

Руководство пользователя



Atlansys Software

Atlansys **ESS Server**

Atlansys Enterprise Security System

Руководство пользователя

Версия 5.0.4

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.

Copyright © ООО «Программные системы Атлансис», 2020

Содержание

| | |
|--|----|
| Введение | vi |
| 1. Назначение документа | vi |
| 2. Сведения о продукте | vi |
| 3. Технические характеристики | vi |
| 4. Системные требования | vi |
| 5. Лицензионный договор | vi |
| 1. Установка и удаление программного обеспечения | 1 |
| 1.1. Установка программного обеспечения с помощью интерактивного инсталлятора | 1 |
| 1.2. Обновление программного обеспечения | 7 |
| 1.3. Установка программного обеспечения с использованием конфигурационного файла | 10 |
| 1.4. Удаление программного обеспечения | 11 |
| 2. Консоль криптосервера | 12 |
| 2.1. Назначение | 12 |
| 2.2. Запуск программы | 12 |
| 2.3. Интерфейс | 12 |
| 2.4. Настройки продукта | 14 |
| 3. Работа с криптоконтейнерами | 16 |
| 3.1. Введение | 16 |
| 3.2. Создание криптоконтейнера | 16 |
| 3.3. Добавление криптоконтейнера | 19 |
| 3.4. Работа с криптоконтейнерами | 20 |
| 3.5. Удаление криптоконтейнера | 22 |
| 4. Работа с криптодисками | 25 |
| 4.1. Введение | 25 |
| 4.2. Создание криптодиска | 25 |
| 4.3. Добавление криптодиска | 31 |
| 4.4. Работа с криптодисками | 32 |
| 4.5. Удаление криптодиска | 34 |
| 5. Свойства криптообъекта | 36 |
| 5.1. Диалог свойств криптообъекта | 36 |
| 5.2. Изменение пароля и сертификатов | 37 |
| 5.3. Дополнительно | 40 |
| 5.4. Пользовательские скрипты | 40 |
| 6. Журнал событий | 42 |
| 6.1. Журнал событий | 42 |
| 7. Техническая поддержка | 46 |
| A. Лицензионный договор | 47 |
| A.1. Лицензионный договор с конечным пользователем | 47 |

Список иллюстраций

| | |
|--|----|
| 1.1. Установка Atlansys Enterprise Security System | 1 |
| 1.2. Лицензионный договор | 2 |
| 1.3. Регистрация | 3 |
| 1.4. Выбор компонентов консоли управления криптосервером | 4 |
| 1.5. Выбор каталога для установки программы | 5 |
| 1.6. Запуск процесса установки | 6 |
| 1.7. Процесс установки | 6 |
| 1.8. Завершение установки | 7 |
| 1.9. Обновление Atlansys Enterprise Security System | 8 |
| 1.10. Процесс установки | 9 |
| 1.11. Завершение установки | 10 |
| 2.1. Запуск Консоли криптосервера | 12 |
| 2.2. Аутентификация на криптосервере | 12 |
| 2.3. Главное окно Консоли криптосервера | 13 |
| 2.4. Меню «Файл» | 14 |
| 2.5. Меню «Действия» | 14 |
| 2.6. Меню «Настройки» | 14 |
| 2.7. Язык | 15 |
| 2.8. Регистрация событий | 15 |
| 3.1. Меню «Файл» / «Создать» / «Криптоконтейнер» | 16 |
| 3.2. Мастер создания криптоконтейнеров. | 17 |
| 3.3. Мастер создания криптоконтейнеров. Способы защиты. | 18 |
| 3.4. Мастер создания криптоконтейнеров. Прогресс создания. | 19 |
| 3.5. Меню «Файл» / «Добавить» / «Криптоконтейнер» | 19 |
| 3.6. Мастер добавления криптоконтейнеров | 20 |
| 3.7. Диалог открытия криптоконтейнера | 20 |
| 3.8. Список криптоконтейнеров и криптодисков | 21 |
| 3.9. Меню «Действия» | 22 |
| 3.10. Контекстное меню криптоконтейнера | 22 |
| 3.11. Панель инструментов, кнопка «Открыть» | 22 |
| 3.12. Панель инструментов, кнопка «Удалить» | 23 |
| 3.13. Мастер удаления криптоконтейнеров | 24 |
| 4.1. Меню «Файл» / «Создать» | 25 |
| 4.2. Мастер создания криптодисков. Выбор раздела. | 26 |
| 4.3. Мастер создания криптодисков. Метка диска и описание. | 27 |
| 4.4. Мастер создания криптодисков. Способы защиты. | 28 |
| 4.5. Мастер создания криптодисков. Сводная информация. | 29 |
| 4.6. Мастер создания криптодисков. Предупреждение. | 29 |
| 4.7. Мастер создания криптодисков. Прогресс создания. | 30 |
| 4.8. Процесс преобразования криптодиска. | 30 |
| 4.9. Мастер создания криптодисков. Заполнение случайными данными. | 31 |
| 4.10. Меню «Файл» / «Добавить» / «Криптодиск» | 31 |
| 4.11. Мастер добавления криптодисков. Выбор раздела. | 32 |
| 4.12. Мастер добавления криптодисков. Сводная информация о криптодиске. | 32 |
| 4.13. Меню «Действия» | 33 |
| 4.14. Контекстное меню криптодиска | 33 |
| 4.15. Панель инструментов | 34 |
| 4.16. Диалог открытия криптодиска | 34 |
| 4.17. Панель инструментов, кнопка «Удалить» | 34 |
| 4.18. Мастер удаления криптодисков | 35 |
| 5.1. Кнопка вызова диалога свойств криптообъекта | 36 |
| 5.2. Диалог свойств криптообъекта - Информация | 37 |
| 5.3. Диалог свойств криптообъекта - Информация | 37 |
| 5.4. Диалог свойств криптообъекта - Защита | 38 |
| 5.5. Диалог свойств криптообъекта - Защита | 38 |

| | |
|---|----|
| 5.6. Диалог изменения пароля | 39 |
| 5.7. Диалог изменения списка существующих сертификатов | 39 |
| 5.8. Диалог «Список сертификатов» | 40 |
| 5.9. Диалог свойств криптообъекта - Дополнительно | 40 |
| 5.10. Диалог свойств криптообъекта - Пользовательские скрипты | 41 |
| 6.1. Запуск журнала событий | 42 |
| 6.2. Окно журнала событий | 43 |
| 6.3. Информация по лог сообщению | 44 |
| 6.4. Настройки журнала регистрации событий | 44 |
| 6.5. Фильтр журнала событий | 45 |

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

Продукт Atlansys Enterprise Security System обеспечивает хранение данных пользователей на защищенных с помощью криптографического шифрования сетевых дисках, размещенных на выделенном сервере. Защита данных на дисках осуществляется с помощью сертификатов или паролей.

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

3. Технические характеристики

| | |
|---|--|
| Поддерживаемые операционные системы | ОС Windows 7, Windows 8, Windows 8.1, Windows 10 |
| Поддержка файловых систем | FAT, FAT32, NTFS |
| Создание криптоархивов | Нет |
| Создание криптоконтейнеров | Есть |
| Создание криптодисков с сохранением существующих данных | Есть |
| Поддерживаемые алгоритмы шифрования. (В зависимости от типа поставки продукта набор алгоритмов шифрования может отличаться от указанных). | AES, Blowfish |
| Алгоритмы гарантированного уничтожения файлов | ГОСТ P50739-95, DoD 5220.22-M, NAVSO P-5239-26 |
| Максимальный размер защищаемых дисков | Ограничен файловой системой диска |

1

4. Системные требования

| | |
|--|---|
| Процессор | Intel Pentium III, AMD Athlon или выше |
| Операционная система для сервера | Windows Server 2008, 2012, 2016, 2019 |
| Операционная система для консоли управления сервером | Windows 7, Windows 8, Windows 8.1, Windows 10 |
| Объем оперативной памяти | не менее 128 Мбайт |
| Свободное место на диске | минимум 50 Мбайт |
| Разрешение экрана | минимум 800x600 пикселей |
| Привод CD-ROM | при инсталляции с компакт-диска |
| Подключение к Internet | для регистрации продукта |

5. Лицензионный договор

Приложение А данного руководства содержит текст Лицензионного договора, с которым необходимо ознакомиться перед установкой, копированием или каким-либо другим использованием данного продукта.

¹В зависимости от типа поставки продукта набор алгоритмов шифрования может отличаться от указанных.

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 администратора необходимо выполнить следующие действия:

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

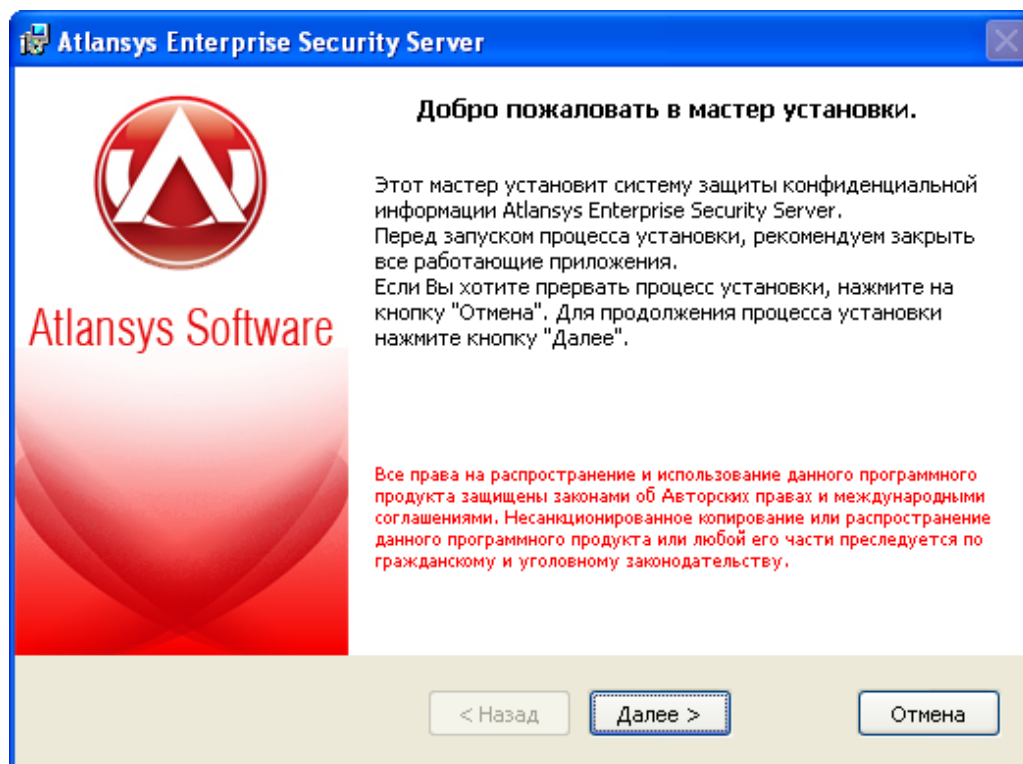


Рисунок 1.1. Установка Atlansys Enterprise Security System

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».

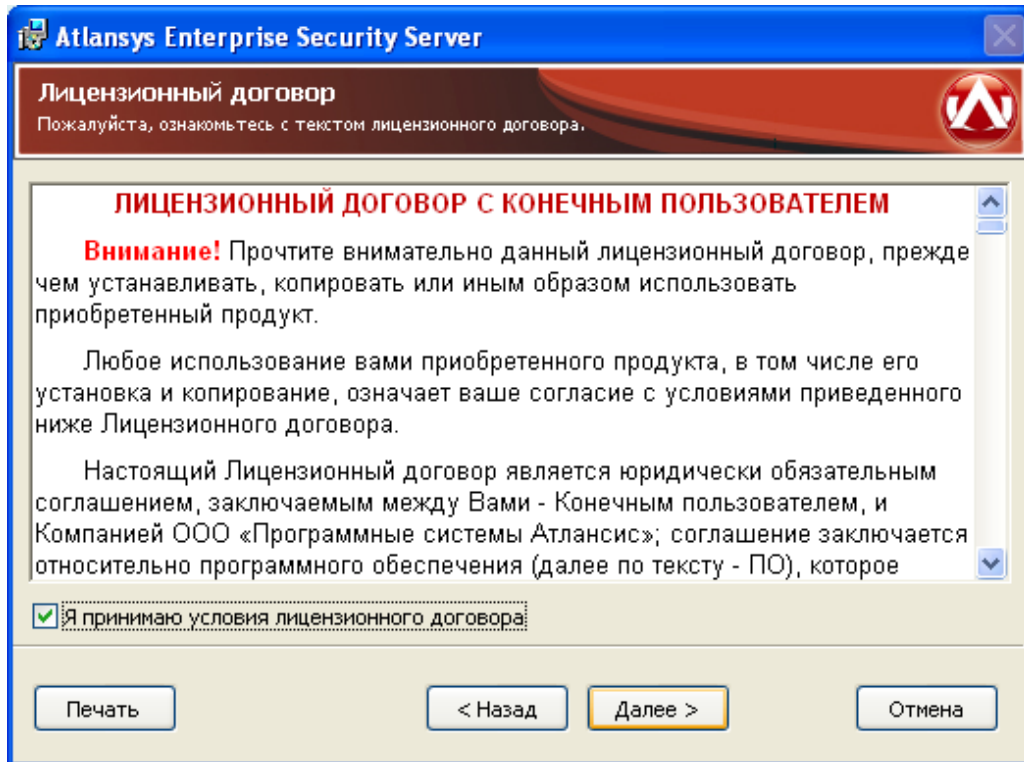
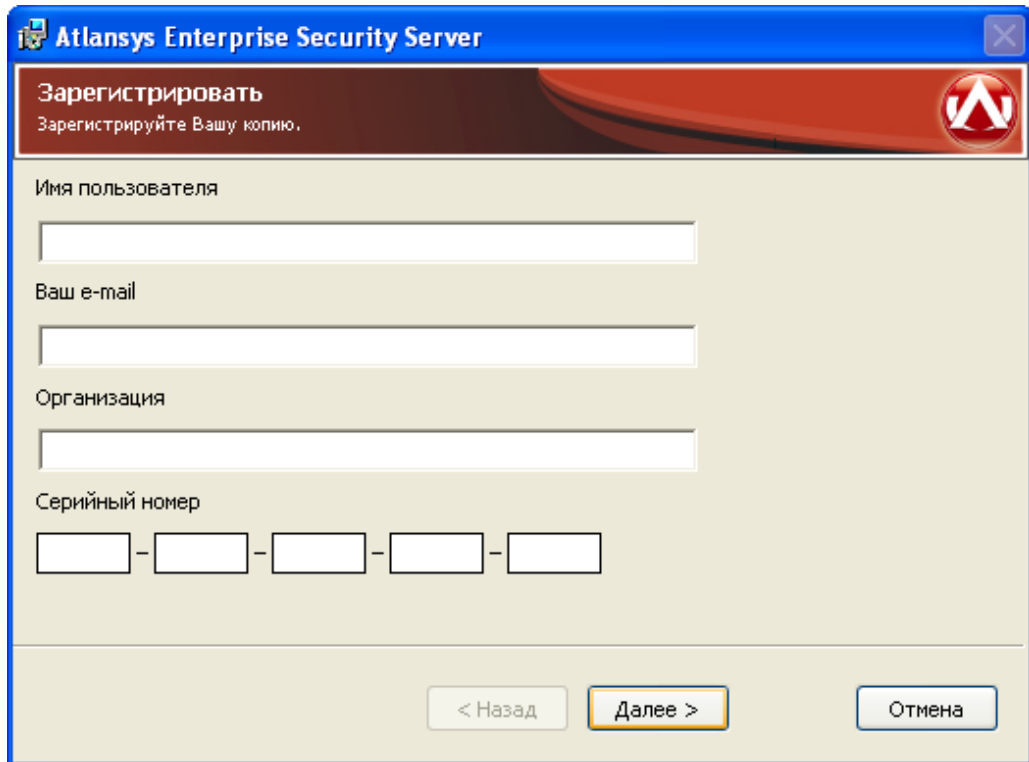


Рисунок 1.2. Лицензионный договор

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».



