стойкости к подбору. Качественный пароль должен содержать не менее восьми символов из букв в верхнем и нижнем регистре, минимум одну цифру и минимум один спецсимвол. При достижении необходимого качества пароля поле ввода окрашивается в зеленый цвет, после чего необходимо повторить ввод пароля в поле "Подтверждение пароля". Когда оба пароля совпадут, оба поля ввода пароля окрасятся в зеленый цвет.

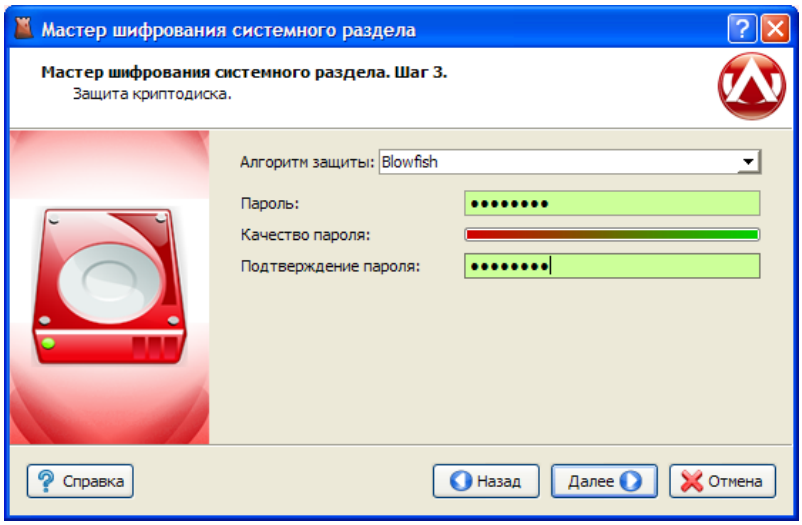

Рисунок 5.4. Мастер шифрования системного раздела. Защита.

Важно

Если пароль окажется потерян, восстановить загрузку операционной системы будет невозможно.

Следующая страница отображает сводную информацию о создаваемом криптодиске.

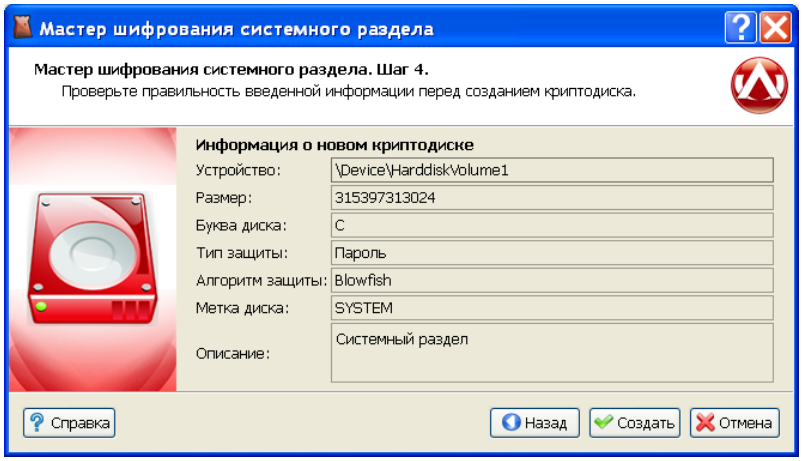

Рисунок 5.5. Мастер шифрования системного раздела. Сводная информация.

После этого появится окно с прогрессом создания криптодиска, в котором отображается прогресс создания, количество прошедшего времени с начала создания криптодиска, прогноз оставшегося времени.

Важно

В процессе создания криптодиска не выключайте компьютер до окончания процесса создания криптодиска.

После успешного завершения работы Мастера появится сообщение "Криптодиск создан успешно". Однако, для полного завершения шифрования системного раздела необходима перезагрузка компьютера, о чем Мастер предупредит пользователя.

5.3. Работа с зашифрованным системным разделом

При следующем запуске компьютера (или после перезагрузки) система предложит ввести пароль, который был задан на этапе "Защита" при создании шифрованного системного раздела. Без ввода корректного пароля операционную систему загрузить не удастся.

После ввода корректного пароля операционная система загрузится в штатном режиме. Работа в ней ничем не отличается от работы с обычным, незашифрованным системным разделом.

5.4. Дешифрация системного раздела

Расшифрование системного раздела позволяет снять криптографическую защиту. Мастер расшифрования запускается либо во всплывающем меню при клике правой кнопкой мыши на системном разделе в интерфейсе Навигатора, либо через панель инструментов.

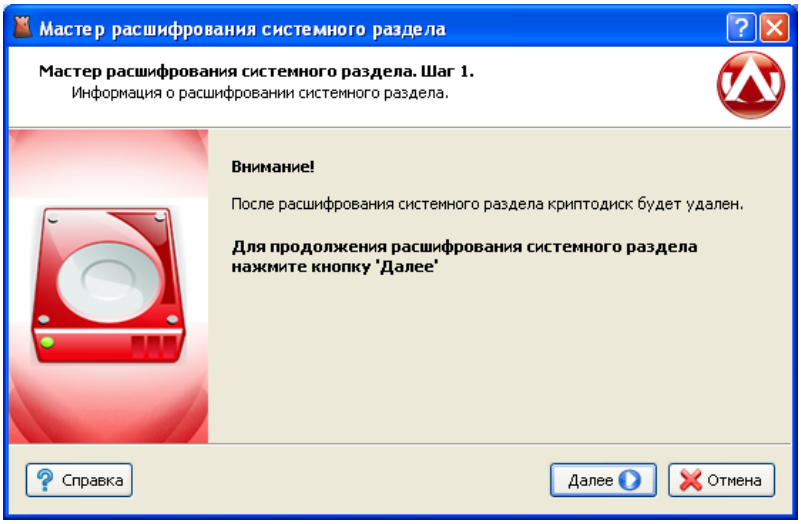

Рисунок 5.6. Мастер расшифрования системного раздела

После нажатия на кнопку "Далее" начинается процесс расшифрации. Не выключайте компьютер до окончания процесса!

5.5. Восстановления пароля зашифрованного системного раздела

Важно

Восстановление пароля доступно только для клиентов работающих в управляемом режиме.

Для восстановления пароля необходимо создать диск восстановления. Для этого нужно записать загрузочный образ **AtlansysRecoveryDisk.iso** из каталога установки Atlansys Enterprise Security System на компакт-диск или на флэш-диск с возможностью загрузки. Для создания диска восстановления можно воспользоваться любой удобной программой записи и следовать инструкциям, описанным в документации к этой программе. Далее на компьютере необходимо указать устройство, с которого выполнять загрузку: cdrom (или флэш-диск). Если все сделано правильно, при следующем запуске компьютера (или перезагрузке) произойдет загрузка с диска восстановления .

Рисунок 5.7. Начальный экран загрузки диска восстановления

После загрузки отобразится главное окно программы. Определены следующие действия: показ информации о системном диске Atlansys и восстановление пароля.

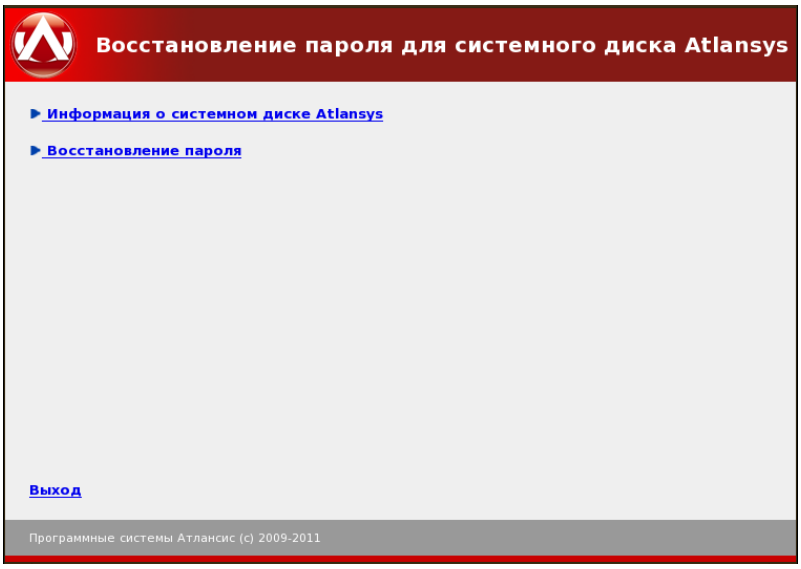

Рисунок 5.8. Главное окно программы.

Для показа информации о системном диске Atlansys необходимо из списка доступных устройств выбрать системный диск Atlansys и нажать на кнопку 'Показать информацию'.

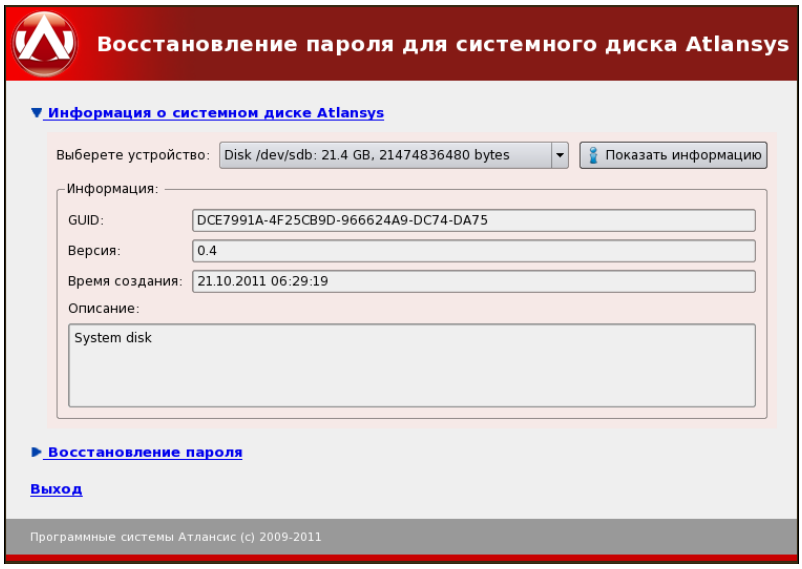

Рисунок 5.9. Показать информацию о системном диске Atlansys.

Важно

Перед операцией восстановления пароля необходимо создать файл с ключевым материалом на Центре Управления, при помощи функции "Восстановление ключей" консоли управления. Полученный файл следует записать на носитель(cdrom или флэш-диск) и подключить данный носитель к компьютеру до начала загрузки диска восстановления.

Для восстановления пароля необходимо выбрать из списка доступных устройств системный диск Atlansys, выбрать путь к файлу с ключевым материалом и нажать на кнопку 'Восстановить пароль'.

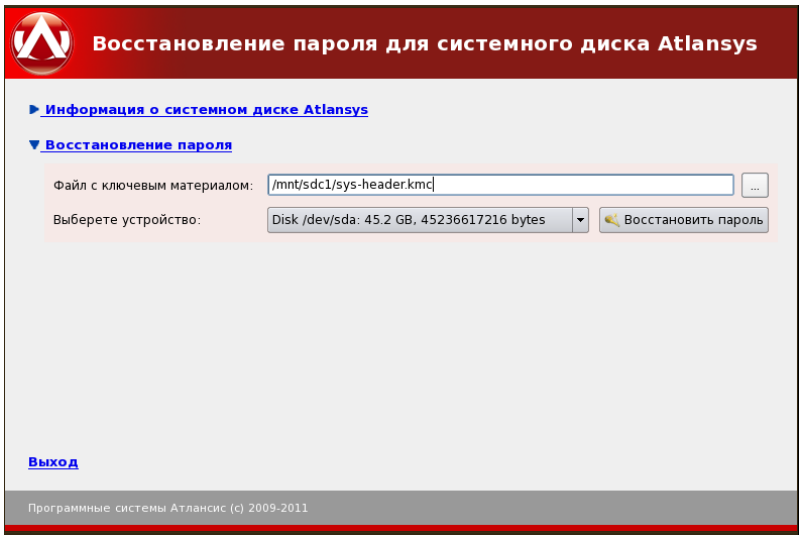

Рисунок 5.10. Восстановление пароля.

Если операция восстановления пароля прошла успешно, то покажется информационное окно с подтверждением успеха операции.

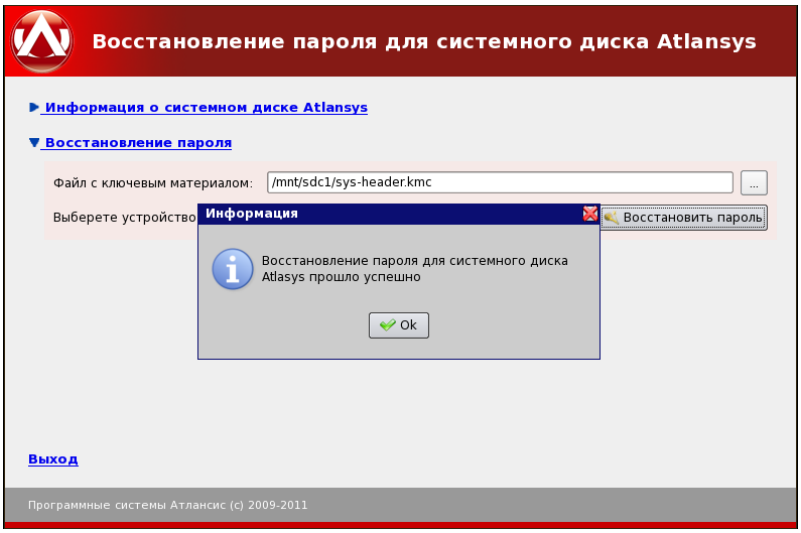

Рисунок 5.11. Восстановление пароля.

