Общество с ограниченной ответственностью
«ГАЗИНФОРМСЕРВИС»

Программно-аппаратный комплекс доверенной загрузки «Блокхост-МДЗ»

Описание применения

Аннотация

Настоящий документ содержит описание применения программно-аппаратного комплекса доверенной загрузки «Блокхост-МДЗ» (далее по тексту – ПАК «Блокхост-МДЗ»).

В разделе «Назначение ПАК «Блокхост-МДЗ» указаны назначение комплекса, его состав и выполняемые им функции.

В разделе «Условия применения» приводится перечень программных и аппаратных компонент, необходимых для функционирования комплекса, а также функциональные ограничения на его применение.

В разделе «Входные и выходные данные» указаны входных и выходных данных для каждой из подсистем комплекса.

В разделе «Подсистема шифрования» описана консоль управления подсистемы, указаны основные настройки и функции подсистемы, операции выполнения функций по шагам и режимы работы подсистемы.

В разделе «Подсистема очистки памяти» описана консоль управления подсистемы, указаны настройки подсистемы, основные функции работы со списком контролируемых процессов, их выполнение по шагам.

В разделе «Подсистема контроля целостности» описана консоль управления подсистемы, указаны настройки подсистемы, основные функции работы со списком контролируемых объектов, их выполнение по шагам, и возможности просмотра событий.

В разделе «Подсистема гарантированного удаления» описан механизм гарантированного удаления.

Список сокращений

БСВВ – базовая система ввода-вывода
ЖМД – жесткий магнитный диск
МДЗ – модуль доверенной загрузки
НСД – несанкционированный доступ
ОС – операционная система
ПАК – программно-аппаратный комплекс
ПК – персональный компьютер
ПЭВМ – персональная электронная вычислительная машина

Содержание

1 Назначение ПАК «Блокхост-МДЗ»

Программно-аппаратный комплекс доверенной загрузки «Блокхост-МДЗ» предназначен для решения следующих задач:

- усиления защиты входа на персональный компьютер, используя процедуру дополнительной аутентификации пользователей до загрузки операционной системы;
- обеспечения конфиденциальности данных, хранимых на электронных носителях, путем шифрования их содержимого;
- контроля целостности контролируемых объектов с заданной периодичностью;
- выполнения гарантированного удаления файлов без возможности их восстановления;
- очистки оперативной памяти, ранее использованную для хранения защищаемых данных.

ПАК «Блокхост-МДЗ» состоит из 4 компонент:

- подсистема шифрования;
- подсистема очистки памяти;
- подсистема контроля целостности;
- подсистема гарантированного удаления.

Подсистема шифрования выполняет следующие функции:

- выполнение “прозрачного” зашифрования и расшифрования дисков и USB носителей по алгоритмам AES-256 LRW и ГОСТ 28147-89, где в качестве носителей для хранения ключевой информации могут использоваться электронные идентификаторы eToken Pro, eToken Pro (Java), eToken NG-FLASH, eToken NG-OTP, eToken SC, ruToken, USB-накопители или дискеты;
- поддержка двух типов усиленной аутентификации до загрузки операционной системы: с использованием электронного идентификатора eToken Pro\NG-FLASH\ NG-OTP или по паролю, вводимого пользователем;
- отключение и подключение пользовательских дисков;
- перезагрузка ПЭВМ после трех неудачных попыток аутентификации.

Подсистема контроля целостности осуществляет периодический контроль целостности файлов и содержимого каталогов на ПЭВМ. Подсистема состоит из двух отдельных модулей – под управлением ОС Windows и Linux, соответственно.

Подсистема очистки памяти выполняет очистку областей оперативной памяти после завершения контролируемых процессов, что предотвращает считывание информации ограниченного доступа.

Подсистема гарантированного удаления исключает считывание остаточной информации на диске после удаления файлов. Удаление файлов происходит трехкратным затиранием содержимого по алгоритму в соответствии с ГОСТ Р50739-95. Подсистема состоит из двух отдельных модулей, устанавливаемых по выбору пользователя:

- модуль гарантированного удаления всех объектов файловой системы на ПЭВМ, удаляемых стандартным способом (функционирует на 32-bit ОС);
- модуль гарантированного удаления выбранных объектов файловой системы по требованию пользователя (функционирует на 32/64-bit ОС).

Состояние подсистем шифрования, контроля целостности, очистки памяти, гарантированного удаления ПАК «Блокхост-МДЗ» отражается пиктограммой. Если подсистемы

работают в штатном режиме, в области уведомлений будет отображаться пиктограмма  . Если кликнуть по пиктограмме правой кнопкой мыши, отобразится текущее состояние подсистем (Рисунок 1.1).

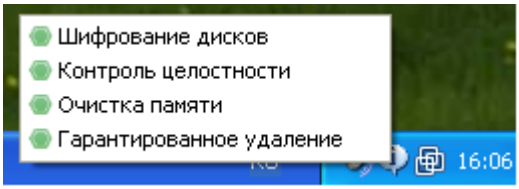

Рисунок 1.1 – Состояние подсистем

Все события подсистем шифрования, контроля целостности, очистки памяти, гарантированного удаления записываются в специальный журнал **«Блокхост-МДЗ»**, который можно открыть через консоль «Управление компьютером» → «Просмотр событий» (Рисунок 1.2).

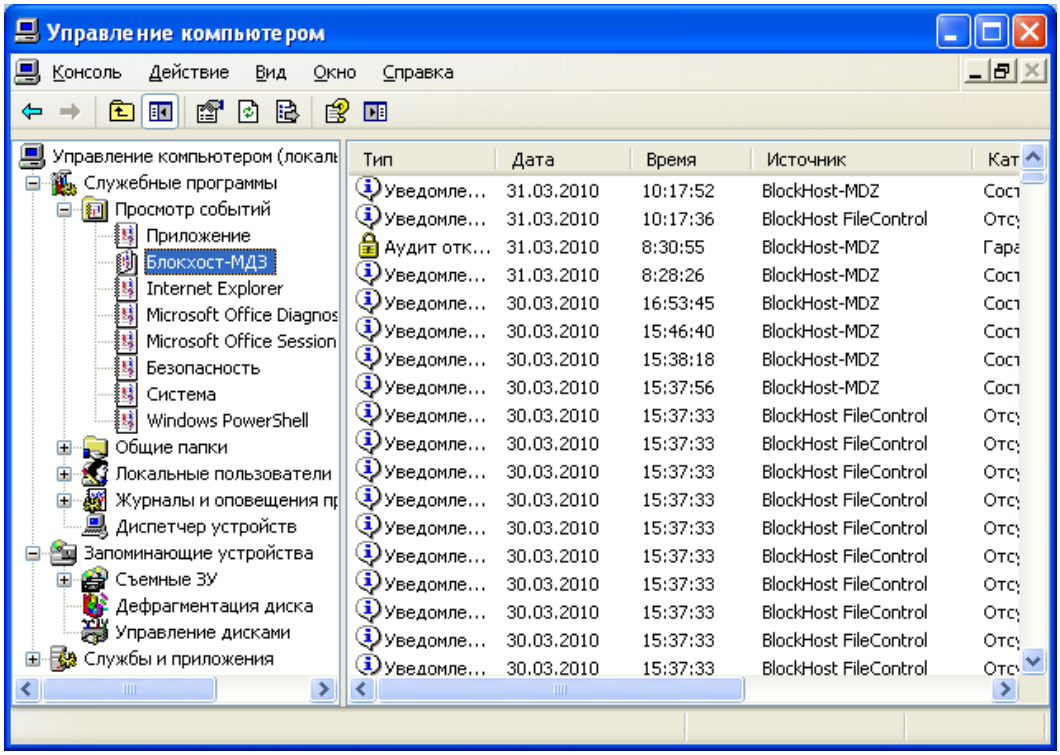

Рисунок 1.2 – Журнал событий Блокхост-МДЗ

Для того чтобы просмотреть информацию о событии, необходимо дважды щелкнуть на интересующее событие в журнале **«Блокхост-МДЗ»**. Информация о событии откроется в новом окне (Рисунок 1.3).

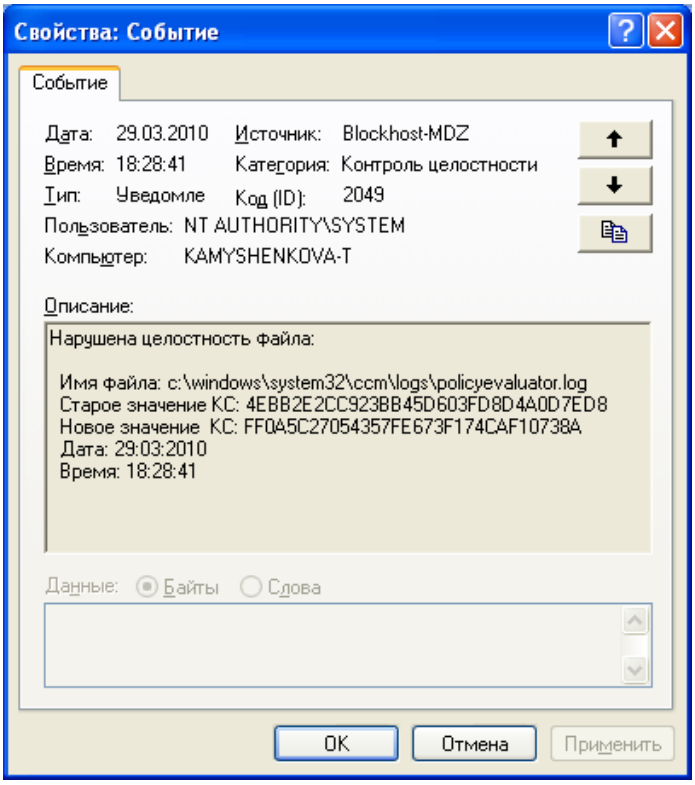

Рисунок 1.3 – Информация о событии

2 Условия применения

Для установки ПАК «Блокхост-МДЗ» ПЭВМ должен иметь следующий минимальный состав технических и программных средств:

- контроллером жестких дисков IDE или SATA;
- ЖМД объемом не менее 4Гб;
- дисплей SVGA;
- клавиатура AT или PS/2;
- контроллер USB 2.0 и выше;
- BIOS (БСВВ) системной платы должен поддерживать прерывание дискового сервиса INT 13h;
- ключевой носитель информации выбранного типа: eToken Pro, eToken Pro (Java), eToken NG-FLASH, eToken NG-OTP, eToken SC, ruToken, USB-накопитель, дискета.

ПАК «Блокхост-МДЗ» функционирует под управлением ОС MS Windows XP/2003/2008/Vista/7 и Linux. Для ОС MS Windows дополнительно должно быть установлено следующее программное обеспечение:

- набор драйверов eToken RTE 3.6x/PKI Client 5.1 (при использовании электронных идентификаторов eToken);
- набор драйверов ruToken (при использовании электронных использовании идентификаторов ruToken);
- СКЗИ «КриптоПро CSP» версии 3.6.1 (при шифровании носителей по алгоритму ГОСТ 28147-89);
- Microsoft .Net Framework 2.0 или выше (при использовании подсистемы контроля целостности и/или подсистемы очистки памяти).

Для ОС Linux при вычислении хеш-сумм файловых объектов по алгоритму ГОСТ Р 34.11-94 должна быть установлена СКЗИ «КриптоПро CSP» (версия 3.6)

Минимальные требования к производительности ПК обусловлены требованиями используемых ОС.

ПАК «Блокхост-МДЗ» имеет следующие ограничения:

- для зашифровывания системного раздела (раздел, на котором установлена ОС MS Windows), данный раздел должен быть загрузочным (содержать файлы NTLDR, Boot.ini и др.);
- не поддерживает шифрование динамических разделов.

3 Входные и выходные данные

3.1 Входные данные

Входными данными для комплекса является информация на жестких дисках, подлежащая защите от несанкционированного доступа.

3.2 Выходные данные

3.2.1 Подсистема шифрования

Выходными данными подсистемы шифрования являются посекторно зашифрованные разделы жесткого диска.

Системный зашифрованный раздел имеет структуру, отображенную на рисунке 3.2.1.1. Пользовательский раздел имеет аналогичную структуру за тем исключением, что ключ шифрования раздела хранится в ключевом контейнере криптопровайдера, а заголовок раздела содержит дополнительные поля для работы с криптопровайдером.