Atlansys Enterprise Security Server

Зарегистрировать
Зарегистрируйте Вашу копию.

Имя пользователя

Ваш e-mail

Организация

Серийный номер
 - - - -

< Назад **Далее >** Отмена

Рисунок 1.3. Регистрация

4. Выбрать компоненты программного обеспечения, которые необходимо установить. По умолчанию на рабочую станцию администратора будут установлены все компоненты консоли управления.

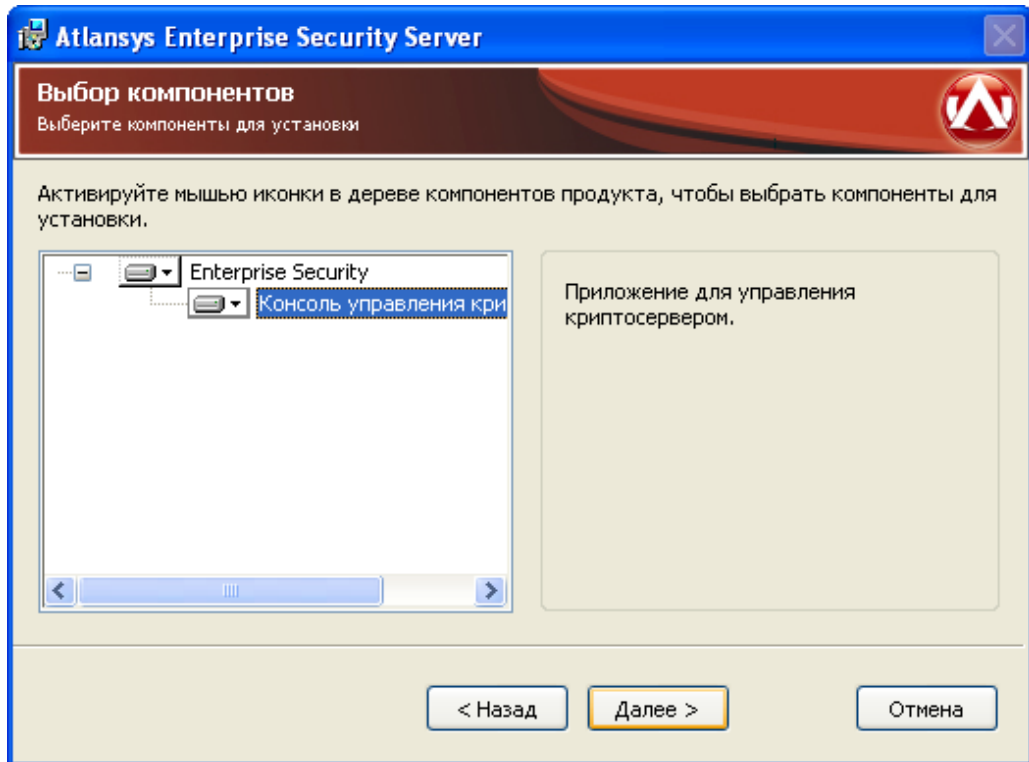


Рисунок 1.4. Выбор компонентов консоли управления криптосервером

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

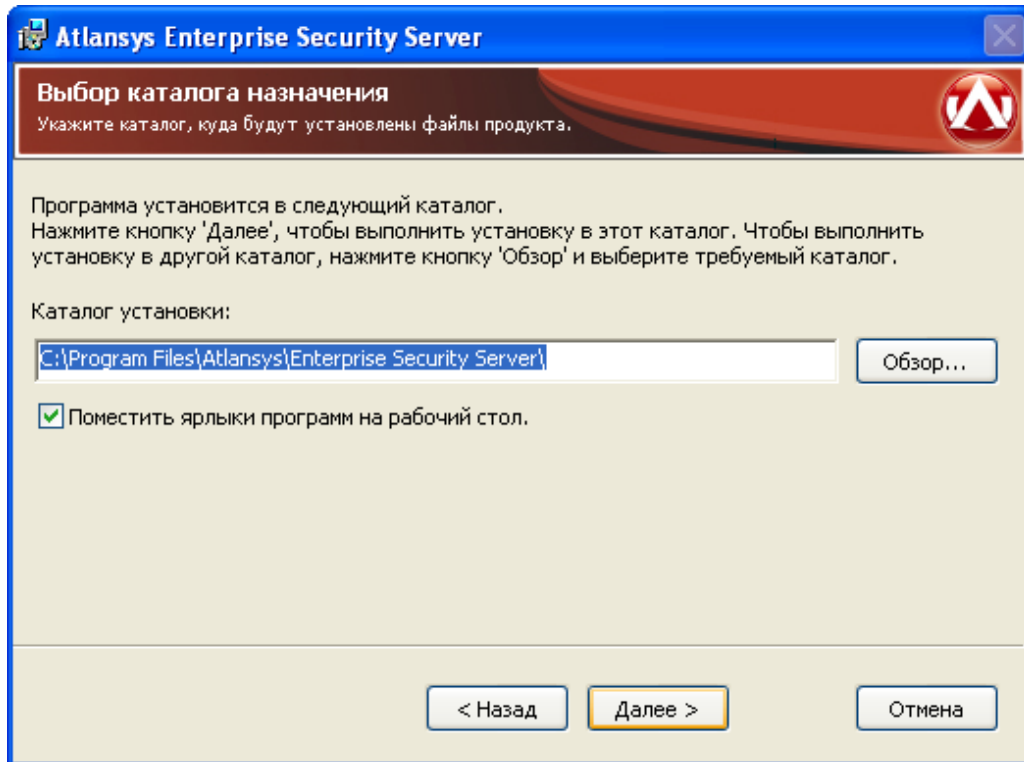


Рисунок 1.5. Выбор каталога для установки программы

6. При необходимости, можно нажать на кнопку «Назад» и изменить ранее введенные параметры. Для запуска процесса установки необходимо нажать кнопку «Установить». (Рисунок 1.6)

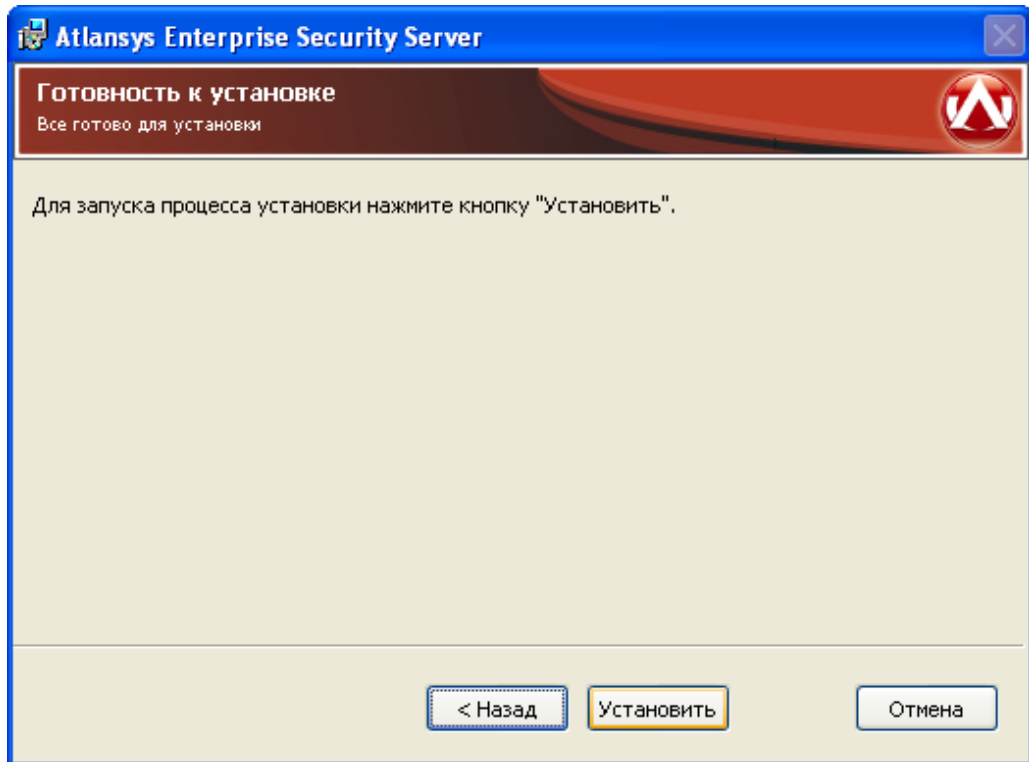


Рисунок 1.6. Запуск процесса установки

7. После этого появится окно, отображающее процесс установки программного обеспечения. (Рисунок 1.7)

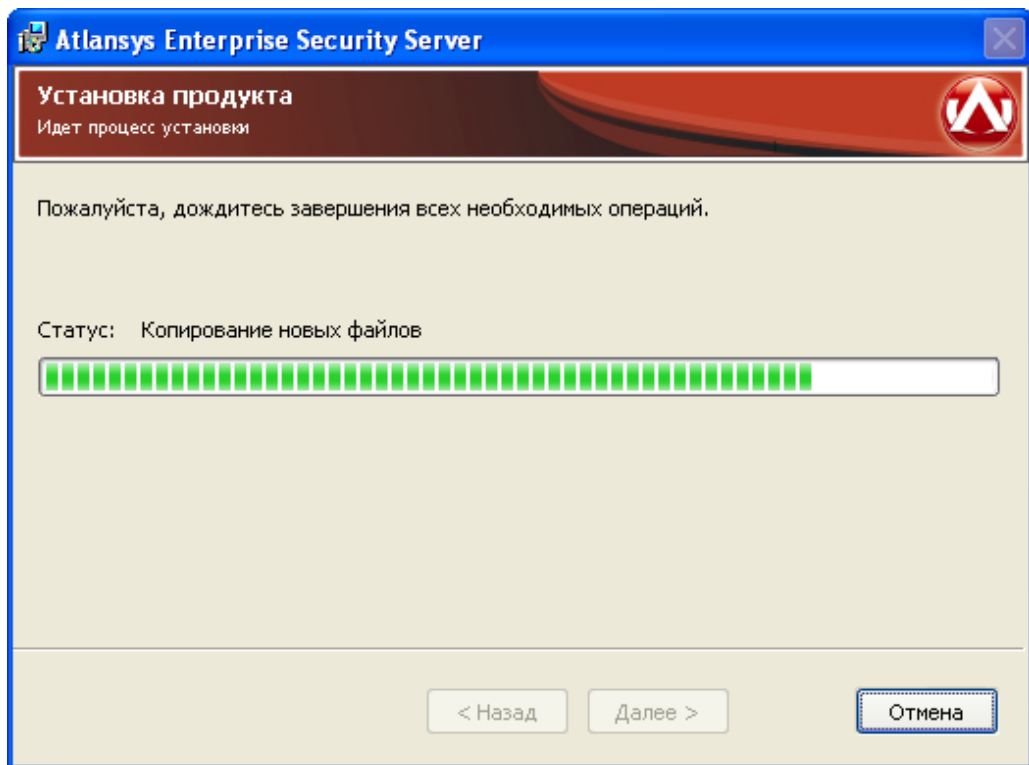


Рисунок 1.7. Процесс установки

8. Для окончания процесса установки необходимо нажать на кнопку «Завершить». (Рисунок 1.8)

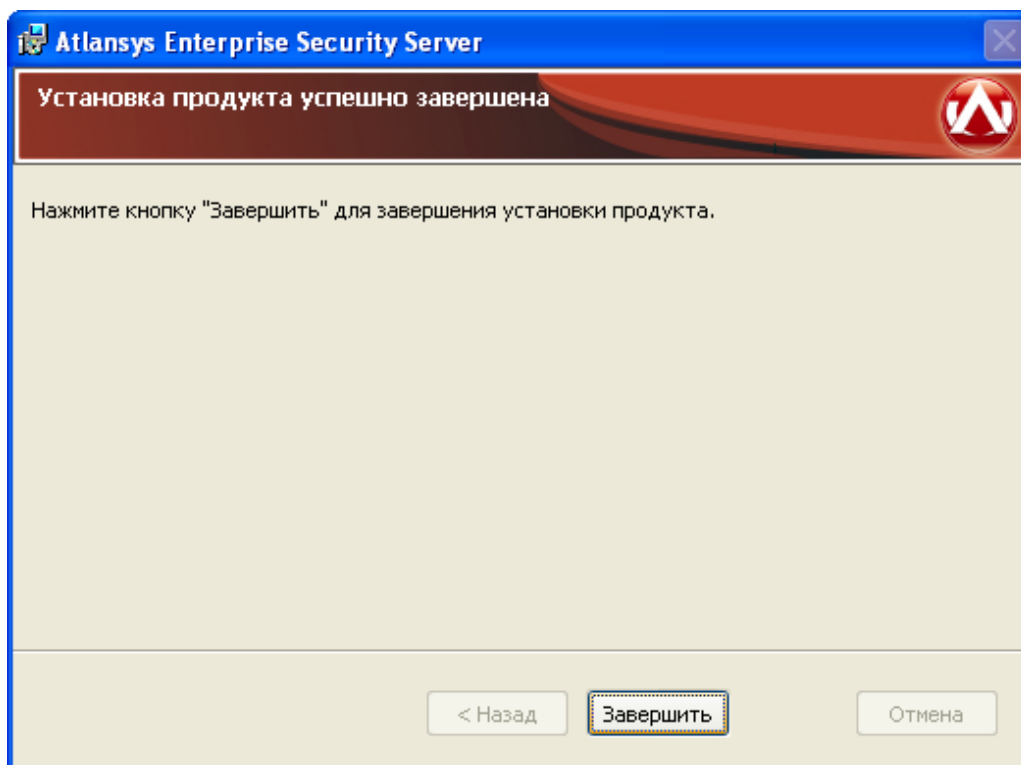


Рисунок 1.8. Завершение установки

1.2. Обновление программного обеспечения

Если на рабочей станции администратора или на сервере 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 на сервере 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 инсталлятора Atlansys Enterprise Security System **Atlansys-ESS-CSRV-(номер версии)-setup.msi**. Инсталлятор отобразит номер версии установленного продукта и номер новой версии. Нажать кнопку «Далее». (Рисунок 1.9)



Рисунок 1.9. Обновление Atlansys Enterprise Security System

2. После этого появится окно, отображающее процесс обновления программного обеспечения. (Рисунок 1.10)

