Руководство пользователя

Atlansys Software

Atlansys Bastion Pro

Atlansys Bastion Pro
Руководство пользователя

Atlansys Software

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 гаратнтий 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 Atlansys Software для получения ее копии.

Компания Atlansys Software 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 Atlansys Software, ее поставщики, партнеры или дистрибьютеры были заранее извещены о возможности такого ущерба.

Содержание

Список иллюстраций

Введение

1. Назначение документа

Данное руководство пользователя содержит сведения по установке и эксплуатации Atlansys Bastion Pro и предназначено для конечных пользователей системы.

2. Сведения о продукте

Программный продукт Atlansys Bastion Pro предназначен для криптографической защиты конфиденциальной информации на рабочих станциях. Защита информации осуществляется с помощью шифрования пользовательских данных криптостойкими алгоритмами, гарантирующими надежную защиту от несанкционированного доступа к конфиденциальной информации. Atlansys Bastion Pro 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. (Глава 3)

- *Криптодиски*, представляющие собой полностью зашифрованные разделы жестких дисков или флэш-накопителей. (Глава 4)

- *Гарантированного удаления* файлов, которая обеспечивает полное уничтожение данных в файлах и невозможность восстановления информации из них программными средствами. (Глава 5)

В разделе Глоссарий приведено объяснение терминов, используемых в данном руководстве.

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

3. Технические характеристики

Поддерживаемые операционные системы	Windows XP, Windows Vista, Windows 7
Поддержка файловых систем	FAT, FAT32, NTFS
Создание криптоконтейнеров	Есть
Создание криптодисков с сохранением существующих данных	Есть, для файловых систем FAT, FAT32, NTFS, в том числе на съёмных носителях
Поддерживаемые алгоритмы шифрования[1]	AES, Blowfish
Алгоритмы гарантированного уничтожения файлов	ГОСТ Р50739-95, 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	Windows XP, Windows Vista, Windows 7

[1] В зависимости от типа поставки продукта набор алгоритмов шифрования может отличатся от указанных.

Объём оперативной памяти	не менее 128 Мбайт
Свободное место на диске	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 A 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 Bastion Pro:

- 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 Bastion Pro **Atlansys-Bastion-Pro-5.0.4-setup.msi**.(Рисунок 1.1)

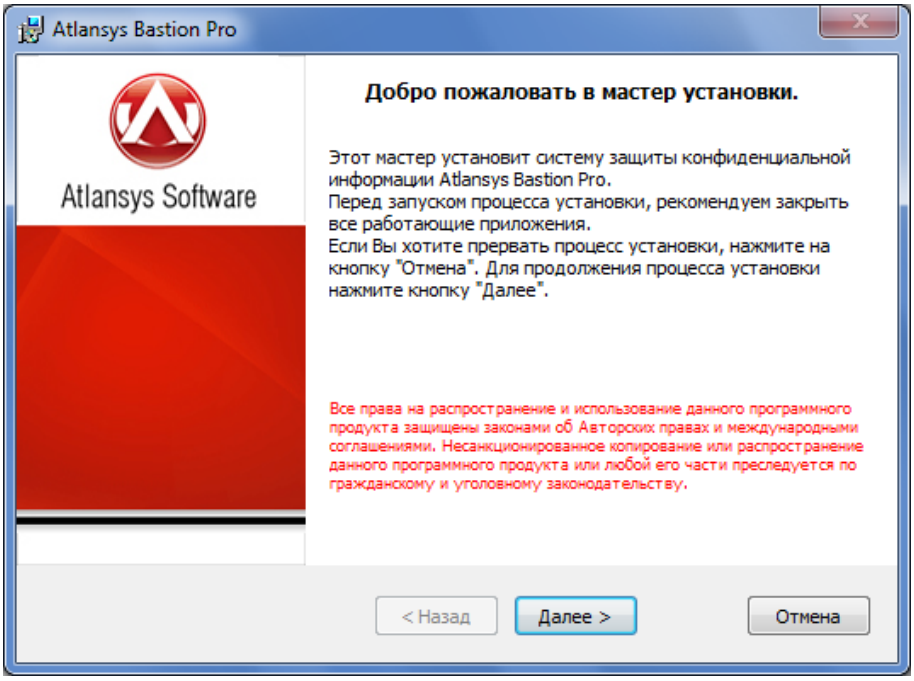

Рисунок 1.1. Установка Atlansys Bastion Pro

2. Нажать кнопку «Далее», после чего появится диалоговое окно, 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».

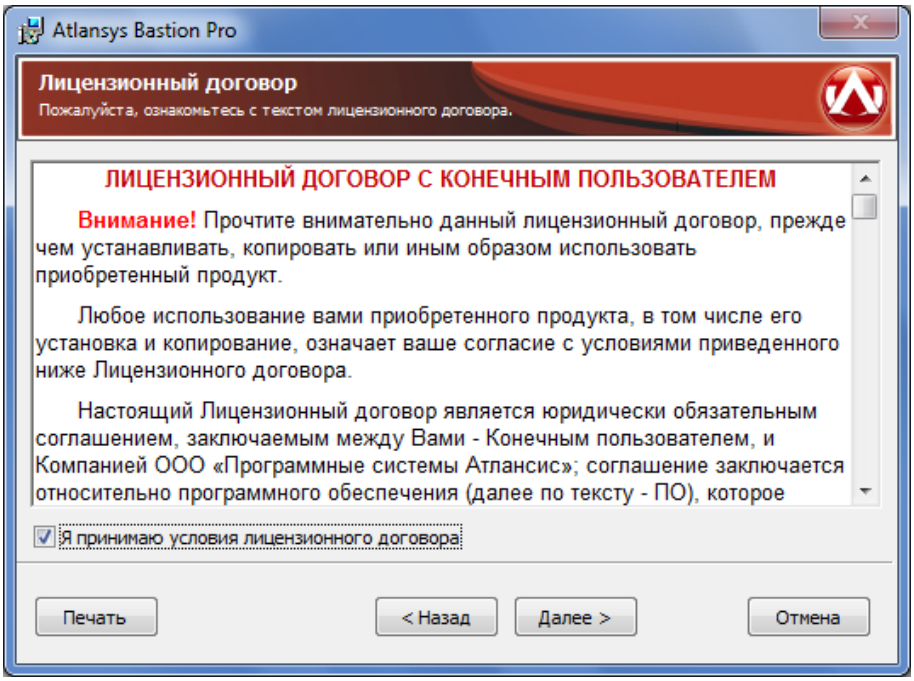

Рисунок 1.2. Лицензионный договор

3. Ввести имя пользователя, e-mail, название организации, 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".

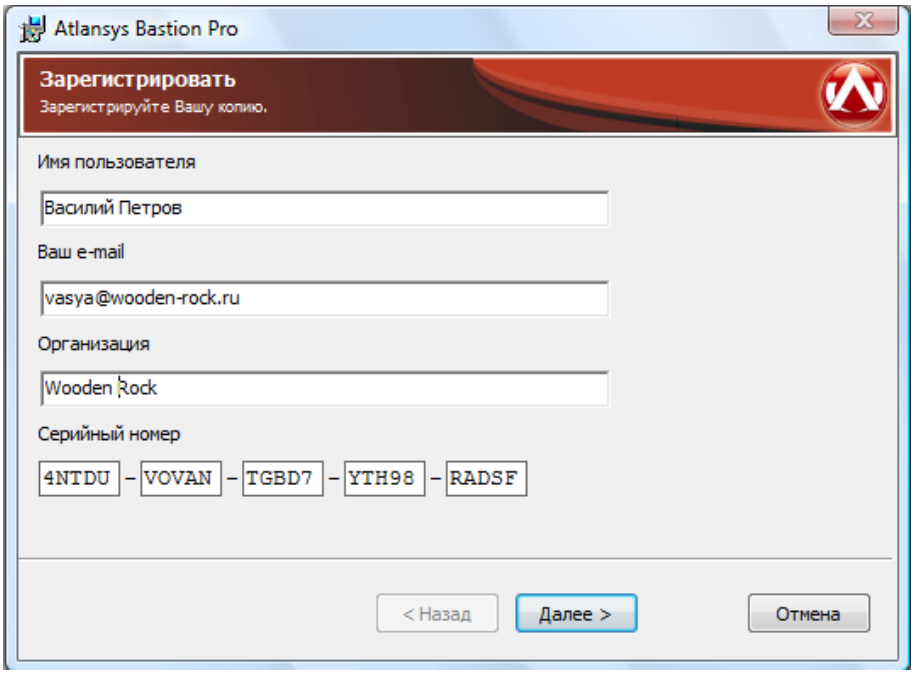

Рисунок 1.3. Регистрация

4. 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».

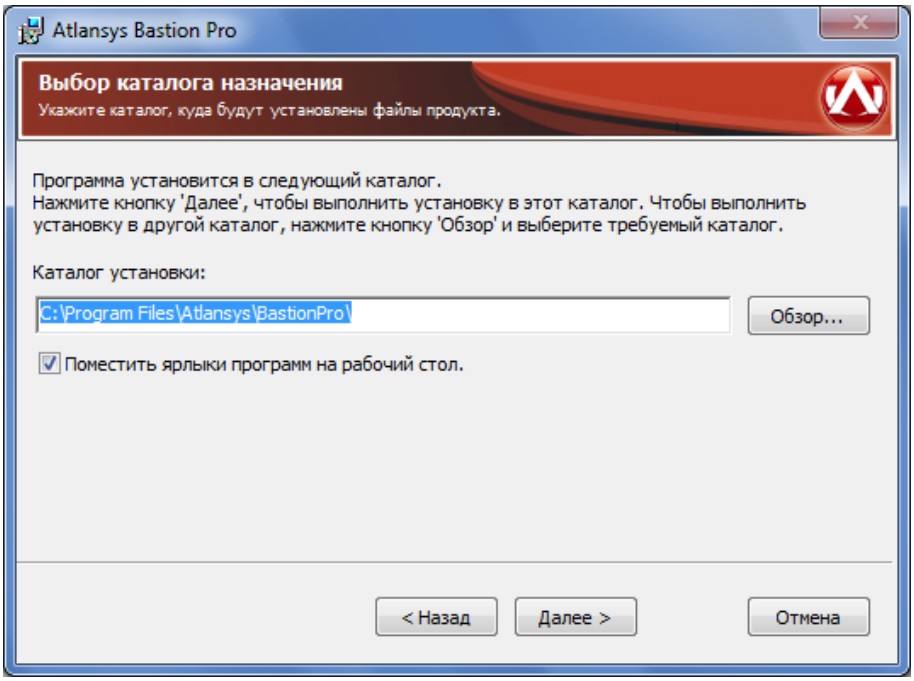

Рисунок 1.4. Выбор каталога для установки программы

5. При необходимости, можно нажать на кнопку "Назад" и изменить ранее введеные параметры. Для запуска процесса установки необходимо нажать кнопку «Установить».

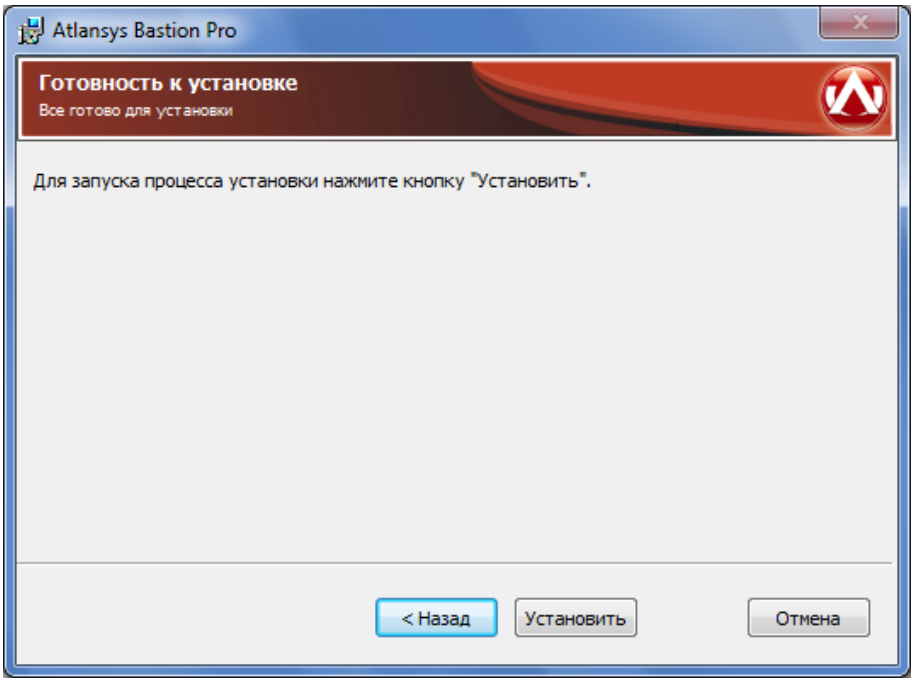

Рисунок 1.5. Запуск процесса установки

6. После этого появится окно, отображающее процесс установки программного обеспечения.