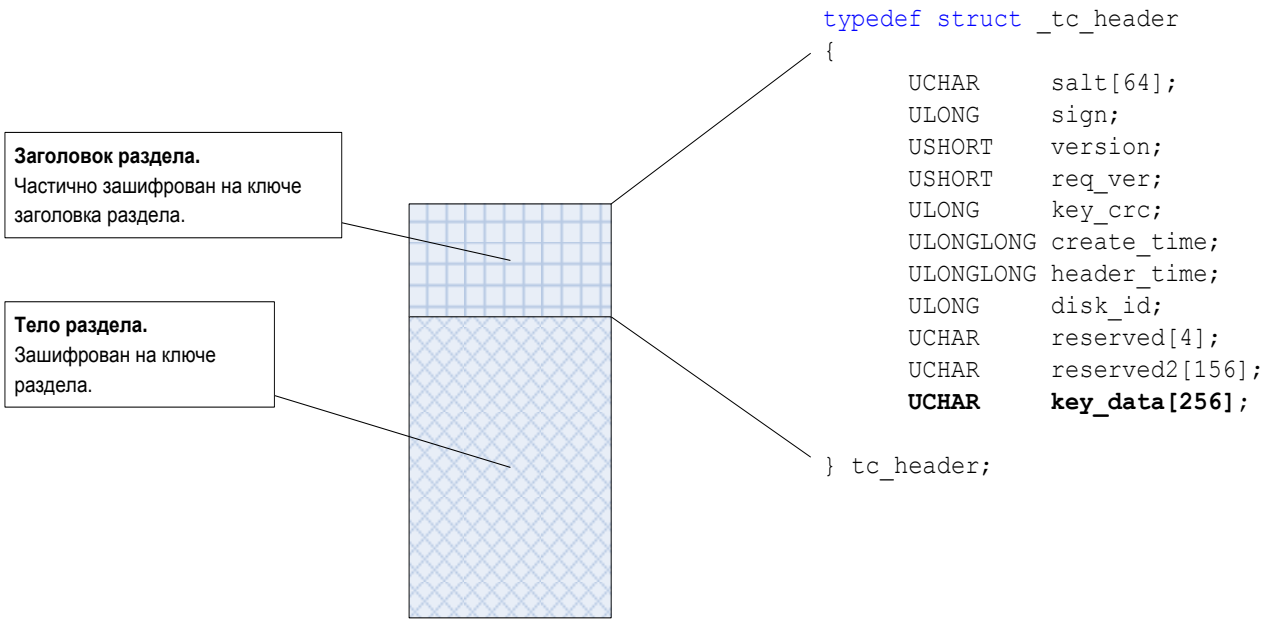

Рисунок 3.2.1.1 – Структура зашифрованного раздела

В процессе шифрования каждый сектор зашифровывается и сдвигается на одну позицию (в сторону увеличения номеров секторов), в первый сектор записывается специальная структура – «Заголовок раздела», который содержит служебную информацию, в том числе зашифрованный ключ шифрования раздела. Если зашифровыванию подвергается системный раздел, то в нулевую дорожку HDD записывается сжатый образ модуля управления доступом.

3.2.2 Подсистема контроля целостности

Выходными данными подсистемы контроля целостности является информация о состоянии файлов и каталогов, поставленных на контроль.

3.2.3 Подсистема очистки памяти

Выходными данными подсистемы очистки памяти является информация о состоянии контролируемых процессов.

3.2.4 Подсистема гарантированного удаления

Выходными данными подсистемы гарантированного удаления является информация об удаленных пользователем файлах.

4 Подсистема шифрования

4.1 Настройка подсистемы шифрования

Управление подсистемой шифрования осуществляется через консоль управления, представленной на рисунке 4.1.1.

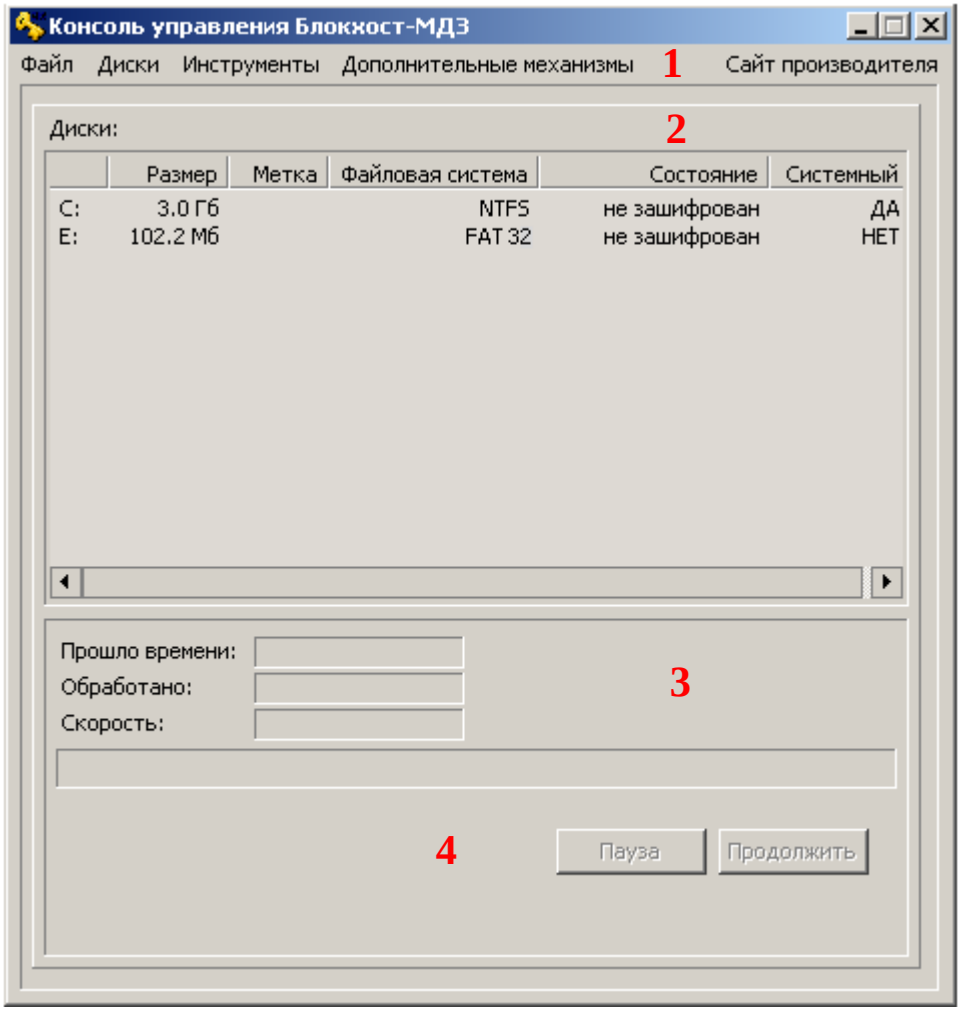

Рисунок 4.1.1 – Окно консоли управления

Окно консоли управления подсистемы шифрования ПАК «Блокхост-МДЗ» состоит из 4-х основных частей:

1. Главная панель. Предоставляет доступ ко всем функциям подсистемы.
2. Список дисков. Отображает информацию о состоянии дисков имеющихся в системе. Данный список обладает контекстным меню, для более быстрого доступа к функциям подсистемы.
3. Часть окна, в которой отображается процесс зашифровывания/расшифровывания дисков.
4. Кнопки «Пауза» и «Продолжить» применяются для приостановки и продолжения операции шифрования разделов.

Доступ к настройкам подсистемы шифрования осуществляется через главное меню «Инструменты» → «Настройки». Окно настроек представлено на рисунке 4.1.2.

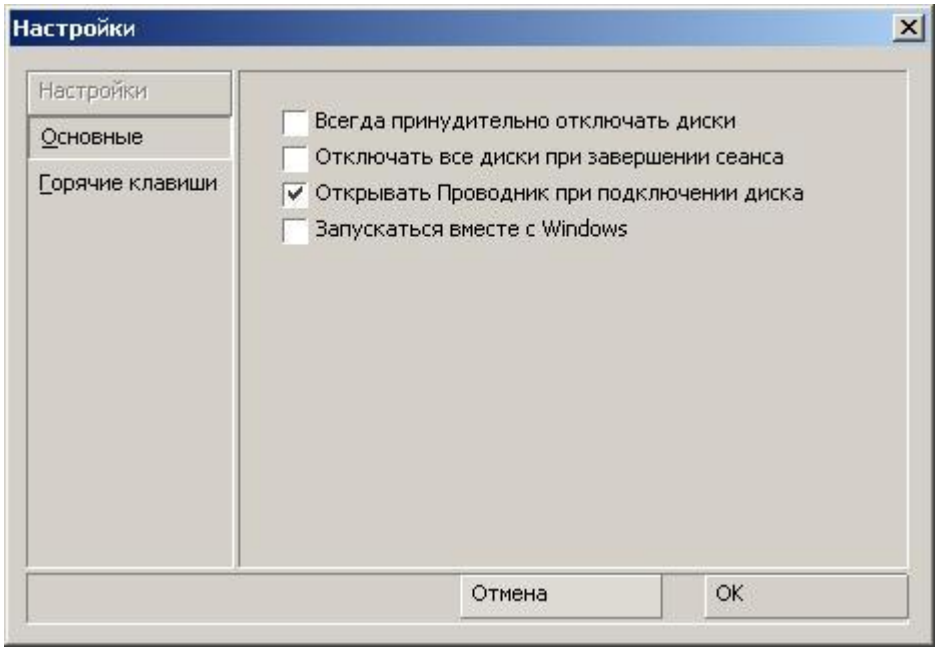

Рисунок 4.1.2 – Окно настроек подсистемы шифрования

Во вкладке «Основные» доступны следующие настройки:

- *Всегда принудительно отключать диски* – Проводить принудительное отключение в случае если файлы на зашифрованном диске заняты, не выдавая окна запроса;
- *Отключать все диски при завершении сеанса* - Отключать все диски при завершении сеанса работы с ОС;
- *Открывать Проводник при подключении диска* – Открывать окно Проводника при подключении зашифрованного диска;
- *Запускаться вместе с Windows* – Запуск консоли управления ПАК «Блокхост-МДЗ» производится вместе с ОС Windows.

На вкладке «Горячие клавиши» имеется возможность определить сочетание клавиш на клавиатуре для быстрого доступа к наиболее используемым операциям подсистемы шифрования ПАК «Блокхост-МДЗ».

4.2 Основные функции подсистемы шифрования

Подсистема шифрования выполняет следующие функции:

- зашифровывание системного раздела;
- расшифровывание системного раздела;
- зашифровывание пользовательского раздела;
- расшифровывание пользовательского раздела;
- отключение пользовательского раздела;
- подключение пользовательского раздела;
- смена носителя ключевой информации к зашифрованным дискам;
- резервирование ключевого носителя;
- активация режима «Замок»;
- отключение режима «Замок».

Функции зашифровывания и расшифровывания дисков, активизации и отключения режима «Замок», смены носителей к системному диску могут выполняться только пользователем, включенным в группу локальных администраторов.

Для сохранности конфиденциальных данных с помощью подсистемы шифрования ПАК «Блокхост-МДЗ» необходимо, чтобы был создан и подключен хотя бы один зашифрованный диск.

С подключенным зашифрованным диском можно обращаться так же, как и с обычным диском: форматировать, создавать на нём файлы и папки, редактировать их, распоряжаться доступом к ним, проверять диск на наличие ошибок. Все данные на таком диске будут шифроваться в фоновом режиме.

Примечание

Для того чтобы предотвратить несанкционированный доступ к данным на зашифрованном диске, необходимо отключать его всякий раз, когда на нем не производится операций с файлами и папками. Отключить системный (загрузочный) диск нельзя.

4.2.1 Создание зашифрованного системного (загрузочного) диска

Для того чтобы зашифровать диск, необходимо выполнить следующие операции:

1. Запустить консоль управления подсистемой шифрования ПАК «Блокхост-МДЗ».
2. Вставить в свободный usb-порт электронный идентификатор eToken Pro, eToken NG-FLASH.
3. Выделить в списке дисков загрузочный диск (для такого диска в поле «Системный» будет стоять значение «ДА» см. рисунок 4.2.1.1).

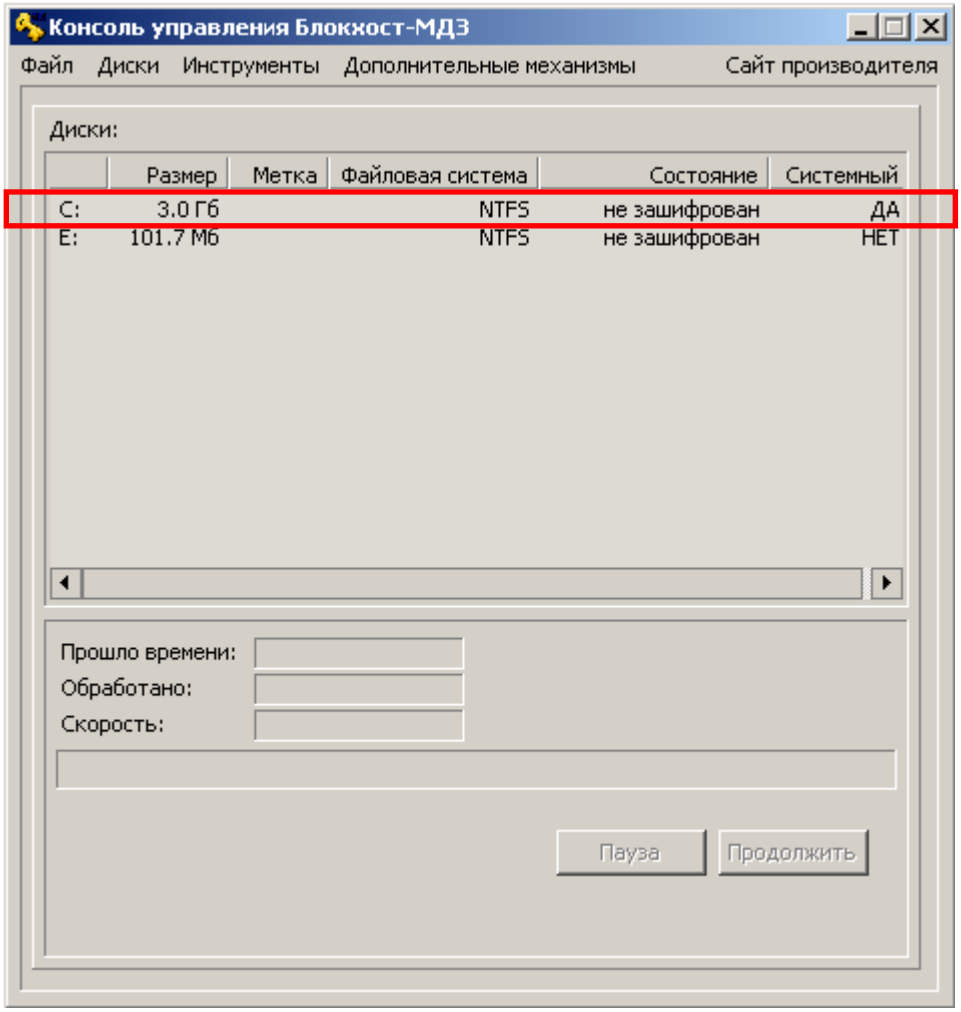

Рисунок 4.2.1.1 – Выбор загрузочного диска

4. Щелкнуть правой кнопкой мыши на выделенной строке и в контекстном меню выбрать пункт «Зашифровать» (Рисунок 4.2.1.2).