Глава 6. Работа с автономными криптофлэш дисками

6.1. Введение

В данном разделе описывается работа с автономными криптофлэш дисками, их создание, подключение, удаление и основные действия над ними. Автономный криптофлэш диск представляет собой зашифрованное съемное устройство (обычно это USB-flash накопитель), с которым можно работать, не имея установленного на компьютере клиента Atlansys Enterprise Security System.

6.2. Создание автономного криптофлэш диска

Важно

Создание автономного криптофлэш диска на съемных носителях размером более 32 Гб не поддерживается!

Для того, чтобы создать автономный криптофлэш диск, необходимо выбрать в главном меню Навигатора пункт «Файл» / «Создать» / «Автономный криптофлэш диск».

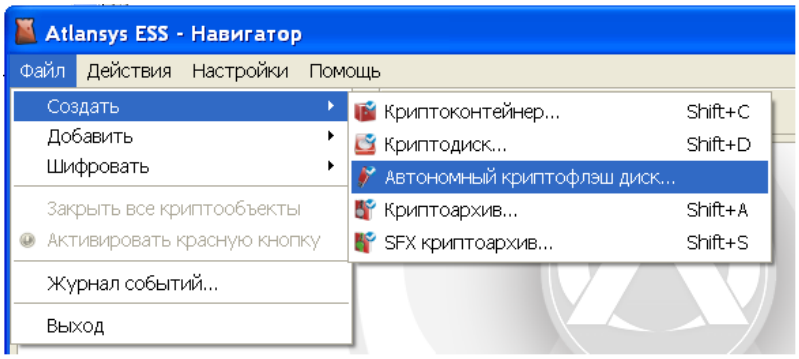

Рисунок 6.1. Меню «Файл» / «Создать»

В появившемся окне выбрать из списка съемное устройство, на котором будет создаваться автономный криптофлэш диск, и нажать кнопку «Далее».

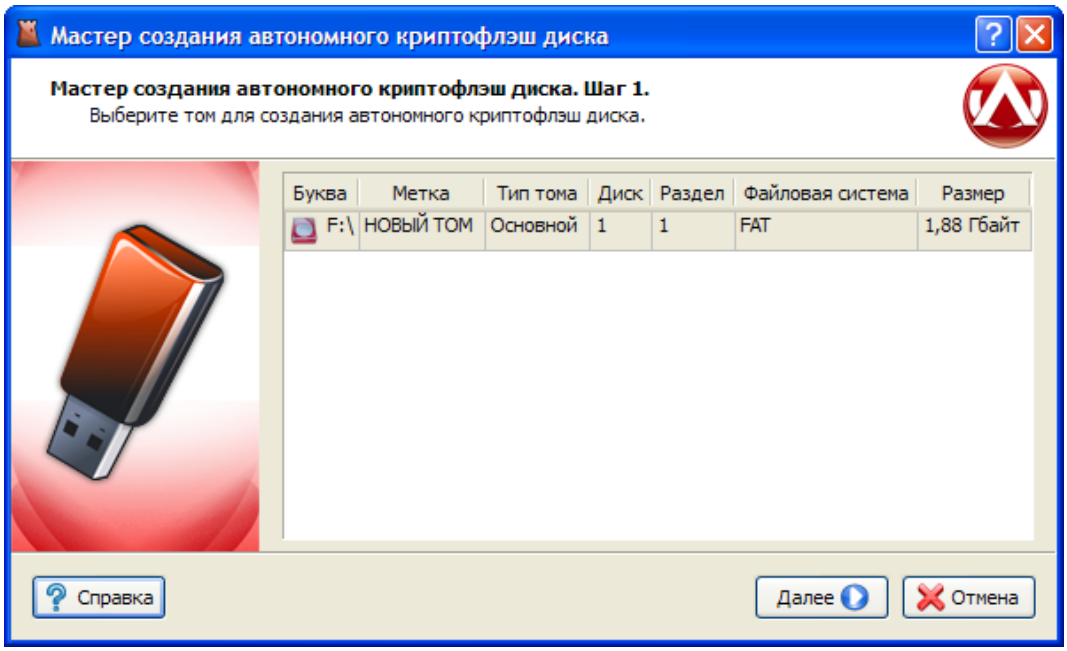

Рисунок 6.2. Мастер создания автономного криптофлэш диска. Выбор раздела.

После нажатия на кнопку «Далее» Мастер перейдет на окно выбора типа защиты. На данном шаге необходимо выбрать способы защиты криптофлэш диска. Возможны различные комбинации защиты:

- с помощью пароля;
- с помощью сертификата или набора сертификатов;
- с помощью пароля и сертификатов одновременно, в этом случае при отсутствии необходимого сертификата для открытия криптодиска можно будет использовать пароль.

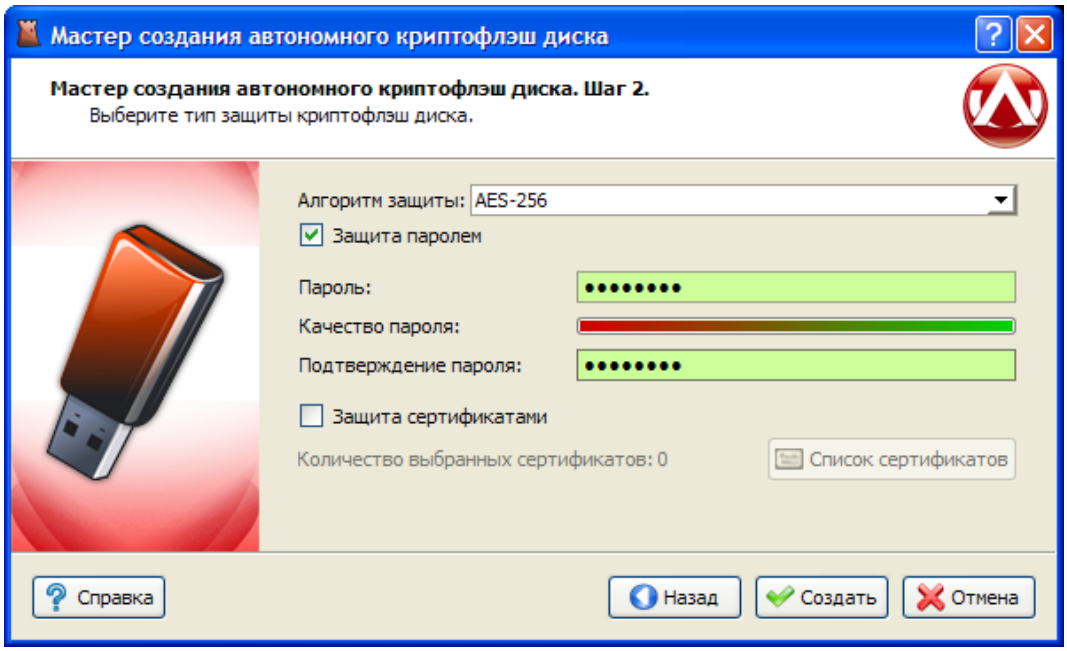

Рисунок 6.3. Мастер создания автономного криптофлэш диска. Способы защиты.

Для защиты с помощью пароля необходимо выбрать чекбокс «Пароль защиты» и ввести пароль в поля «Пароль» и «Подтверждение пароля». При вводе пароля в поле «Качество пароля» будет отображаться его качественные характеристики по стойкости к подбору. Качественный пароль должен содержать не

менее восьми символов из букв в верхнем и нижнем регистре, минимум одну цифру и минимум один спецсимвол. При достижении необходимого качества пароля поле ввода окрашивается в зеленый цвет, после чего необходимо повторить ввод пароля в поле «Подтверждение пароля». Когда оба пароля совпадут, оба поля ввода пароля окрасятся в зеленый цвет.

При использовании сертификатов для защиты необходимо выбрать чекбокс «Сертификаты защиты» и нажать кнопку «Список сертификатов». В окне списка сертификатов необходимо нажать на кнопку «Добавить сертификаты», после чего откроется диалог добавления сертификатов, в котором выбираются необходимые сертификаты пользователей, которым будет предоставлен доступ к создаваемому криптофлэш диску. После закрытия диалога со списком сертификатов в окне Мастера создания криптофлэш диска отобразится количество выбранных сертификатов.

Замечание

Как минимум один из выбранных сертификатов должен содержать закрытый ключ, с помощью которого расшифровывается содержимое криптофлэш диска. В противном случае доступ к его содержимому на данной рабочей станции будет невозможен.

После выбора способов защиты необходимо нажать кнопку «Создать».

После этого появится окно создания автономного криптофлэш диска, в котором отображается прогресс создания, количество прошедшего времени с начала создания и прогноз оставшегося времени.

Важно

В процессе создания автономного криптофлэш диска не выключайте компьютер и не извлекайте носитель до окончания процесса создания.

После успешного завершения создания появится сообщение «Автономный криптофлэш диск создан успешно».

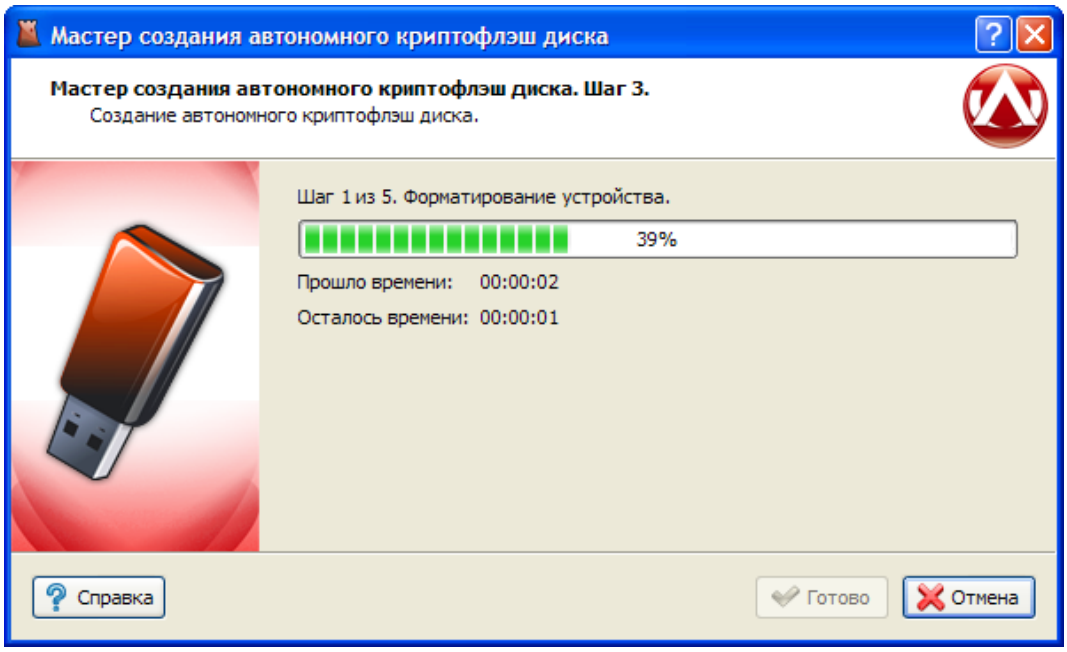

Рисунок 6.4. Мастер создания автономного криптофлэш диска. Прогресс создания.

6.3. Работа с автономным криптофлэш диском

После успешного создания закрытый криптофлэш диск в системе будет отображаться точно также, как и до создания, но за счет того, что на нем появилась защищенная область, его размер станет существенно

меньше. На нем появится исполняемый файл **flash_launcher.exe**, при помощи которого происходит управление защищенной областью вашего устройства.

Важно

Для запуска программы **flash_launcher** необходимо иметь права администратора операционной системы.

Запуск программы вызовет стандартный диалог открытия криптодисков, такой же, как в клиенте Atlansys Enterprise Security System, в котором потребуется ввести пароль, если криптофлэш диск был защищен при помощи пароля, а также выбрать букву (при желании), под которой защищенный раздел криптофлэш диска будет отображаться в системе.

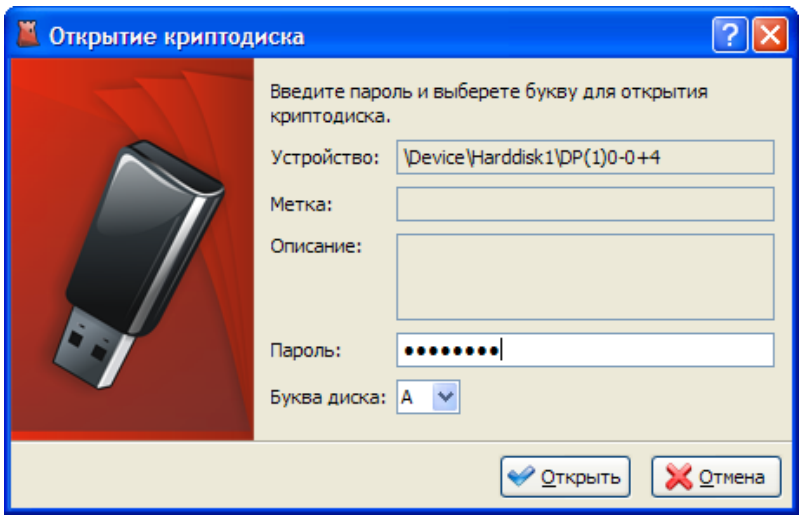

Рисунок 6.5. Стандартный диалог открытия криптодиска.