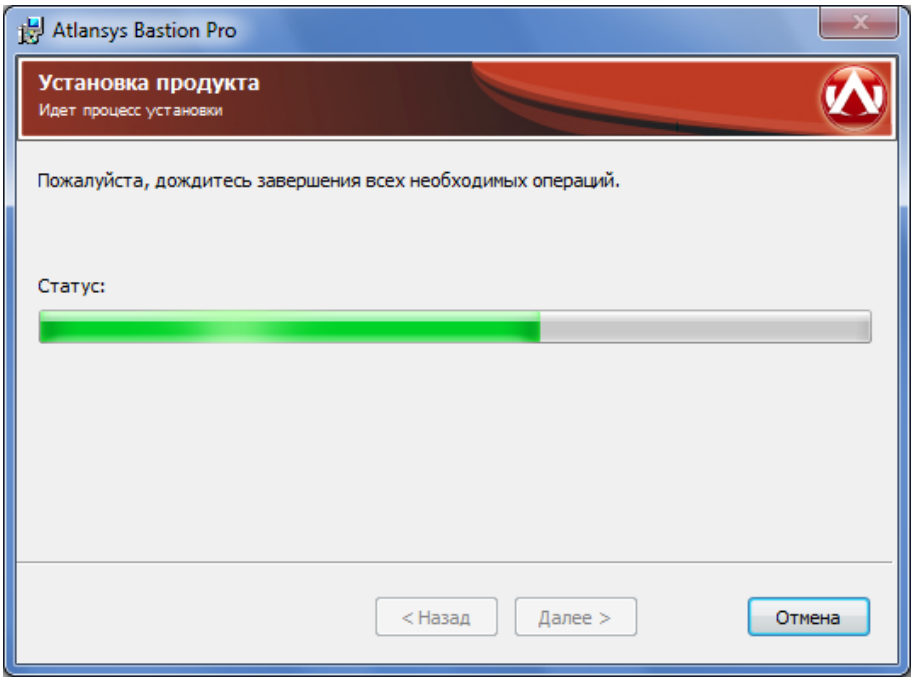

Рисунок 1.6. Процесс установки

7. Для окончания процесса установки необходимо нажать на кнопку «Завершить».

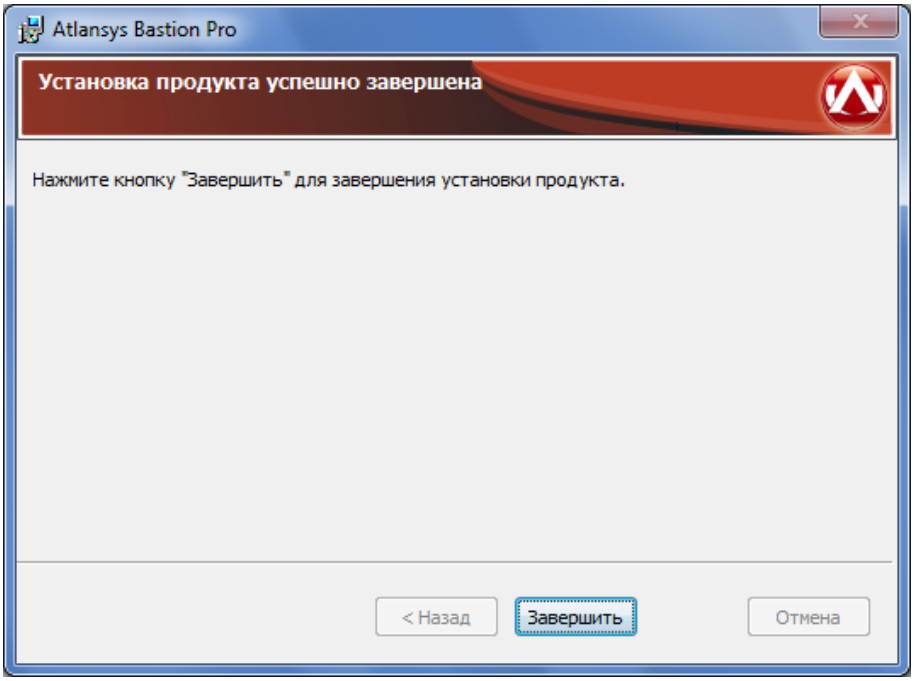

Рисунок 1.7. Завершение установки

1.2. Обновление программного обеспечения

Если на рабочей станции уже установлена более ранняя версия продукта, то при установке новой версии, совместимой с предыдущей, произведется её автоматическое обновление.

Важно

Версия продукта 5.0.x не совместима с предыдущими версиями Atlansys Bastion Pro. Криптообъекты, созданные ранними версиями продукта не поддерживаются. Версии Atlansys Bastion Pro 3.x.x, 4.x.x. могут использоваться параллельно с текущей версией продукта, при этом рекомендуется создать криптоконтейнеры или криптодиски с использованием новой версии продукта, скопировать в них всю информацию из криптообъектов старых версий и использовать вновь созданные криптообъекты.

Описание совместимости других версий программного обеспечения, для которых возможно обновление, смотрите в поставляемой с инсталлятором документации или на сайте производителя. Все конфигурационные файлы предыдущей совместимой 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 Bastion Pro необходимо:

1. Запустить программу инсталятора Atlansys Bastion Pro **Atlansys-Bastion-Pro-5.0.4-setup.msi**. Нажать кнопку "Далее". (Рисунок 1.8)

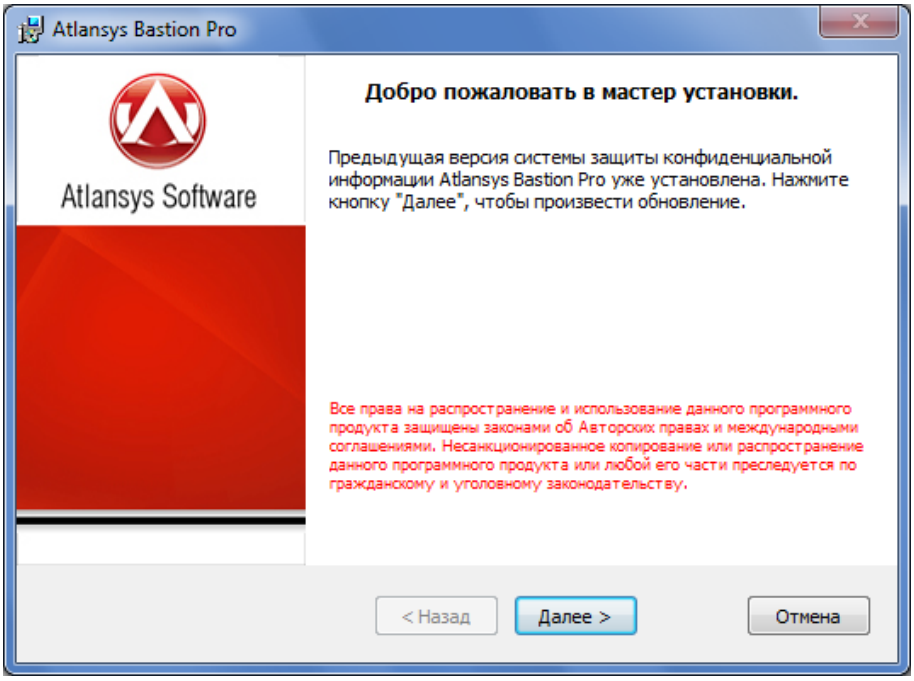

Рисунок 1.8. Обновление Atlansys Bastion Pro

2. После этого появится окно, отображающее процесс обновления программного обеспечения. (Рисунок 1.9)

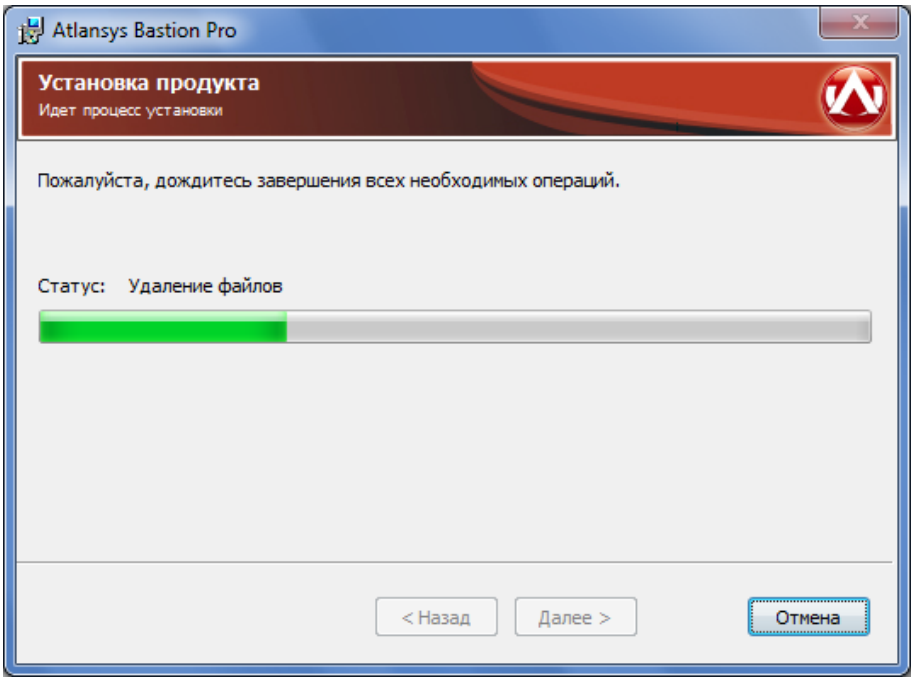

Рисунок 1.9. Процесс установки

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

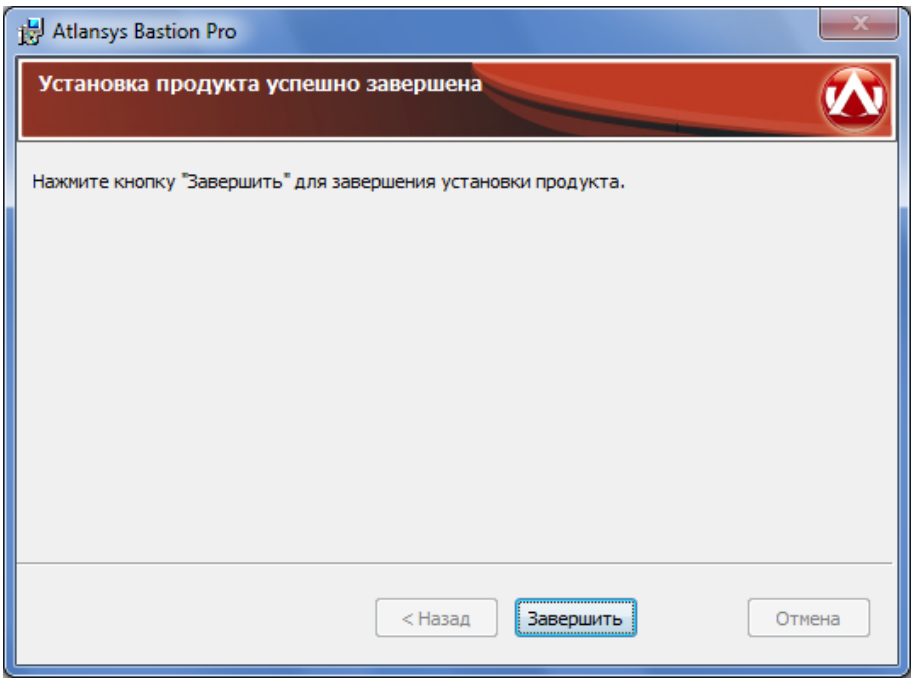

Рисунок 1.10. Завершение установки

1.3. Установка программного обеспечения с использованием конфигурационного файла

Чтобы автоматизировать установку Atlansys Bastion Pro 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-Bastion-Pro-5.0.4-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-Bastion-Pro-5.0.4-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. "**USEREMAIL=e-mail**" - адрес электронной почты пользователя.

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.

Пример файла settings.cfg:

```
# Конфигурация для рабочей станции
INSTALLDIR=C:\Program Files\Atlansys Software\
ADDDEFAULT=CryptoArchive,CryptoCont
PIDKEY=527LD-2TEST-ONLY4-VOVAN-SFXFL
USERNAME=Василий Петров
USEREMAIL=vasya@wooden-rock.ru
COMPANYNAME=Wooden Rock
```

Эти же свойства можно задавать из командной строки. Например:

msiexec /i Atlansys-Bastion-Pro-5.0.4-setup.msi INSTALLDIR="c:\Program Files\Atlansys" ADDDEFAULT=ALL PIDKEY=527LD-4TEST-ONLY2-VOVAN-SFXFL USERNAME="Василий Петров" USEREMAIL="vasya@wooden-rock.ru" COMPANYNAME="Wooden Rock"

1.4. Удаление программного обеспечения

Для удаления программного обеспечения необходимо выполнить следующие действия:

1. Закрыть все программы, использующие криптоконтейнеры и криптодиски.

2. 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 выберать Atlansys Bastion Pro. Для удаления Atlansys Bastion Pro необходимо нажать на кнопку "Удалить". Появится окно для подтверждения запроса удаления. Необходимо нажать на кнопку "Да", после чего начнется процесс удаления Atlansys Bastion Pro с рабочей станции.

Глава 2. Atlansys Bastion Pro

2.1. Назначение

Atlansys Bastion Pro - это основное приложение продукта, в котором сосредоточено управление над всем комплексом программ и подключаемых модулей.

2.2. Запуск приложения

Запуск приложения осуществляется либо через ярлык на рабочем столе компьютера, либо через выбор соответствующего пунта меню "**Пуск / Все программы / Atlansys/ Bastion Pro / Atlansys Bastion Pro**" (Рисунок 2.1).

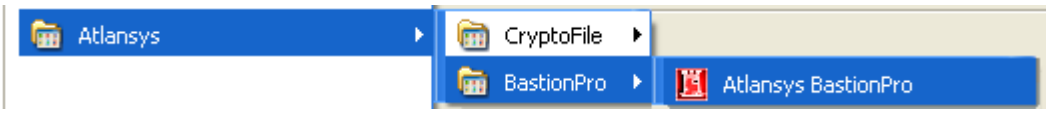

Рисунок 2.1. Запуск Atlansys Bastion Pro через меню Пуск

2.3. Интерфейс главного окна приложения

После первого запуска Atlansys Bastion Pro на экране появится главное окно приложения. Главное окно состоит из следующих разделов:

1. Главное меню.
2. Кнопки для перехода к соответствующими модулям.
3. Координаты службы технической поддержки.