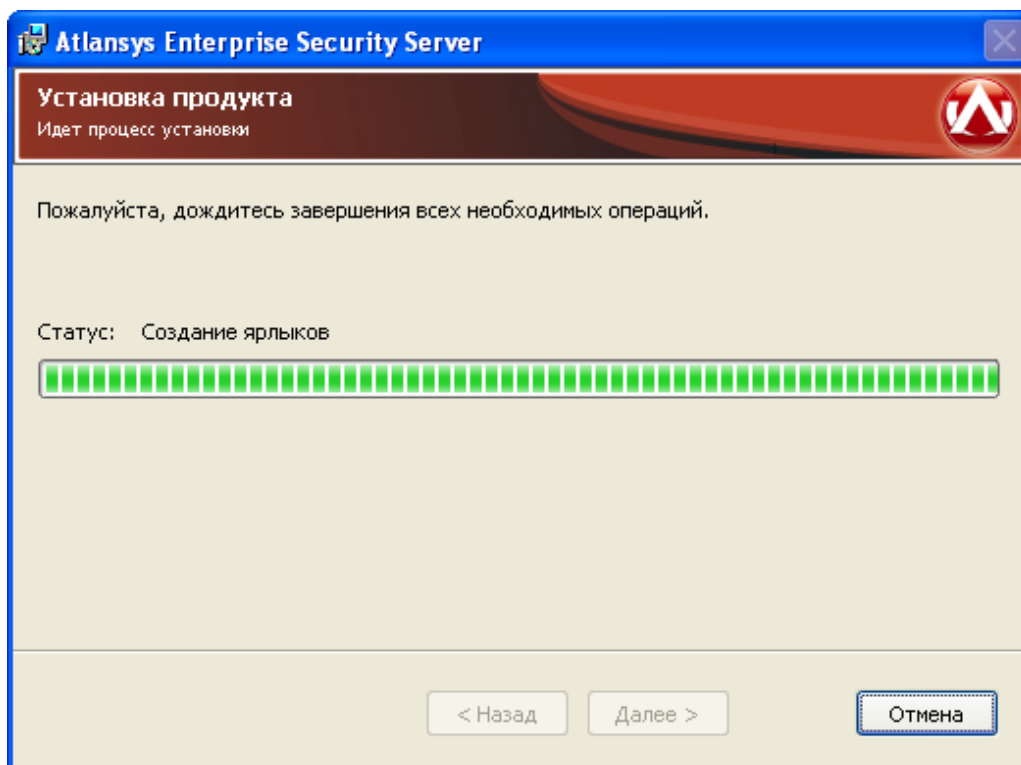


Рисунок 1.10. Процесс установки

3. Для окончания процесса установки необходимо нажать на кнопку «Завершить». (Рисунок 1.11)

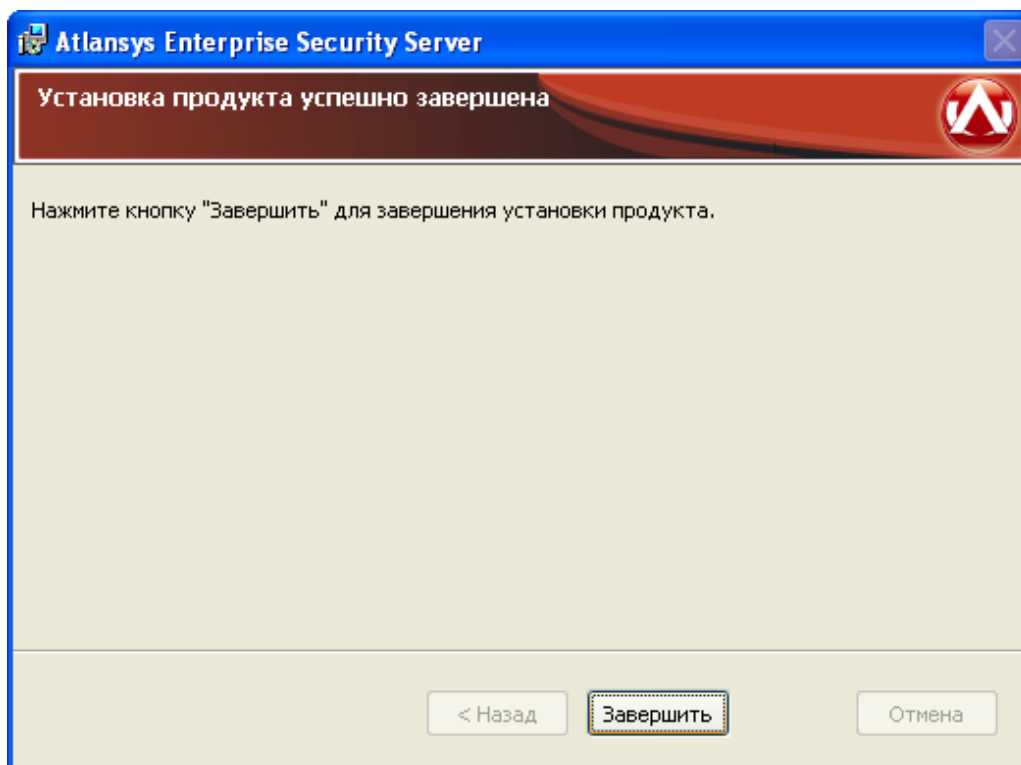


Рисунок 1.11. Завершение установки

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 инсталлятор в неинтерактивном режиме необходимо выполнить в командной строке команду установки с флагом /qn:

```
msiexec /i Atlansys-ESS-CSRV-(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-CSRV-(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:
 - CryptoCont – криптоконтейнеры;
 - CryptoDisk – криптодиски.
7. **"CONTROL_CENTER = address"** - IP-адрес или доменное имя центра управления. Если этот параметр указан, то производится установка управляемого сервера.

Пример файла settings.cfg:

```
# Конфигурация для рабочей станции администратора
INSTALLDIR=C:\Program Files\AtlansysESS\ CONTROL_CENTER=192.168.66.33
ADDDEFAULT=ALL PIDKEY=527LD-2TEST-ONLY4-VOVAN-SFXFL USERNAME=Василий
Петров GROUP=sale COMPANYNAME=000 Деревянная Скала
```

Эти же свойства можно задавать из командной строки. Например:

```
msiexec /i Atlansys-ESS-CSRV-(номер версии)-setup.msi INSTALLDIR="c:\Program Files\AtlansysESS"
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 Консоль Администратора, если она была запущена.
2. Запустить приложение Установка и удаление программ (Пуск / Панель управления / Установка и удаление программ), из списка программ выбрать Atlansys Enterprise Security Server.

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

Глава 2. Консоль криптосервера

2.1. Назначение

Консоль криптосервера - это приложение, предназначенное для настройки и оперативного управления криптосервером. Содержит такие разделы, как учетные записи администраторов, группы пользователей, хранилище ключей, удаленное управление, восстановление ключей.

2.2. Запуск программы

Запуск программы осуществляется либо через ярлык на рабочем столе Windows, либо через меню «Пуск / Все программы / Atlansys / Enterprise Security Server / Консоль криптосервера».

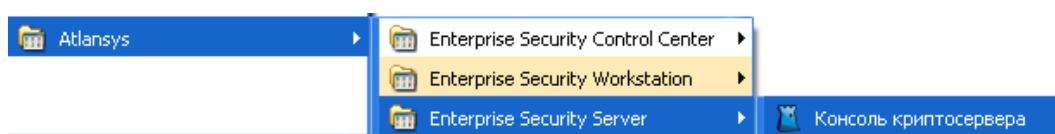


Рисунок 2.1. Запуск Консоли криптосервера

2.3. Интерфейс

При запуске Консоли криптосервера, появится окно аутентификации на криптосервере. В поля необходимо ввести имя пользователя, пароль и адрес криптосервера.

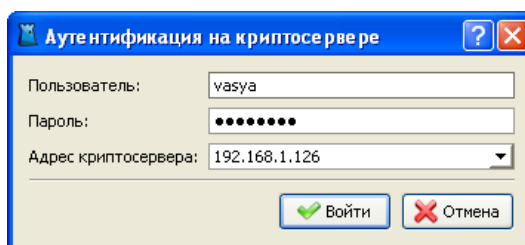


Рисунок 2.2. Аутентификация на криптосервере

После успешной аутентификации при первом запуске консоли открывается доступ к элементам управления:

1. Главное меню.
2. Кнопки быстрого перехода к соответствующими модулями Консоли.
3. Адреса службы технической поддержки продукта.
4. Индикатор подключения и адрес криптосервера, к которому подключена консоль.

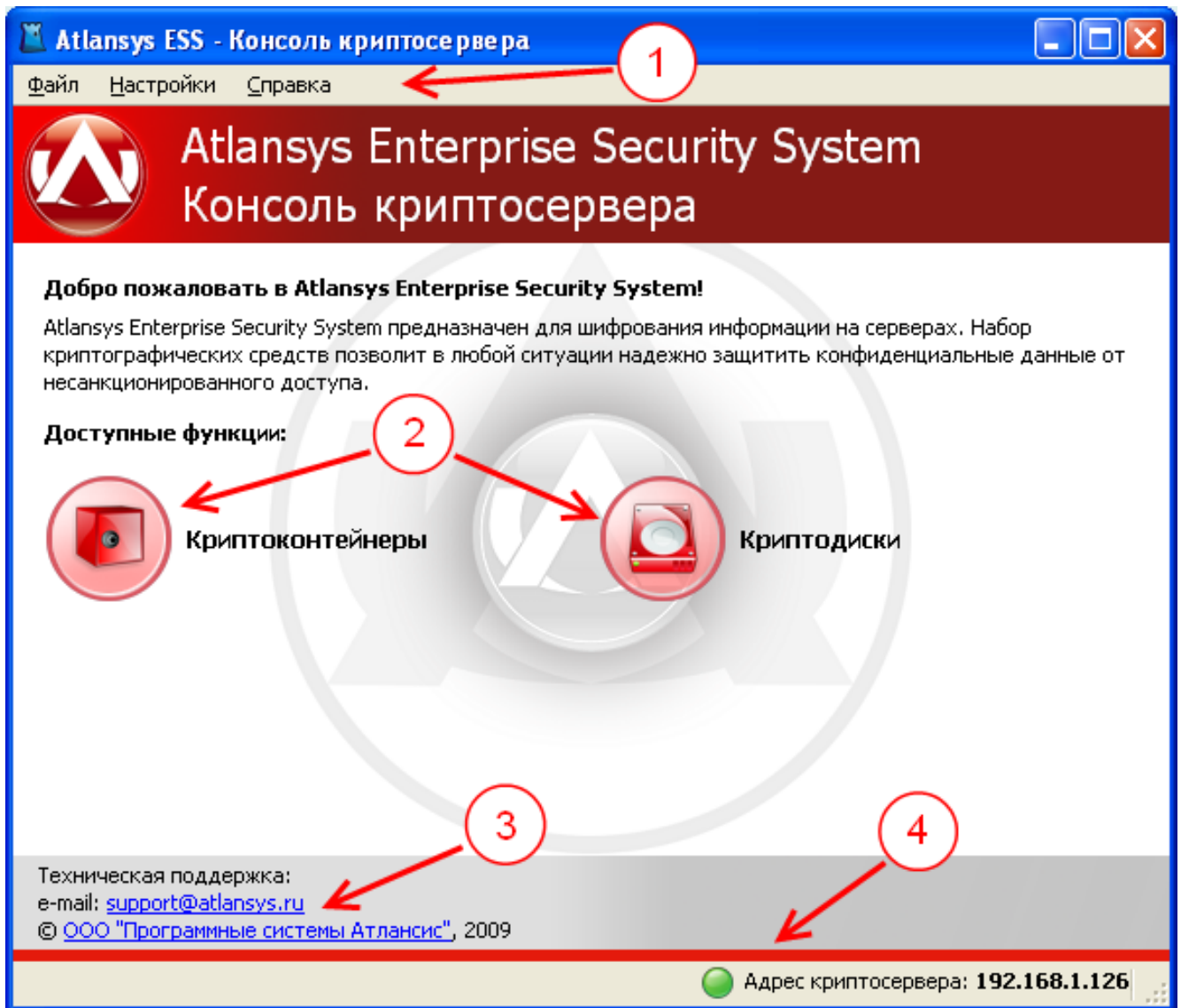


Рисунок 2.3. Главное окно Консоли криптосервера

1. Меню «Файл» содержит подменю:

- «Создать» - для создания новых криптоконтейнеров, криптодисков.
- «Добавить» - для добавления существующих криптоконтейнеров и криптодисков, которые были созданы на других серверах или рабочих станциях.
- «Закрыть все криптообъекты» - быстрое закрытие всех открытых криптоконтейнеров и криптодисков.
- «Журнал событий» - окно для просмотра журнала регистрации событий, происходящих в системе.
- «Выход» - для выхода из консоли криптосервера.

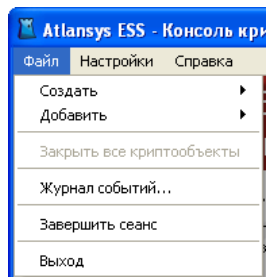


Рисунок 2.4. Меню «Файл»

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

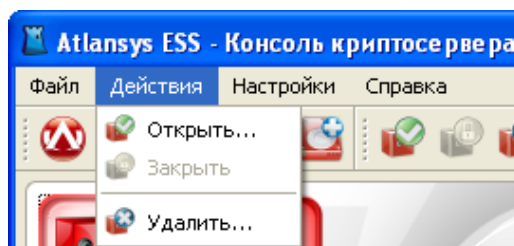


Рисунок 2.5. Меню «Действия»

3. Меню «Настройки» содержит подменю:

- «Настройки...» - для вызова диалога настройки параметров работы приложения.
- «Список плагинов...» - для отображения списка загруженных модулей (плагинов) консоли.
- «Сворачивать в трей» - для сворачивания окна консоли в системный трей, при нажатии на кнопки закрытия или минимизации окна, что позволяет обеспечить быстрый доступ к консоли криптосервера без её повторной загрузки.

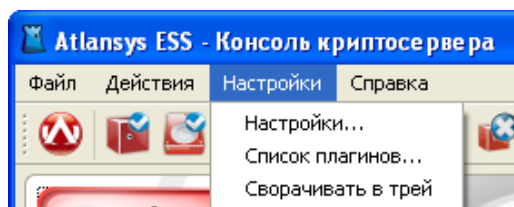


Рисунок 2.6. Меню «Настройки»

4. Меню «Справка» содержит пункты:

- «Главное меню» - для перехода на главную страницу.
- «Справка» - для вызова справки по программе.
- «О программе» - для вызова диалога «О программе», в котором содержится информация о версии программы, параметрах регистрации, и доступных лицензиях.

2.4. Настройки продукта

Для уточнения параметров работы продукта используется диалог настроек, который вызывается через главное меню "Настройки / Настройки...". С левой стороны диалога расположена панель доступных для

управления модулей, при выборе которых с правой стороны отображаются текущие параметры выбранного модуля.



Замечание

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

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

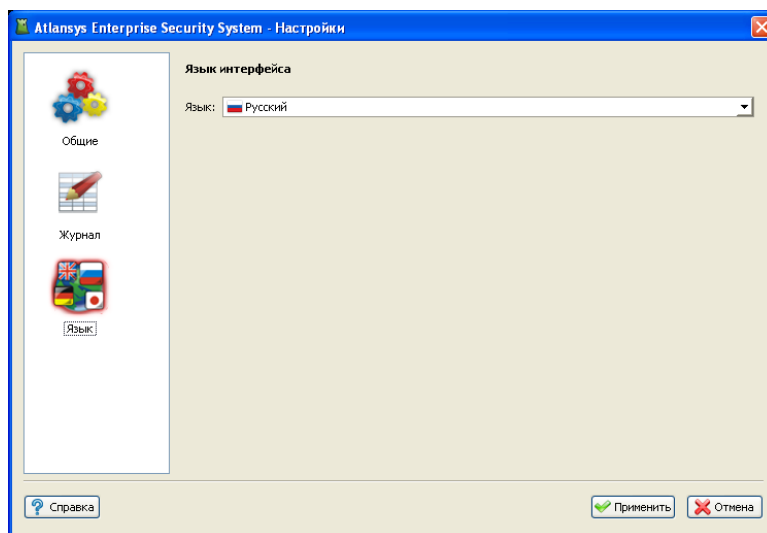


Рисунок 2.7. Язык

2. "Регистрация событий" - задаёт параметры регистрации сообщений в локальной базе и отправки лог-сообщений на внешний syslog-сервер.
 - "База данных лог-сообщений" - задаётся путь к файлу базы данных лог-сообщений. Рекомендуется оставить этот параметр по умолчанию. База данных состоит из одного файла, который создаётся автоматически при старте системы, если по указанному пути он не был найден.