Если данные указаны верно, после нажатия кнопки «Открыть» начнется процесс открытия защищенного раздела. После успешного открытия, в системном трее появится значок программы **flash_launcher** и соответствующее сообщение.

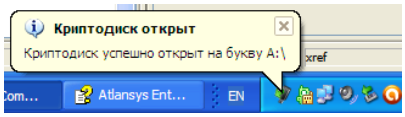

Рисунок 6.6. Сообщение об успешном открытии криптофлэш диска.

После успешного открытия, в системе появится новый диск, открытый на ранее выбранную букву, с которым можно работать, как с любым обычным диском операционной системы. При этом открытый раздел, на котором находится программа **flash_launcher.exe**, станет недоступным вплоть до закрытия защищенного раздела.

По щелчку правой кнопкой мыши на значке в системном трее появляется меню программы, из которого можно вызвать диалог «О программе» или закрыть защищенный раздел (пункт «Извлечь диск»).

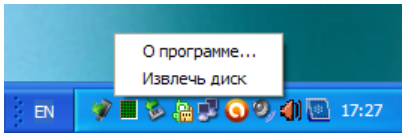

Рисунок 6.7. Меню программы в системном трее.

Чтобы закрыть защищенный раздел, следует выбрать пункт в контекстном меню программы в системном трее «Извлечь диск». После этого буква защищенного раздела в операционной системе исчезнет, а откры-

тый раздел криптофлэш диска снова станет доступен. Далее для извлечения устройства необходимо воспользоваться стандартным механизмом операционной системы.

Важно

В случае небезопасного извлечения устройства (минуя пункт меню «Извлечь диск»), сохранность данных на защищенном разделе не гарантируется!

Глава 7. Свойства криптообъекта

7.1. Диалог свойств криптообъекта

У любого криптообъекта (криптодиска или криптоконтейнера) есть ряд настраиваемых свойств. Диалог свойств криптообъета вызывается путем выбора пункта «Свойства» в главном или контекстном меню или по нажатию кнопки на панели инструменов криптообъекта.

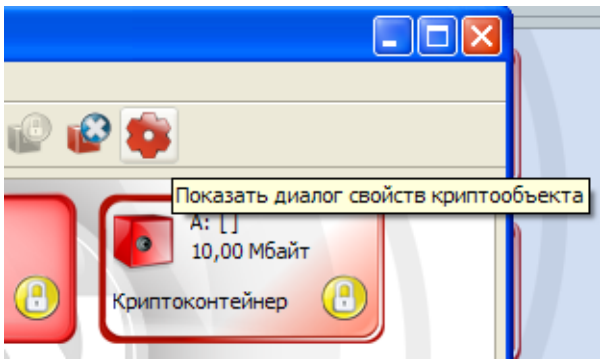

Рисунок 7.1. Кнопка вызова диалога свойств криптообъекта

После этого откроется диалог свойств криптообъекта, который одинаков и для криптодисков, и для криптоконтейнеров.

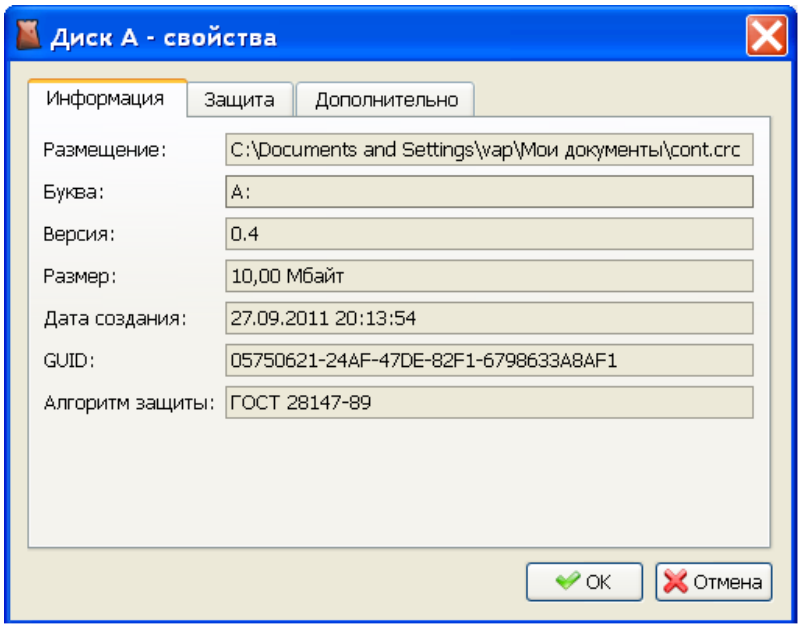

Рисунок 7.2. Диалог свойств криптообъекта - Информация

Вкладка «Информация» отображает основную информацию по данному криптообъекту и не является редактируемой.

7.2. Изменение пароля и сертификатов

На вкладке «Защита» можно изменить пароль и сертификаты защиты криптообъекта.

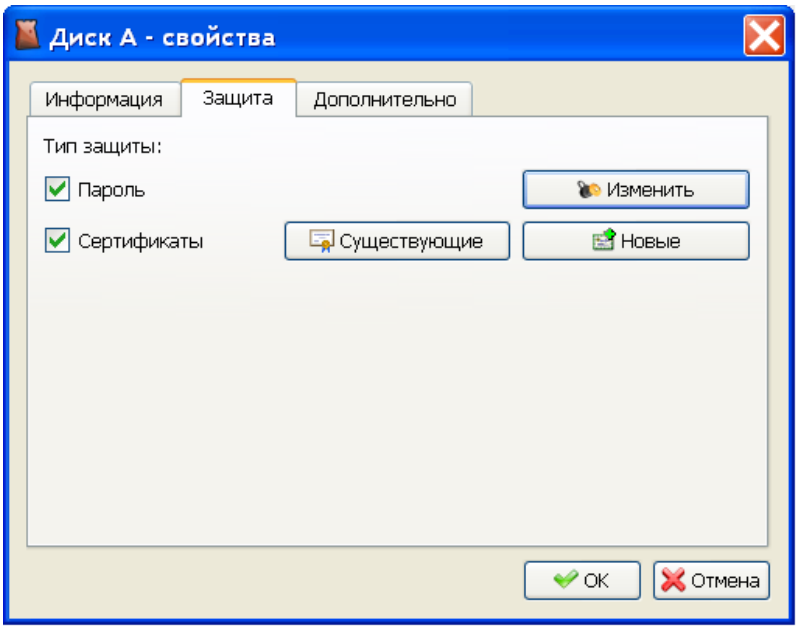

Рисунок 7.3. Диалог свойств криптообъекта - Защита

В зависимости от текущего типа защиты криптообъекта, на вкладке будут выбраны соответствующие чекбоксы.

Чекбокс «Пароль» включает или отключает защиту паролем. Для вызова диалога изменения пароля требуется нажать кнопку «Изменить».

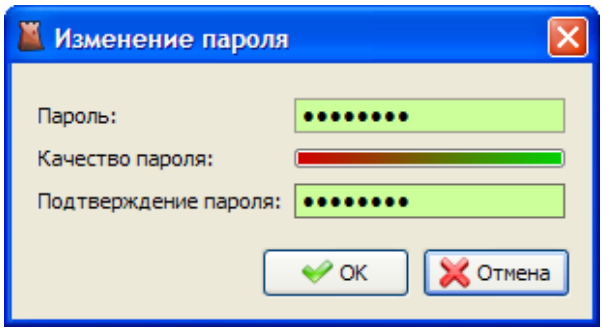

Рисунок 7.4. Диалог изменения пароля

Чтобы изменить список уже существующих сертификатов защиты, необходимо нажать кнопку «Существующие», и в появившемся диалоге отредактировать список сертификатов. В списке возможно только удаление.

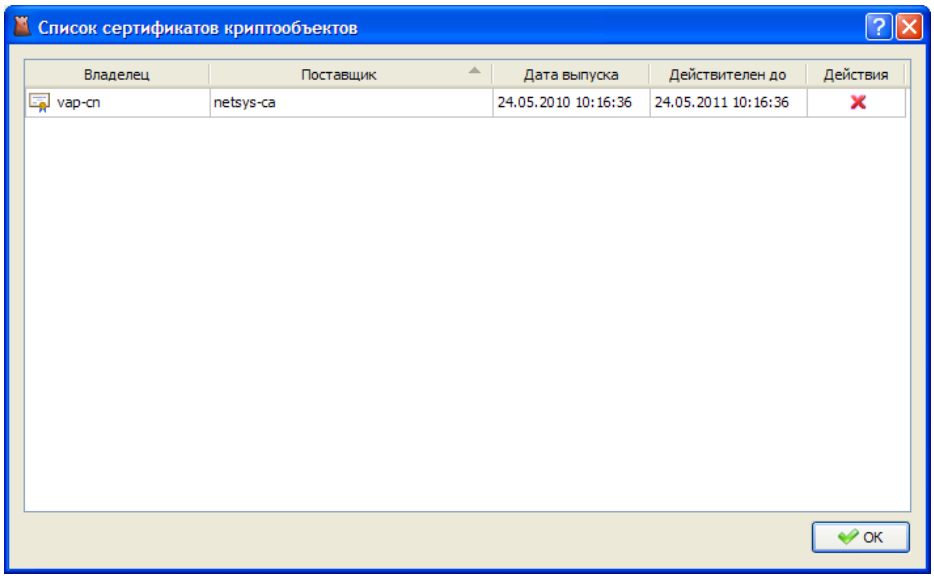

Рисунок 7.5. Диалог изменения списка существующих сертификатов

Чтобы добавить новые сертификаты защиты, необходимо нажать кнопку «Существующие» и в появившемся диалоге «Список сертификатов» следует перенести нужные сертификаты из списка «Доступные сертификаты» в список «Сертификаты защиты данных».

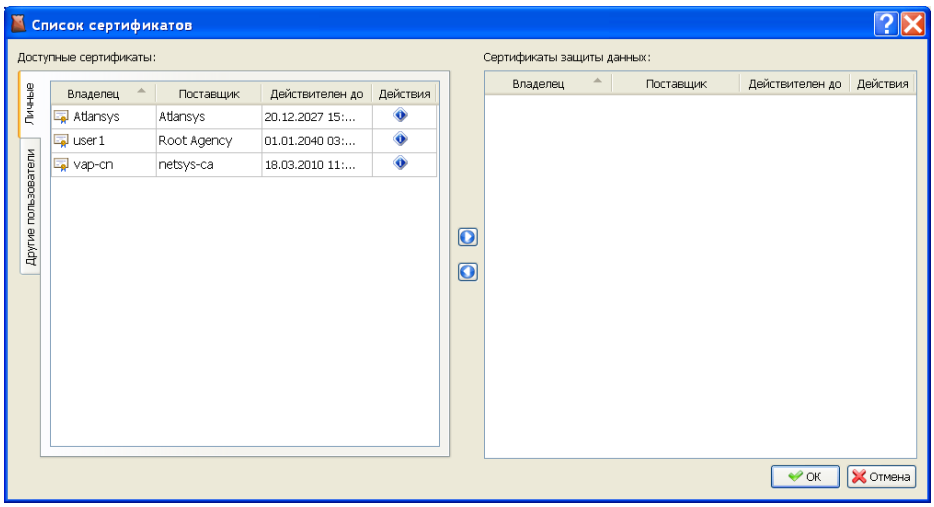

Рисунок 7.6. Диалог «Список сертификатов»

Применение новых свойств происходит после нажания кнопки «ОК» в диалоге «Список сертификатов».

7.3. Дополнительно

На вкладке «Дополнительно» можно выбрать параметр «Автоматическое открытие после перезагрузке», по которому при запуске операционной системы криптообъект будет автоматически открыт.

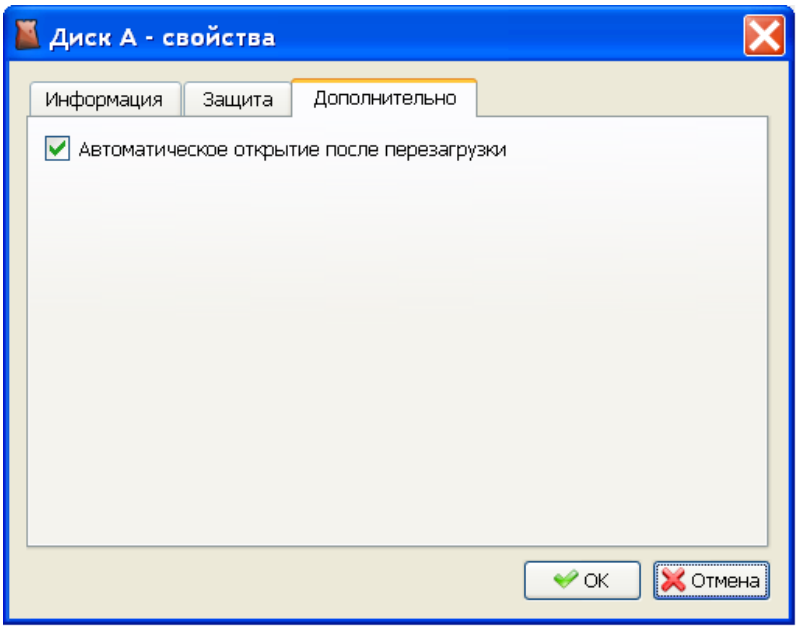

Рисунок 7.7. Диалог свойств криптообъекта - Дополнительно

Глава 8. Работа с криптоархивами

Криптоархив представляет собой зашифрованный сертификатами архив, который можно передавать через сеть Интернет или при помощи электронных носителей.