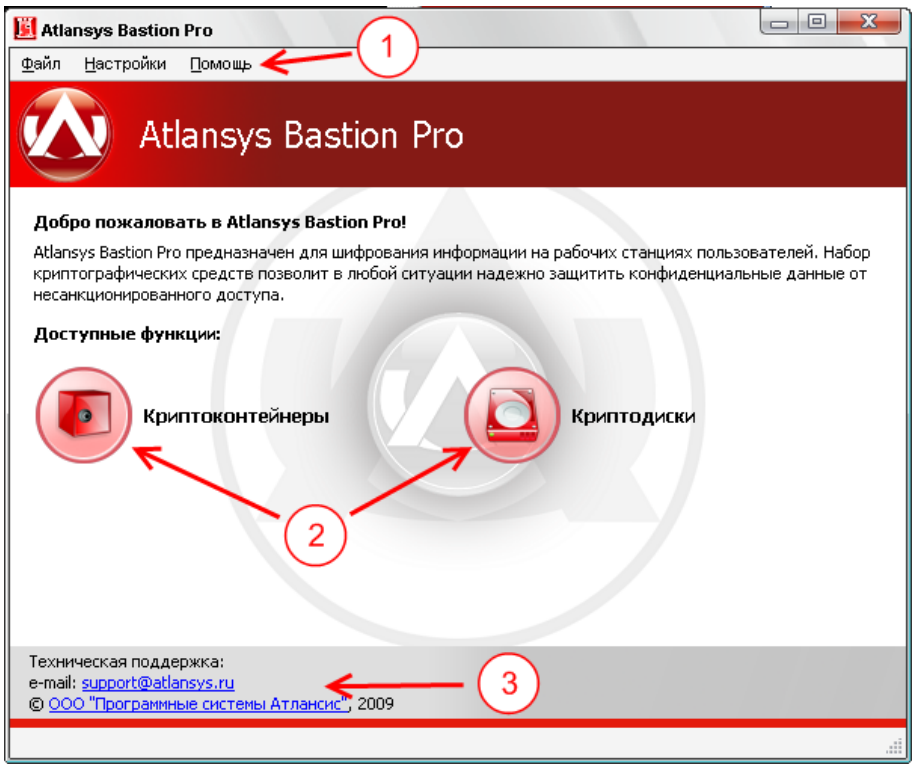

Рисунок 2.2. Главное окно

1. Меню "Файл" содержит подменю:

- "Создать" - для создания новых криптоконтейнеров, криптодисков.
- "Добавить" - для добавления в список существующих криптоконтейнеров и криптодисков, которые были созданы на других рабочих станциях.
- "Закрыть все криптообъекты" - быстрое закрытие всех открытых криптоконтейнеров и криптодисков.
- "Активировать красную кнопку" - активация действий, заданных на Красную кнопку.
- "Журнал событий" - окно для просмотра журнала регистрации событий, происходящих в системе.
- "Выход" - для выхода из приложения.

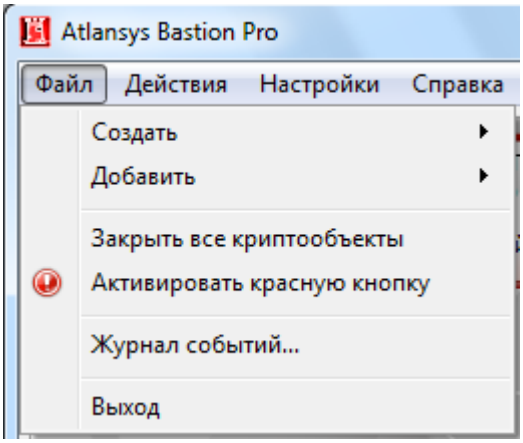

Рисунок 2.3. Меню "Файл"

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

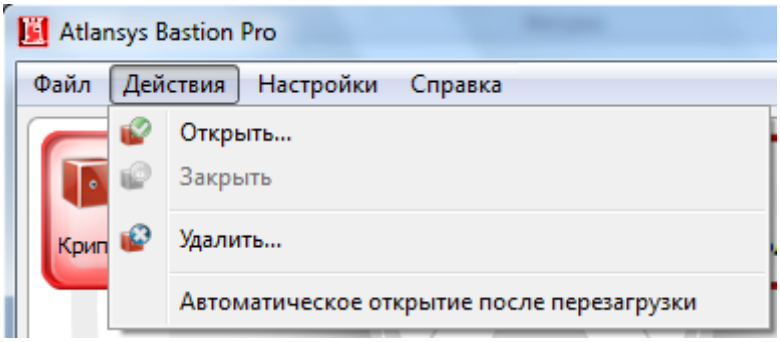

Рисунок 2.4. Меню "Действия"

3. Меню "Настройки" содержит подменю:
   - "Настройки" - вызов диалога настроек продукта.
   - "Список плагинов..." - для отображения списка загруженных модулей (плагинов).
   - "Сворачивать в трей" - для сворачивания окна в системный трей, при нажатии на кнопки закрытия или минимизации главного окна, что позволяет обеспечить быстрый доступ к приложению без его повторной загрузки.
4. Меню "Помощь" содержит пункты:
   - "Главное меню" - переход на стартовую страницу приложения.

- "Справка" - для вызова справки по программе.
- "Обновить лицензию" - для вызова диалога обновления лицензии.
- "Зарегистрировать" - для вызова диалога регистрации продукта на сайте разработчика.
- "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 отличатся от приведённых в данном Руководстве.

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

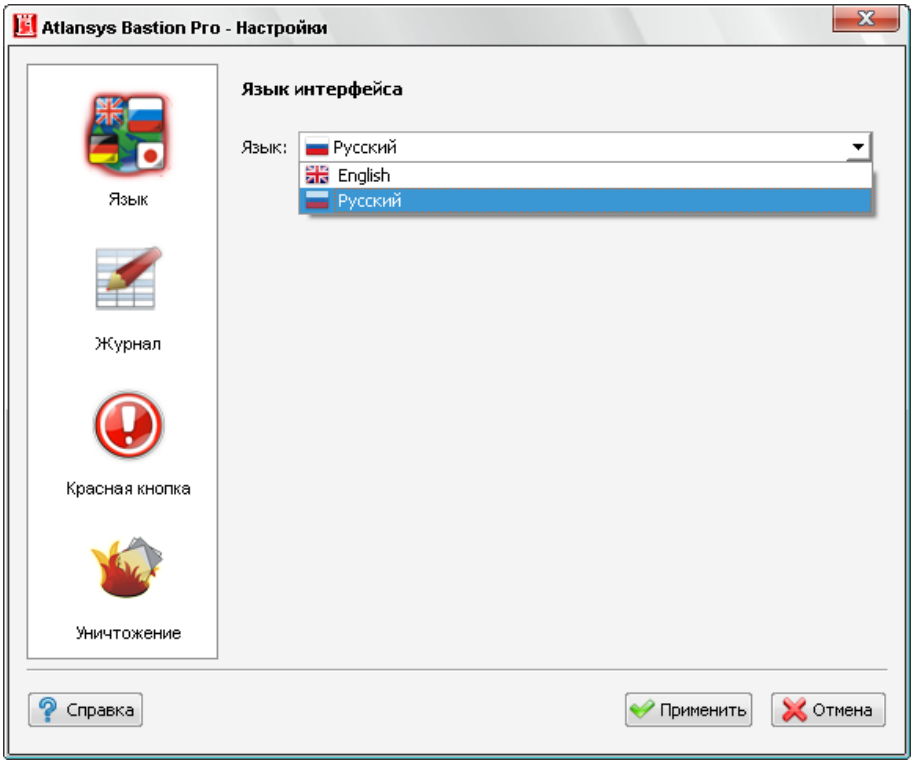

Рисунок 2.5. Язык

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.

- "Syslog-сервер" - задаётся IP-адрес сервера для передачи на него лог-сообщений по протоколу syslog. Лог-сообщения передаются по протоколу UDP на порт 514, при использовании в сети межсетевых экранов их необходимо настроить для пропускания данных пакетов от рабочих станций к syslog-серверу.

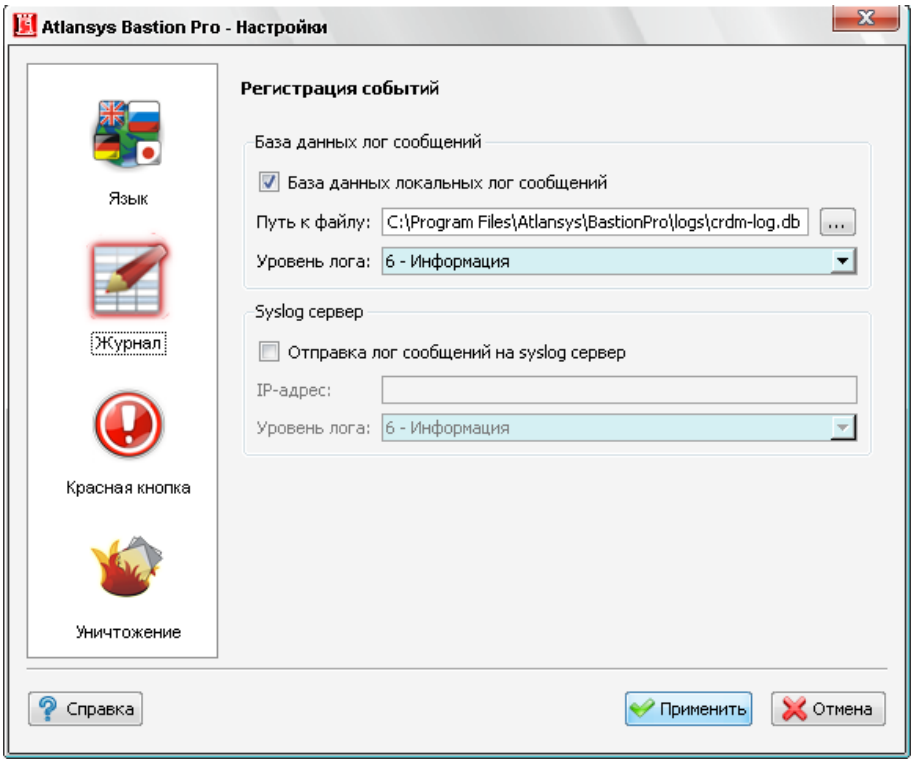

Рисунок 2.6. Регистрация событий

3. "Красная кнопка" - настройки действий при активации механизма "Красной кнопки", который включается пользователем в критической ситуации, когда необходимо быстро закрыть доступ к открытым криптообъектам. По умолчанию красная кнопка не активирована и никаких действий не производится. При активации красной кнопки она может включатся либо через главное меню "Файл / Активировать красную кнопку", либо с помощью горячих клавиш, комбинация которых задаётся в настройках. Необходимо так же задать действия при активации красной кнопки. По умолчанию - это закрытие всех открытых криптообъёктов, дополнительно можно перезагрузить или выключить компьютер, чтобы полностью блокировать доступ к криптообъектам.

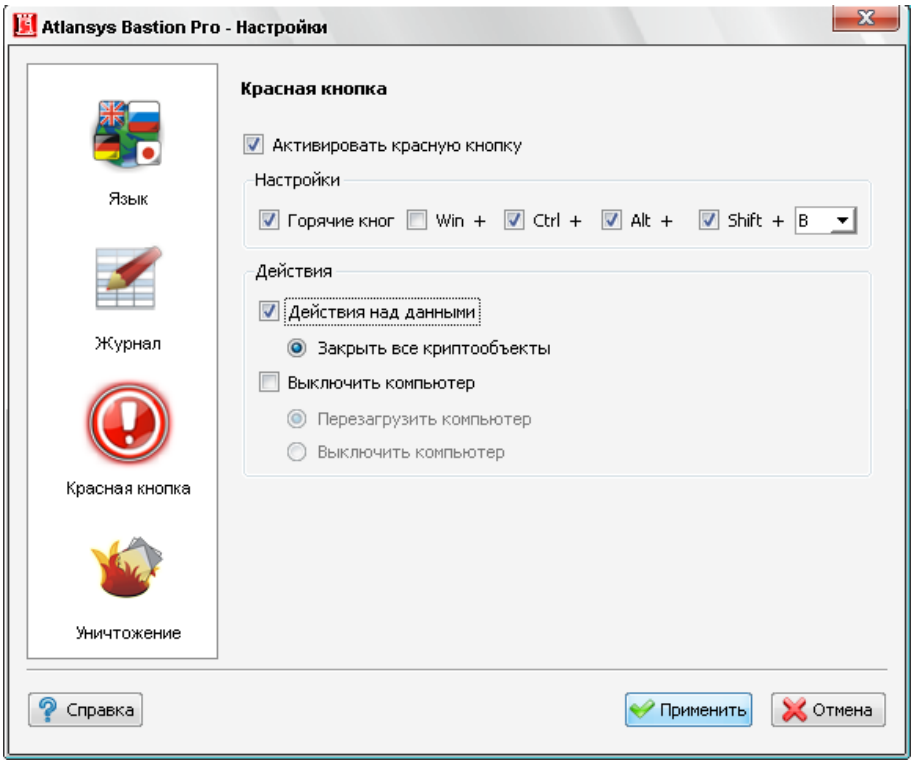

Рисунок 2.7. Красная кнопка

4. "Уничтожение данных" - задаёт алгоритм уничтожения данных по умолчанию, который применяется для уничтожения файлов через контекстное меню Проводника Windows.