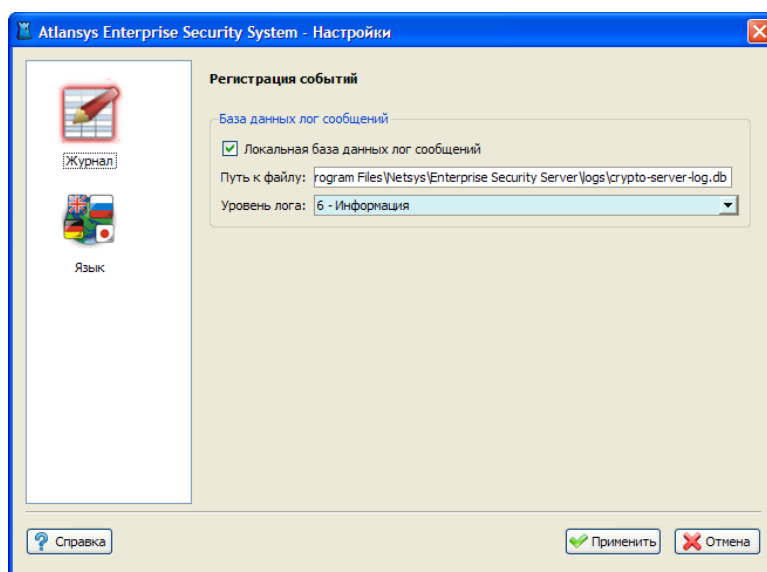


Рисунок 2.8. Регистрация событий

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 консоли криптосервера выбрать в главном меню пункты «Файл» / «Создать» / «Криптоконтейнер...»

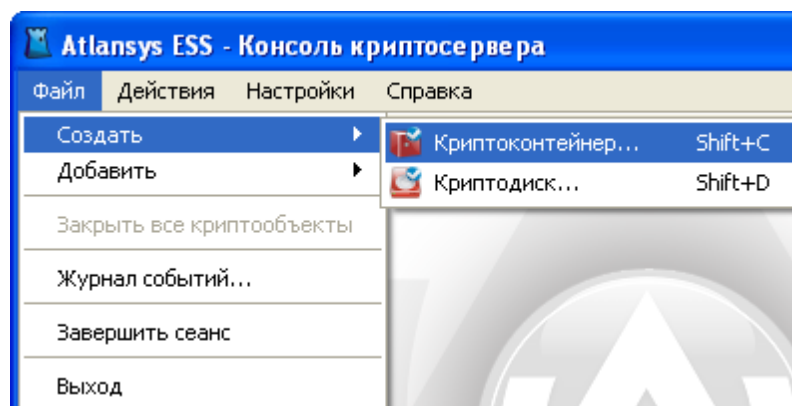


Рисунок 3.1. Меню «Файл» / «Создать» / «Криптоконтейнер»

После чего запустится Мастер создания криптоконтейнеров. В появившемся окне необходимо задать полное имя файла криптоконтейнера.

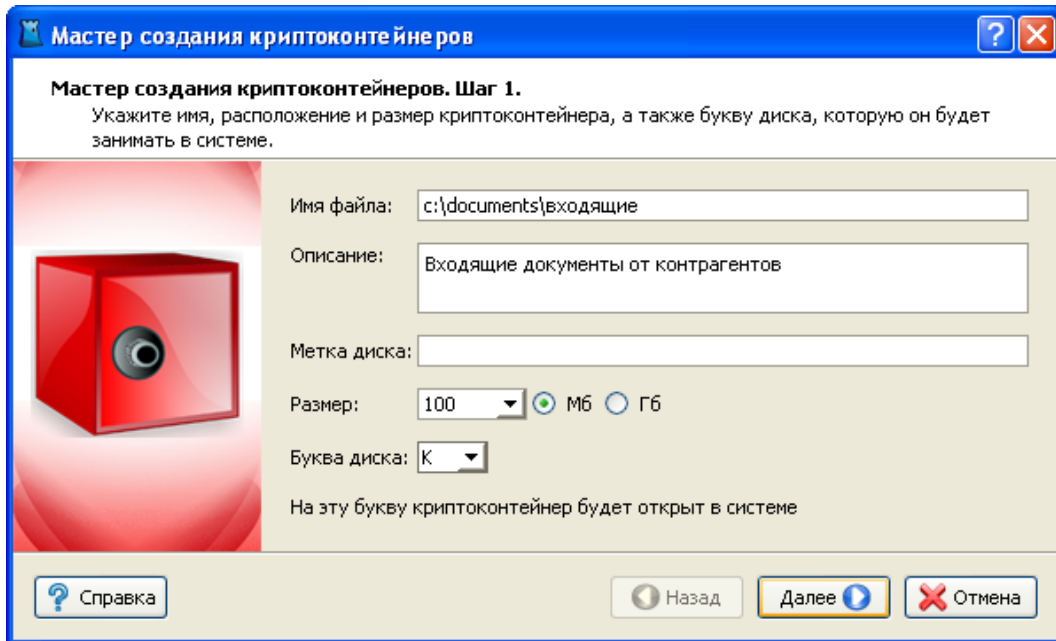


Рисунок 3.2. Мастер создания криптоконтейнеров.

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.

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.

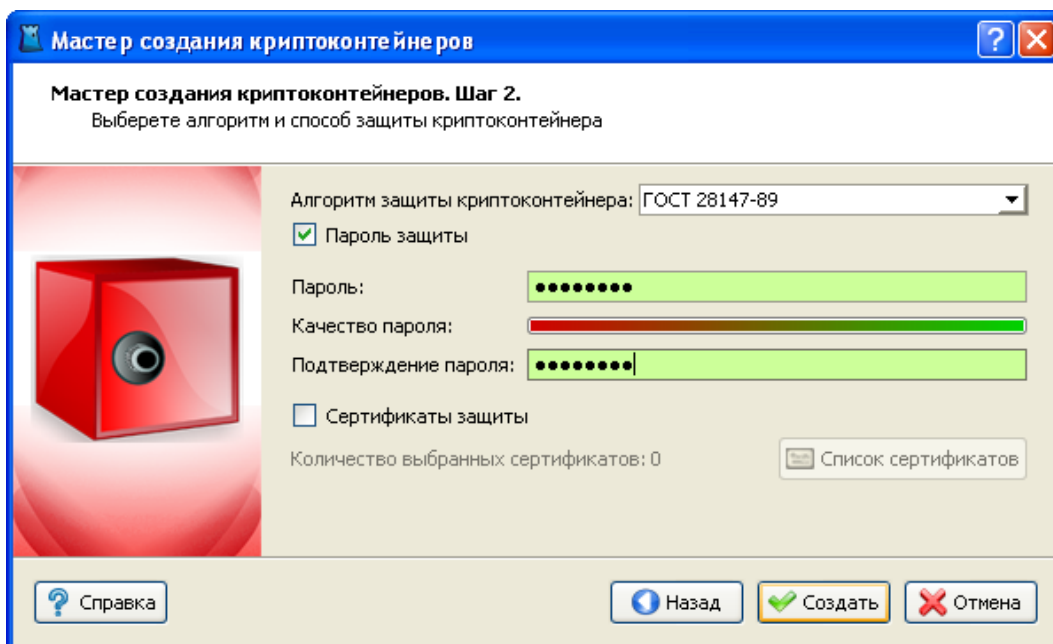


Рисунок 3.3. Мастер создания криптоконтейнеров. Способы защиты.

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 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 криптоконтейнеру. 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 данном сервере 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 списке криптосервера.

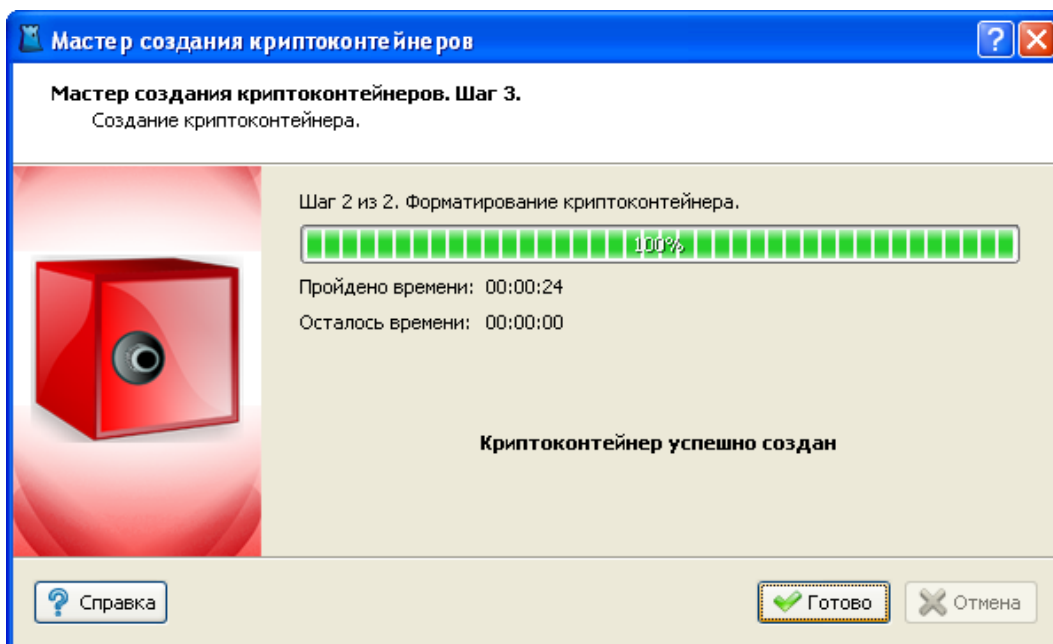


Рисунок 3.4. Мастер создания криптоконтейнеров. Прогресс создания.

3.3. Добавление криптоконтейнера

Для добавления криптоконтейнера, созданного на другой рабочей станции или сервере в список крипто-сервера, необходимо выбрать в Главном меню пункт «Файл» / «Добавить» / «Криптоконтейнер».

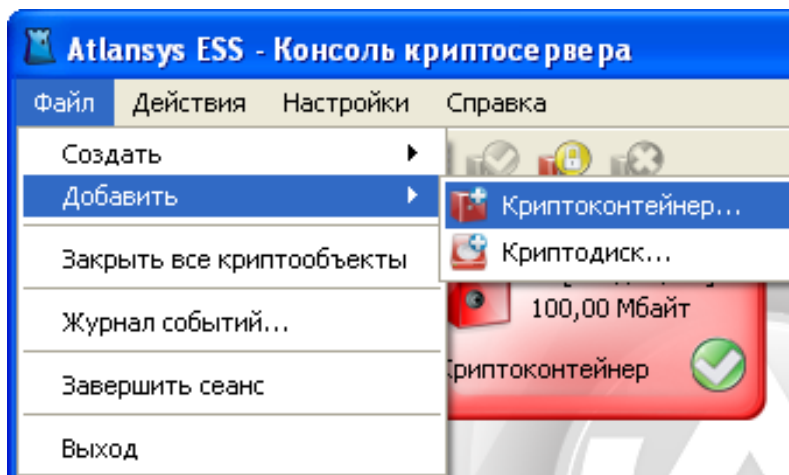


Рисунок 3.5. Меню «Файл» / «Добавить» / «Криптоконтейнер»

В появившемся окне Мастера добавления криптоконтейнеров ввести полный путь к файлу криптоконтейнера. Если формат криптоконтейнера поддерживается текущей версией криптосервера, то 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 криптосервера. Если криптоконтейнер защищен сертификатом и его закрытый ключ имеется в системе, криптоконтейнер автоматически откроется.

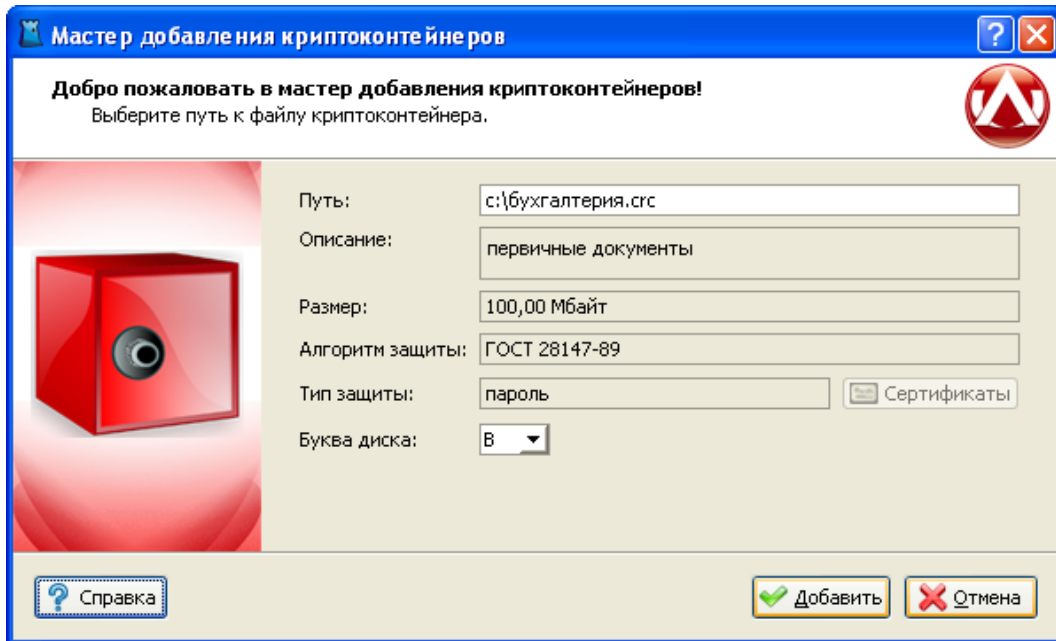


Рисунок 3.6. Мастер добавления криптоконтейнеров

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.

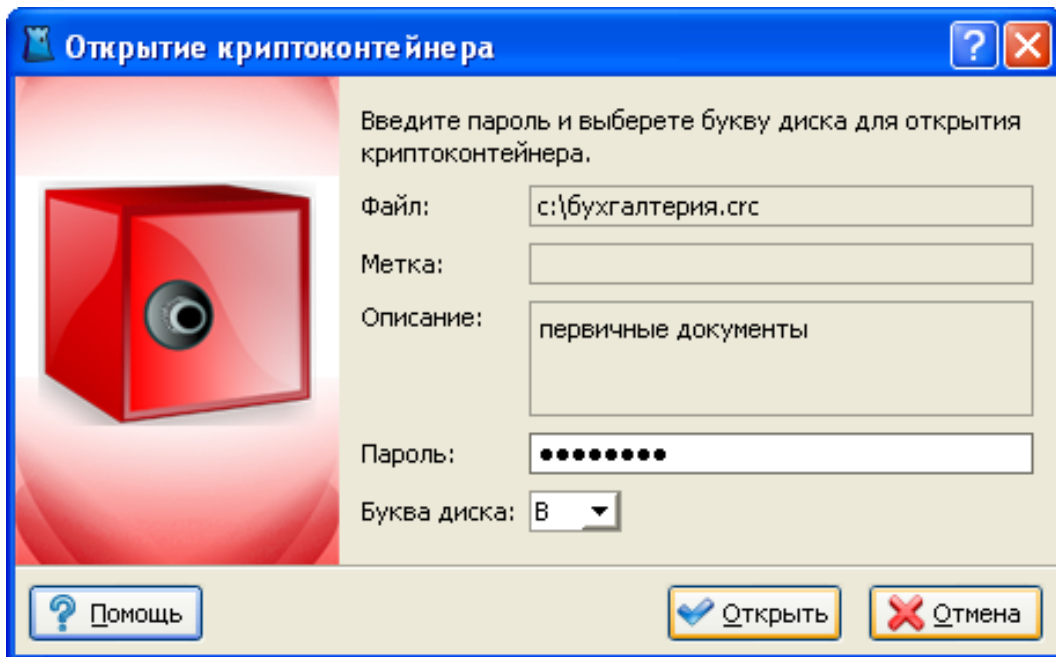


Рисунок 3.7. Диалог открытия криптоконтейнера

3.4. Работа с криптоконтейнерами

При создании или добавлении нового криптоконтейнера он автоматически открывается и имеет состояние «Открыт», что отображается на его иконке. Все криптоконтейнеры и криптодиски отображаются в списке консоли. Текущий активный элемент выделяется рамкой, при этом его параметры выводятся в нижней части окна. 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.