8.1. Создание криптоархивов

Процесс создания криптоархивов начинается непосредственно из контекстного меню проводника Windows или из главного меню Навигатора.

В проводнике Windows требуется выделить необходимые файлы, далее в контекстном меню проводника выбрать пункт меню «Atlansys Enterprise Security System / Создать криптоархив...».

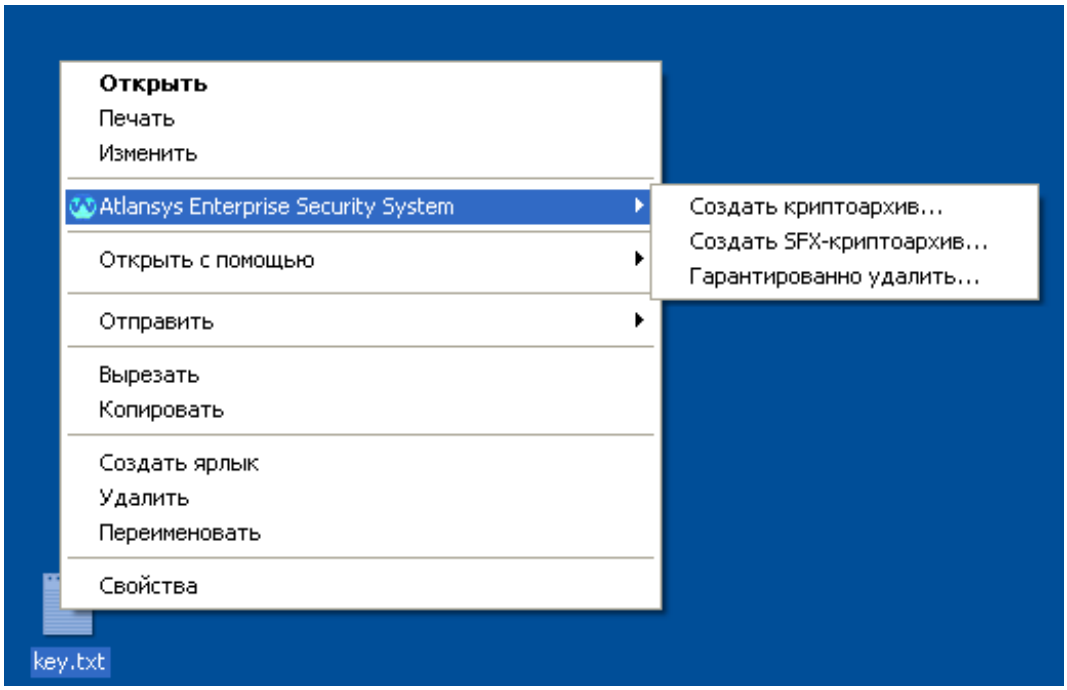

Рисунок 8.1. Запуск Atlansys ESS / Криптоархив

После этого откроется приложение создания криптоархивов.

Интерфейс

Внешний вид первой страницы «Список файлов криптоархива» диалога «Atlansys Enterprise Security System / Криптоархив»:

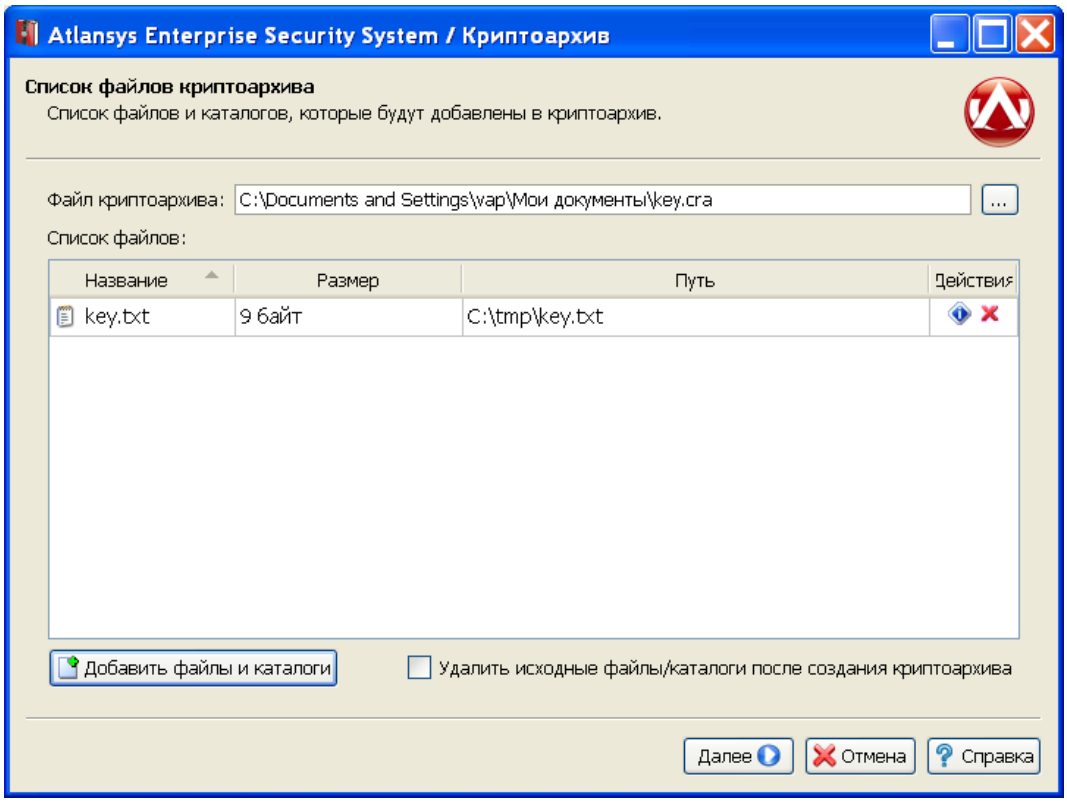

Рисунок 8.2. Окно «Atlansys Enterprise Security System / Криптоархив»

Для создания криптоархива необходимо задать путь расположения создаваемого файла криптоархива. Путь задаётся при помощьи диалога «Выбор имени файла криптоархива», который открывается при нажатии на кнопку «...», или путём ввода в строке «Файл криптоархива:». Далее формируется список файлов и каталогов, которые будут входить в состав криптоархива. Добавление новых файлов и каталогов осуществляется при помощи диалога «Выберете файлы и каталоги», который открывается при нажатии на кнопку «Добавить файлы и каталоги». Для удаления пунктов(файлов или каталогов) из таблицы «Список файлов» криптоархива необходимо нажать на кнопку «Удалить пункт из списка», которая находиться в поле «Действия» для строки удаляемого пункта. Для просмотра свойств пункта(файла или каталога) в таблицы «Список файлов» криптоархива необходимо нажать на кнопку «Показать дополнительную информацию об этом пункте», которая находиться в поле «Действия» для строки выбранного пункта. Также можно задать опцию «Удалить исходные файлы / каталоги после создания криптоархива».

Внешний вид второй страницы «Тип защиты» диалога «Atlansys Enterprise Security System / Криптоархив»:

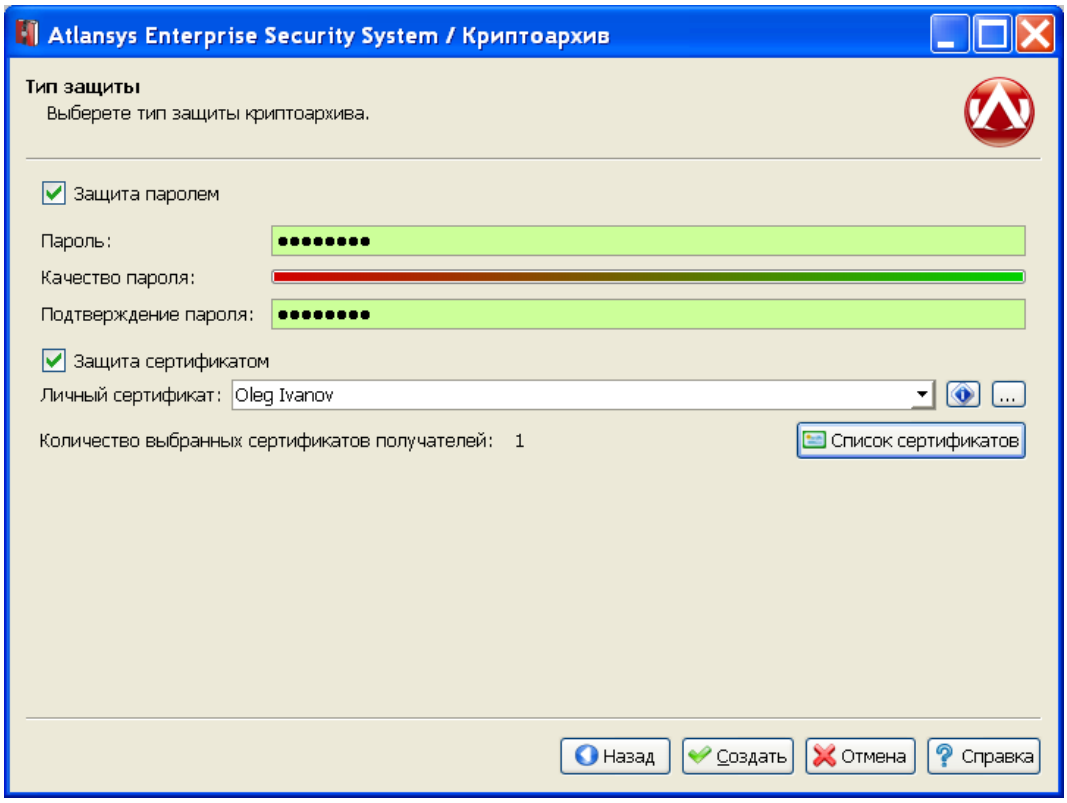

Рисунок 8.3. Окно «Список сертификатов»

На второй странице «Тип защиты» задаётся тип защиты криптоархива. Присуствуют два типа защиты: паролем или сертификатом. Для защиты паролем необходимо выбрать пункт «Защита паролем», ввести и поддтвердить пароль в полях «Пароль» и «Подтверждение пароля» соответственно. Вводимый пароль должен отвечать требованиям качества. Уровень качества пароля можно наблюдать в поле «Качество пароля». Для защиты сертификатом необходимо выбрать пункт «Защита сертификатом», задать личный сертификат и сертификаты получателей. Личный сертификат задаётся в диалоге «Выбор личного сертификата», который открывается при нажатии на кнопку «...». Свойства личного сертификата можно просмотреть в диалоге «Сертификат», который открывается при нажатии на кнопку «Отображение дополнительной информации о личном сертификате».

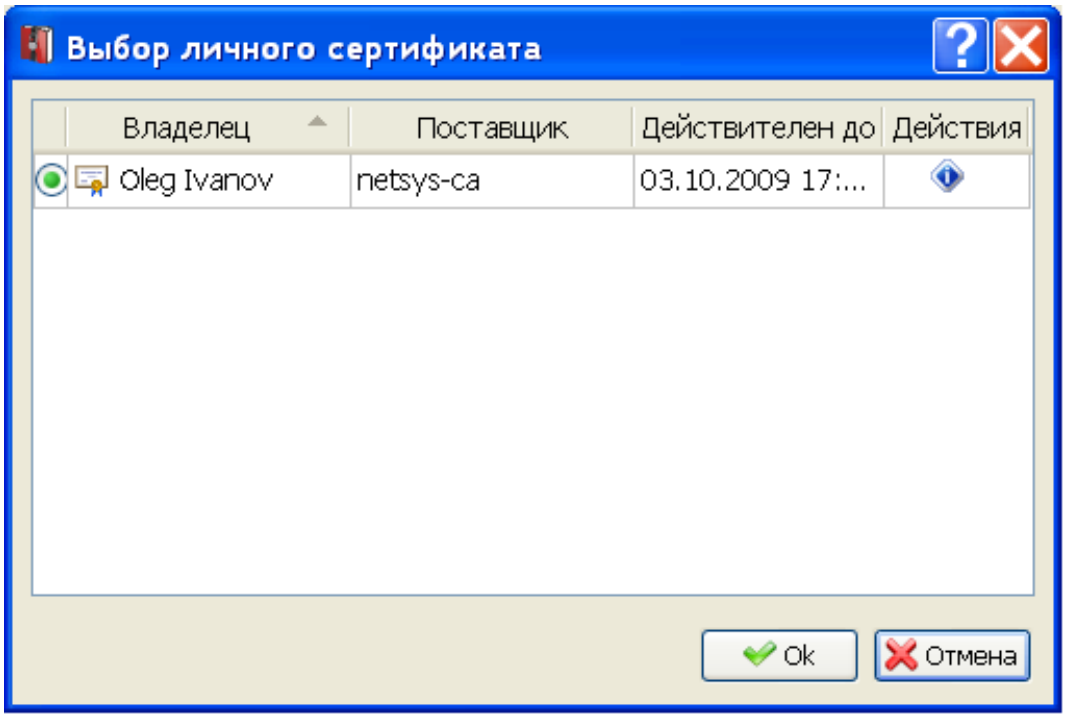

Рисунок 8.4. Окно «Выбор личного сертификата»

Сертификаты получателей задаются в диалоге «Список сертификатов», который открывается при нажатии на кнопку «Список сертификатов». Также количество выбранных сертификатов получателей отображается в поле «Количество выбранных сертификатов получателей».