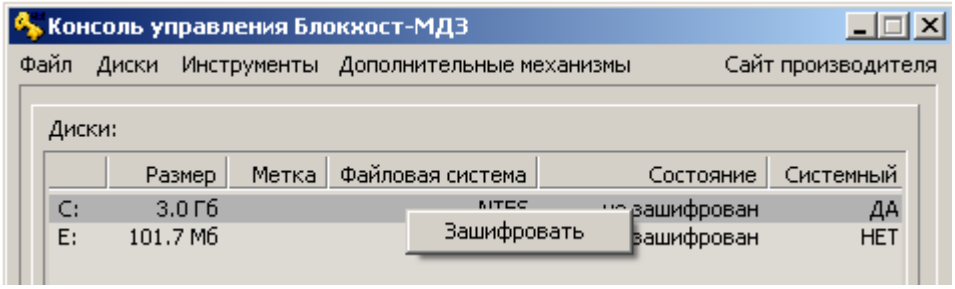

Рисунок 4.2.1.2 – Выбор пункта «Зашифровать» в контекстном меню

5. В открывшемся диалоговом окне (Рисунок 4.2.1.3) необходимо:

- в поле «Криптопровайдер» выбрать криптопровайдера или оставить тот криптопровайдер, который установлен по умолчанию;
- в поле «Алгоритм шифрования» указать необходимый алгоритм шифрования;
- в поле «Режим шифрования» выбрать или оставить установленный по умолчанию режим шифрования.

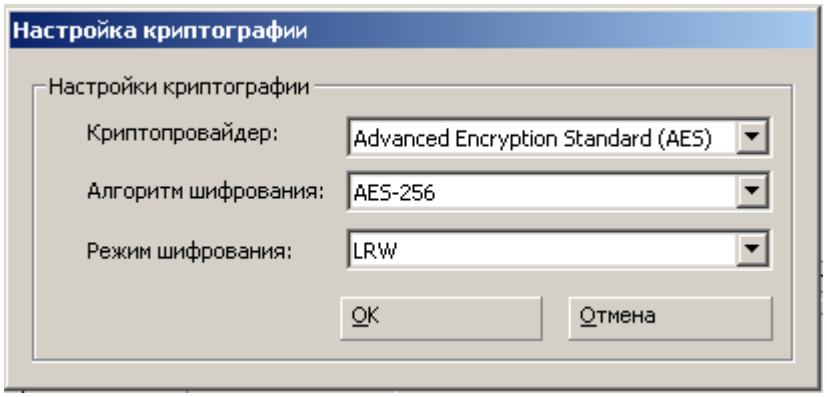

Рисунок 4.2.1.3 – Настройки криптографии.

6. В открывшемся диалоговом окне (Рисунок 4.2.1.4) необходимо:
- выбрать из выпадающего списка «Ключевой носитель» имя виртуального карт-ридера, к которому подключен электронный идентификатор eToken Pro, eToken NG-FLASH;
- в поле «PIN-код» ввести PIN-код электронного идентификатора;
- в поле «Повтор» осуществить повторный ввод PIN-кода.

В диалоговом окне (Рисунок 4.2.1.4) указывается ключевой носитель, на который будет записан ключ шифрования. Также имеется возможность шифрования системных дисков по паролю, без использования ключевого носителя. Для этого необходимо активировать поле «Использовать пароль» и ввести пароль в соответствующие поля. В этом же окне существует возможность просмотра пароля и резервирования ключевой информации на другой носитель при установленных галочках на соответствующих пунктах: «Показать» и «Резервировать».

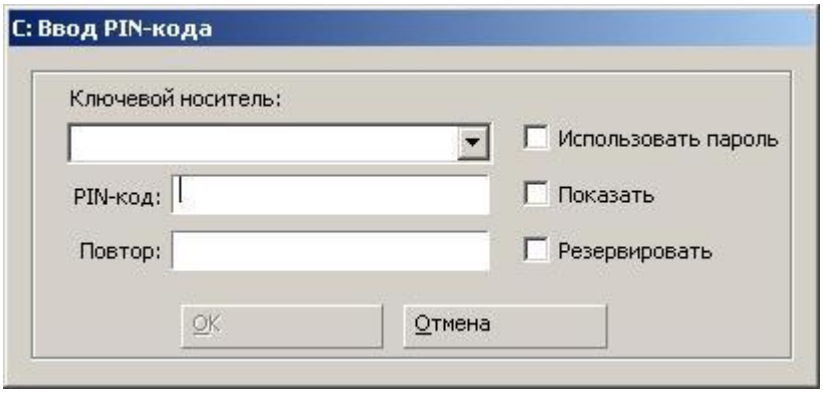

Рисунок 4.2.1.4 – Ввод PIN-кода eToken Pro

7. Если значения, введенные в поля «PIN-код» и «Повтор», совпадают, тогда становится возможным нажатие на кнопку «ОК».

8. Если была установлена галочка напротив пункта «Резервировать» в окне ввода PIN-кода (Рисунок 4.2.1.4), то после нажатия кнопки «ОК» в окне ввода PIN-кода появится диалоговое окно резервирования ключевой информации (Рисунок 4.2.1.5), в котором необходимо:
- в поле резервный носитель выбрать имя виртуального карт-ридера, к которому подключен резервный электронный идентификатор eToken Pro, eToken NG-FLASH.
- в поле PIN-код ввести PIN-код резервного электронного идентификатора.

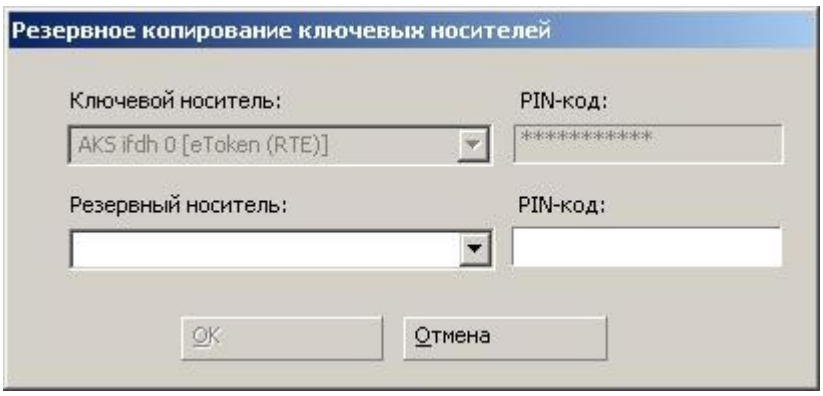

Рисунок 4.2.1.5 – Резервное копирование ключевых носителей

9. Если же резервирование ключевых носителей не было включено и PIN-код был введен верно (Рисунок 4.2.1.4), то после нажатия кнопки «ОК» в окне ввода PIN-кода запустится процесс фонового шифрования загрузочного диска (Рисунок 4.2.1.6). В случае неверного ввода PIN-кода консоль управления выведет сообщение об ошибке.

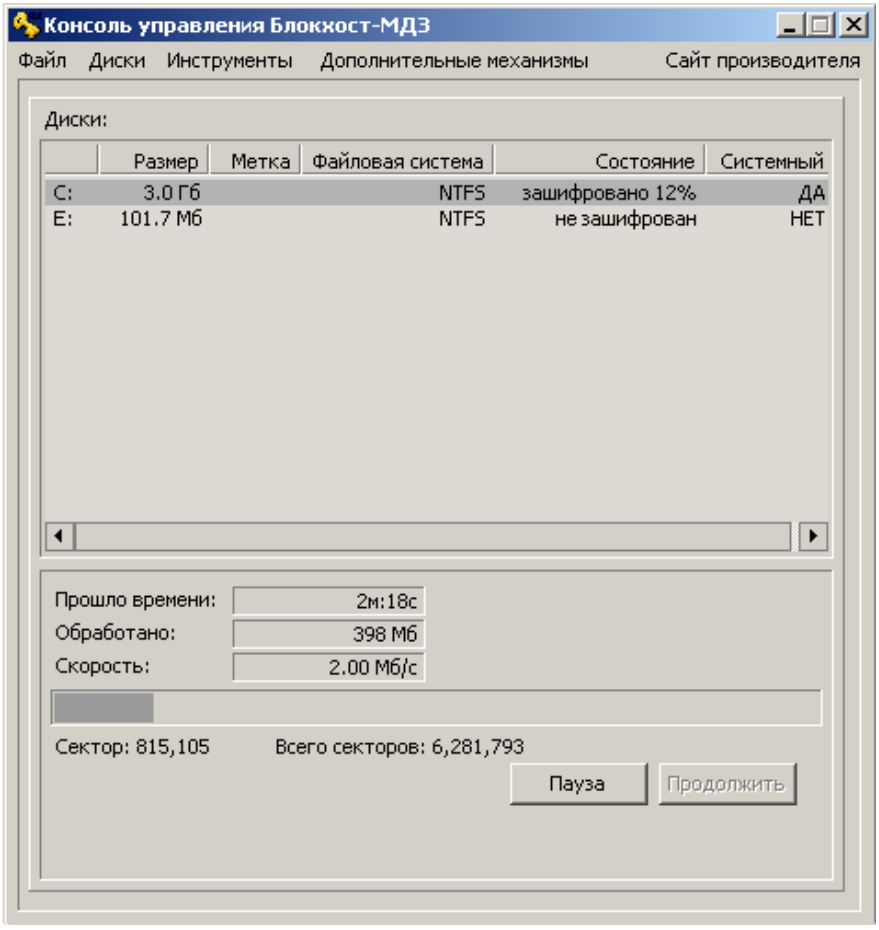

Рисунок 4.2.1.6 – Отображение процесса зашифровывания диска

О том, что процесс зашифровывания активен, свидетельствует строка «зашифровано» с указанием количества процентов готовности в поле «Состояние».

Примечание

Во время зашифровывания системный диск полностью готов к работе — на нем можно создавать и удалять файлы, выполнять проверку, определять права доступа. Отключать системный диск нельзя.

Когда диск полностью зашифрован и готов к работе поле «Состояние» принимает значение «Зашифрован».

После зашифровывания системного диска меняется режим загрузки операционной системы. При включении компьютера, его перезагрузке или выходе из «спящего» режима выдается запрос аутентификации. В этом окне требуется подключить eToken, который использовался для зашифровывания системного диска (Рисунок 4.2.1.7). В случае шифрования системного диска по паролю, появится окно, показанное на рис. 4.2.1.8.

Рисунок 4.2.1.7 – Начальное окно аутентификации при загрузке системы

10. Для загрузки операционной системы необходимо подключить eToken к компьютеру и ввести PIN-код (Рисунок 4.2.1.8).

Рисунок 4.2.1.8 – Ввод PIN-кода eToken

Примечание

Перед зашифровыванием загрузочного диска, убедитесь, что данный раздел является также и системным (см. Условия применения).

Процесс зашифровывания работает в фоновом режиме и не препятствует нормальной работе пользователя.

Программно-аппаратный комплекс поддерживает одновременное зашифровывание нескольких дисков, каждый диск шифруется в собственном системном потоке.

4.2.1.1 Дозашифровывание системного (загрузочного) диска

В подсистеме шифрования ПАК «Блокхост-МДЗ» реализована операция дозашифровывания системного (загрузочного) диска, на случай если во время выполнения операции шифрования системного диска по некоторым причинам произошло прерывание работы ОС (выключение питания компьютера). После произошедшего прерывания необходимо включить компьютер и загрузить ОС. Во время загрузки ОС выдается запрос аутентификации (Рисунок 4.2.1.1.1). Для загрузки ОС необходимо подключить eToken (если он использовался при шифровании системного диска) к компьютеру и ввести PIN-код (Рисунок 4.2.1.1.2).

Рисунок 4.2.1.1.1 – Запрос аутентификации

Рисунок 4.2.1.1.2 – Ввод PIN-кода (eToken-а или пароль, на котором происходило шифрование)

Примечание

После аварийной перезагрузки ПК в момент зашифрования/расшифрования диска до

начала загрузки ОС необходимо дождаться завершения работы программы проверки диска CHKDSK.

После загрузки ОС необходимо выполнить следующие операции:

1. Запустить консоль управления подсистемой шифрования ПАК «Блокхост-МДЗ».

2. Выделить в списке разделов (дисков) недозашифрованный системный раздел (диск). Для такого раздела (диска) в поле «Системный» будет стоять значение «ДА», в поле «Состояние» значение «Зашифровано» с указанием количества процентов готовности, а в поле «Файловая система» будет отсутствовать значение (Рисунок 4.2.1.1.3).