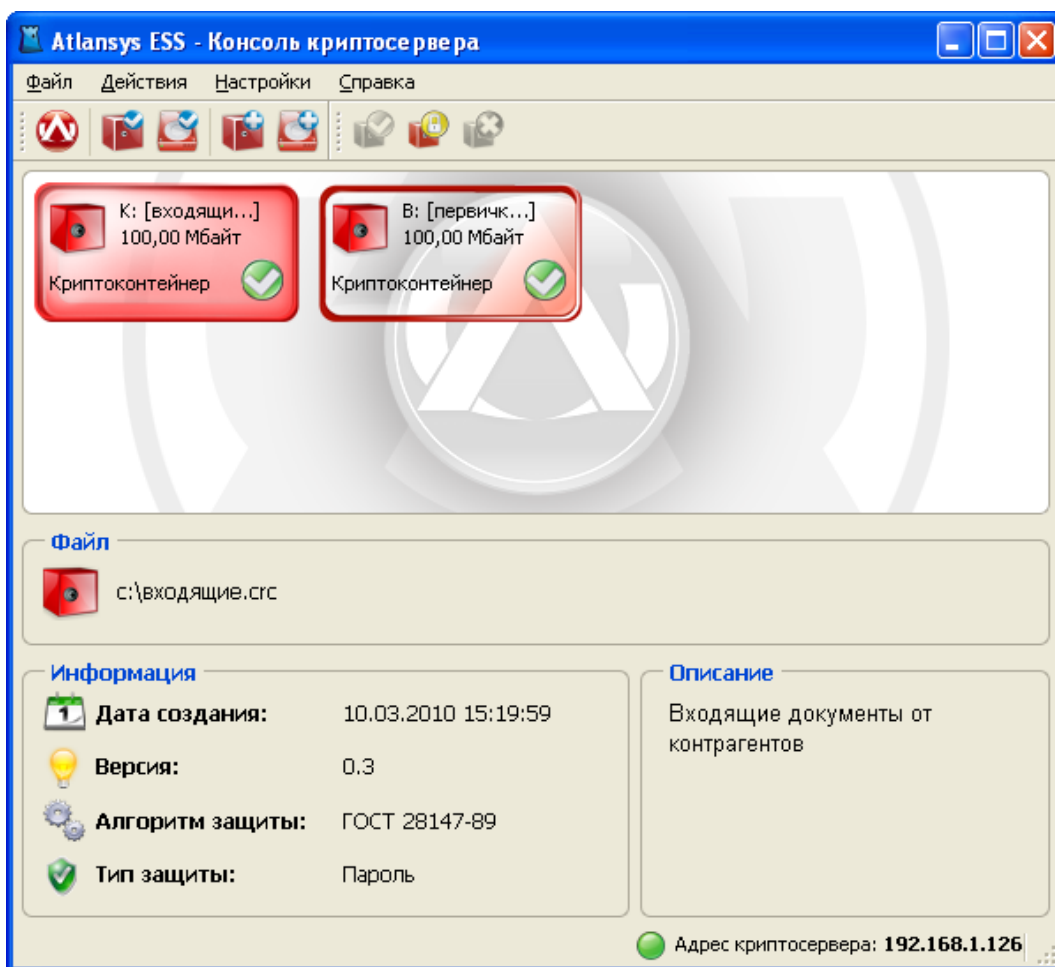


Рисунок 3.8. Список криптоконтейнеров и криптодисков

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

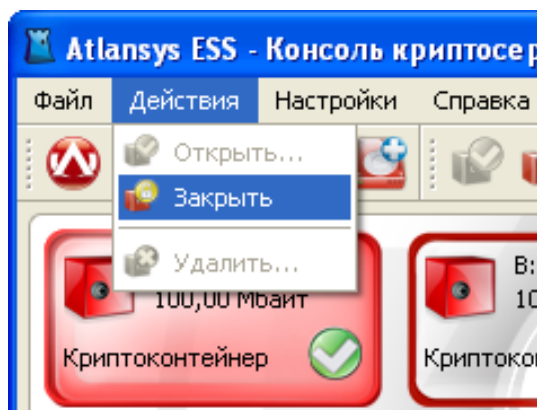


Рисунок 3.9. Меню «Действия»

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

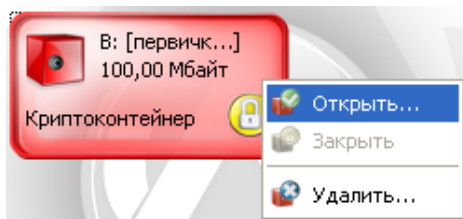


Рисунок 3.10. Контекстное меню криптоконтейнера

Либо нажать кнопку «Открыть» на панели инструментов. Двойной щелчок мыши на криптоконтейнере также позволяет его открыть.

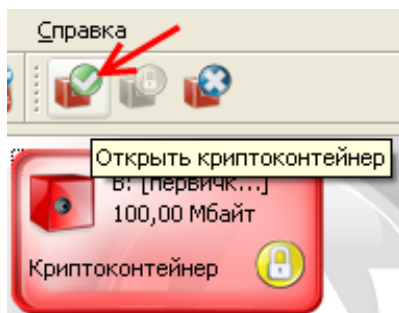


Рисунок 3.11. Панель инструментов, кнопка «Открыть»

Если криптоконтейнер защищен сертификатами, и в системе имеется закрытый ключ хотя бы к одному сертификату, криптоконтейнер откроется. 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 «Заккрыть», либо в панели инструментов нажать на кнопку «Удалить».

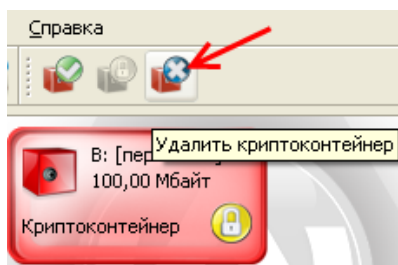


Рисунок 3.12. Панель инструментов, кнопка «Удалить»

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 криптосервера. При этом файл криптоконтейнера и все данные, содержащиеся в нем, не удаляются. Данный способ может использоваться при переносе криптоконтейнера на другой сервер или 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 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.

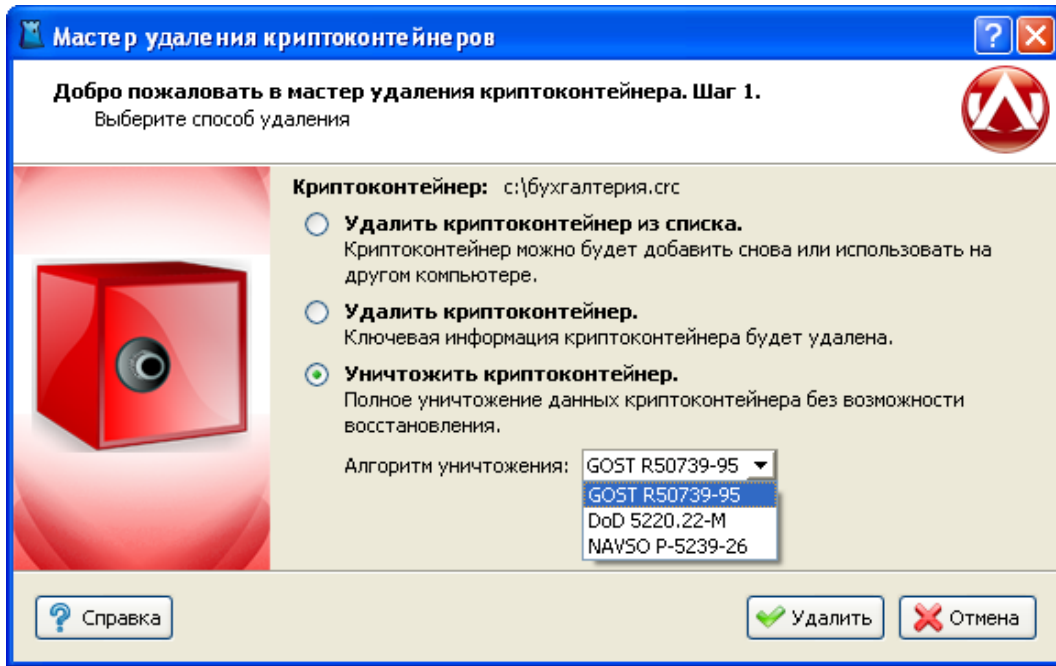


Рисунок 3.13. Мастер удаления криптоконтейнеров



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 консоли пункт «Файл» / «Создать» / «Криптодиск».

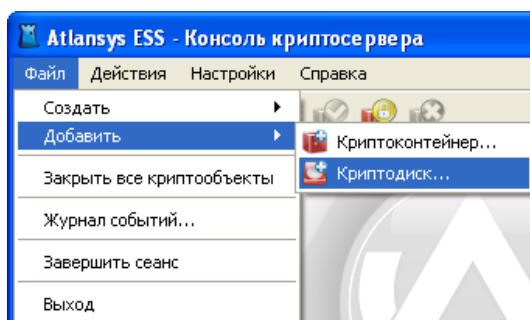


Рисунок 4.1. Меню «Файл» / «Создать»

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

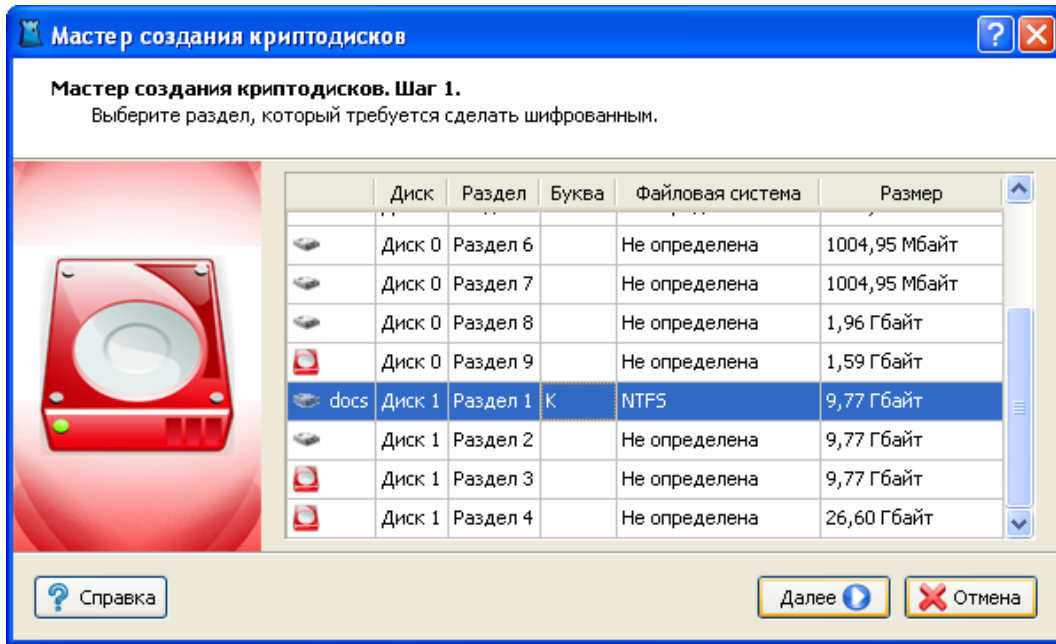


Рисунок 4.2. Мастер создания криптодисков. Выбор раздела.



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.

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.

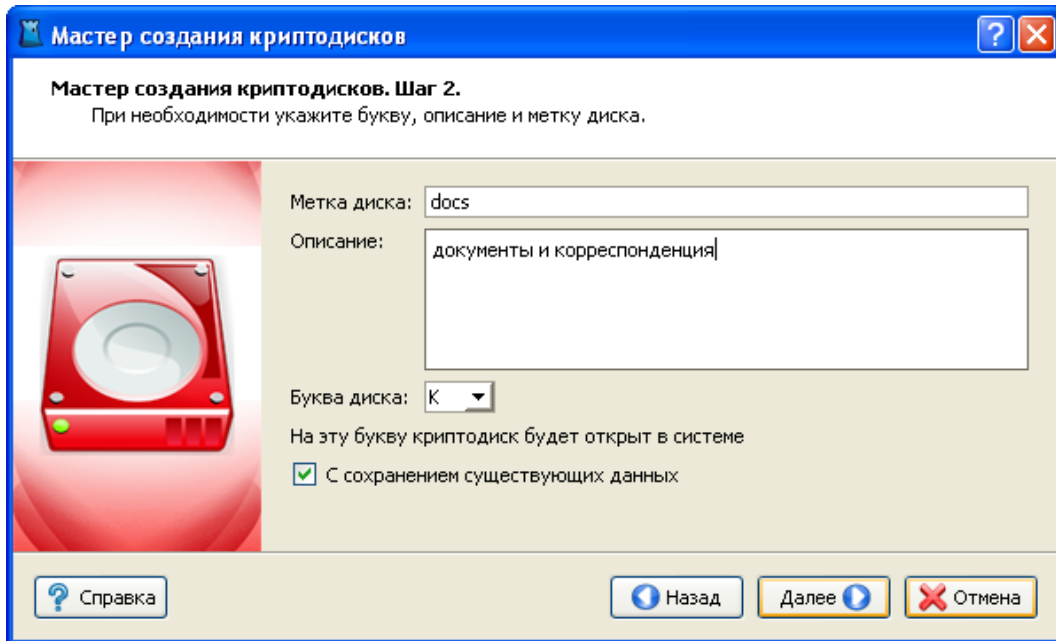


Рисунок 4.3. Мастер создания криптодисков. Метка диска и описание.



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.

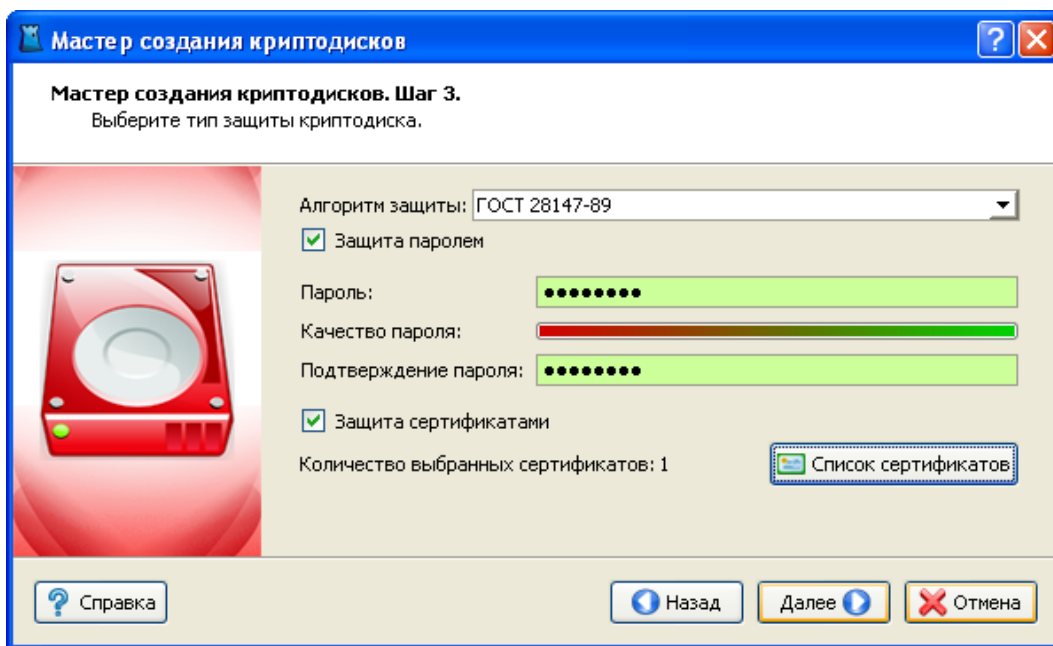


Рисунок 4.4. Мастер создания криптодисков. Способы защиты.