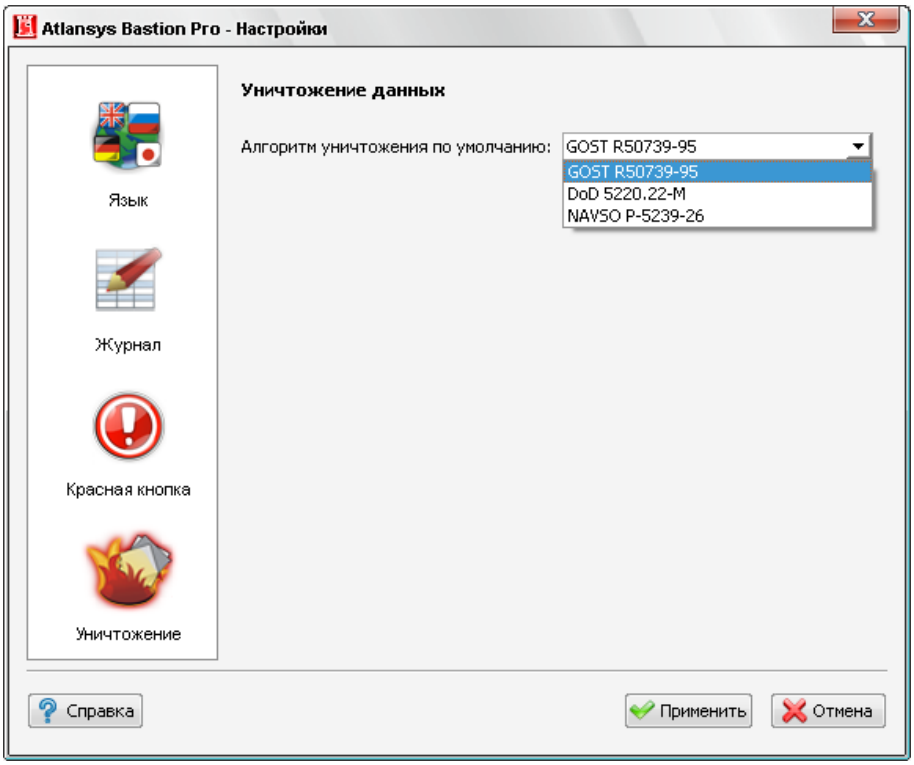

Рисунок 2.8. Уничтожение данных

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.

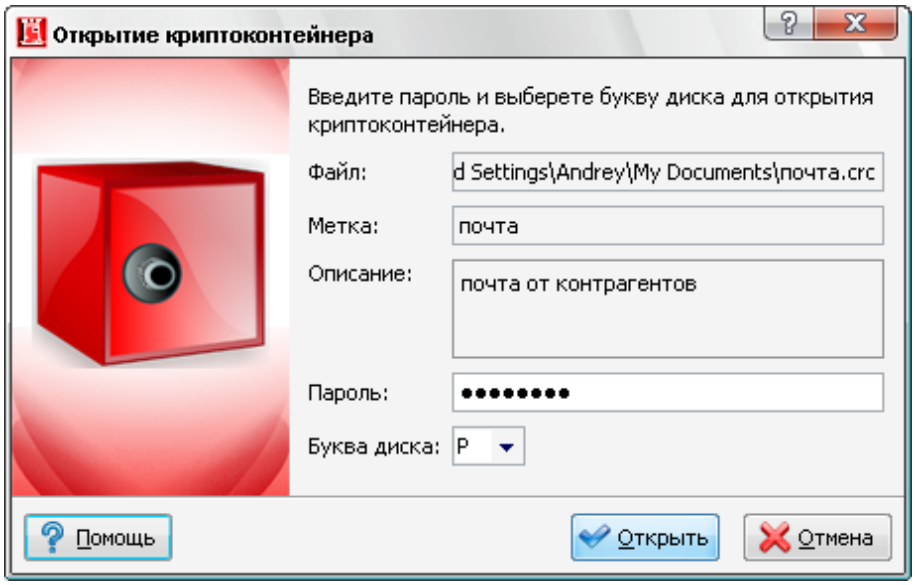

Рисунок 2.9. Автооткрытие криптоконтейнера

В процессе автоматического открытия криптообъектов в системном трее появится значок диалога автооткрытия, в котором отображаются все криптообъекты, подлежащие автооткрытию с отображением их состояния. При нажатии на этот значок отобразится диалог автооткрытия критообъектов, в котором отображается процесс открытия и состояния криптообъектов.

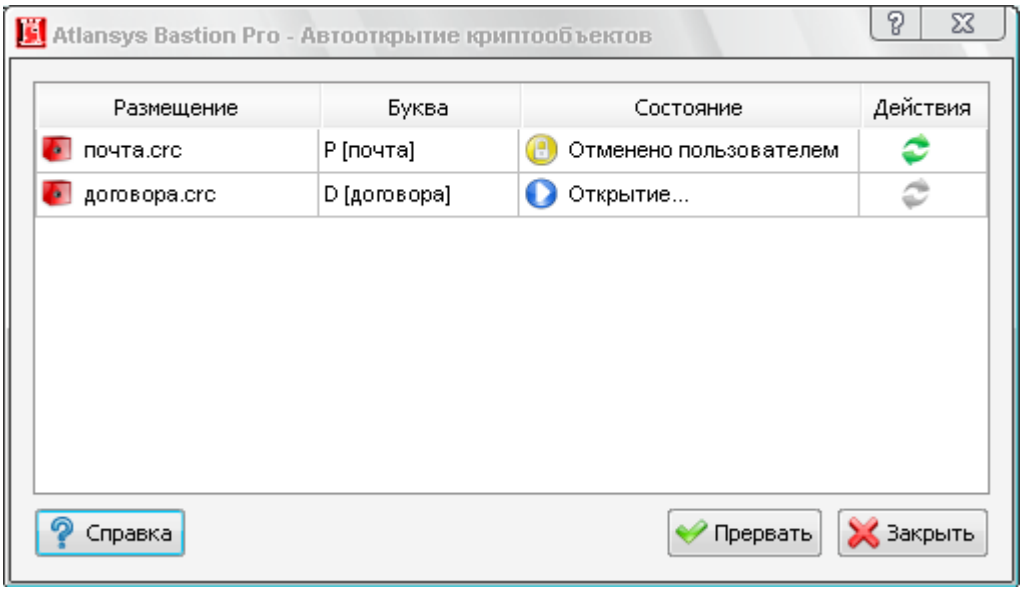

Рисунок 2.10. Диалог автооткрытия криптообъектов

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 Bastion Pro может поддерживать разный набор функций. Таким образом, при необходимости включения новой функциональности не требуется приобретать и пе-

реустанавливать 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 продукта. 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, использовать для создания архивных копий конфиденциальной информации.

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 Навигаторе выбрать в главном меню пункты "Файл" / "Создать" / "Криптоконтейнер..."

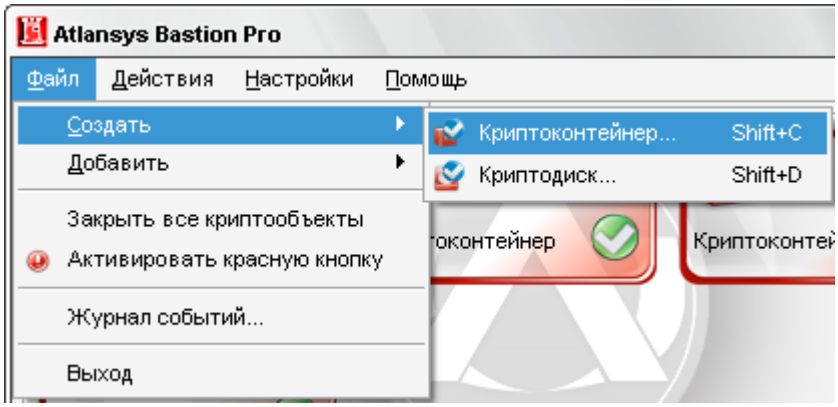

Рисунок 3.1. Меню "Файл" / "Создать"

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 "...".

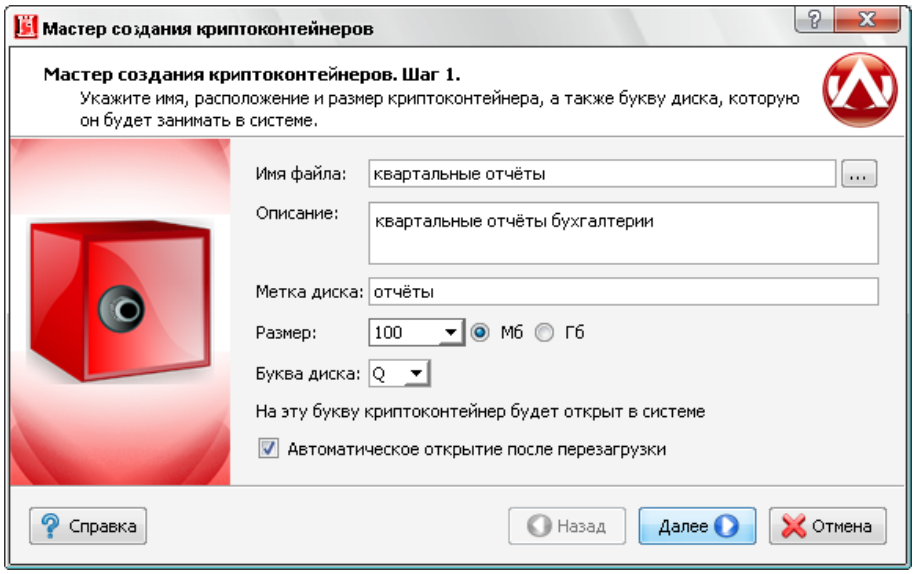

Рисунок 3.2. Мастер создания криптоконтейнеров.

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 после перезагрузки системы следует оставить выбранным чекбокс автоматического открытия. При входе пользователя в систему после перезагрузки криптоконтейнер будет автоматически открываться, при необходимости будет запрашиваться пароль.

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.

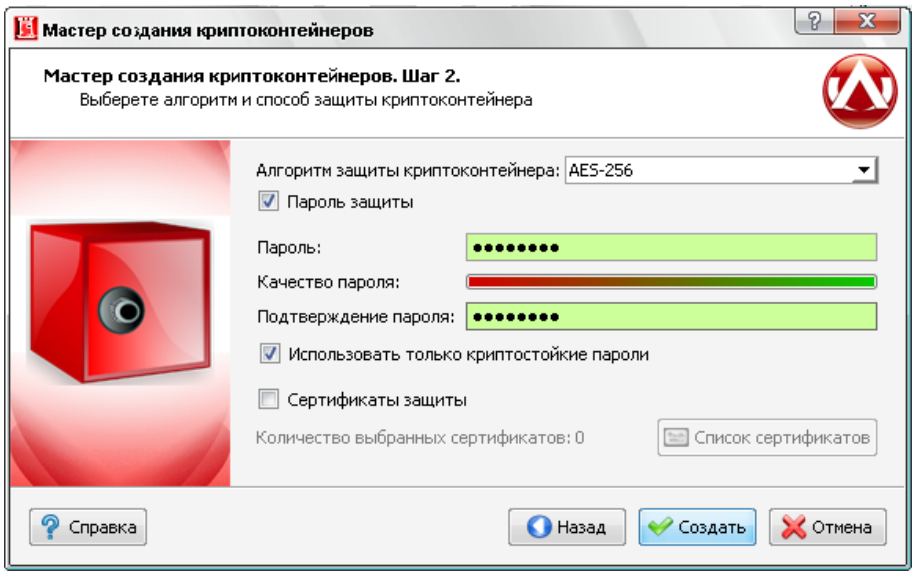

Рисунок 3.3. Мастер создания криптоконтейнеров. Способы защиты.

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 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. Теперь криптоконтейнер можно использовать как обычный диск Windows.

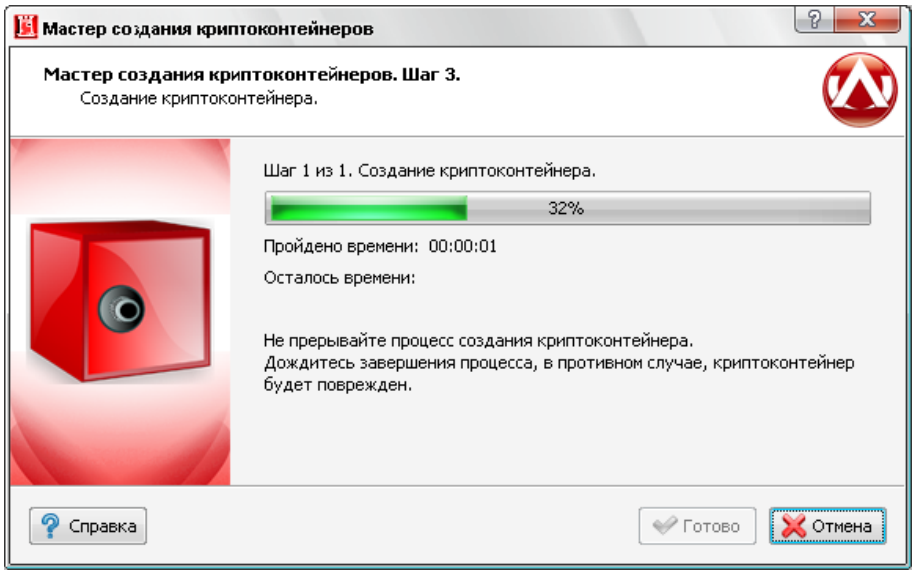

Рисунок 3.4. Мастер создания криптоконтейнеров. Прогресс создания.