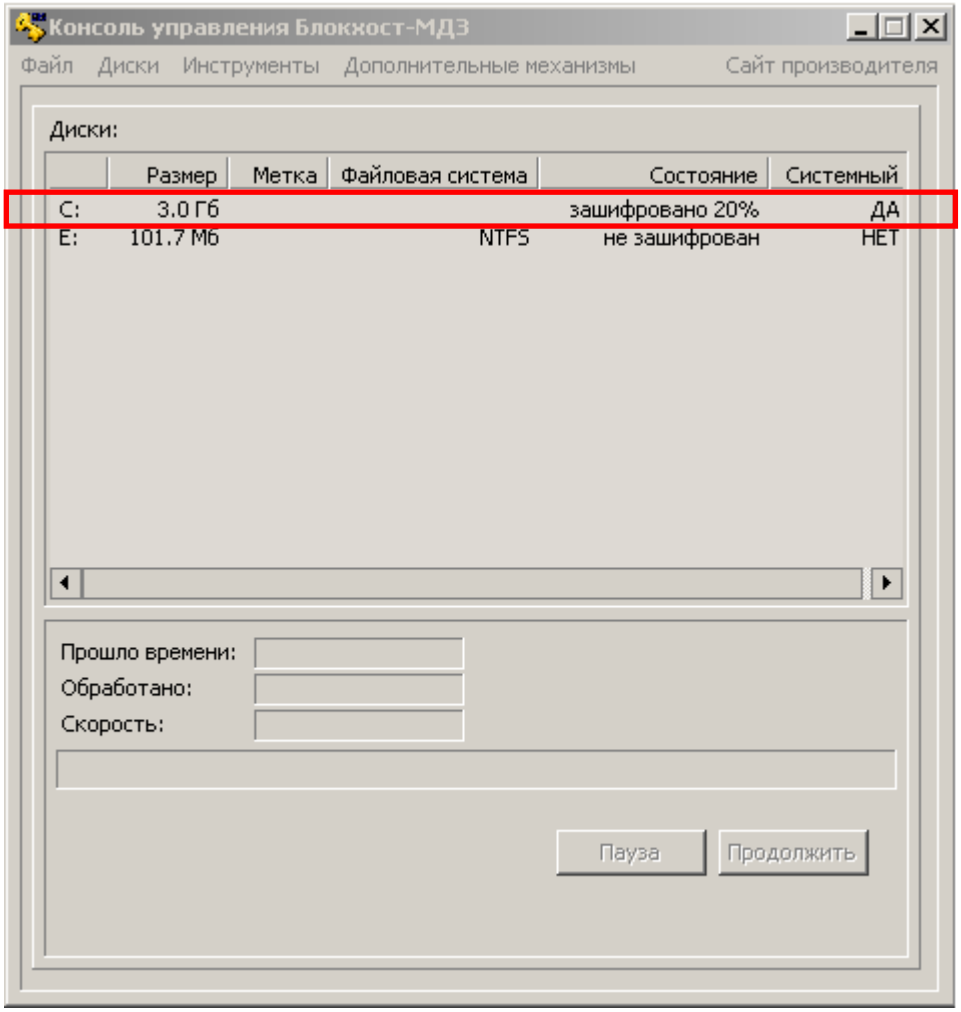

Рисунок 4.2.1.1.3 – Выбор недозашифрованного системного диска

3. Щелкнуть правой кнопкой мыши на выбранной строке, и в открывшемся контекстном меню (Рисунок 4.2.1.1.4) выбрать пункт «Закончить зашифрование», после чего запустится процесс шифрования загрузочного диска (Рисунок 4.2.1.1.5).

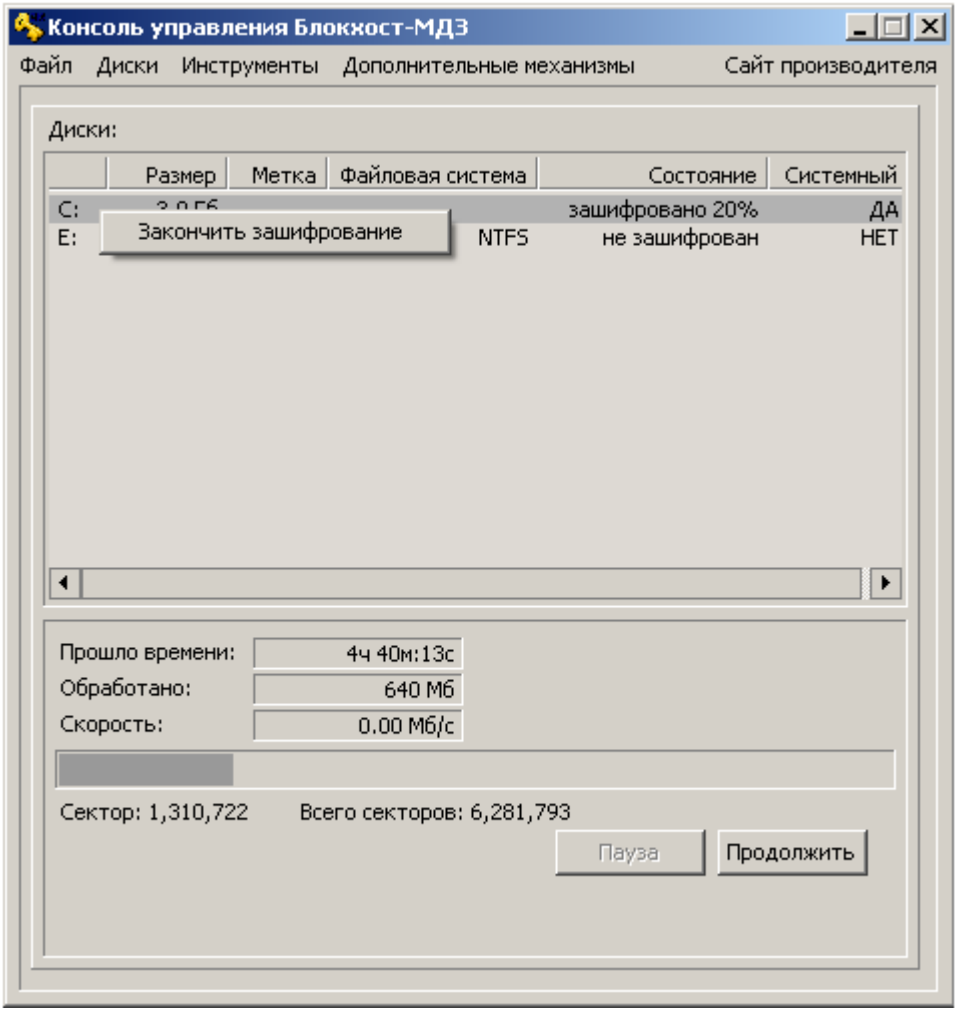

Рисунок 4.2.1.1.4 – Выбор пункта «Закончить зашифрование» в контекстном меню

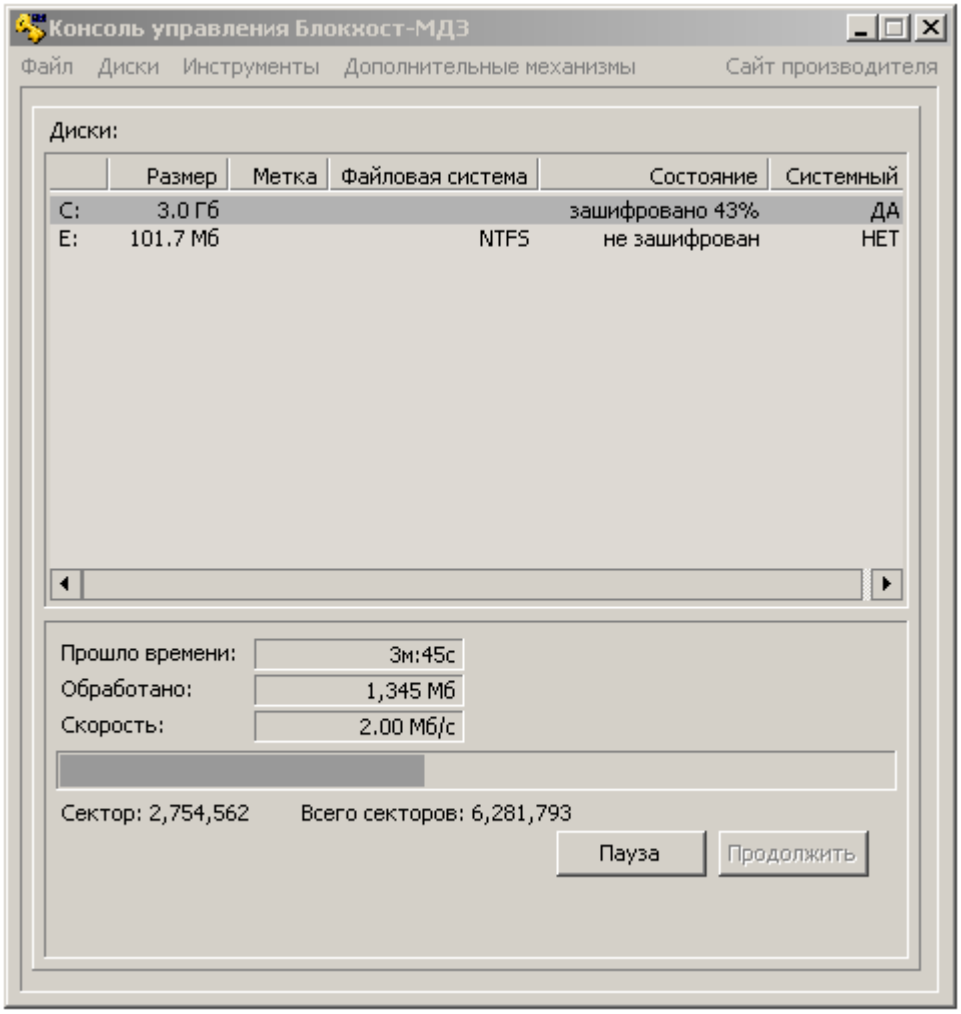

Рисунок 4.2.1.1.5 – Отображение процесса зашифрования системного диска

О том, что процесс шифрования активен, свидетельствует строка «зашифровано» с указанием количества процентов готовности в поле «Состояние».

Когда диск полностью зашифрован и готов к работе поле «Состояние» принимает значение «Зашифрован».

4.2.2 Расшифровывание системного диска

Для того чтобы расшифровать системный диск, необходимо выполнить следующие операции:

1. Запустить консоль управления ПАК «Блокхост-МДЗ».
2. Выделить в списке разделов (дисков) зашифрованный системный раздел (диск). Для такого раздела (диска) в поле «Системный» будет стоять значение «ДА» (Рисунок 4.2.2.1), а в поле «Состояние» значение «зашифрован».

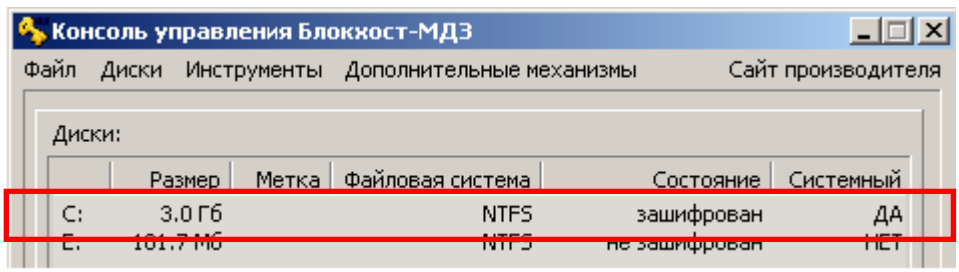

Рисунок 4.2.2.1 – Выбор зашифрованного системного диска

3. Щелкнуть правой кнопкой мыши на выделенной строке, и в открывшемся контекстном меню выбрать пункт «Расшифровать» (Рисунок 4.2.2.2), после чего появится запрос подтверждения (Рисунок 4.2.2.3).

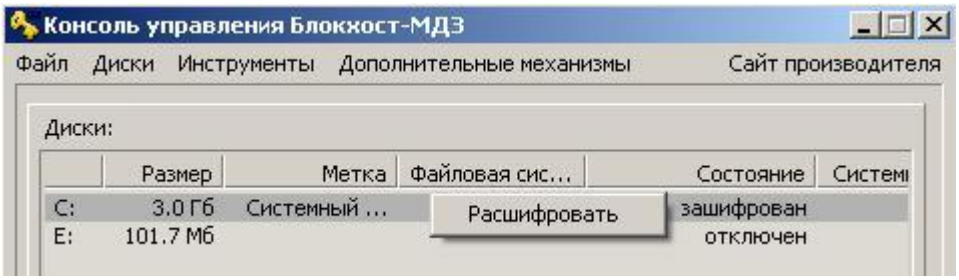

Рисунок 4.2.2.2 – Выбор пункта «Расшифровать» в контекстном меню

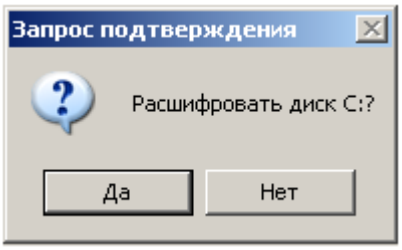

Рисунок 4.2.2.3 - Запрос подтверждения

4. В окне запроса подтверждения нажать кнопку «Да».
5. В открывшемся диалоговом окне (Рисунок 4.2.2.4) необходимо:
   - в выпадающем списке «Ключевой носитель» выбрать имя виртуального карт-ридера, к которому подключен электронный идентификатор, на основе которого был зашифрован диск;
   - в поле «PIN-код» ввести пароль доступа к идентификатору.

Если системный диск был зашифрован по паролю, то в диалоговом окне (Рисунок 4.2.2.4) необходимо активировать поле «Использовать пароль» и ввести пароль в соответствующее поле.