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 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 криптодиску. После закрытия диалога со списком сертификатов в окне Мастера создания криптодисков 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 данном сервере 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».

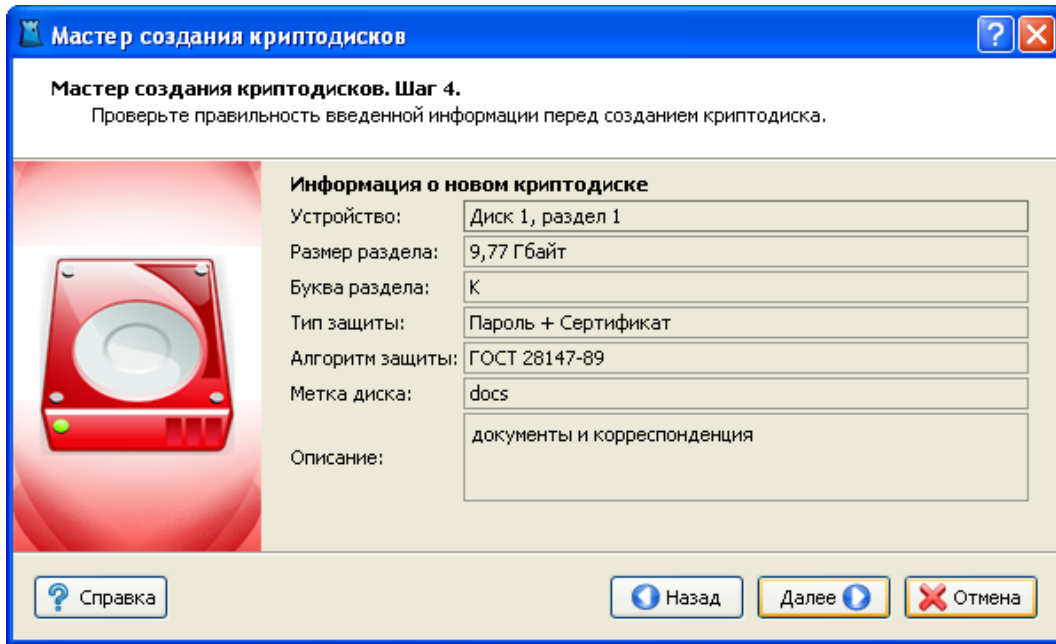


Рисунок 4.5. Мастер создания криптодисков. Сводная информация.

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 ознакомиться с предупреждением и нажать кнопку «Создать».

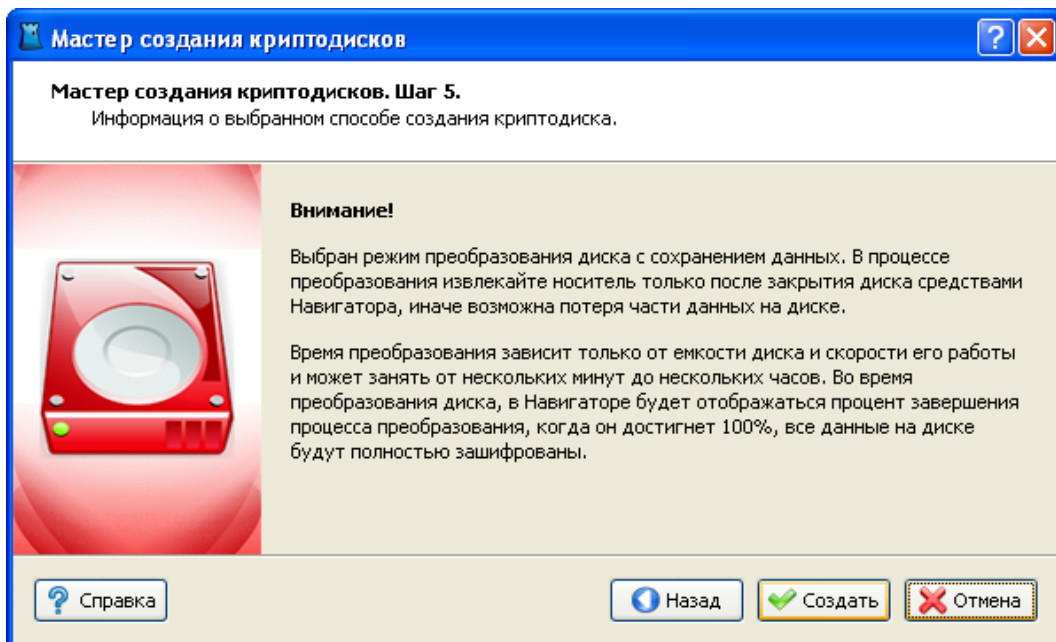


Рисунок 4.6. Мастер создания криптодисков. Предупреждение.

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 криптосервера.

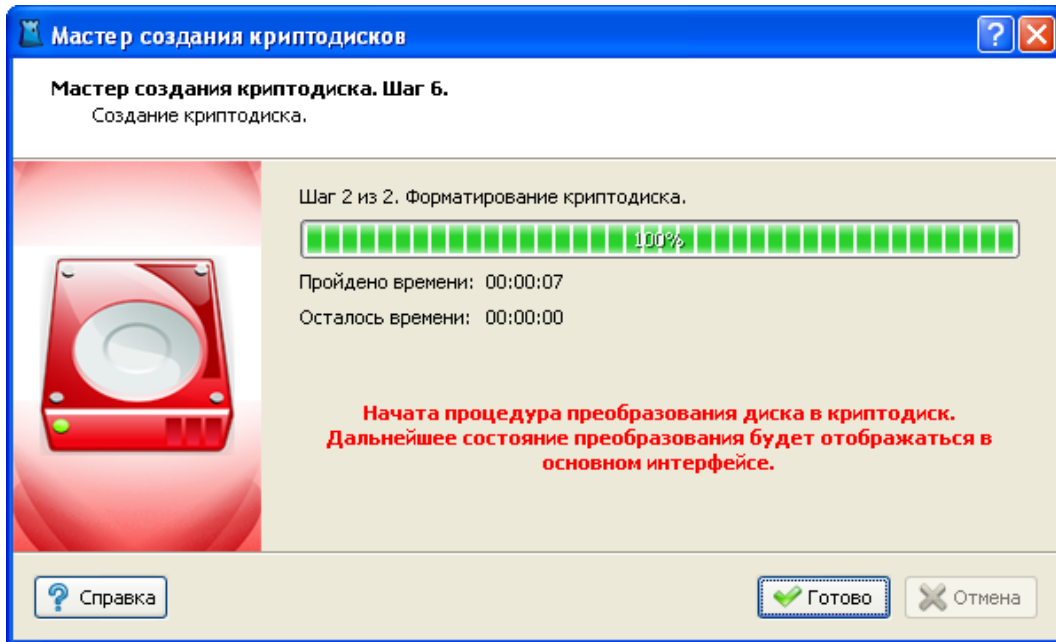


Рисунок 4.7. Мастер создания криптодисков. Прогресс создания.

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

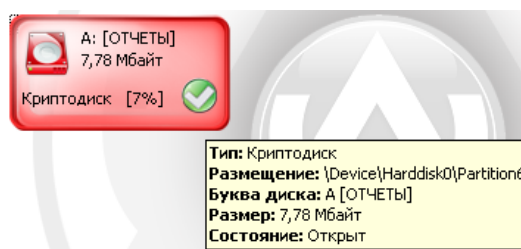


Рисунок 4.8. Процесс преобразования криптодиска.



Важно

Криптодиски на извлекаемых устройствах должны закрываться стандартными средствами консоли криптосервера 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». По умолчанию он отключен для скорости создания криптодиска. Однако в целях увеличения безопасности использования криптодиска рекомендуется включить этот чекбокс, тем самым уничтожатся все данные, ранее существовавшие на диске.

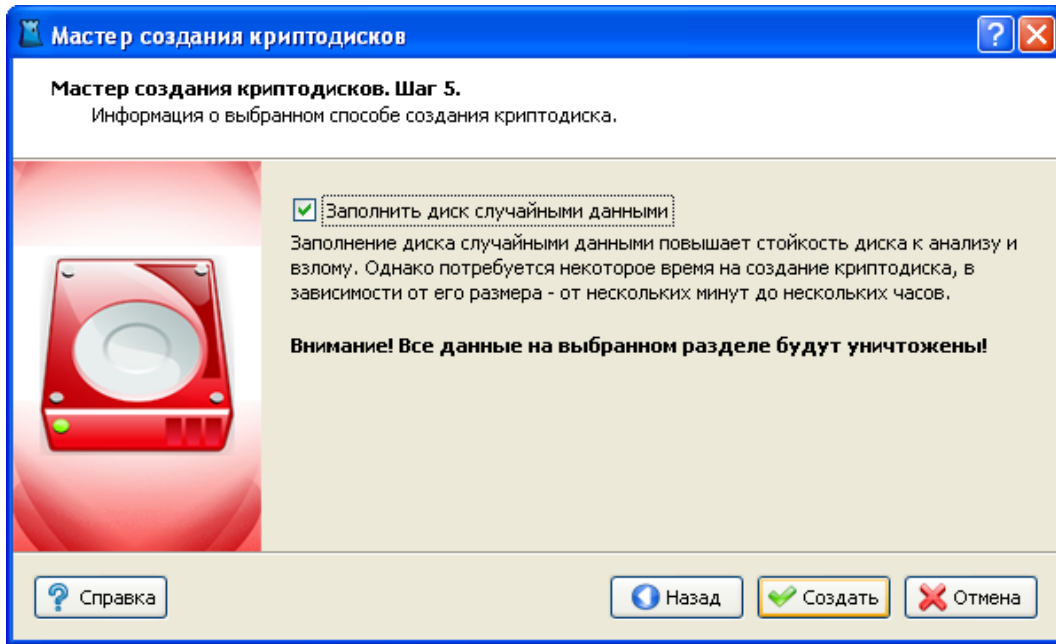


Рисунок 4.9. Мастер создания криптодисков. Заполнение случайными данными.



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 пункт «Файл» / «Добавить» / «Криптодиск...».

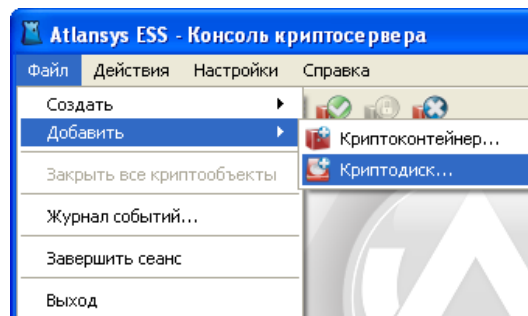


Рисунок 4.10. Меню «Файл» / «Добавить» / «Криптодиск»

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 криптосервера.

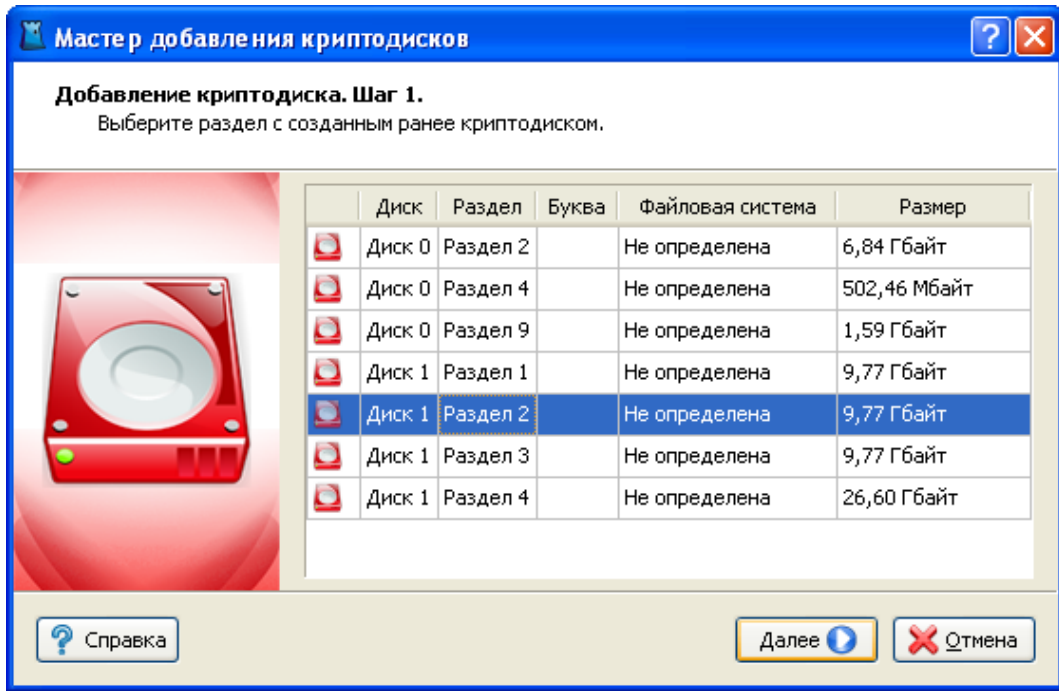


Рисунок 4.11. Мастер добавления криптодисков. Выбор раздела.

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 криптосервера. Если криптодиск защищён паролем, то появится диалог ввода пароля для открытия этого криптодиска.

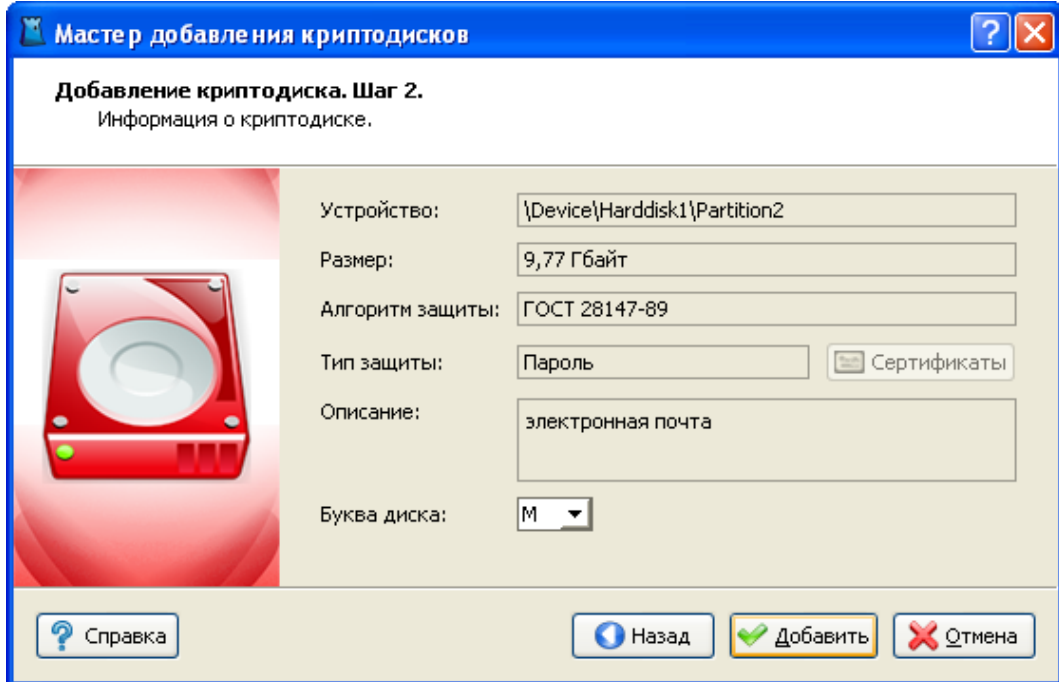


Рисунок 4.12. Мастер добавления криптодисков. Сводная информация о криптодиске.