3.3. Добавление криптоконтейнера

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

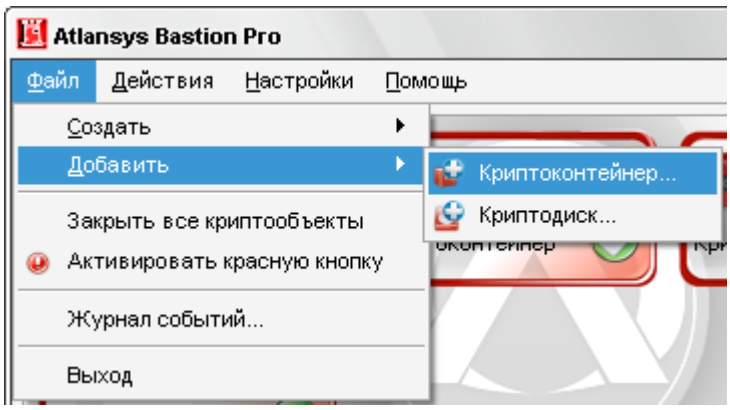

Рисунок 3.5. Меню "Файл" / "Добавить"

В появившемся окне Мастера добавления криптоконтейнеров выбрать файл криптоконтейнера. Если формат криптоконтейнера поддерживается текущей версией Навигатора, 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 Навигатора. Если криптоконтейнер защищен сертификатом и его закрытый ключ имеется в системе, криптоконтейнер автоматически откроется, и на выбранной букве диска запустится Проводник Windows.

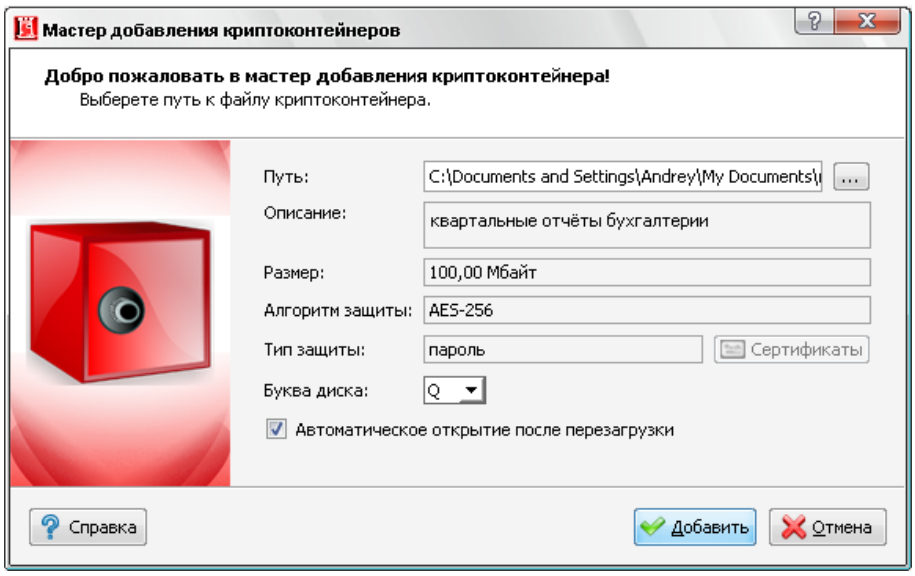

Рисунок 3.6. Мастер добавления криптоконтейнеров

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.

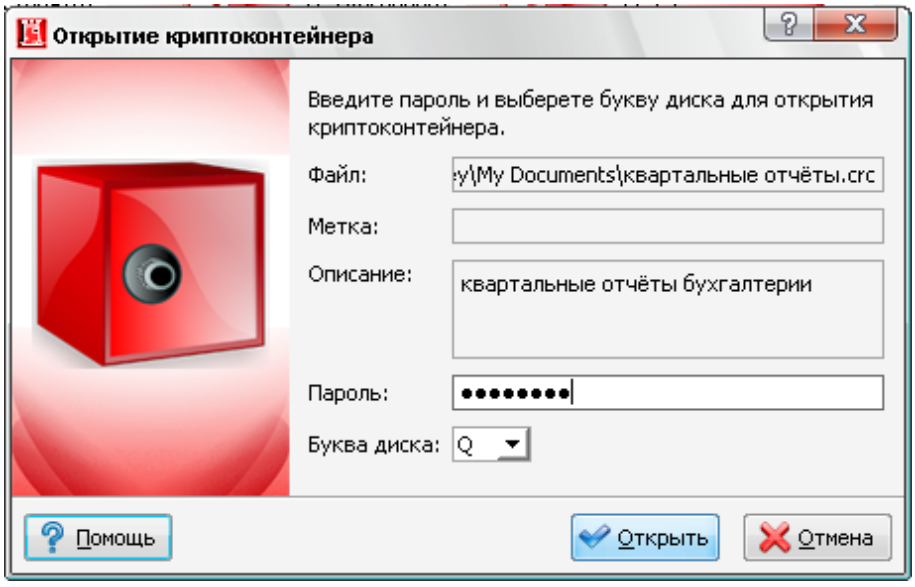

Рисунок 3.7. Диалог открытия криптоконтейнера

3.4. Работа с криптоконтейнерами

При создании или добавлении нового криптоконтейнера он автоматически открывается и имеет состояние "Открыт", что отображается на его иконке в списке. 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.

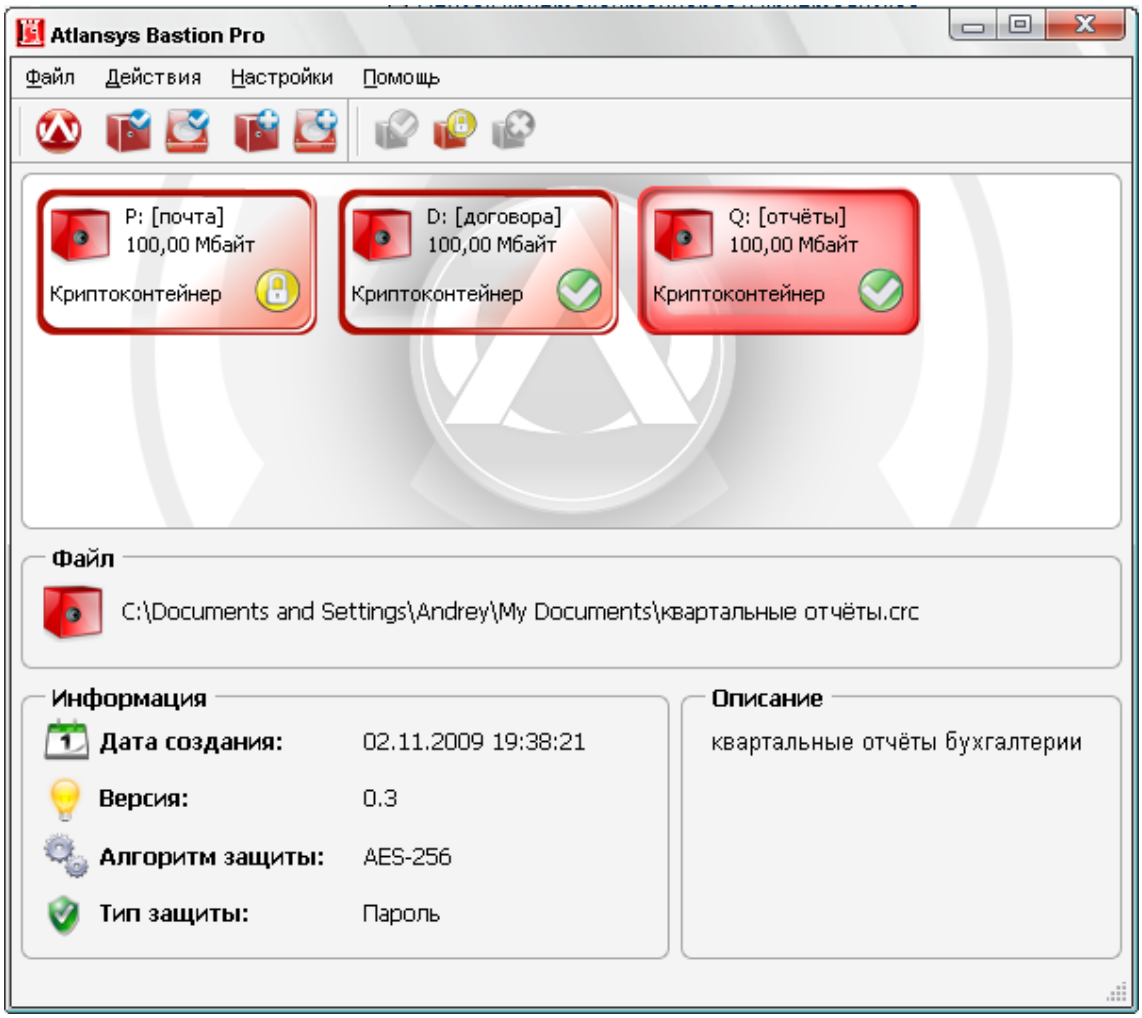

Рисунок 3.8. Список криптоконтейнеров и криптодисков

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

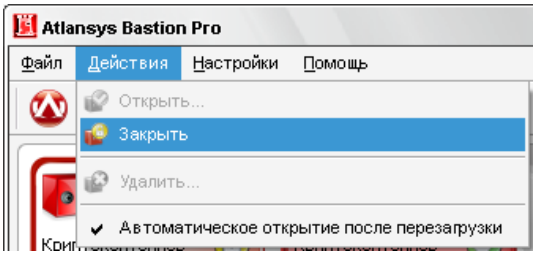

Рисунок 3.9. Меню "Действия"

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

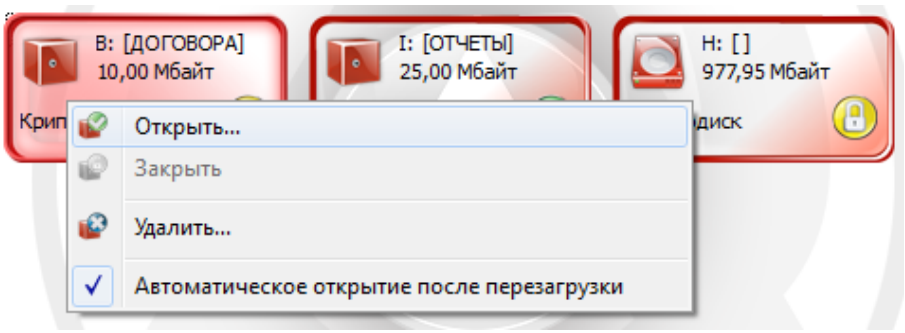

Рисунок 3.10. Контекстное меню криптоконтейнера

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

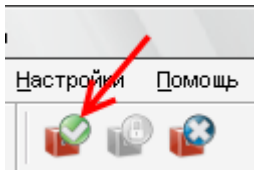

Рисунок 3.11. Панель инструментов, кнопка "Открыть"

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 "Закрыть", либо в панели инструментов нажать на кнопку "Удалить".

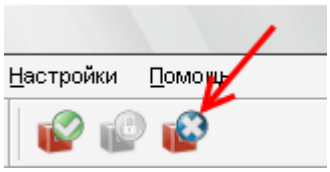

Рисунок 3.12. Панель инструментов, кнопка "Удалить"

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

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

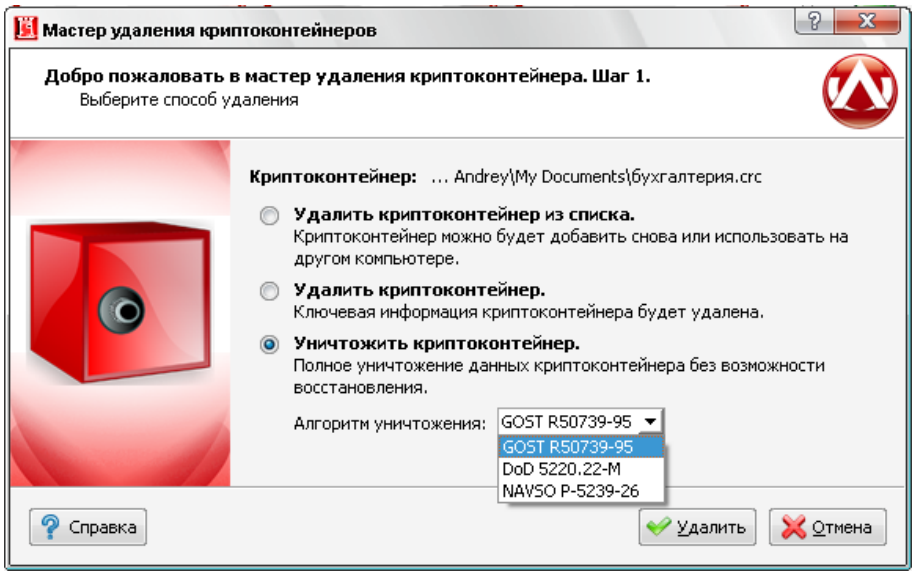

Рисунок 3.13. Мастер удаления криптоконтейнеров

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".

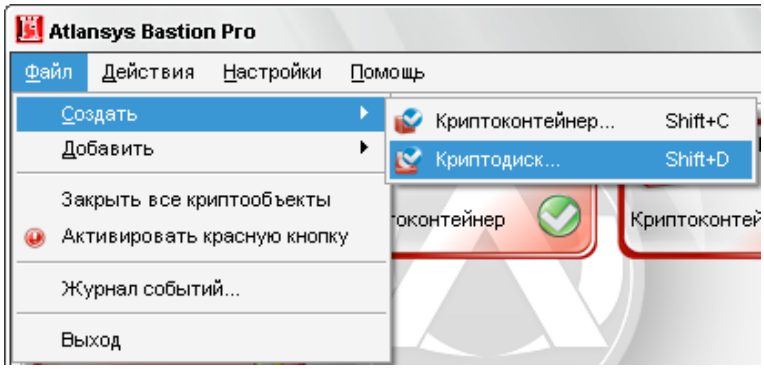

Рисунок 4.1. Меню "Файл" / "Создать"

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

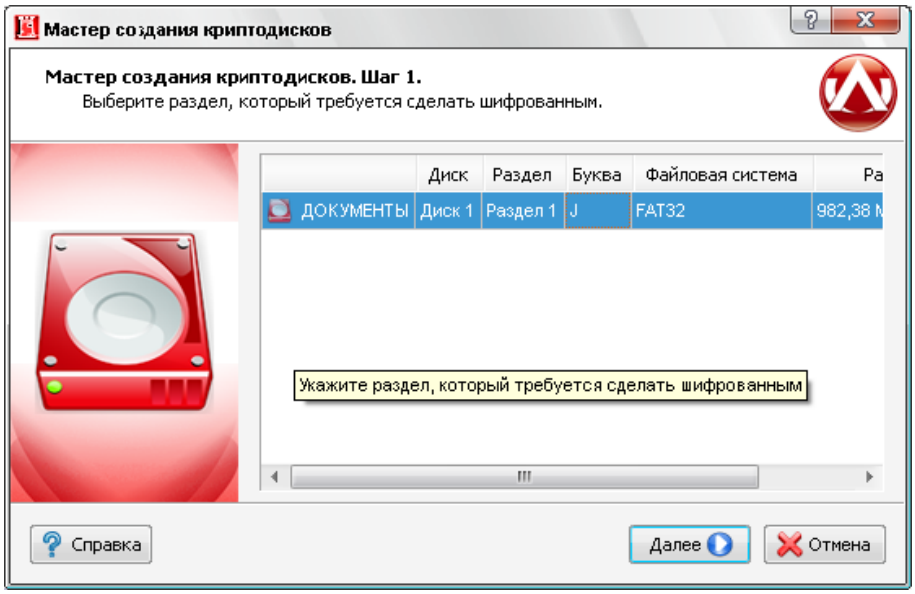

Рисунок 4.2. Мастер создания криптодисков. Выбор раздела.