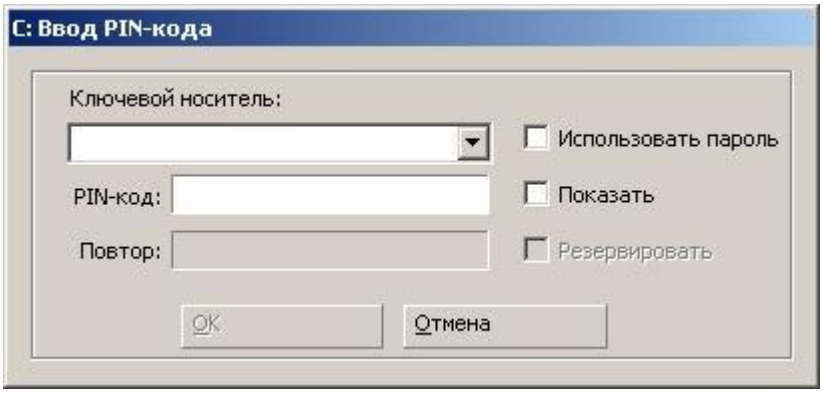

Рисунок 4.2.2.4 - Диалоговое окно ввода PIN-кода

После ввода пароля в поле «PIN-код» становится возможным нажатие на кнопку «ОК».

6. Нажать кнопку «ОК». Запустится процесс расшифровывания пользовательского диска (Рисунок 4.2.2.5).

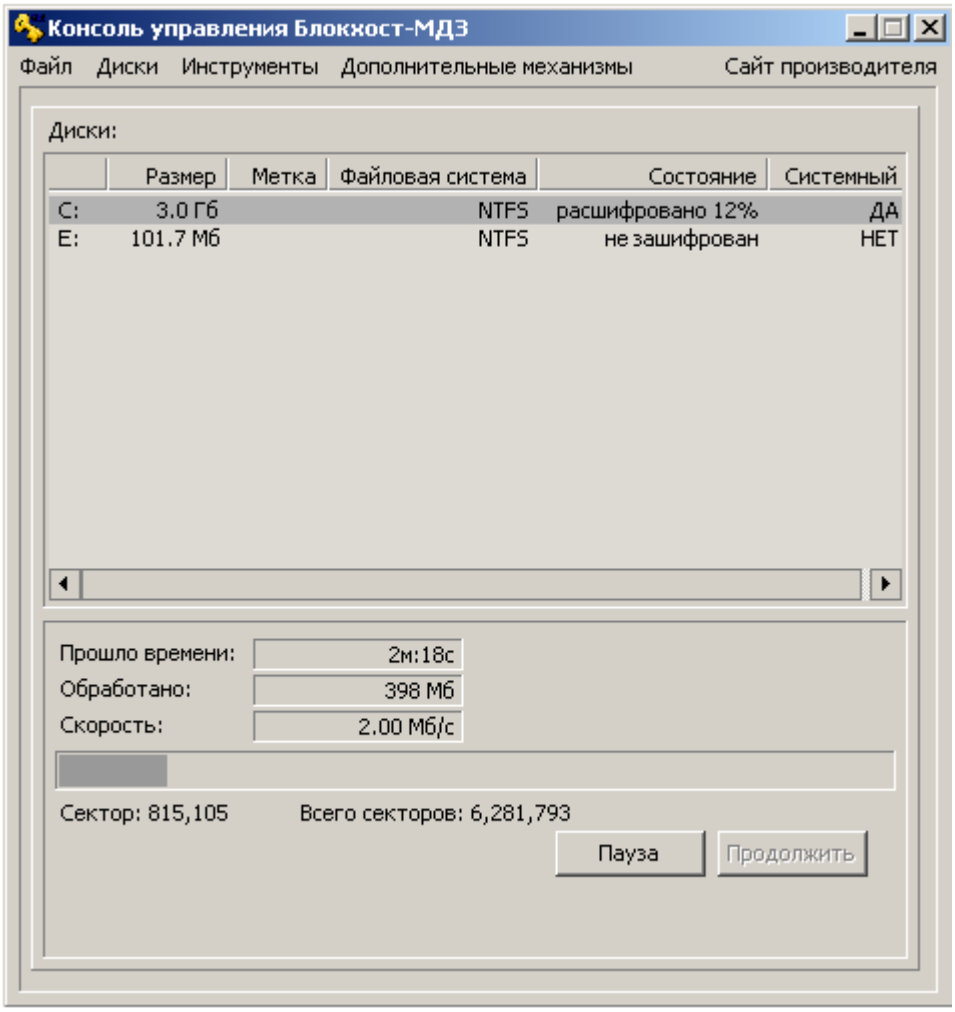

Рисунок 4.2.2.5 – Отображение процесса расшифровывания системного диска

О том, что процесс расшифровывания активен, свидетельствует строка «расшифровано» с указанием количества процентов готовности в поле «Состояние».

Когда диск полностью расшифрован и готов к работе поле «Состояние» принимает значение «Не зашифрован».

Примечание

Процесс расшифровывания работает в фоновом режиме и не препятствует нормальной работе пользователя.

Программно-аппаратный комплекс поддерживает одновременное расшифровывание нескольких дисков, каждый диск шифруется в собственном системном потоке.

4.2.2.1 Дорасшифровывание системного (загрузочного) диска

В подсистеме шифрования ПАК «Блокхост-МДЗ» реализована операция дорасшифровывания системного (загрузочного) диска, на случай если во время выполнения операции расшифровывания системного диска по некоторым причинам произошло прерывание работы ОС (выключение питания компьютера). После произошедшего прерывания необходимо включить компьютер и загрузить ОС. Во время загрузки ОС выдается запрос аутентификации (Рисунок 4.2.2.1.1). Для загрузки ОС необходимо подключить eToken (если он использовался при расшифровывании системного диска) к компьютеру и ввести PIN-код (Рисунок 4.2.2.1.2).

Рисунок 4.2.2.1.1 – Запрос аутентификации

Рисунок 4.2.2.1.2 – Ввод PIN-кода (eToken-а или пароль, на котором происходило шифрование)

Примечание

Во время загрузки ОС необходимо дождаться завершения работы программы проверки диска CHKDSK.

После загрузки ОС необходимо выполнить следующие операции:

1. Запустить консоль управления подсистемы шифрования ПАК «Блокхост-МДЗ».
2. Выделить в списке разделов (дисков) недорасшифрованный системный раздел (диск). Для такого раздела (диска) в поле «Системный» будет стоять значение «ДА» (Рисунок 4.2.2.1.3), в поле «Состояние» значение «расшифровано» с указанием количества процентов готовности, а в поле «Файловая система» отсутствует значение.

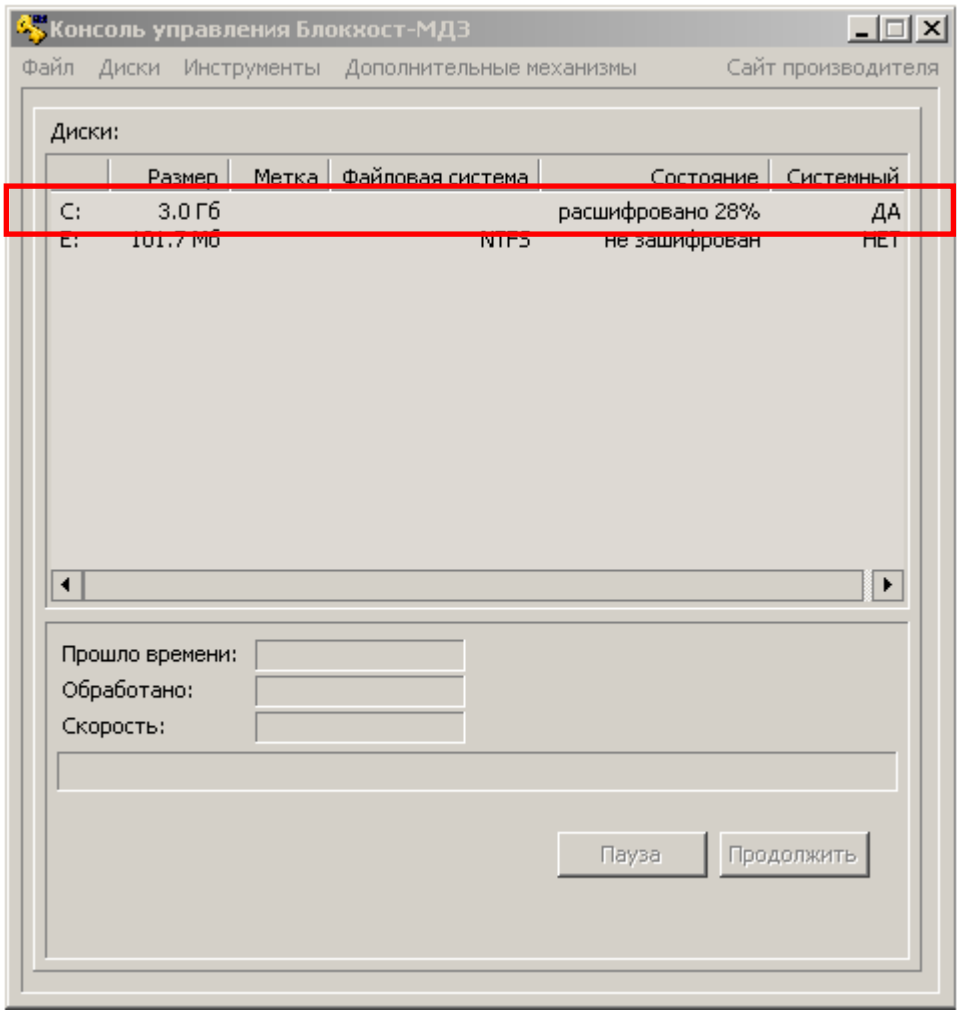

Рисунок 4.2.2.1.3 – Выбор недорасшифрованного системного диска

3. Щелкнуть правой кнопкой мыши на выбранной строке, и в открывшемся контекстном меню (Рисунок 4.2.2.1.4) выбрать пункт «Закончить расшифрование», после чего запустится процесс расшифровывания загрузочного диска (Рисунок 4.2.2.1.5).