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 консоли криптосервера. Текущий

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

- устройство, на котором создан криптодиск;
- дата создания;
- версия типа криптозащиты;
- 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 консоли, затем в главном меню выбрать пункт «Действия» / «Закрыть». Либо в контекстном меню криптодиска выбрать пункт «Закрыть». Либо нажать кнопку «Закрыть» на панели инструментов.

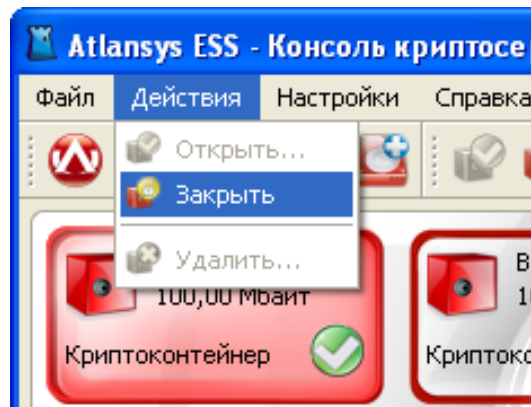


Рисунок 4.13. Меню «Действия»

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

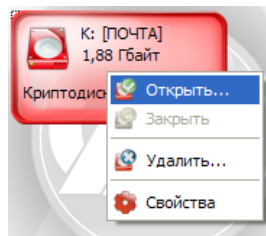


Рисунок 4.14. Контекстное меню криптодиска

Либо нажать кнопку «Открыть» на панели инструментов. Двойной щелчок мыши на иконке криптодиска в списке криптообъектов также открывает криптодиск.

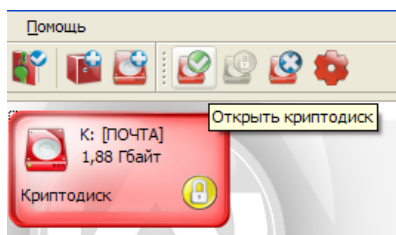


Рисунок 4.15. Панель инструментов

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

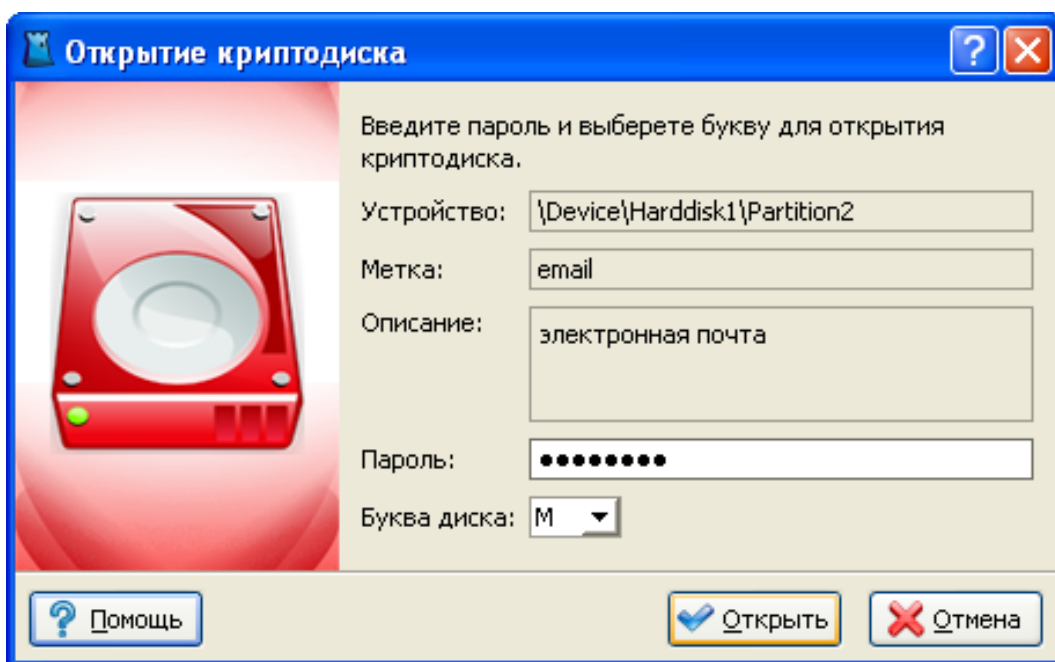


Рисунок 4.16. Диалог открытия криптодиска

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».

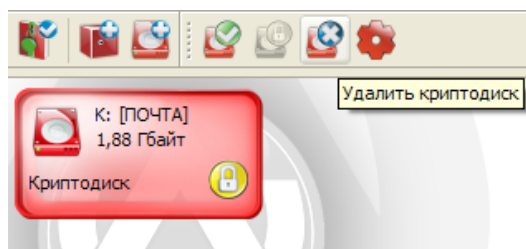


Рисунок 4.17. Панель инструментов, кнопка «Удалить»

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 криптосервера. При этом криптодиск и все данные, содержащиеся в нем не удаляются. Данный способ может использоваться при переносе криптодиска на другой сервер или 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.

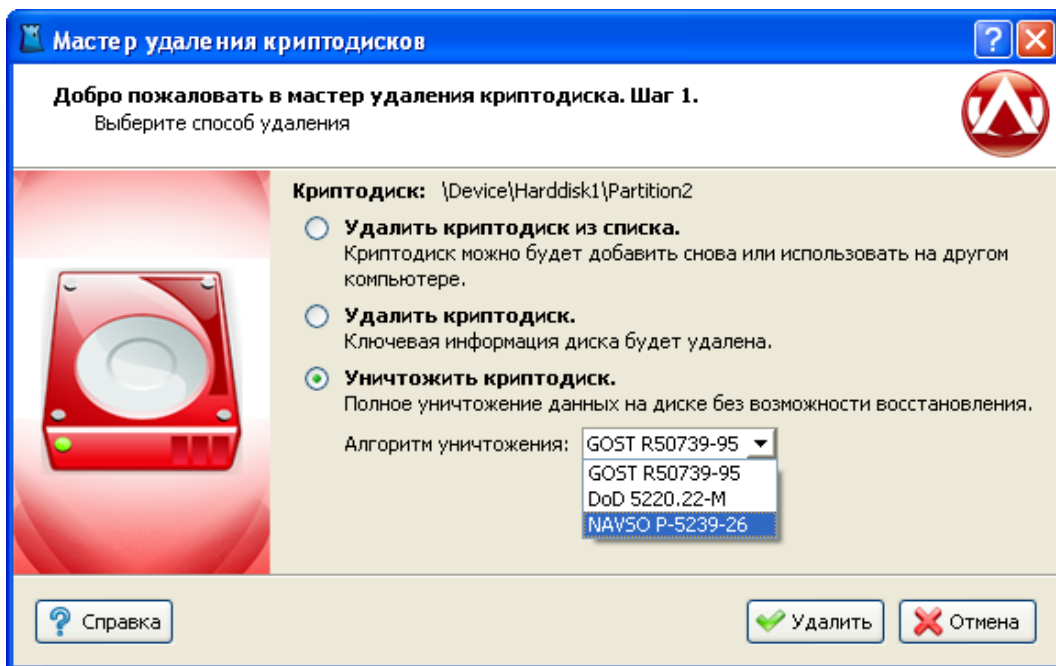


Рисунок 4.18. Мастер удаления криптодисков



Важно

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

Глава 5. Свойства криптообъекта

5.1. Диалог свойств криптообъекта

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

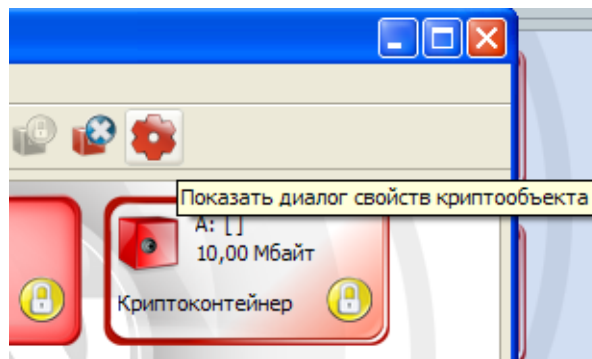


Рисунок 5.1. Кнопка вызова диалога свойств криптообъекта

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

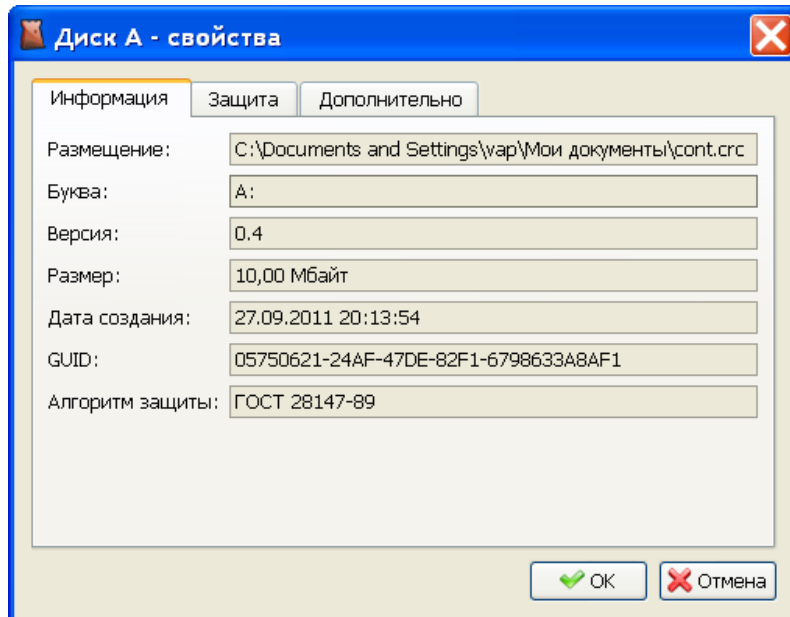


Рисунок 5.2. Диалог свойств криптообъекта - Информация

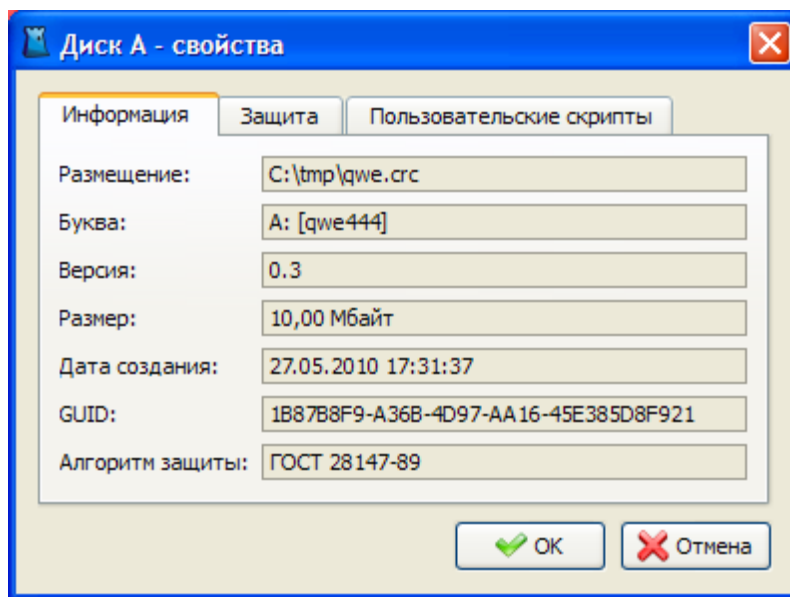


Рисунок 5.3. Диалог свойств криптообъекта - Информация

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

5.2. Изменение пароля и сертификатов

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

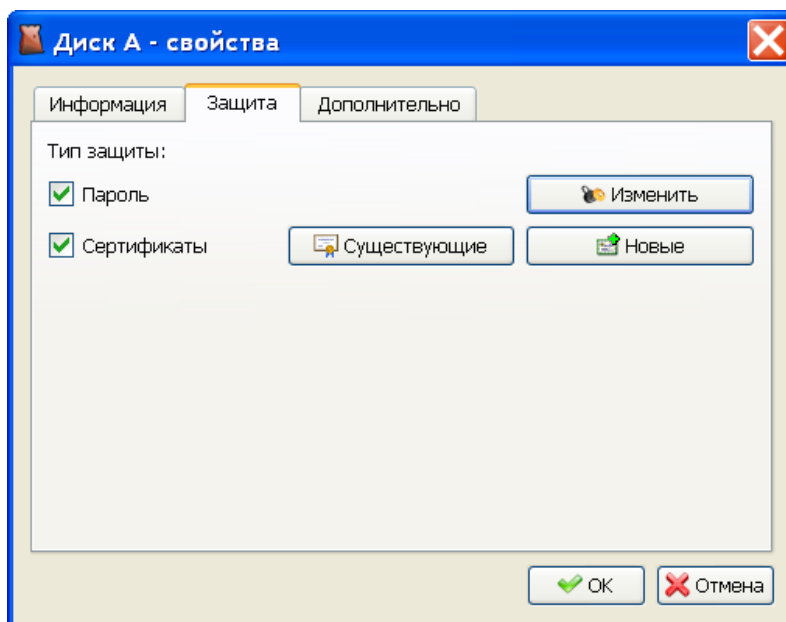


Рисунок 5.4. Диалог свойств криптообъекта - Защита

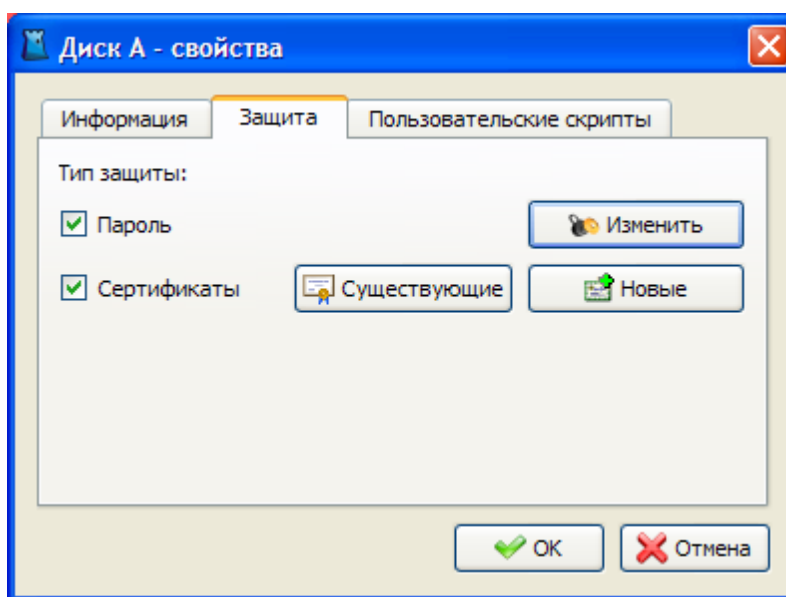


Рисунок 5.5. Диалог свойств криптообъекта - Защита

В зависимости от текущего типа защиты криптообъекта, на вкладке будут выбраны соответствующие чек-боксы.