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 Bastion Pro 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.

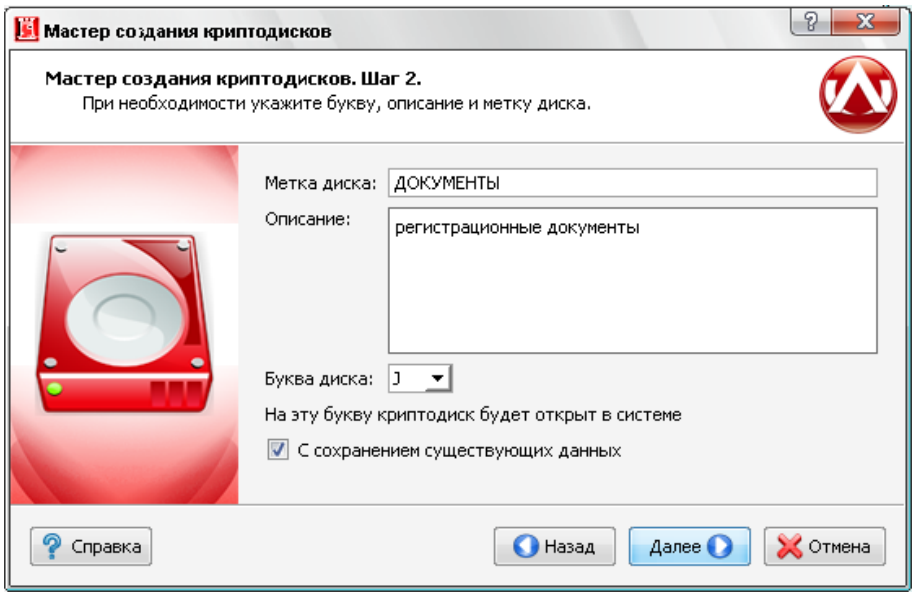

Рисунок 4.3. Мастер создания криптодисков. Метка диска и описание.

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 крпитодиска. 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.

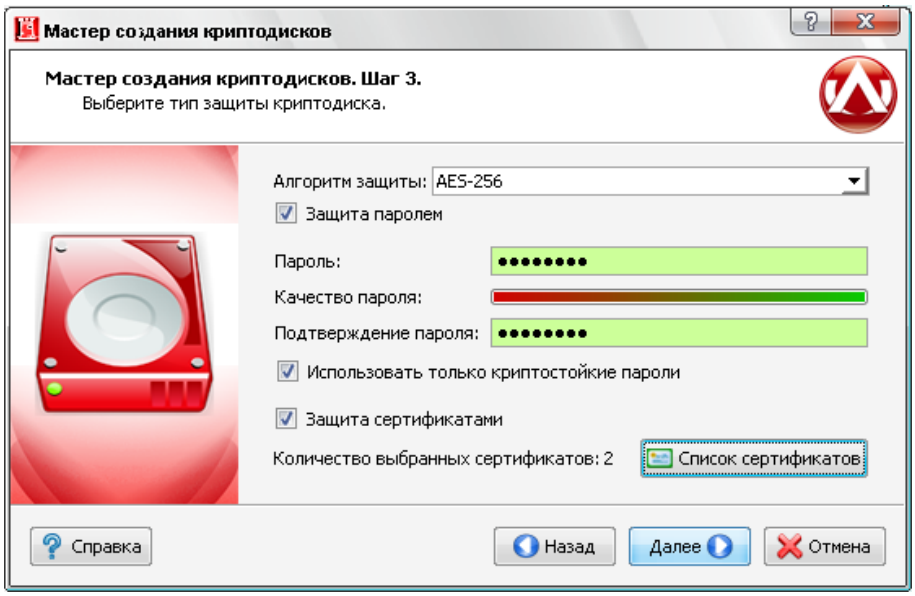

Рисунок 4.4. Мастер создания криптодисков. Способы защиты.

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 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".

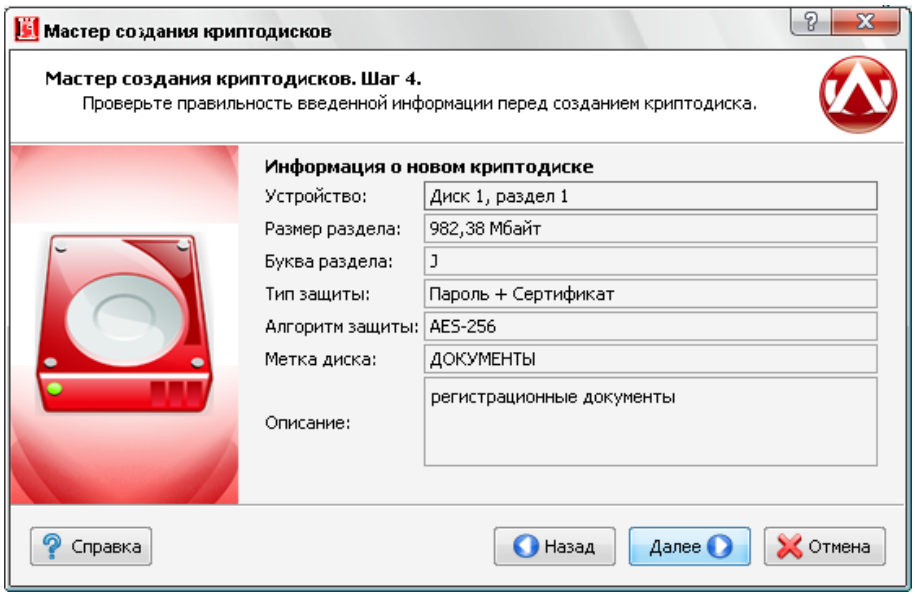

Рисунок 4.5. Мастер создания криптодисков. Сводная информация.

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".

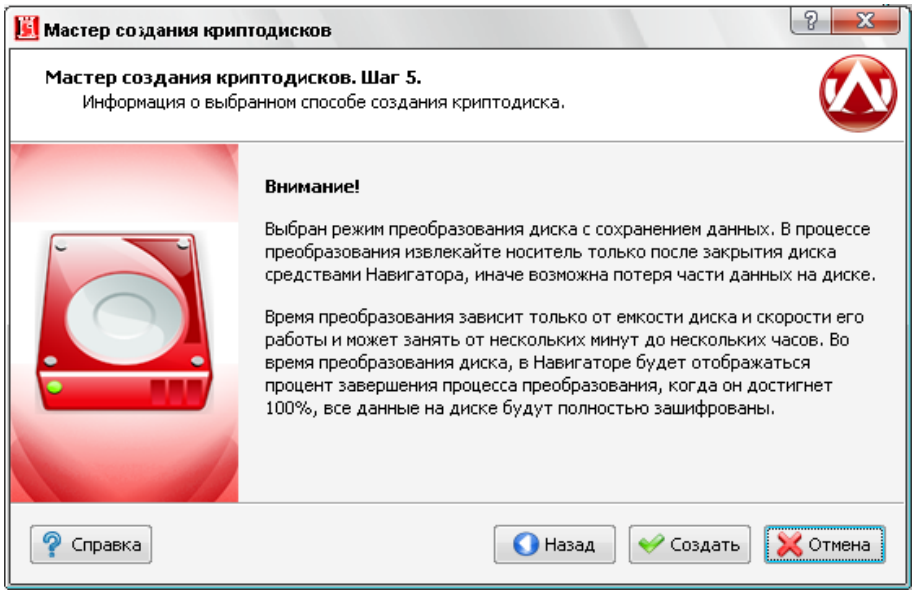

Рисунок 4.6. Мастер создания криптодисков. Предупреждение.

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 и запустится Проводник Windows на открытом криптодиске.

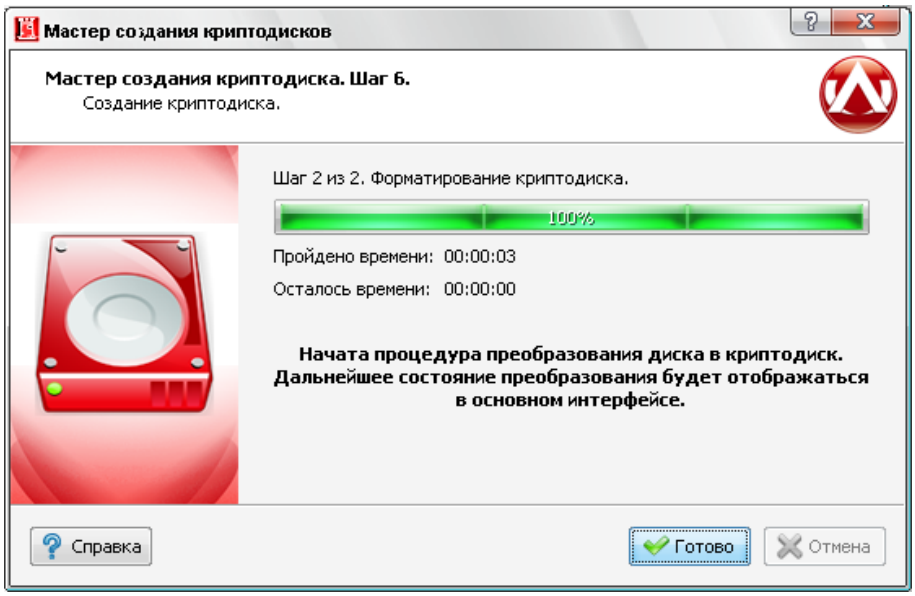

Рисунок 4.7. Мастер создания криптодисков. Прогресс создания.

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.

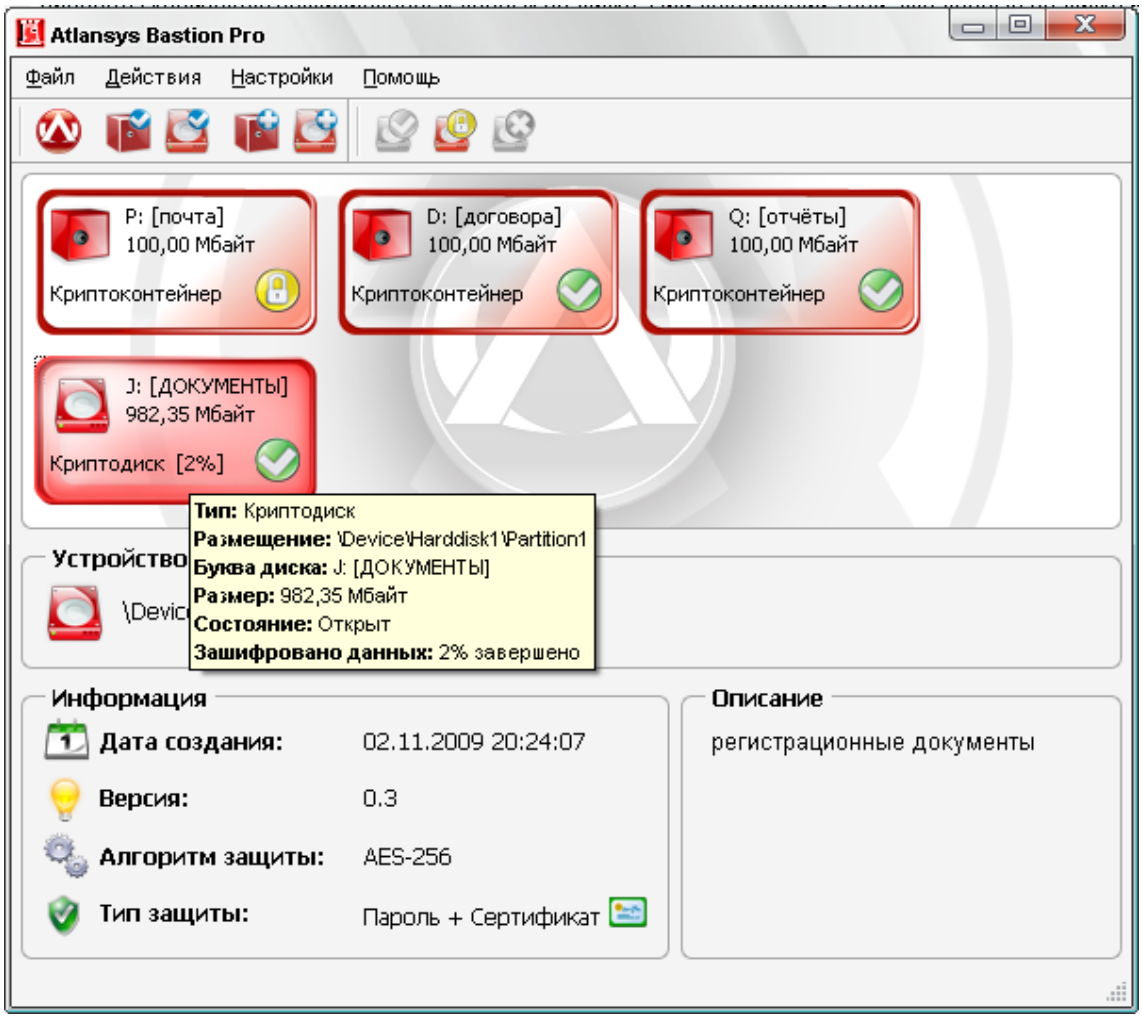

Рисунок 4.8. Процесс преобразования криптодиска.