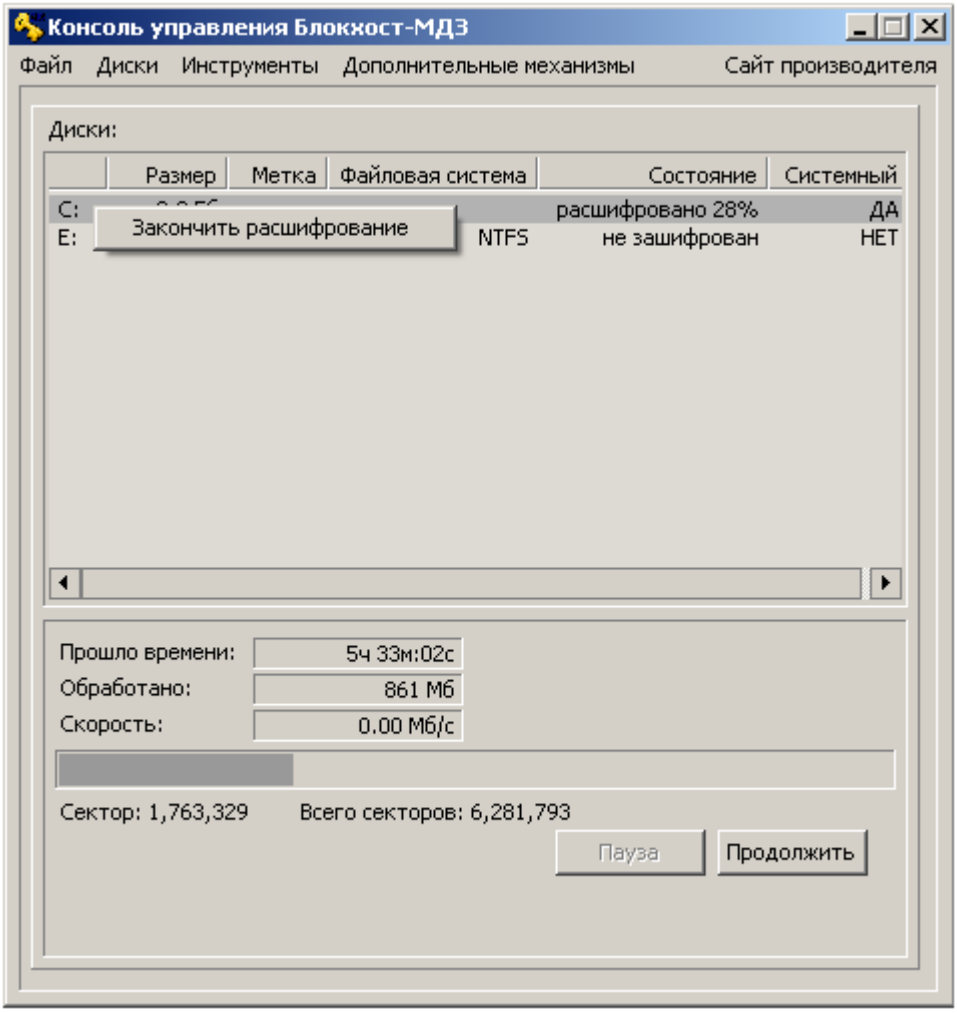

Рисунок 4.2.2.1.4 – Выбор пункта «Закончить расшифрование» в контекстном меню

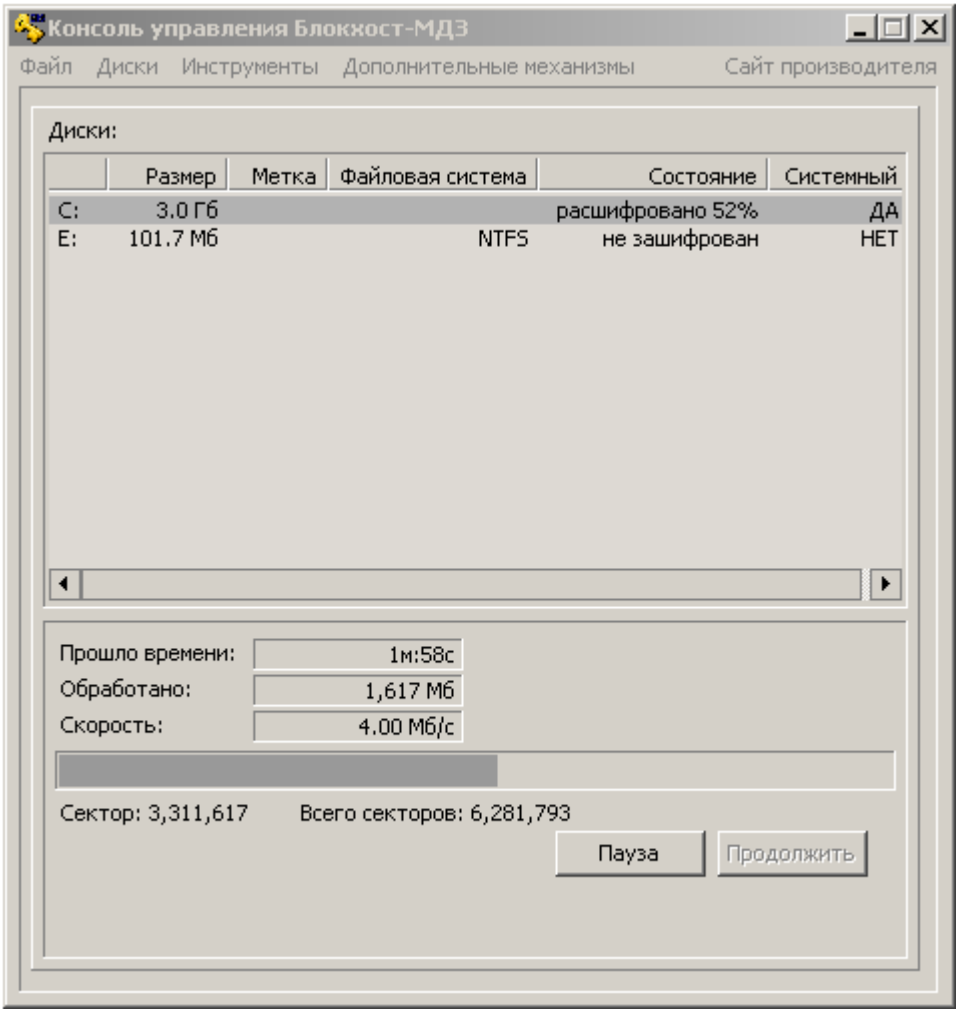

Рисунок 4.2.2.1.5 – Отображение процесса расшифровывания системного диска

О том, что процесс расшифровывания активен, свидетельствует строка «расшифровано» с указанием количества процентов готовности в поле «Состояние».

Когда диск полностью расшифрован и готов к работе, поле «Состояние» принимает значение «Не зашифрован».

4.2.3 Создание зашифрованного пользовательского диска

Для того чтобы зашифровать диск, необходимо выполнить следующие операции:

1. Запустить консоль управления подсистемы шифрования ПАК «Блокхост-МДЗ».
2. Выделить в списке дисков пользовательский диск (для такого диска в поле «Системный» будет стоять значение «НЕТ» см. рисунок 4.2.3.1).

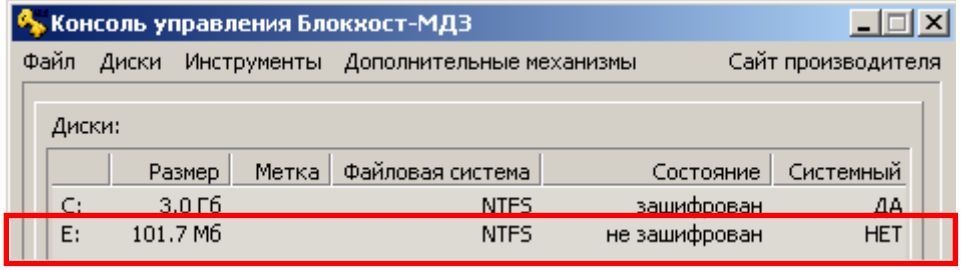

Рисунок 4.2.3.1 – Выбор пользовательского диска

3. Щелкнуть правой кнопкой мыши на выделенной строке, и в открывшемся окне выбрать пункт «Зашифровать» (Рисунок 4.2.3.2).

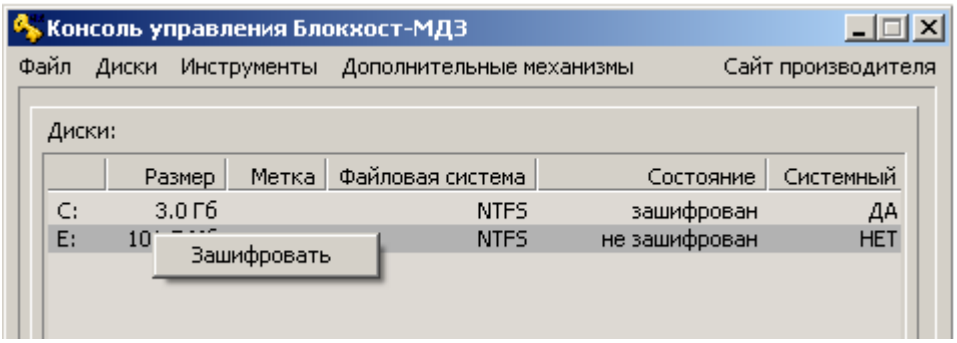

Рисунок 4.2.3.2 – Выбор пункта «Зашифровать» в контекстном меню

4. В открывшемся диалоговом окне (Рисунок 4.2.3.3) необходимо:
   - в поле «Криптопровайдер» выбрать криптопровайдера или оставить тот криптопровайдер, который установлен по умолчанию;
   - в поле «Алгоритм шифрования» указать необходимый алгоритм шифрования;
   - в поле «Режим шифрования» выбрать или оставить установленный по умолчанию режим шифрования.

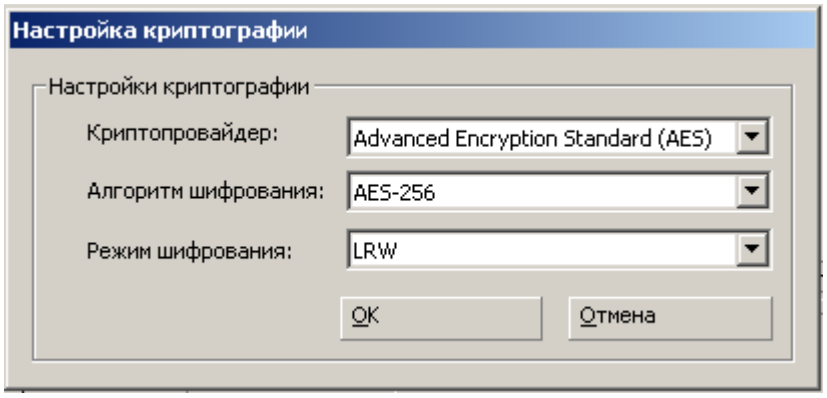

Рисунок 4.2.3.3 – Настройки криптографии

5. В открывшемся диалоговом окне (Рисунок 4.2.3.4) необходимо:
   - в выпадающем списке «Ключевой носитель» выбрать имя виртуального карт-ридера, к которому подключен электронный идентификатор;
   - в поле «PIN-код» ввести пароль доступа к идентификатору;
   - в поле «Повтор» осуществить повторный ввод пароля.

В диалоговом окне (Рисунок 4.2.3.4) указывается ключевой носитель, на который будет записан ключ шифрования. Также имеется возможность шифрования системных дисков по паролю, без использования ключевого носителя. Для этого необходимо активировать поле «Использовать пароль» и ввести пароль в соответствующие поля. В этом же окне существует возможность просмотра пароля и резервирования ключевой информации на другой носитель при установленных галочках на соответствующих пунктах: «Показать» и «Резервировать».

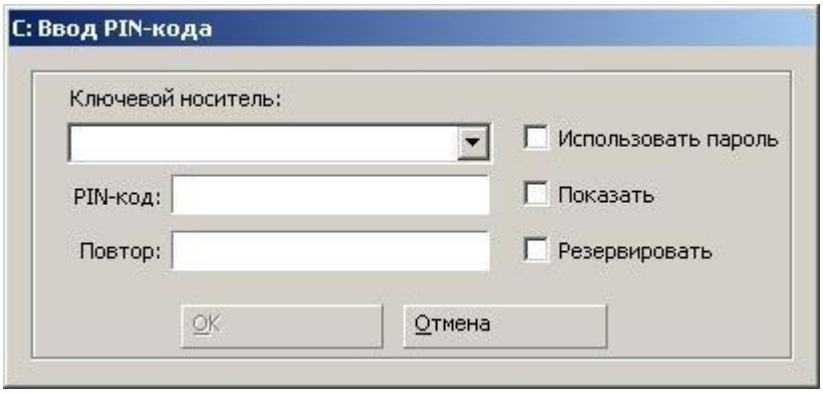

Рисунок 4.2.3.4 – Диалог ввода PIN-кода

Если значения, введенные в поля «PIN-код» и «Повтор», совпадают, тогда становится возможным нажатие на кнопку «ОК».

6. Если была установлена галочка напротив пункта «Резервировать» в окне ввода PIN-кода (Рисунок 4.2.3.4), то после нажатия кнопки «ОК» в окне ввода PIN-кода появится диалоговое окно резервирования ключевой информации (Рисунок 4.2.3.5), в котором необходимо:

- в поле резервный носитель выбрать имя виртуального карт-ридера, к которому подключен резервный ключевой носитель;
- в поле PIN-код ввести PIN-код резервного электронного идентификатора.

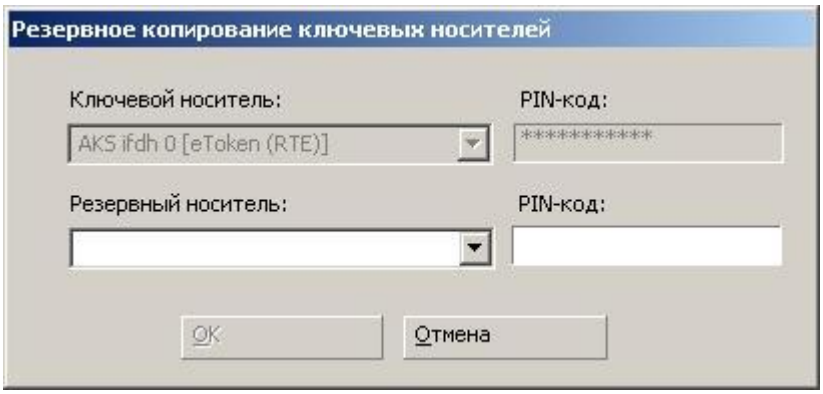

Рисунок 4.2.3.5 – Резервное копирование ключевых носителей

7. Если же резервирование ключевых носителей не было включено и PIN-код был введен верно (Рисунок 4.2.3.4), то после нажатия кнопки «ОК» в окне ввода PIN-кода запустится процесс фонового шифрования загрузочного диска (Рисунок 4.2.3.6). В случае неверного ввода PIN-кода консоль управления выведет сообщение об ошибке.

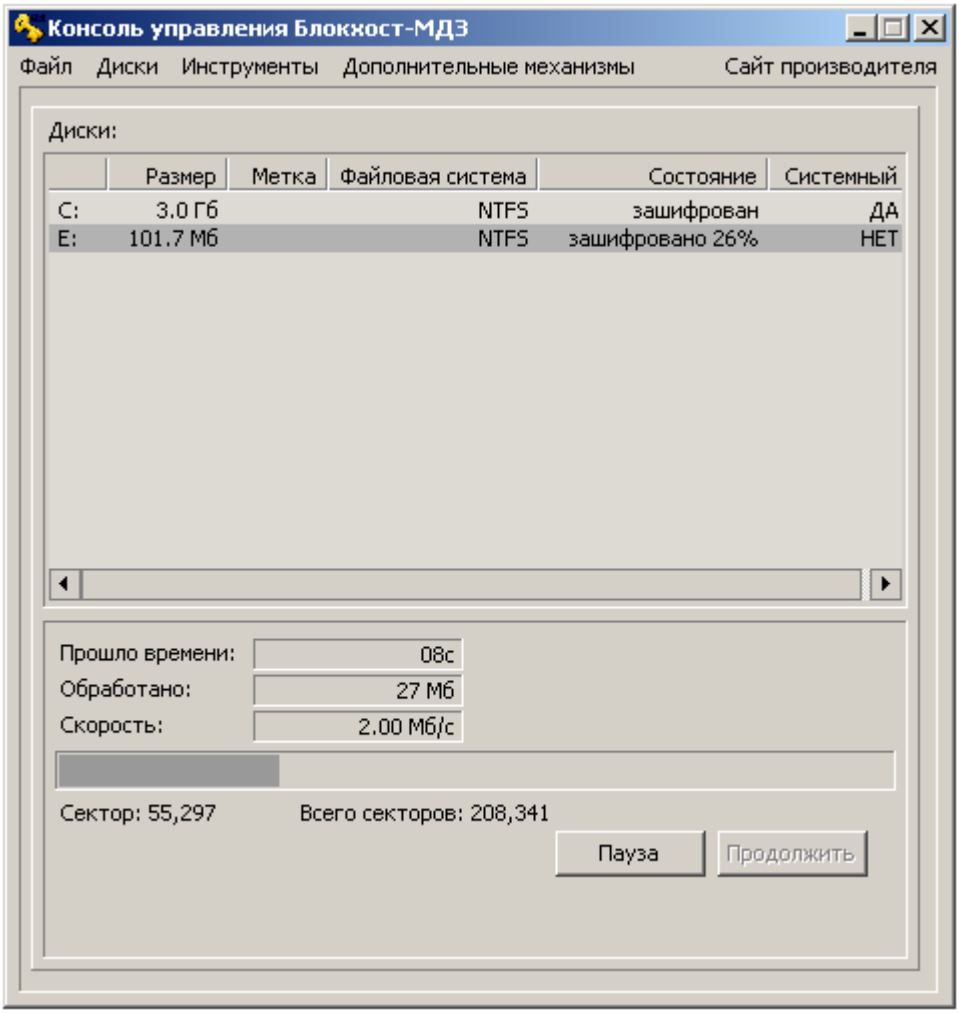

Рисунок 4.2.3.6 – Отображение прогресса процесса зашифровывания диска

О том, что процесс зашифровывания активен, свидетельствует строка «зашифровано» с указанием количества процентов готовности в поле «Состояние».