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

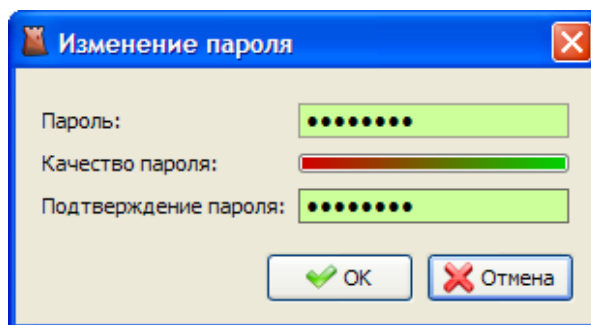


Рисунок 5.6. Диалог изменения пароля

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

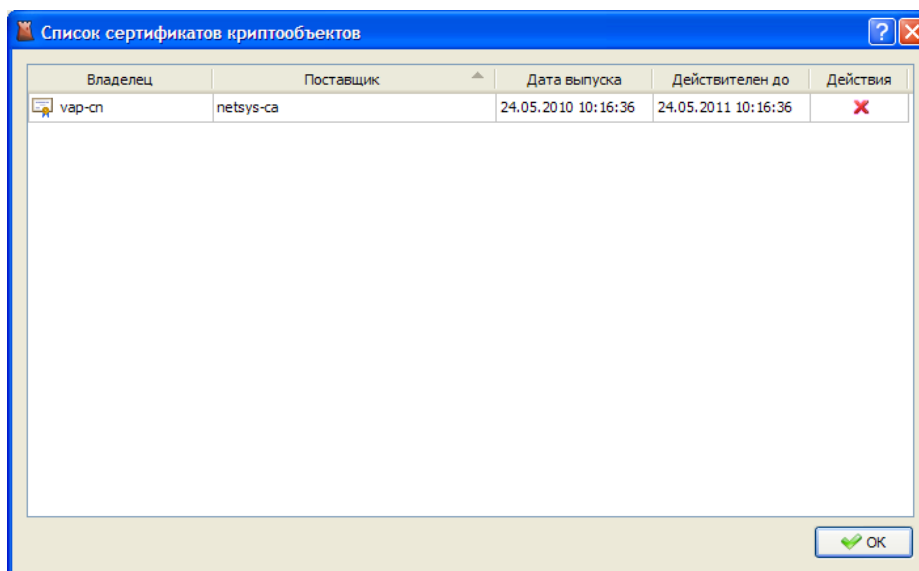


Рисунок 5.7. Диалог изменения списка существующих сертификатов

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».

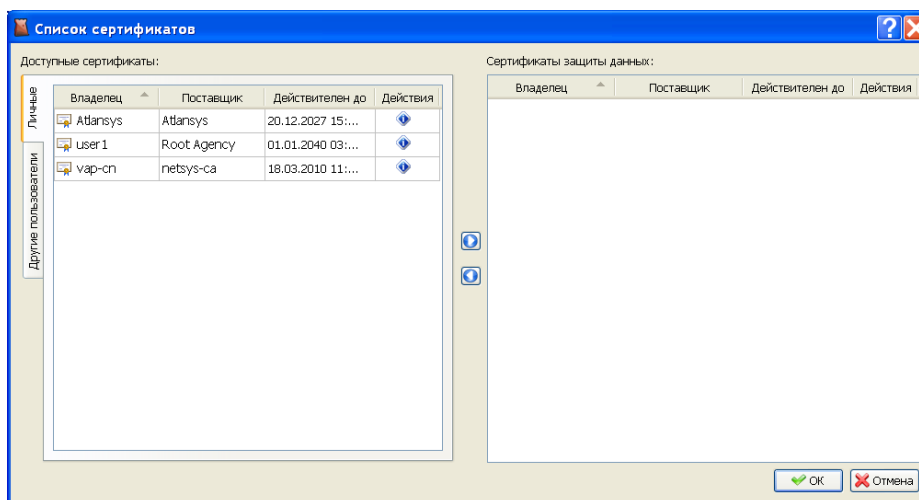


Рисунок 5.8. Диалог «Список сертификатов»

Применение новых свойств происходит после нажатия кнопки «OK» в диалоге «Список сертификатов».

5.3. Дополнительно

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

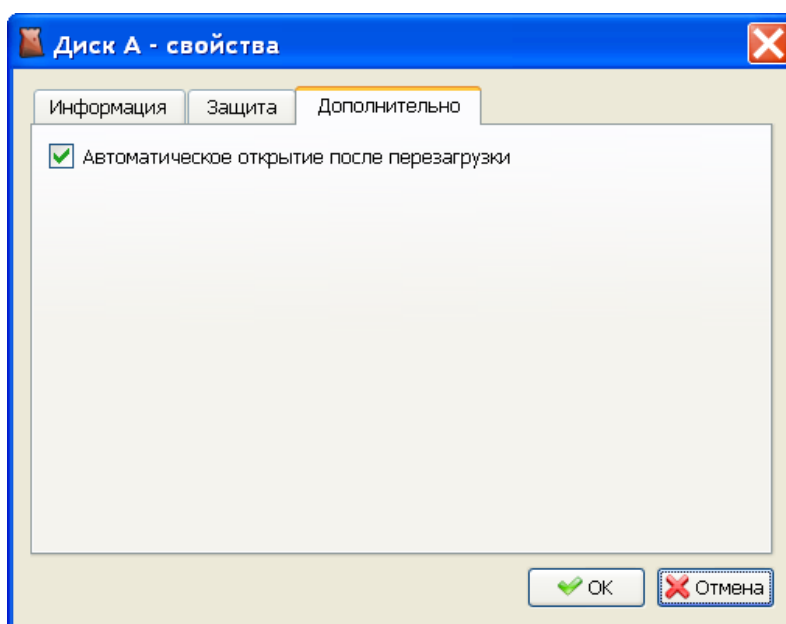


Рисунок 5.9. Диалог свойств криптообъекта - Дополнительно

5.4. Пользовательские скрипты

На вкладке «Пользовательские скрипты» можно назначать автоматическое выполнение каких-либо действий как сразу после открытия криптообъекта, так и после его закрытия. Скриптами могут быть любые исполняемые файлы, bat-файлы или vbs-скрипты, находящиеся на криптосервере.

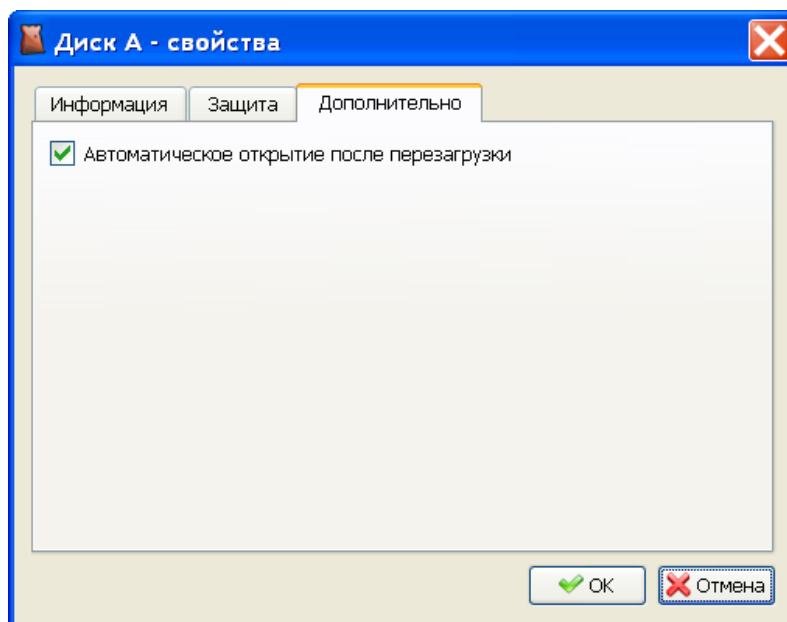


Рисунок 5.10. Диалог свойств криптообъекта - Пользовательские скрипты

Глава 6. Журнал событий

6.1. Журнал событий

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

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

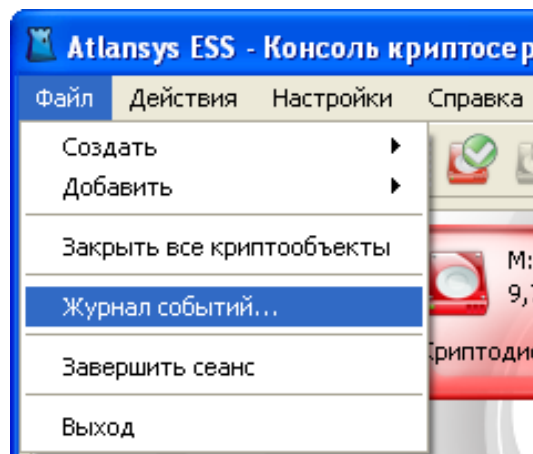


Рисунок 6.1. Запуск журнала событий

После этого отобразится окно журнала событий.

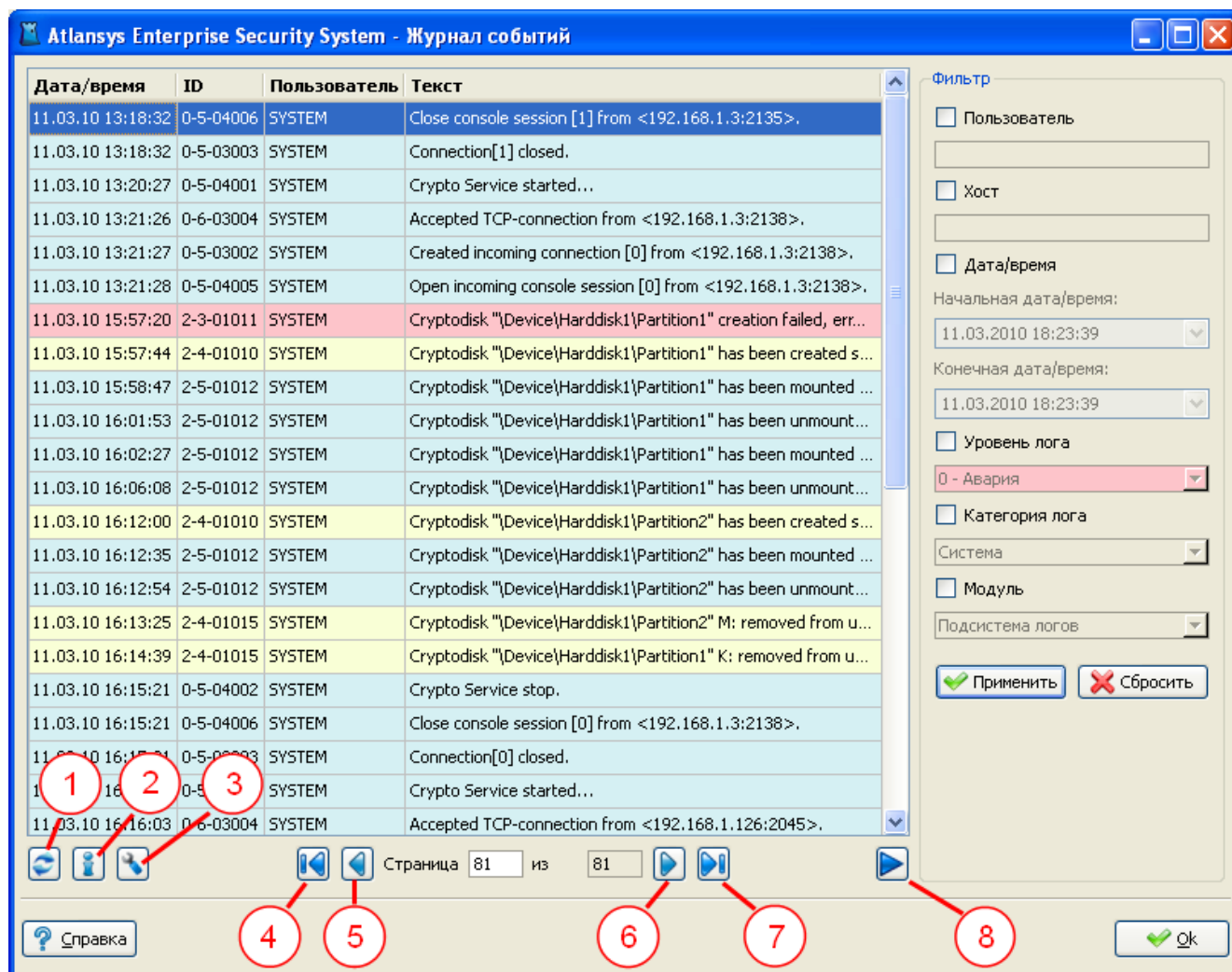


Рисунок 6.2. Окно журнала событий

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:

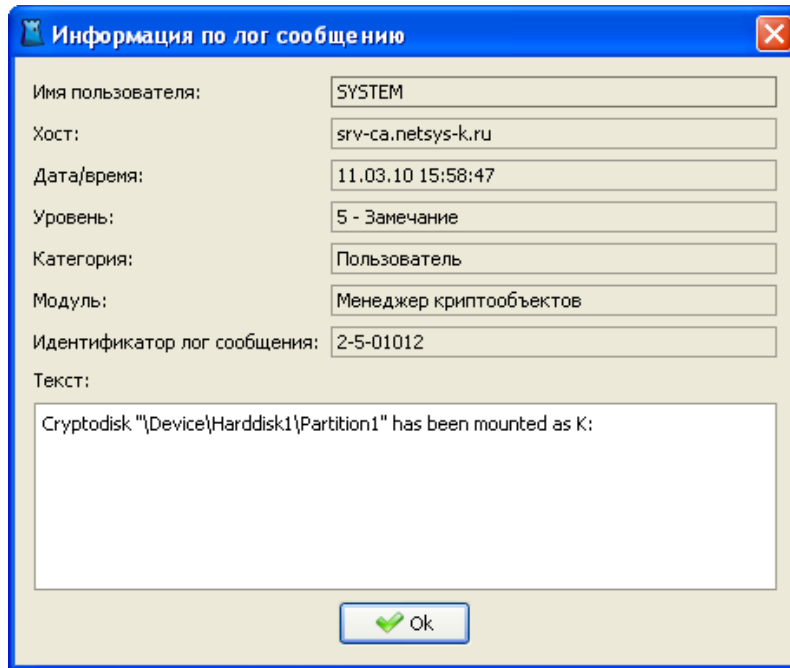


Рисунок 6.3. Информация по лог сообщению

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

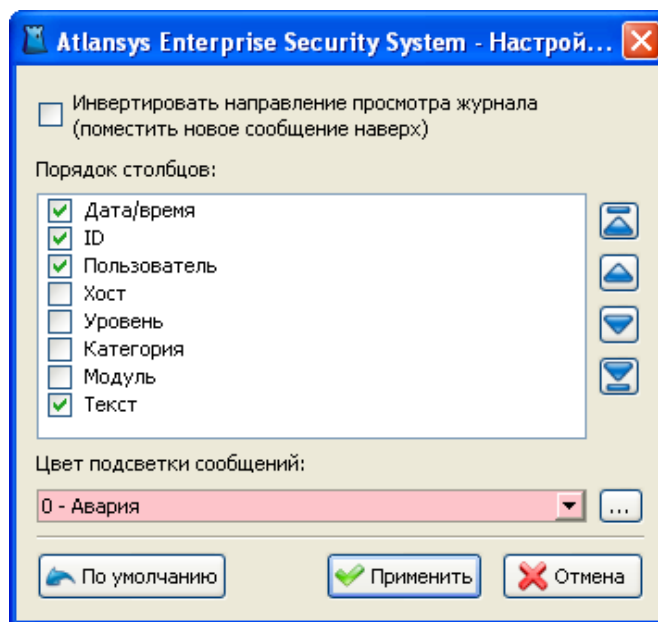


Рисунок 6.4. Настройки журнала регистрации событий

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

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

Фильтр

Пользователь
SYSTEM

Хост
localhost

Дата/время
Начальная дата/время:
04.09.2009 12:27:56

Конечная дата/время:
05.09.2009 13:27:56

Уровень лога
0 - Авария

Категория лога
Система

Модуль
Менеджер криптообъектов

Рисунок 6.5. 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 отображаться 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 7. Техническая поддержка

Техническая поддержка данного продукта осуществляется в рамках правил, опубликованных 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>](mailto: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 возникновении 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 А. Лицензионный договор

А.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 займа.

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 предоставляемых 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. Дезассемблировать, 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 статьёй, 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».