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.

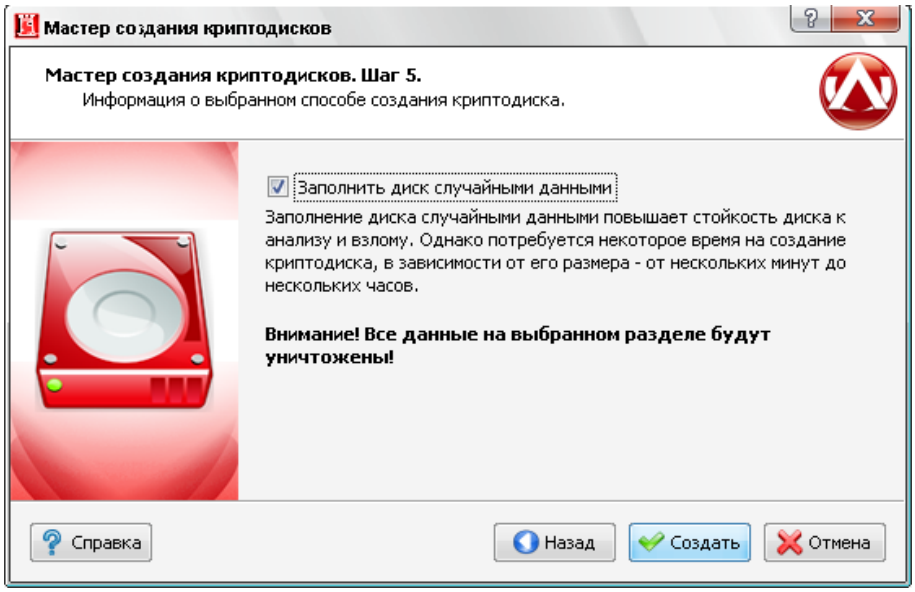

Рисунок 4.9. Мастер создания криптодисков. Заполнение случайными данными.

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...".

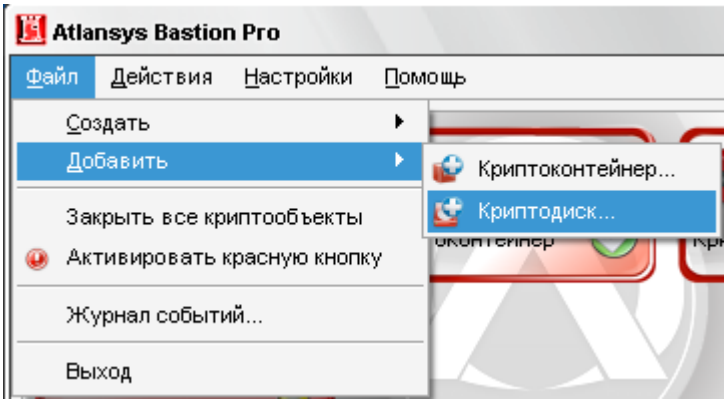

Рисунок 4.10. Меню "Файл" / "Добавить"

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.

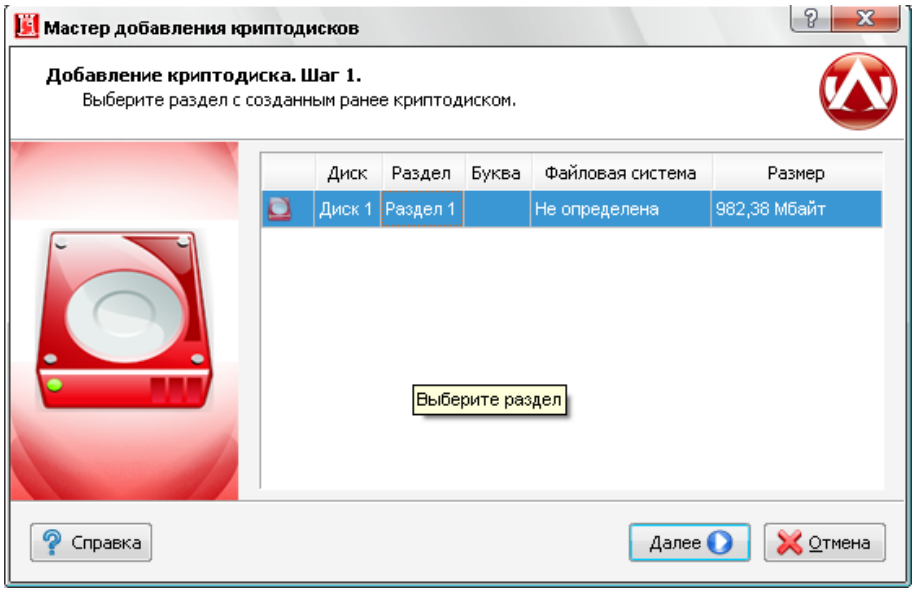

Рисунок 4.11. Мастер добавления криптокодисков. Выбор раздела.

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.

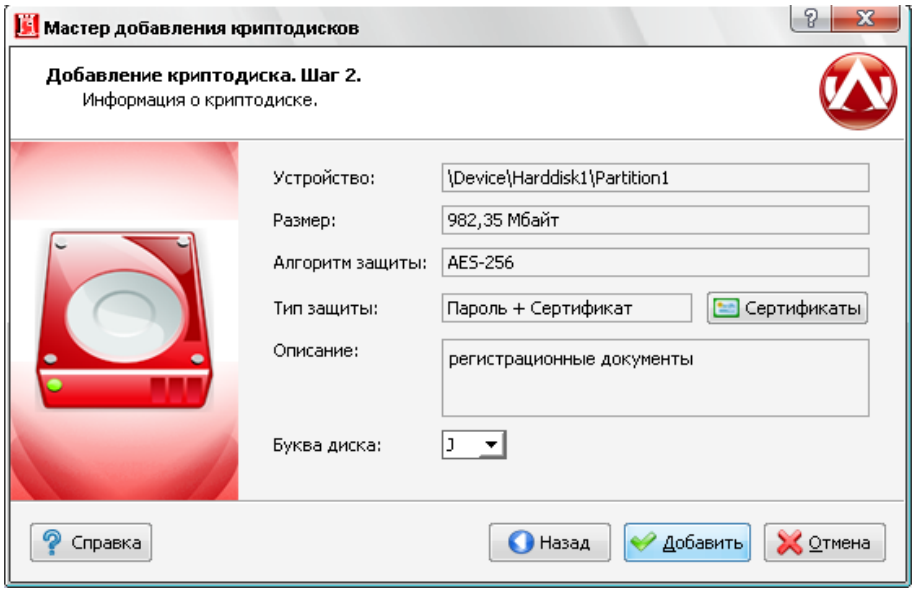

Рисунок 4.12. Мастер добавления криптокодисков. Сводная информация о криптодиске.

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.

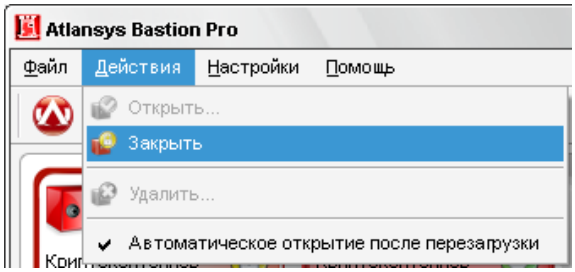

Рисунок 4.13. Меню "Действия"

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

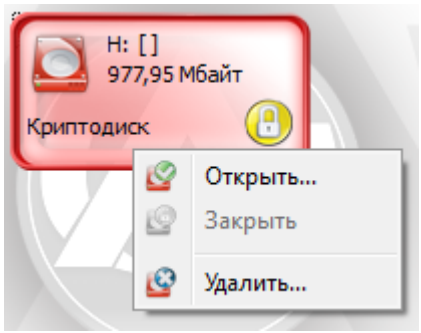

Рисунок 4.14. Контекстное меню криптодиска

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

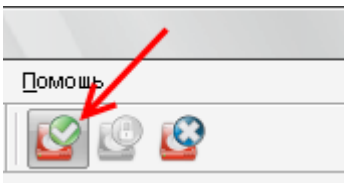

Рисунок 4.15. Панель инструментов

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

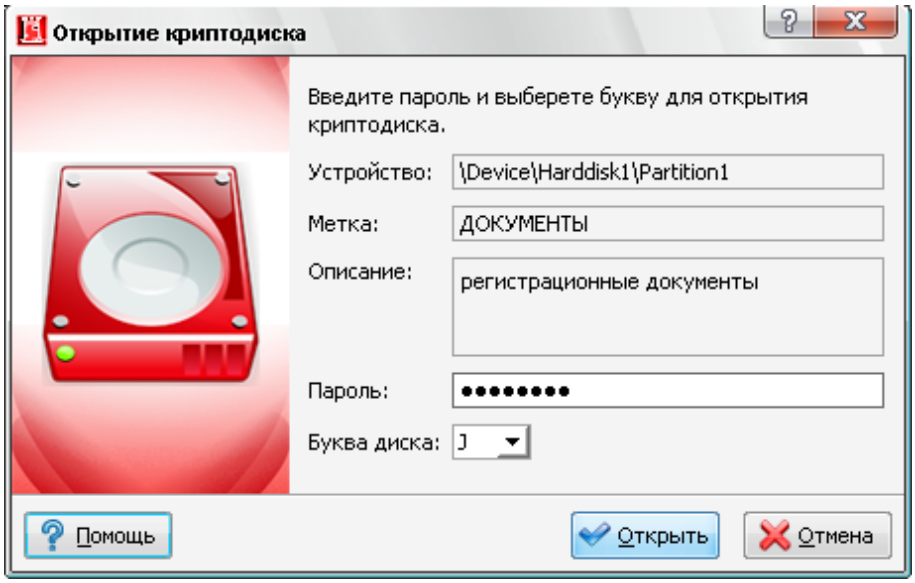

Рисунок 4.16. Диалог открытия криптодиска

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".

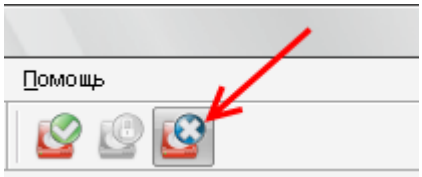

Рисунок 4.17. Панель инструментов, кнопка "Удалить"

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 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 выполняет два цикла записи псевдослучайных значений.

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

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

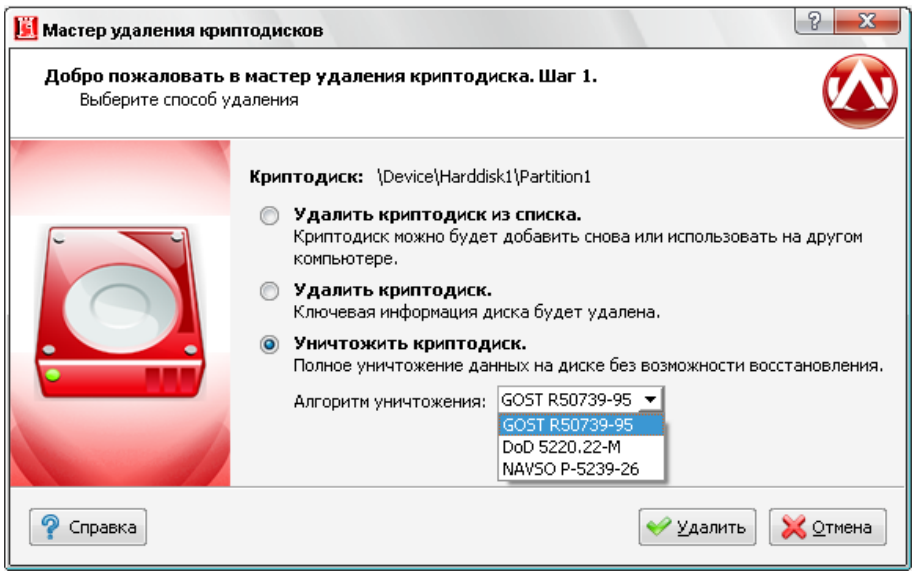

Рисунок 4.18. Мастер удаления криптокодисков

Важно

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

Глава 5. Гарантированное удаление файлов

5.1. 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 Bastion Pro / 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.

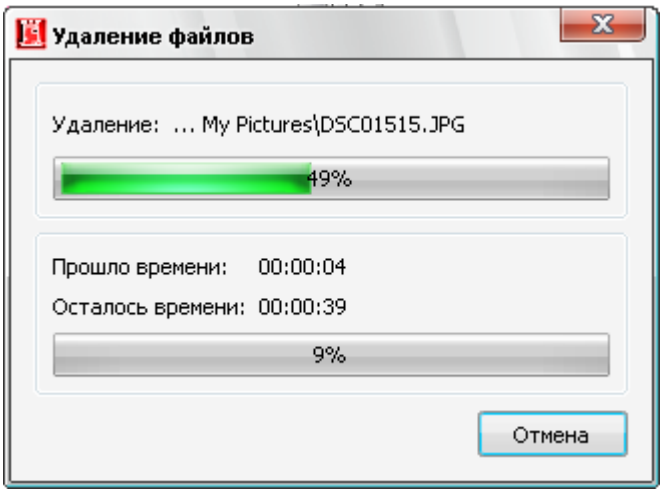

Рисунок 5.1. Диалог удаления файлов

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

Глава 6. Журнал событий

6.1. Журнал событий

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

Чтобы просмотреть журнал регистрации событий, необходимо в главном меню выбрать пункт Файл / Журнал событий...