Когда диск полностью зашифрован и готов к работе поле «Состояние» принимает значение «Зашифрован».

Примечание:

Во время зашифровывания пользовательский диск полностью готов к работе – на нем можно создавать и удалять файлы, выполнять проверку, определять права доступа.

Процесс зашифровывания работает в фоновом режиме и не препятствует нормальной работе пользователя. Программно-аппаратный комплекс поддерживает одновременное зашифровывание нескольких дисков, каждый диск шифруется в собственном системном потоке.

4.2.3.1 Дозашифровывание пользовательского диска

В подсистеме шифрования ПАК «Блокхост-МДЗ» реализована операция дозашифровывания пользовательского диска, на случай если во время выполнения операции шифрования пользовательского диска по некоторым причинам произошло прерывание работы ОС (выключение питания компьютера). После произошедшего прерывания необходимо включить компьютер и загрузить ОС.

Примечание

Во время загрузки ОС необходимо дождаться завершения работы программы проверки диска CHKDSK.

После загрузки ОС необходимо выполнить следующие операции:

1. Запустить консоль управления подсистемы шифрования ПАК «Блокхост-МДЗ».

2. Выделить в списке разделов (дисков) недозашифрованный пользовательский раздел (диск). Для такого раздела (диска) в поле «Системный» будет стоять значение «НЕТ», в поле «Состояние» значение «Зашифровано» с указанием количества процентов готовности, а в поле «Файловая система» будет отсутствовать значение (Рисунок 4.2.3.1.1).

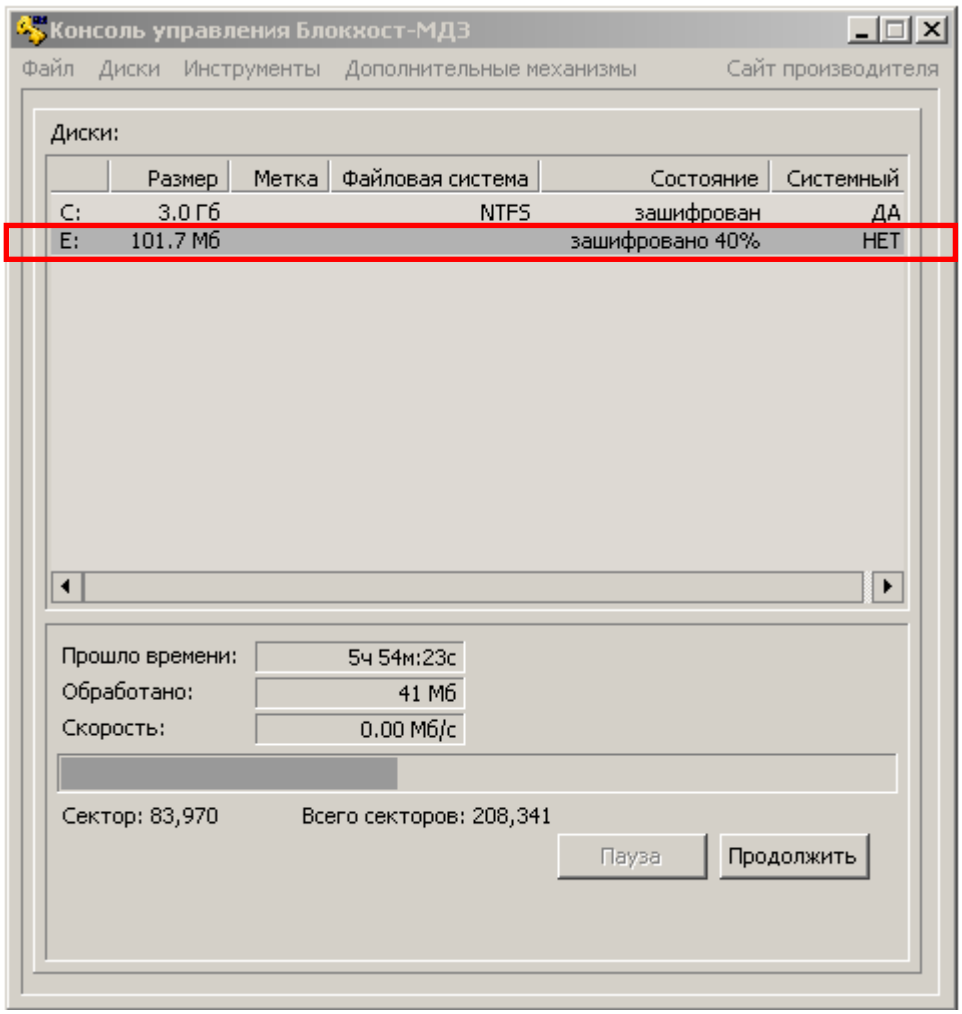

Рисунок 4.2.3.1.1 – Выбор недозашифрованного пользовательского диска

3. Щелкнуть правой кнопкой мыши на выбранной строке, и в открывшемся контекстном меню (Рисунок 4.2.3.1.2) выбрать пункт «Закончить зашифрование», после чего запустится процесс шифрования пользовательского диска (Рисунок 4.2.3.1.3).

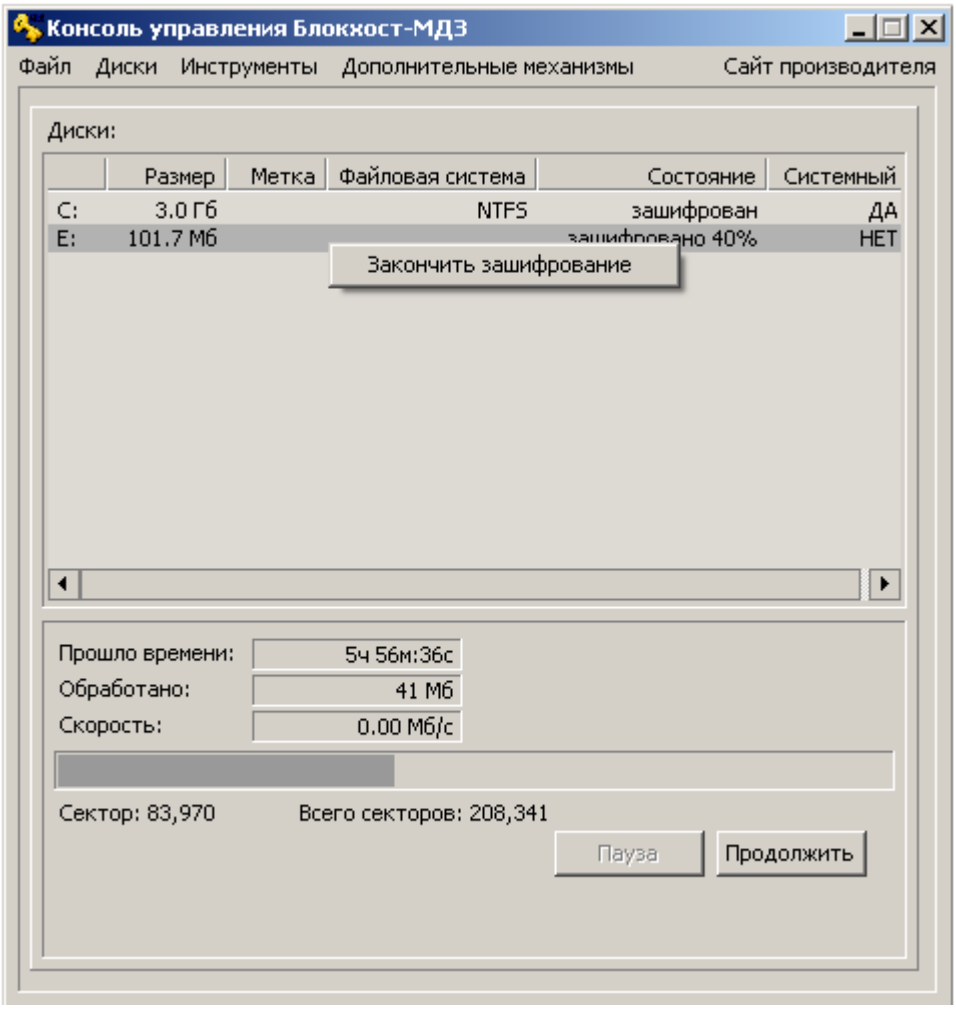

Рисунок 4.2.3.1.2 – Выбор пункта «Закончить зашифрование» в контекстном меню

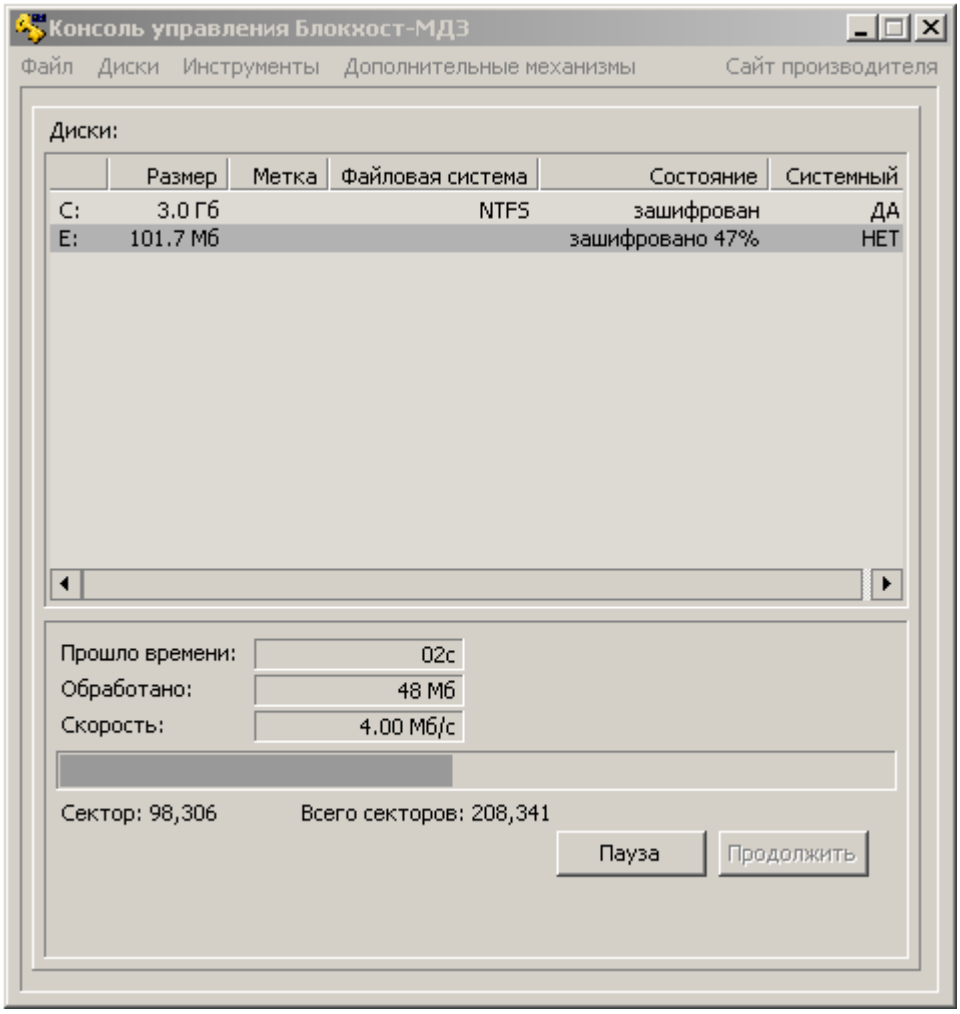

Рисунок 4.2.3.1.3 – Отображение процесса шифрования системного диска

О том, что процесс шифрования активен, свидетельствует строка «зашифровано» с указанием количества процентов готовности в поле «Состояние».

Когда диск полностью зашифрован и готов к работе поле «Состояние» принимает значение «Зашифрован».