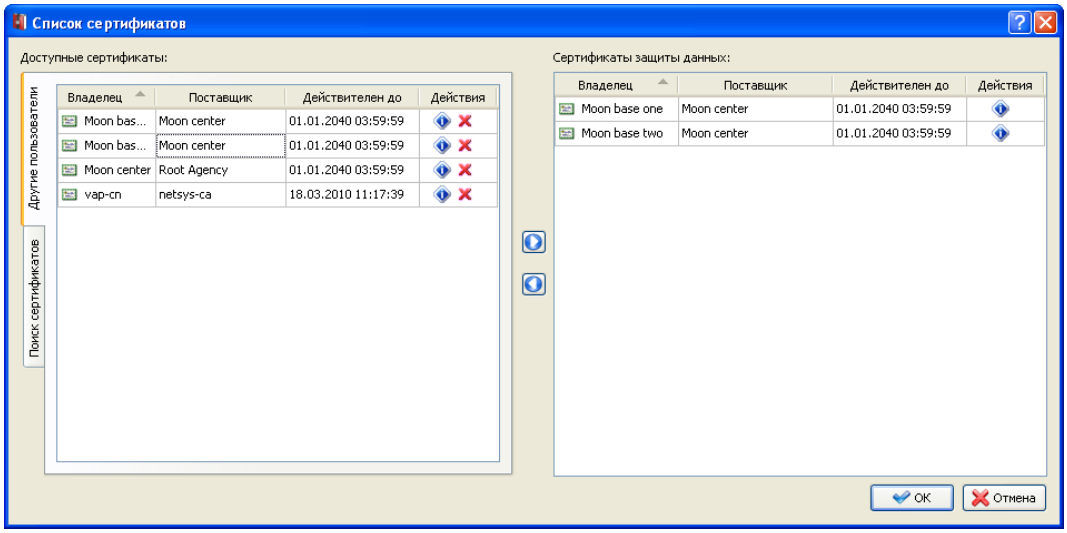

Рисунок 8.5. Окно «Список сертификатов»

После выбора типа защиты криптоархива и ввода данных необходимо нажать кнопку «Создать», после чего начнется процесс создания криптоархива.

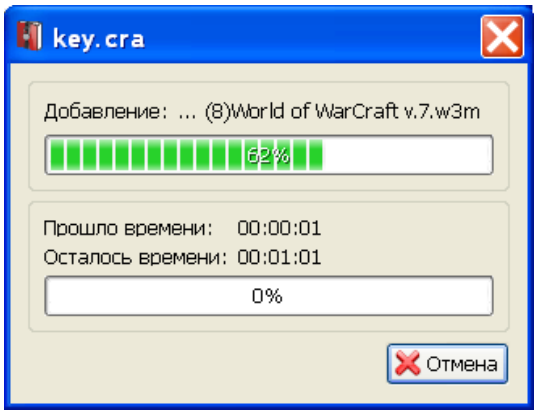

Рисунок 8.6. Прогресс создания криптоархива

По окончании процесса создания криптоархива приложение выдаст соответствующее сообщение.

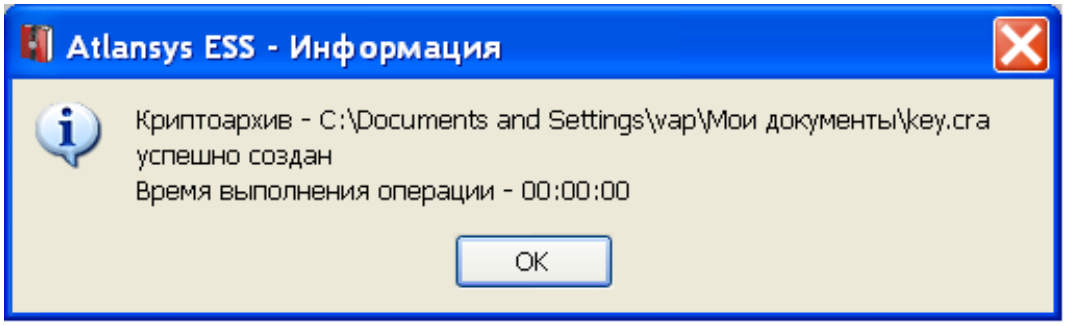

Рисунок 8.7. Завершение создания криптоархива

После успешного создания криптоархива приложение автоматически завершит работу.

8.2. Извлечение данных из криптоархива

Для извлечения данных из криптоархива необходимо в Проводнике Windows в контекстном меню криптоархива выбрать пункт меню Atlansys Enterprise Security System / Распаковать криптоархив. Второй способ - двойной щелчок левой кнопкой мыши на файле криптоархива.

Если в системе имеется хотя бы один сертификат с закрытым ключём, который использовался при создании криптоархива, то появится окно извлечения файлов из криптоархива, в котором отобразится список находящихся в криптоархиве файлов и каталогов. Иначе появится сообщение, что не найден сертификат для расшифровывания криптоархива.

Каталог назначения задает целевой каталог для извлечения выбранных файлов и каталогов. По умолчанию выбраны все файлы и каталоги, если необходимо извлечь только определенные файлы или каталоги, то необходимо отметить чекбоксы только у требуемых файлов и каталогов. Если необходимо извлекать файлы без восстановления структуры каталогов криптоархива, то необходимо установить чекбокс «Распаковать без извлечения путей».

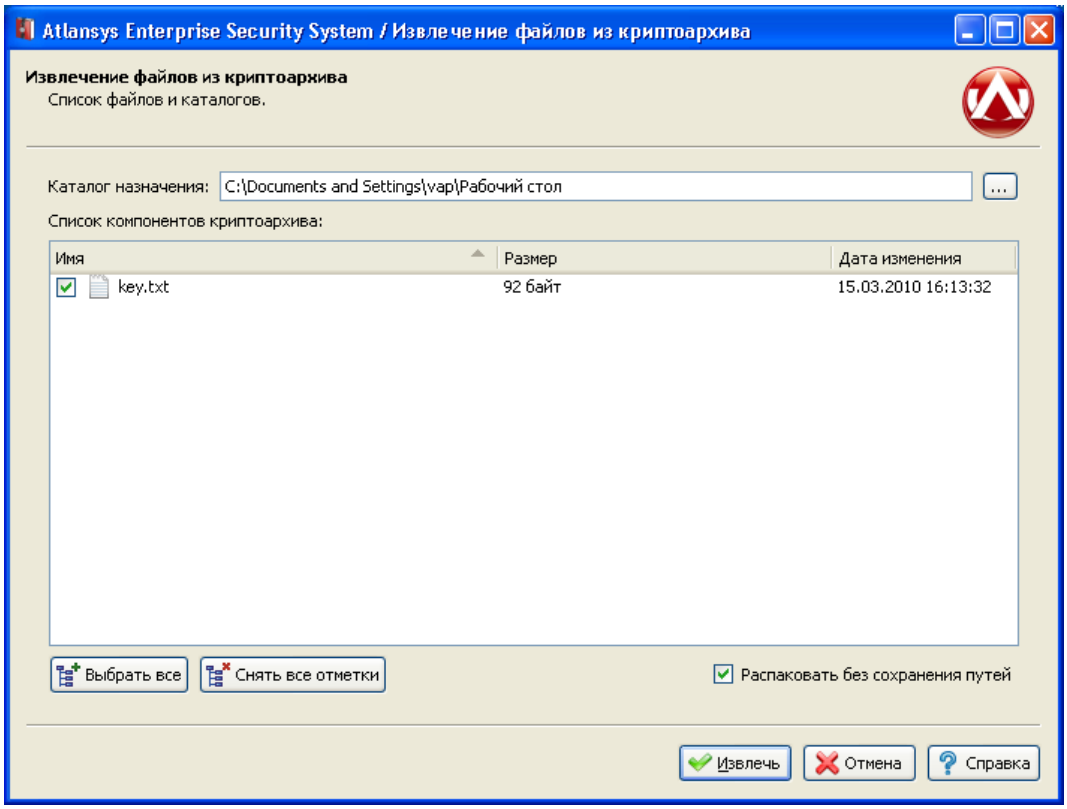

Рисунок 8.8. Окно извлечения данных из криптоархива

После выбора требуемых файлов необходимо нажать на кнопку «Извлечь», после чего начнется процесс распаковки файлов в указанный каталог. При этом отобразится диалог прогресса распаковка, после завершения его работы появится сообщение об успешной распаковки файлов в котором необходимо нажать на кнопку «Ok».

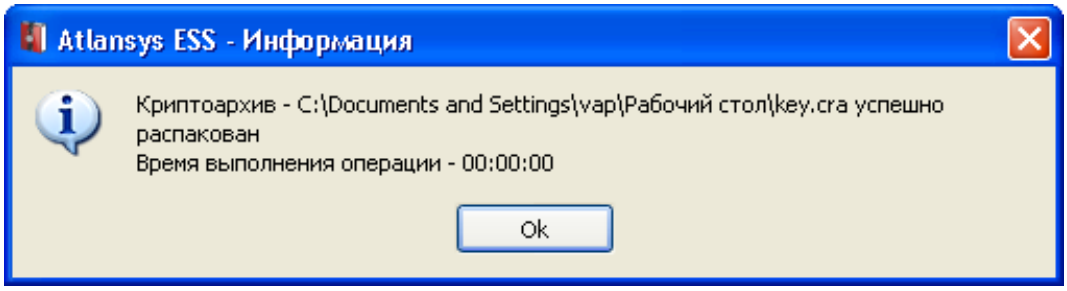

Рисунок 8.9. Завершение извлечения данных из криптоархива

Глава 9. Работа с самораспаковывающимися криптоархивами

Самораспаковывающийся (SFX) криптоархив представляет собой исполнимый модуль, в состав которого входит зашифрованный архив, защищенный паролем. Криптоархив можно безопасно передавать через сеть Интернет или при помощи электронных носителей, при этом его смогут распаковать пользователи, не имеющие Atlansys Enterprise Security System.

Замечание

В текущей версии Atlansys Enterprise Security System самораспаковывающиеся крипто-архивы можно запускать под Windows 7 и более поздних версий Windows.

9.1. Создание самораспаковывающегося криптоархива

Процесс создания криптоархивов начинается непосредственно из контекстного меню Проводника Windows. В Проводнике Windows необходимо выделить файлы, подлежащие архивированию, далее в контектсном меню Проводника выбрать пункт меню Atlansys Enterprise Security System / Создать SFX-криптоархив.

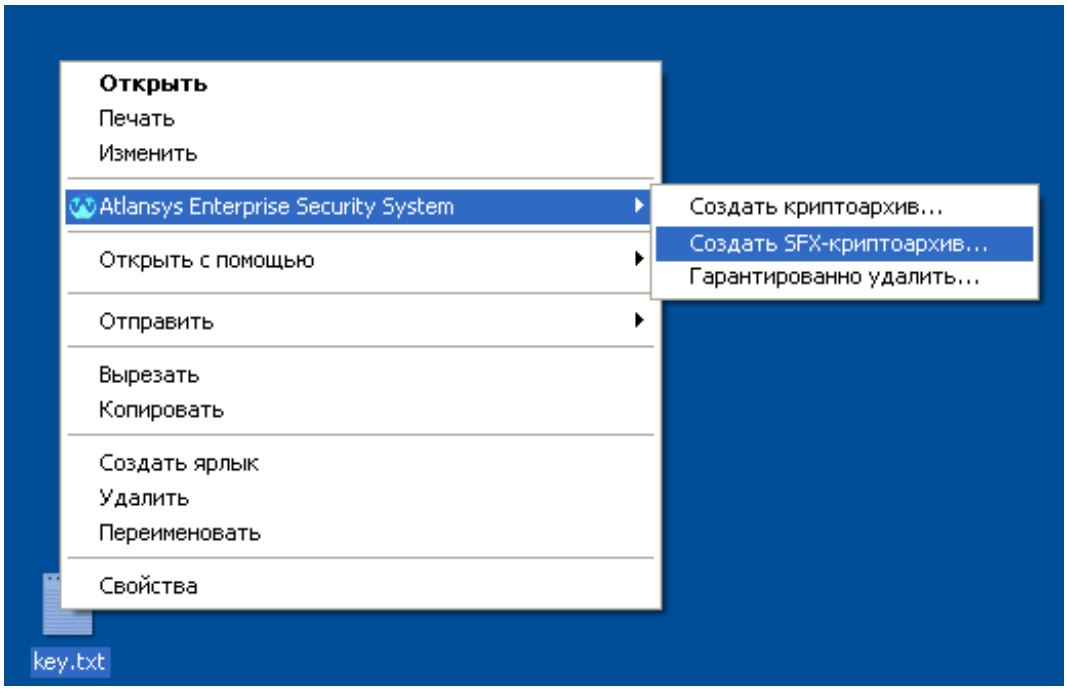

Рисунок 9.1. Создание самораспаковывающегося криптоархива

После этого откроется окно мастера создания самораспаковывающегося криптоархива, внешний вид которого изображен на рисунке:

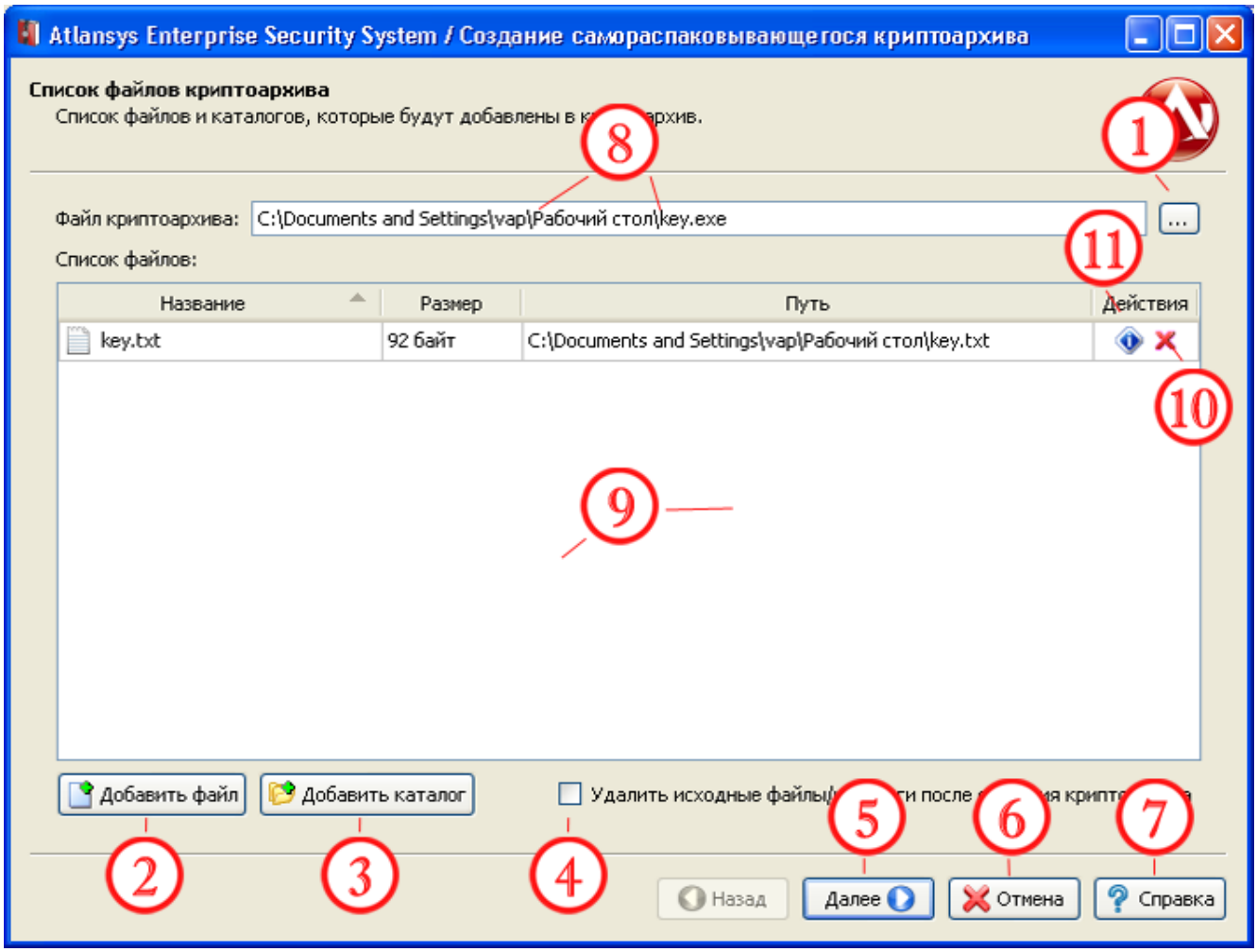

Рисунок 9.2. Окно списка файлов самораспаковывающегося криптоархива

1. Вызов диалога выбора имени и пути к создаваемому криптоархиву.
2. Вызов диалога добавления файла в криптоархив.
3. Вызов диалога добавления каталога в криптоархив.
4. Опция удаления файла / каталога после создания криптоархива.
5. Переход к следующему шагу создания криптоархива.
6. Отмена создания криптоархива и закрытие Мастера.
7. Вызов справки.
8. Путь к создаваемому файлу криптоархива.
9. Список добавляемых в криптоархив файлов.
10. Удаление текущего файла из списка
11. Вызов окна со свойствами текущего файла списка

Для добавления файлов необходимо нажать на кнопку «Добавить файл», в появившемся диалоге выбрать необходимые файлы. Для добавления каталогов необходимо нажать на кнопку «Добавить каталог», в по-

явившемся диалоге выбрать необходимые каталоги, при этом будут добавлены все подкаталоги относительно выбранного. После заполнения списка файлов необходимыми файлами и каталогами необходимо нажать на кнопку «Далее».

Откроется окно ввода пароля, в котором необходимо ввести пароль в поля «Пароль» и «Подтверждение пароля». При вводе пароля в поле «Качество пароля» будет отображаться его качественные характеристики по стойкости к подбору. Качественный пароль должен содержать не менее восьми символов из букв в верхнем и нижнем регистре, минимум одну цифру и минимум один спецсимвол. При достижении необходимого качества пароля поле ввода окрашивается в зеленый цвет, после чего необходимо повторить ввод пароля в поле «Подтверждение пароля». Когда оба пароля совпадут, оба поля ввода пароля окрасятся в зеленый цвет.

Важно

При передаче криптоархива получателю, для передачи пароля используйте защищенные каналы. Не передавайте пароль вместе с криптоархивом.

После ввода пароля необходимо нажать на кнопку «Создать», при этом откроется окно прогресса создания самораспаковывающегося криптоархива.

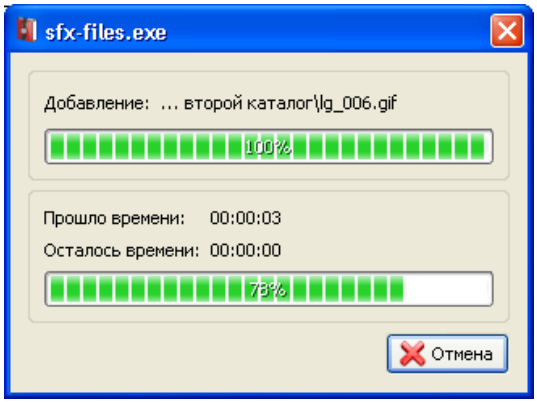

Рисунок 9.3. Прогресс создания самораспаковывающегося криптоархива

После успешного создания криптоархива появится сообщение об его успешном создании.

9.2. Извлечение данных из самораспаковывающегося криптоархива

Для извлечения данных из самораспаковывающегося криптоархива необходимо запустить исполнимый файл самораспаковывающегося криптоархива. После этого появится окно, в котором необходимо ввести пароль, использовавшийся для создания криптоархива и нажать кнопку «Далее».

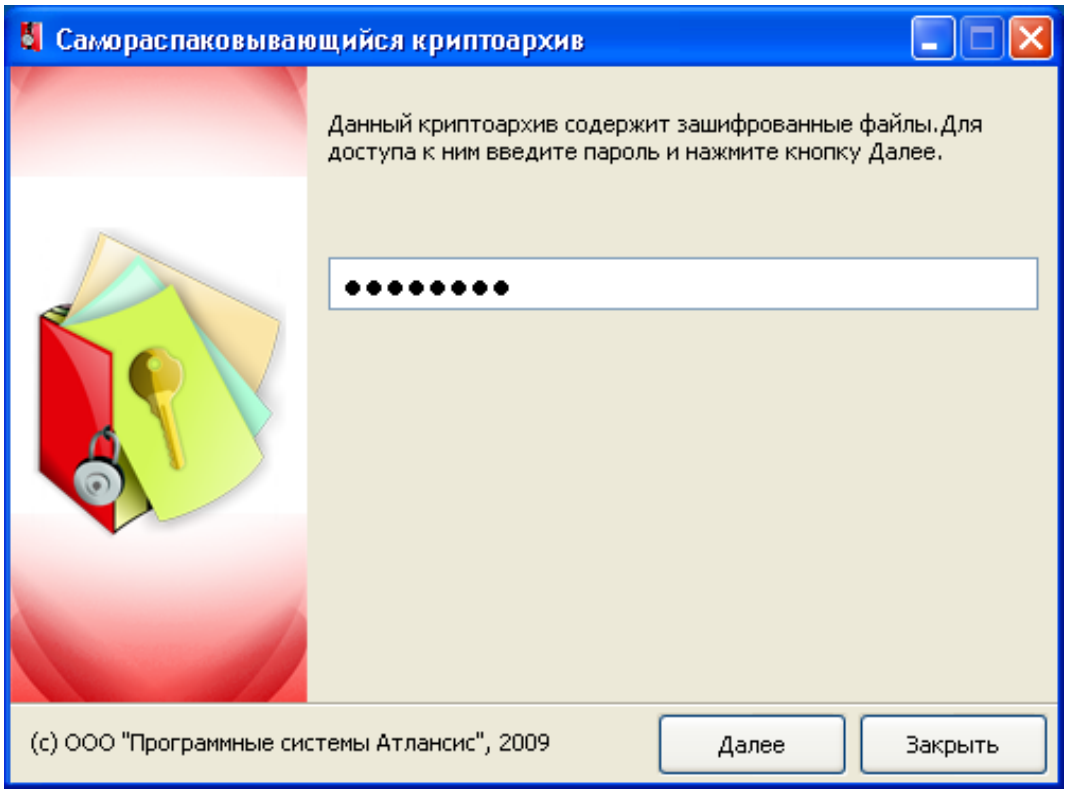

Рисунок 9.4. Самораспаковывающийся криптоархив. Окно ввода пароля.

Если введенный пароль правильный, то в окне отобразятся список файлов и каталогов, входящих в криптоархив и путь для распаковки криптоархива. По умолчанию выбирается каталог, из которого запускался исполнимый модуль самораспаковывающегося криптоархива. Для распаковки необходимо выбрать нужные файлы и нажать на кнопку «Извлечь», после чего начнется процесс распаковки.

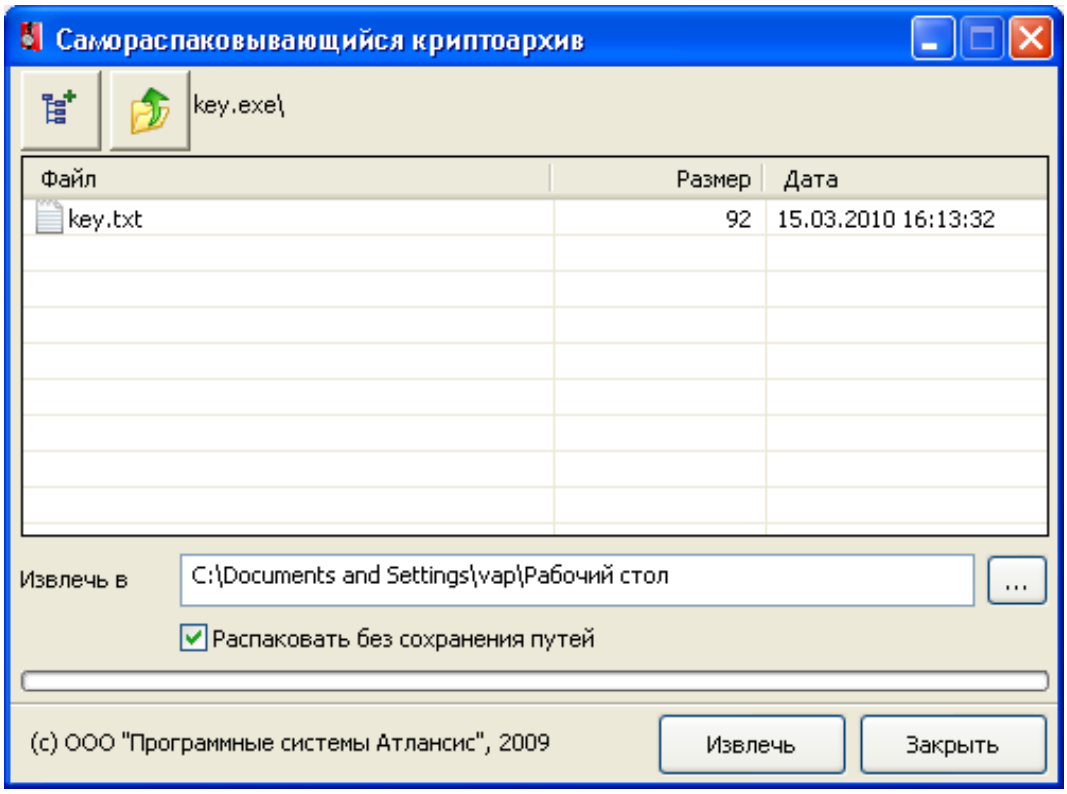

Рисунок 9.5. Самораспаковывающийся криптоархив. Выбор файлов и пути распаковки.

Глава 10. Гарантированное удаление файлов

10.1. Гарантированное удаление

Обычные процедуры удаления файлов в Windows не удаляют содержимого файлов на диске. С помощью специальных утилит возможно полное восстановление данных из удаленных файлов. Для надежного удаления данных необходимо использовать специальные методы гарантированного удаления, которые позволяют максимально уменьшить вероятность восстановления удаленных файлов с помощью программных средств.

Важно

Будьте осторожны! После гарантированного удаления файлов их содержимое невозможно восстановить.

Для гарантированного удаления файлов и каталогов необходимо:

1. В Проводнике Windows выделить необходимые файлы и/или каталоги, далее в контекстном меню Проводника выбрать пункт меню Atlansys Enterprise Security System / Гарантированно удалить.