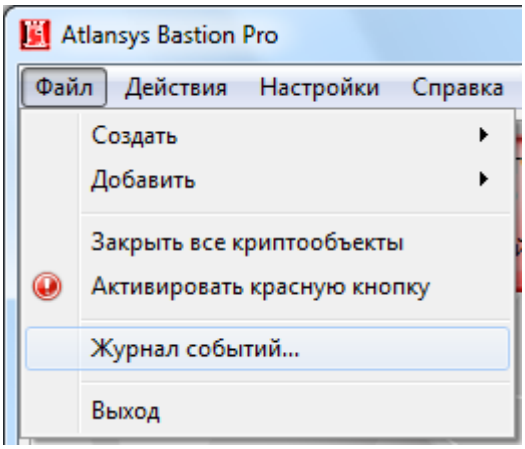

Рисунок 6.1. Запуск журнала событий

После этого отобразится окно журнала событий.

Интерфейс

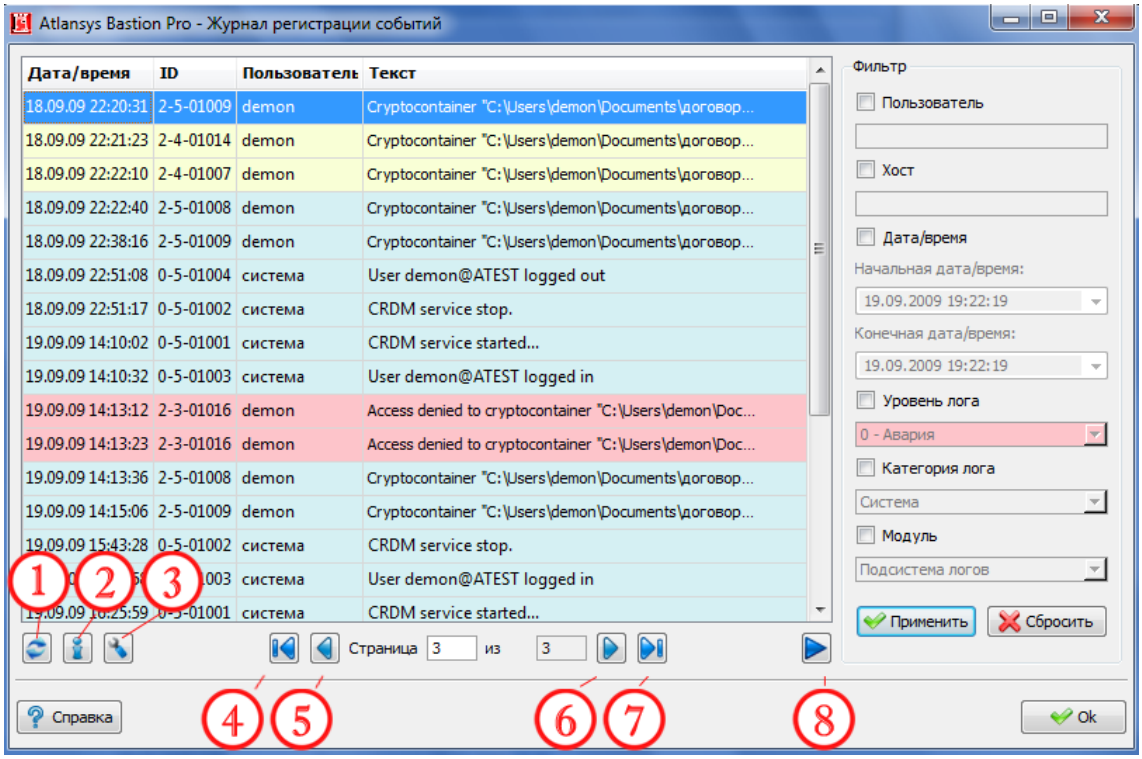

Рисунок 6.2. Окно журнала событий

1. Обновить страницу.
2. Информация по выбранному 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 сообщений.

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

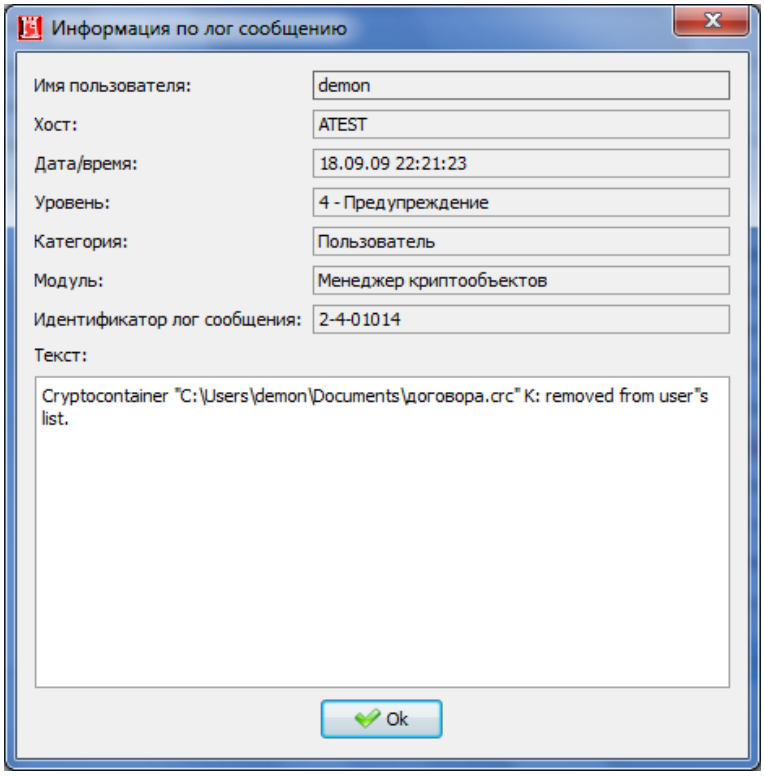

Рисунок 6.3. Информация по лог сообщению

При нажатии на кнопку настроек журнала регистрации событий, отобразится диалог настроек, в котором можно задать порядок отображения сообщений и необходимые столбцы журнала событий:

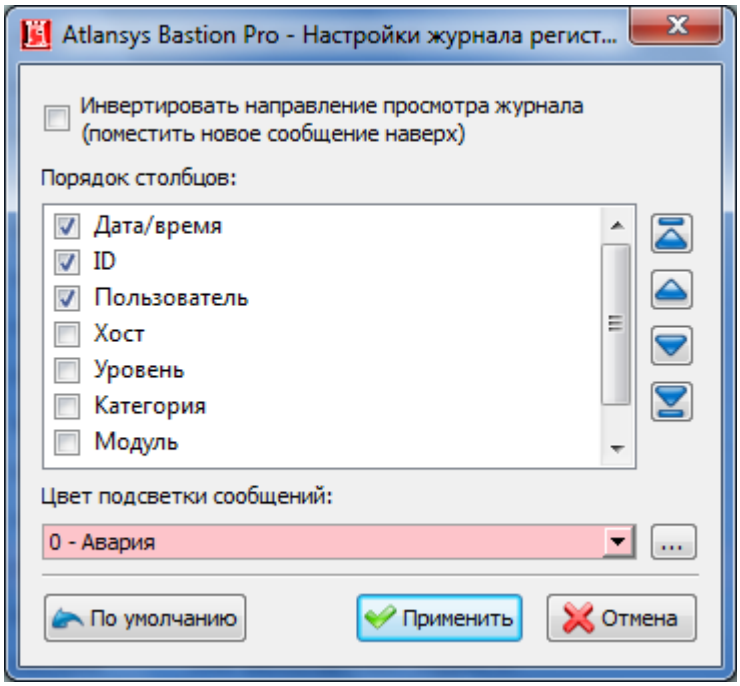

Рисунок 6.4. Настройки журнала регистрации событий

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

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

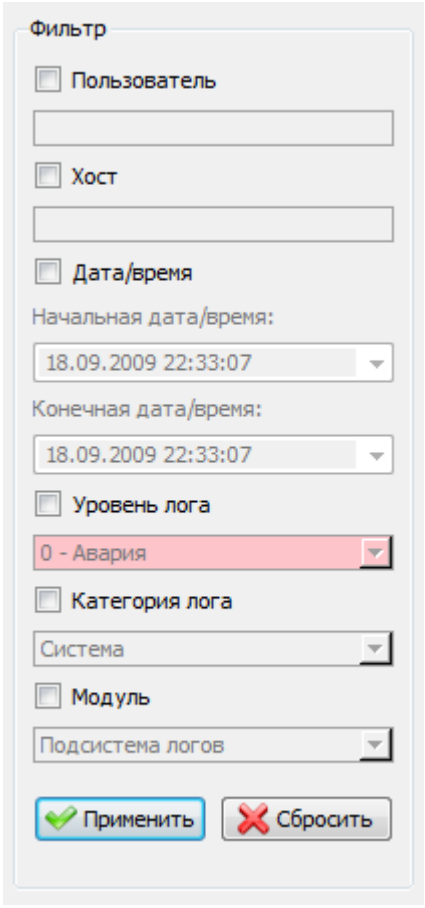

Рисунок 6.5. Фильтр журнала событий

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 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 7. 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 Atlansys Software; 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 Atlansys Software (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 Atlansys Software 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 использоваться 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 Atlansys Software).

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 Atlansys Software открытых материалах. В процессе регистрации в Atlansys Software 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 Atlansys Software.

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 Atlansys Software предоставляет вам услуги по технической поддержке ПО (далее - техническая поддержка) в соответствии с текущими правилами оказания технической поддержки Компании Atlansys Software. Правила публикуются на веб-сайте Компании Atlansys Software 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 Atlansys Software 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 Atlansys Software 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 Atlansys Software 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 Atlansys Software 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 Atlansys Software 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 Atlansys Software 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 Atlansys Software 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 Atlansys Software 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 Atlansys Software 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 Atlansys Software 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 Atlansys Software 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 Atlansys Software, 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 Atlansys Software 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 Atlansys Software не передает вам никаких печатных материалов, включая руководство пользователя.

13.2. Вознаграждением по настоящему Лицензионному договору признается стоимость ПО, установленная Компанией Atlansys Software 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 Atlansys Software гарантирует, что данные, сообщенные вами при установке и регистрации ПО, будут храниться и использоваться исключительно внутри Группы компаний Atlansys Software.

13.6. Компания Atlansys Software гарантирует, что данные, сообщенные вами при активации ПО, будут храниться и использоваться исключительно внутри Компании Atlansys Software.

13.7. Все права на наименования программных продуктов «Atlansys Enterprise Security System», «Atlansys Server», «Atlansys Bastion», «Atlansys BastionPro» принадлежат исключительно Atlansys Software.

Глоссарий

Основные термины и определения

Алгоритм криптографический	Это набор логических правил, определяющих процесс преобразования информации из открытого состояния в зашифрованное (зашифровывание) и, наоборот, из зашифрованного состояния в открытое (расшифровывание). Существует множество криптографических алгоритмов, которые различаются по степени криптостойкости (сложности дешифровывания информации без знания ключа), скорости работы, размеру ключа шифрации. Примеры криптографических алгоритмов: AES, Blowfish, DES, ГОСТ 28147-89.
Закрытие (размонтирование)	Процесс отключения криптоконтейнера или криптодиска как логического диска в операционной системе. Данные на закрытом криптообъекте полностью недоступны.
Ключ шифрования	Это случайная, псевдослучайная или специальным образом сформированная последовательность бит, являющаяся переменным параметром алгоритма шифрования. Если зашифровать одну и ту же информацию одним и тем же алгоритмом, но разными ключами, результаты получатся так же разные. Ключ шифрования имеет одну существенную характеристику - длину, которая, как правило, измеряется в битах. Для большинства алгоритмов большая длина ключа соответствует большей криптостойкости алгоритма.
Криптоархив	Это файл, содержащий полностью зашифрованный и архив сжатых файлов и каталогов. В криптоархиве зашифрована вся информация о файлах, включая их имена и структуру каталогов, что позволяет безопасно пересылать конфеденциальную информацию, если нет необходимости её изменять.
Криптоархив самораспаковывающийся	Это криптоархив, который можно распаковать без инсталляции продукта. Он содержит внутри себя модуль для расшифровывания и распаковки файлов. Может использоваться для пересылки конфиденциальной информации пользователям, не имеющим Atlansys Bastion Pro.
Криптодиск	Это целиком зашифрованный раздел диска или флэш-накопителя. Файловая система раздела зашифровывается полностью, включая служебную информацию.
Криптоконтейнер	Это файл, имеющий определенную структуру, содержащий внутри полностью зашифрованный образ файловой системы, которая может подключаться в виде дискового устройства Windows. Процесс зашифровывания и расшифровывания информации производится автоматически и полностью прозрачен для пользователя. Криптоконтейнеры позволяют безопасно обмениваться большими объемами конфиденциальной информации, которую необходимо редактировать разными пользователями.
Криптообъект	В Atlansys Bastion Pro это общее наименование криптоархивов, криптоконтейнеров или криптодисков.
Открытие (монтирование)	Процесс подключения криптоконтейнера или криптодиска как логического диска в операционной системе. Для открытия криптообъекта в зависимости от типа его защиты может использоваться пароль или сертификат.
Шифрование	Это способ кодирования информации по специальному математическому алгоритму с использованием ключей шифрования для сохранения её конфиденциальности и защиты от несанкционированного просмотра.