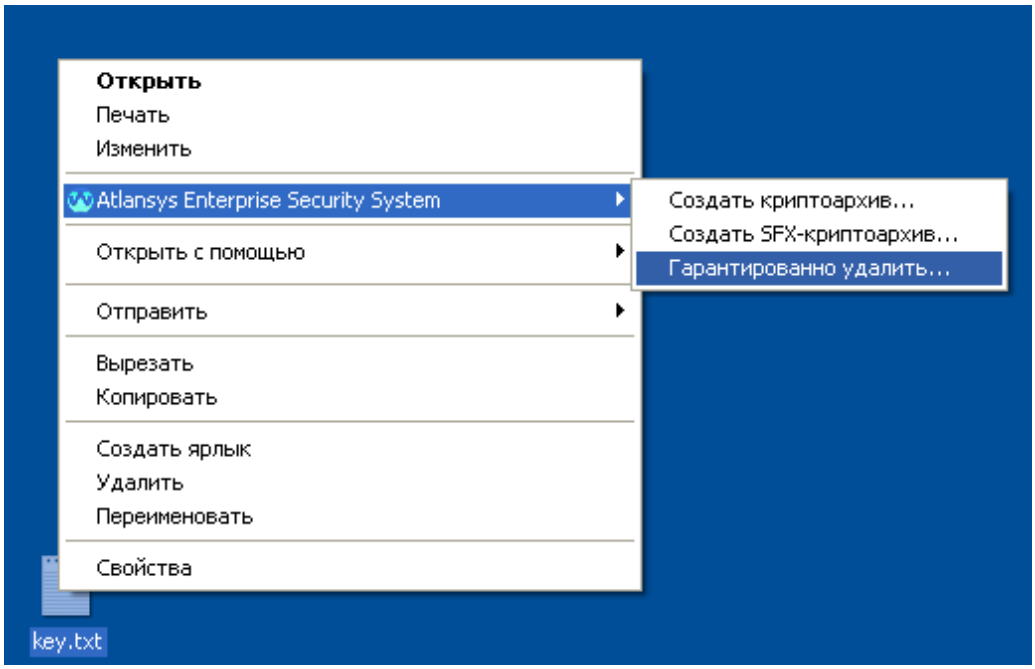

Рисунок 10.1. Контекстное меню Гарантированно удалить.

2. Далее появится предупреждение, о том, что файлы будут удалены без возможности восстановления. Для продолжения необходимо нажать кнопку «Да».

3. После этого появится диалог с прогрессом удаления файлов и каталогов. В нем отображается имя текущего удаляемого файла, проценты обработки данного файла, прошедшее время с начала процесса удаления, время, оставшееся до завершения и общий процент завершения удаления всех выбранных файлов. Прервать процесс удаления можно нажатием на кнопку «Отмена», однако файлы, удаленные к этому моменту, восстановить будет невозможно.

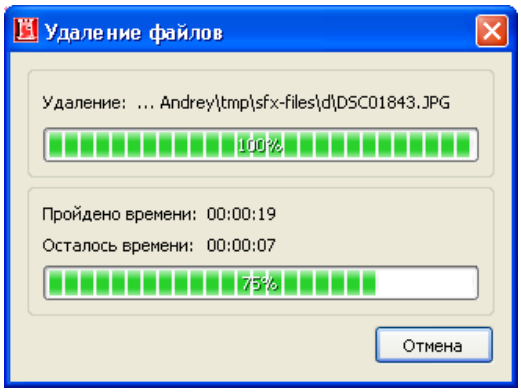

Рисунок 10.2. Диалог удаления файлов

4. После удаления всех файлов диалог удаления файлов закроется автоматически.

Глава 11. Журнал событий

11.1. Журнал событий

Журнал событий служит для отоброжения лог сообщений пользователей. В журнале реализована гибкая система фильтрации логов, по таким критериям, как: имя пользователя, хост, дата, уровень лога, категория лога, модуль.

Чтобы запустить журнал регистрации событий, необходимо в главном меню зайти в подменю «Файл» и выбрать «Журнал событий...»

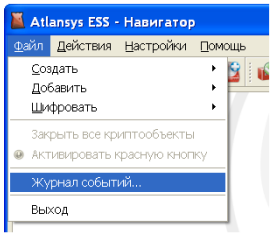

Рисунок 11.1. Запуск журнала событий

После этого отобразится окно журнала событий.

Интерфейс

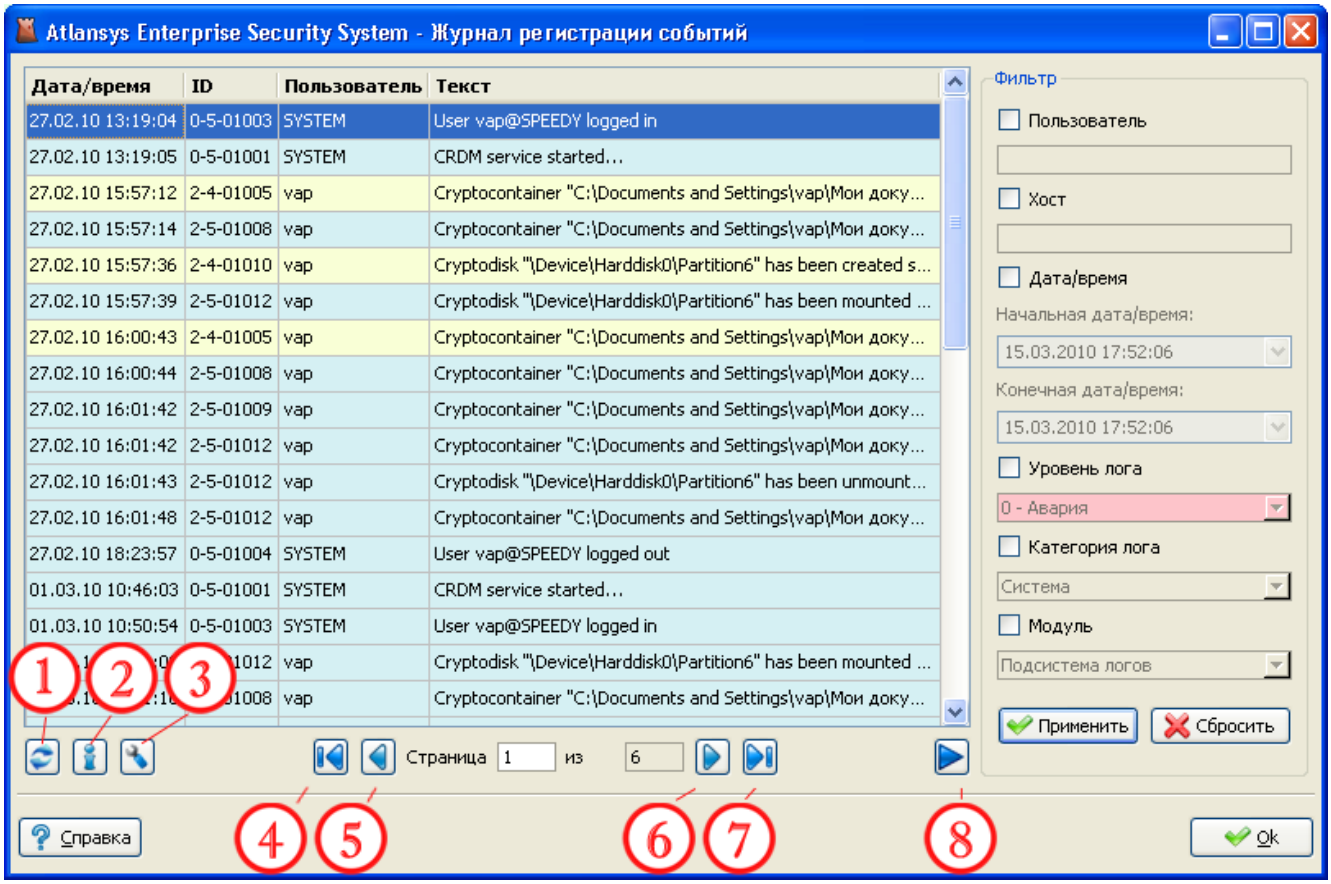

Рисунок 11.2. Окно журнала событий

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

При нажатии на кнопку информации по выбранному сообщению отобразится диалог с полной информацией по этому сообщению:

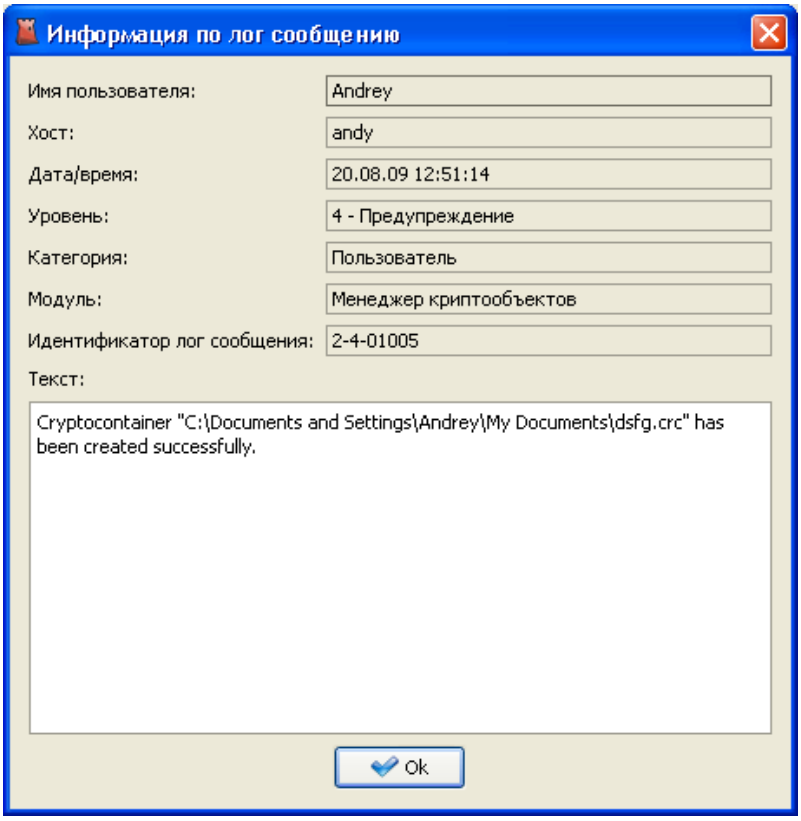

Рисунок 11.3. Информация по лог сообщению

При переходе в настройки журнала регистрации событий, отобразится следующее окно, в котором можно задать порядок отображения сообщений и необходимые столбцы журнала событий:

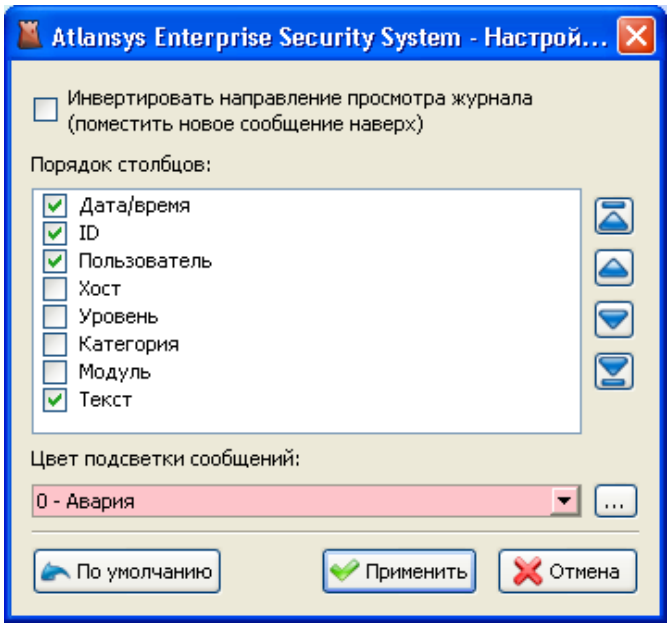

Рисунок 11.4. Настройки журнала регистрации событий

Столбцы можно включать, отмечая соответствующие чекбоксы, и отсортировать в более удобном порядке, выбрав необходимый столбец и нажимая на кнопки перемешения столбца.

Фильтр журнала событий служит для быстрого поиска заданных событий и включает в себя такие пункты, как:

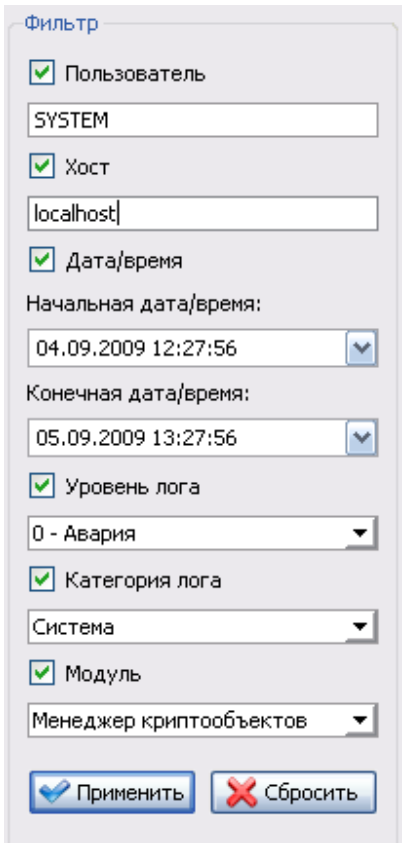

Рисунок 11.5. Фильтр журнала событий

1. Пользователь - идентификатор (имя) пользователя, сгенерировавший событие. События, генерируемые системой, отображаются под именем SYSTEM.
2. Хост - адрес хоста, на котором произошло событие.
3. Дата/время - начальная и конечная даты, в промежуток между которыми произошли события.
4. Уровень лога - уровень отображаемых лог-сообщений. Будут отображатся сообщения с меньшим или равным выбранному.
5. Категория лога - источник сообщений, система или пользователь.
6. Модуль системы, сгенерировавший сообщение.

Для применения настроек фильтрации необходимо нажать кнопку «Применить».

Глава 12. Электронно-цифровая подпись

12.1. Назначение электронно-цифровой подписи (ЭЦП)

Электронно-цифровая подпись служит с одной стороны, для подтверждения владельца подписанного документа, а с другой, обеспечивает гарантию неизменности данных. До использования этой функции, ее следует настроить (см. Раздел 2.4).

12.2. Подписывание файлов

Чтобы подписать файл (или несколько файлов), выделите их в проводнике Windows, и в контекстном меню выберите пункт Atlansys Enterprise Security System / Подписать файлы.

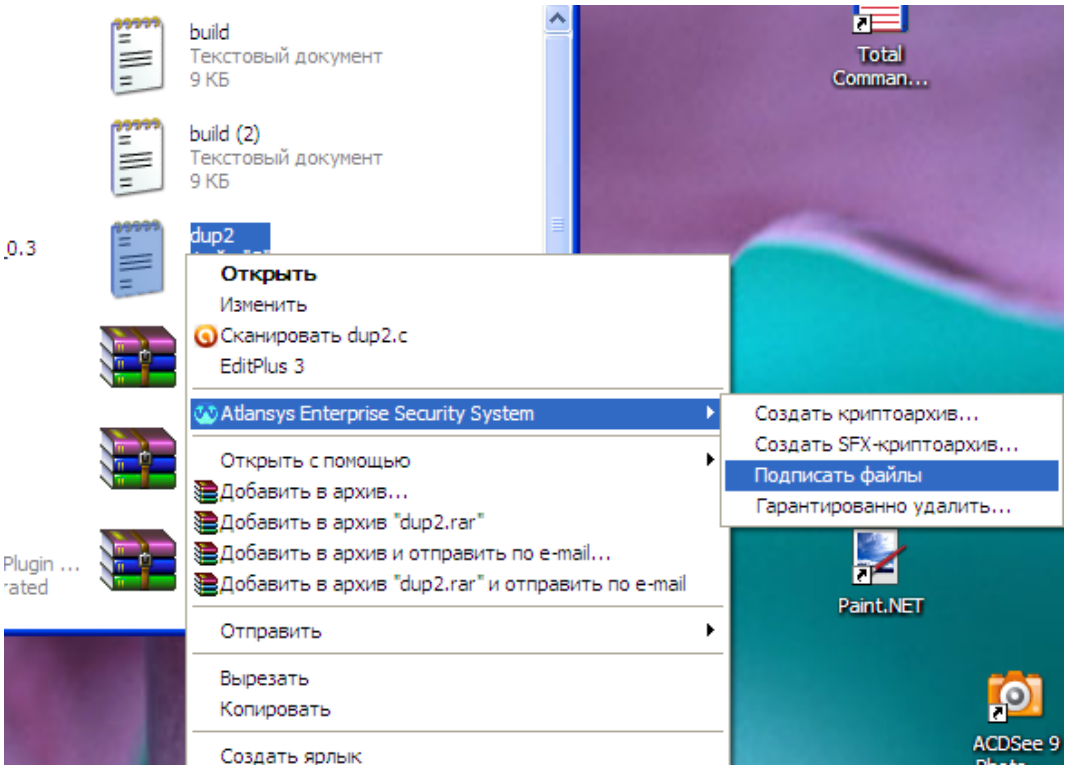

Рисунок 12.1. Выбор файлов для подписывания

Ппоявится диалог с прогрессом выполнения операции подписывания. В случае, если файлы ЭЦП уже существуют, программа выдаст предупреждение с вопросом о перезаписи.

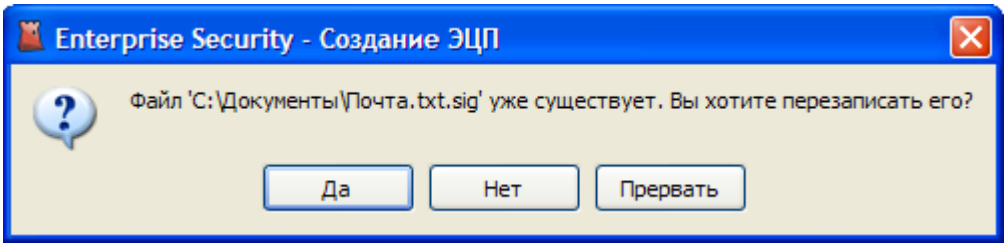

Рисунок 12.2. Вопрос о перезаписи файла ЭЦП

После завершения всех операций в каталоге, где размещены подписываемые файлы, появятся файлы ЭЦП вида <**имя_файла.расширение_файла.sig**>.

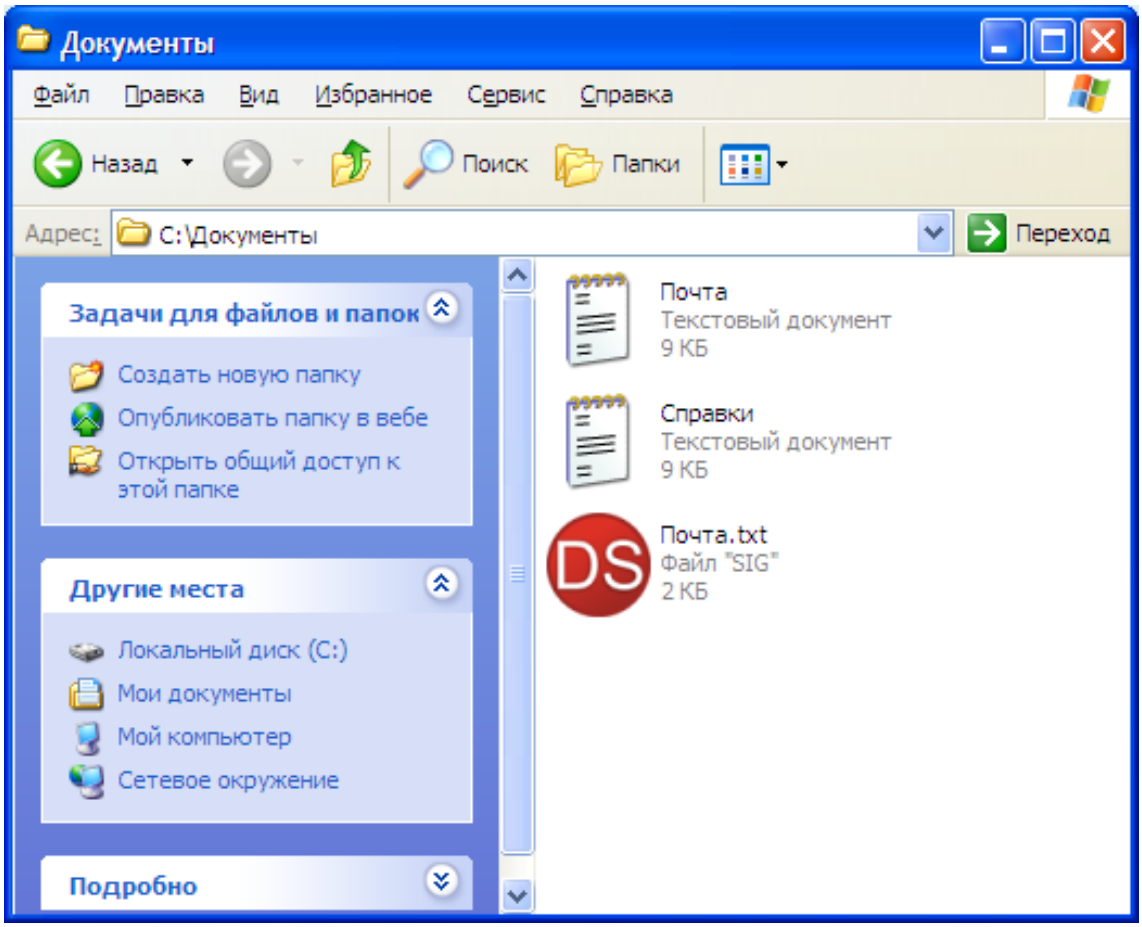

Рисунок 12.3. Список файлов после подписывания

12.3. Проверка ЭЦП

Чтобы проверить ЭЦП, нужно выделить файл цифровой подписи, и в контекстном меню проводника Windows выбрать пункт Atlansys Enterprise Security System / Проверить подпись.

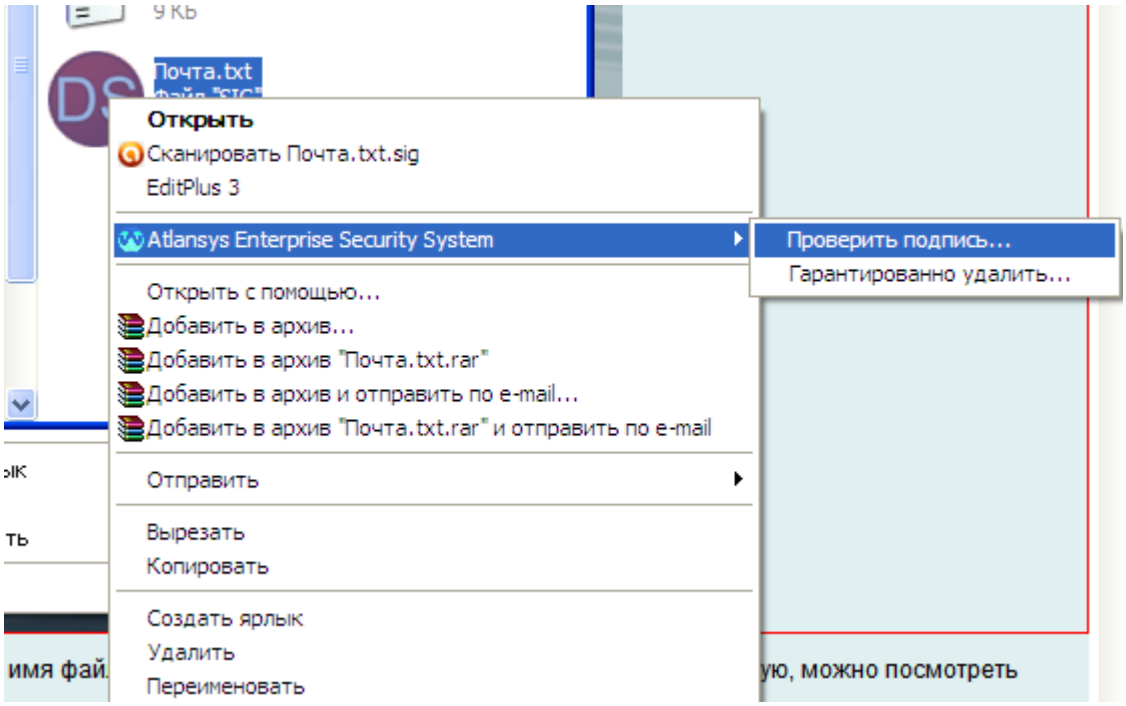

Рисунок 12.4. Выбор файла для проверки ЭЦП

Появится окно проверки цифровой подписи, в котором отображаются имя файла ЭЦП, имя подписавшего, а также кнопка, нажав которую, можно посмотреть информацию о сертификате подписавшего.

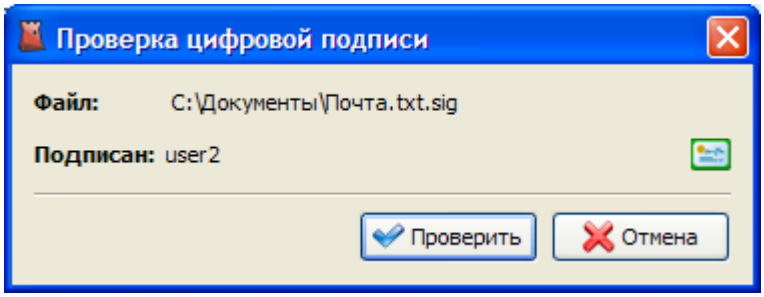

Рисунок 12.5. Диалог проверки ЭЦП

После нажатия на кнопку Проверить начнется процесс проверки ЭЦП. В случае, если сертификат, при помощи которого создавалась ЭЦП, не является валидным, программа выдаст предупреждение.

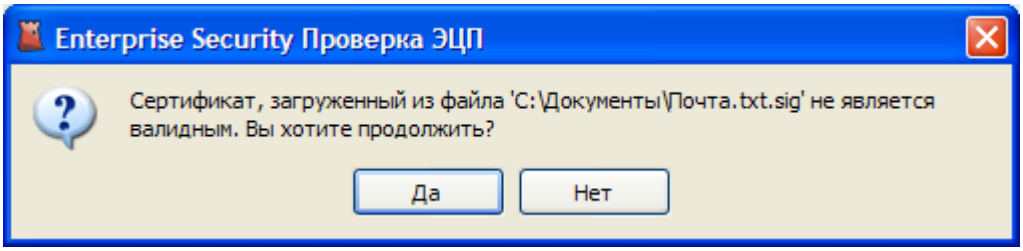

Рисунок 12.6. Предупреждение о невалидном сертификате

Далее появится окно отображения прогресса проверки. В случае успеха проверки, программа выдаст соответствующее сообщение. Если же проверка завершилась неудачей, это значит, что либо подписанный файл был изменен после подписывания, либо был изменен сам файл цифровой подписи.

Глава 13. 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».