4.2.4 Расшифровывание пользовательского диска

Для того чтобы расшифровать пользовательский диск, необходимо выполнить следующие операции:

1. Запустить консоль управления подсистемы шифрования ПАК «Блокхост-МДЗ».
2. Выделить в списке разделов (дисков) зашифрованный пользовательский раздел (диск). Для такого раздела (диска) в поле «Системный» будет стоять значение «НЕТ», а в поле «Состояние» значение «зашифрован» (Рисунок 4.2.4.1).

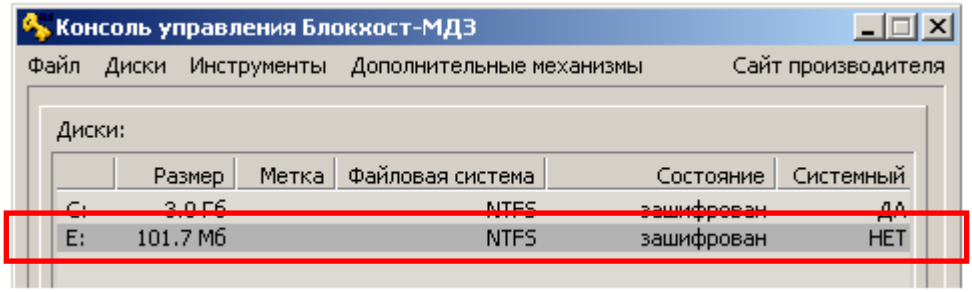

Рисунок 4.2.4.1 – Выбор зашифрованного пользовательского диска

3. Щелкнуть правой кнопкой мыши на выделенной строке, и в появившемся контекстном меню (Рисунок 4.2.4.2) выбрать пункт «Расшифровать», после чего появится запрос подтверждения (Рисунок 4.2.4.3).

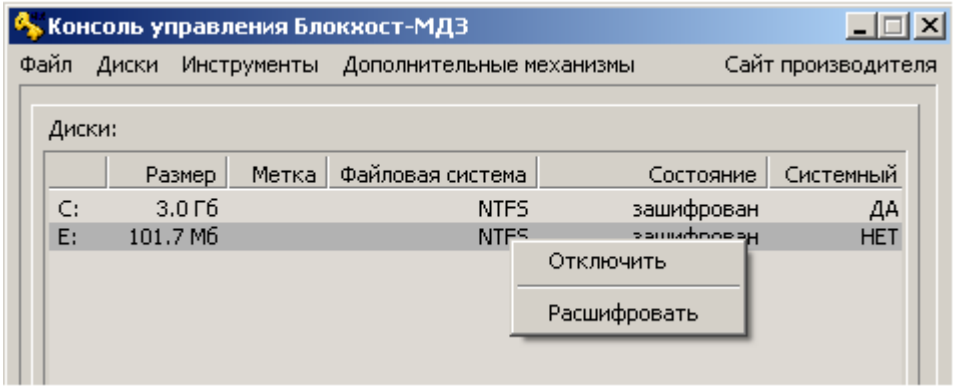

Рисунок 4.2.4.2 – Выбор пункта «Расшифровать» в контекстном меню

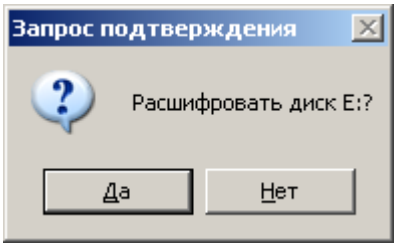

Рисунок 4.2.4.3 – Запрос подтверждения

4. В окне запроса подтверждения нажать кнопку «Да».
5. В открывшемся диалоговом окне (Рисунок 4.2.4.4) необходимо:
   - в выпадающем списке «Ключевой носитель» выбрать имя виртуального карт-ридера, к которому подключен электронный идентификатор, на основе которого был зашифрован диск;
   - в поле «PIN-код» ввести пароль доступа к идентификатору.

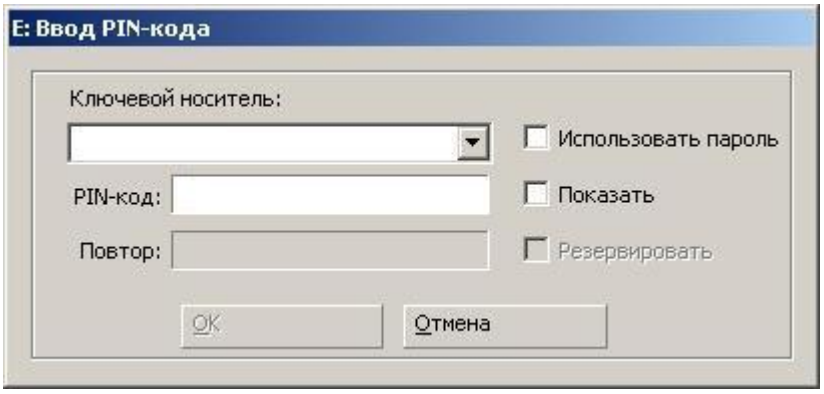

Рисунок 4.2.4.4 – Диалоговое окно ввода PIN-кода

После ввода пароля в поле «PIN-код» становится возможным нажатие на кнопку «ОК».

6. Нажать кнопку «ОК». Запустится процесс расшифровывания пользовательского диска (Рисунок 4.2.4.5).

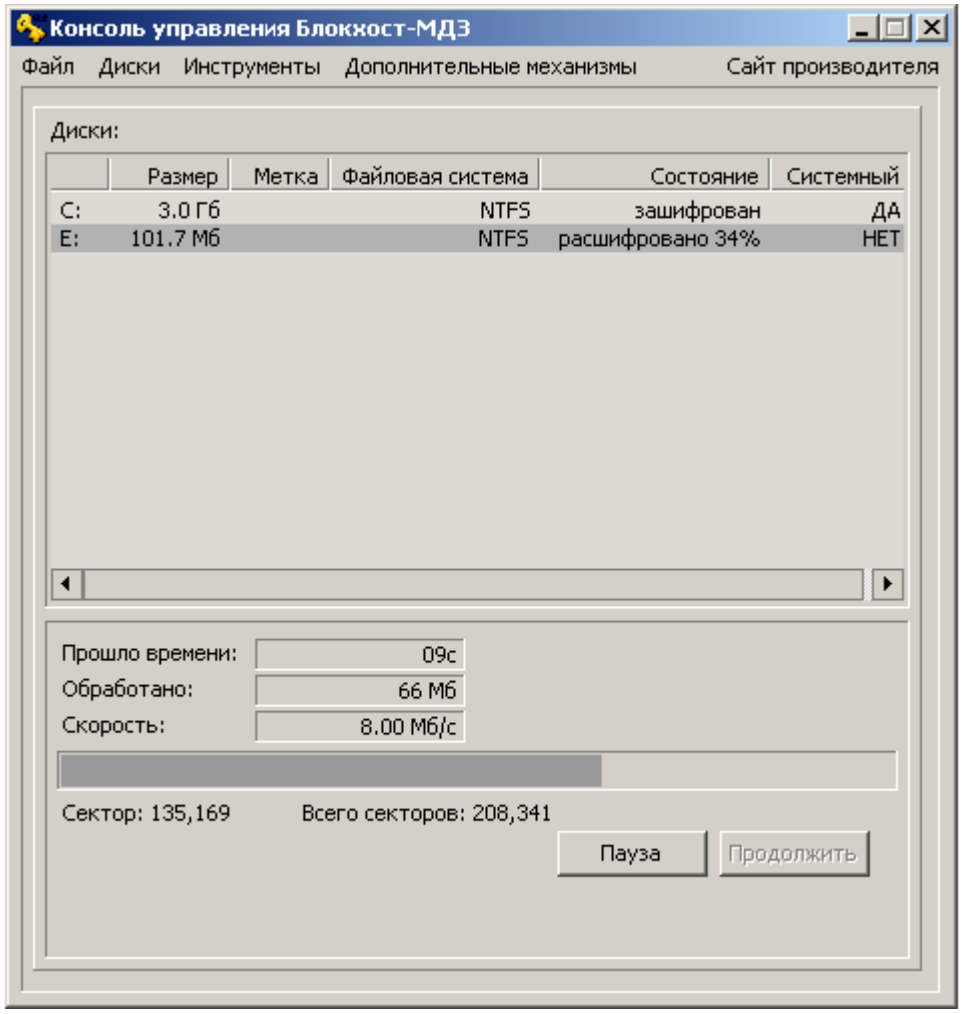

Рисунок 4.2.4.5 – Отображение процесса расшифровывания диска

Когда диск полностью расшифрован и готов к работе, поле «Состояние» принимает значение «не зашифрован».

Примечание:

Процесс расшифровывания работает в фоновом режиме и не препятствует нормальной работе пользователя. Программно-аппаратный комплекс поддерживает одновременное расшифровывание нескольких дисков, каждый диск шифруется в собственном системном потоке.

4.2.4.1 Дорасшифровывание пользовательского диска

В подсистеме шифрования ПАК «Блокхост-МДЗ» реализована операция дорасшифровывания пользовательского диска, на случай если во время выполнения операции расшифровывания пользовательского диска по некоторым причинам произошло прерывание работы ОС (выключение питания компьютера). После произошедшего прерывания необходимо включить компьютер и загрузить ОС.

Примечание

После аварийной перезагрузки ПК в момент зашифрования/расшифрования диска до начала загрузки ОС необходимо дождаться завершения работы программы проверки диска CHKDSK.

После загрузки ОС необходимо выполнить следующие операции:

1. Запустить консоль управления подсистемы шифрования ПАК «Блокхост-МДЗ».

2. Выделить в списке разделов (дисков) неподключенный пользовательский раздел (диск). Для такого раздела (диска) в поле «Системный» будет стоять значение «НЕТ», в поле «Состояние» значение «не зашифрован», а в поле «Файловая система» отсутствует значение.

3. Подключить выбранный пользовательский раздел (диск).

4. Выделить в списке разделов (дисков) недорасшифрованный пользовательский раздел (диск). Для такого раздела (диска) в поле «Системный» будет стоять значение «НЕТ» (Рисунок 4.2.4.1.1), в поле «Состояние» значение «расшифровано» с указанием количества процентов готовности, а в поле «Файловая система» отсутствует значение.

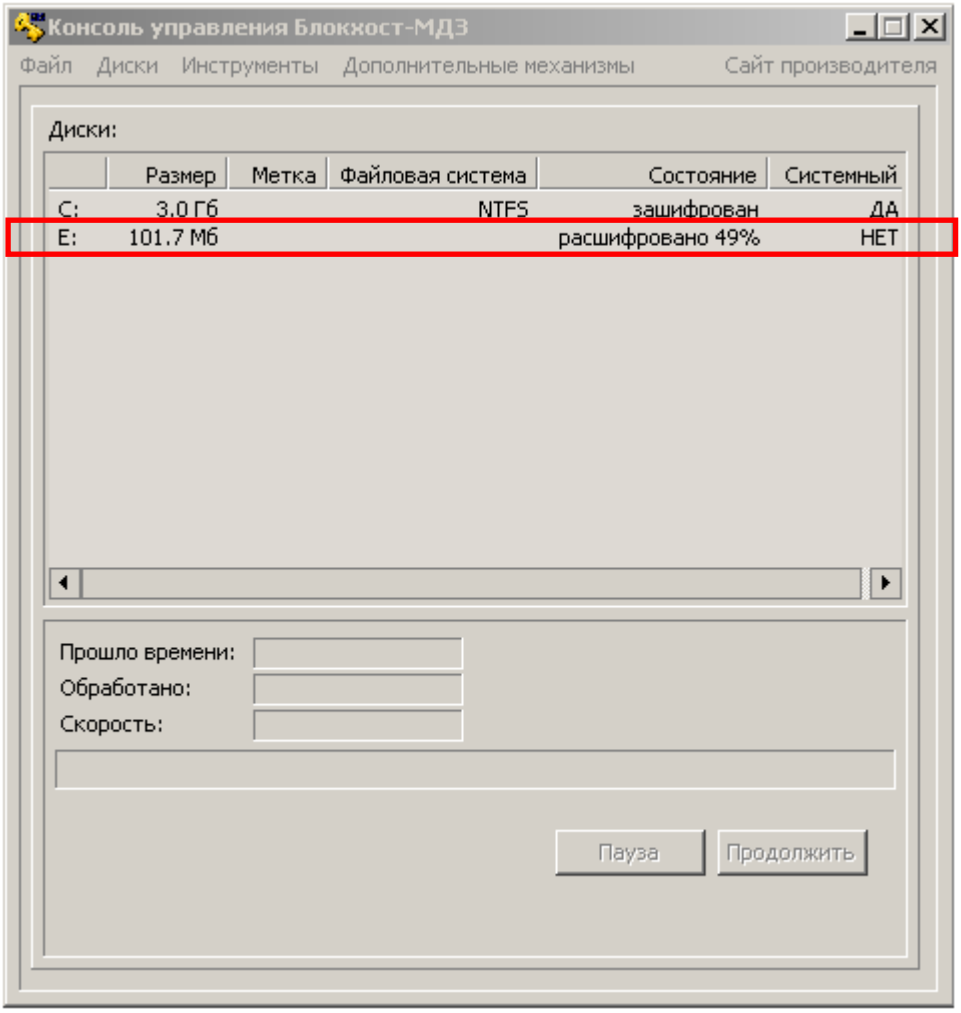

Рисунок 4.2.4.1.1 – Выбор недорасшифрованного системного диска

5. Щелкнуть правой кнопкой мыши на выбранной строке, и в открывшемся контекстном меню (Рисунок 4.2.4.1.2) выбрать пункт «Закончить расшифрование», после чего запустится процесс расшифровывания пользовательского диска (Рисунок 4.2.4.1.3).

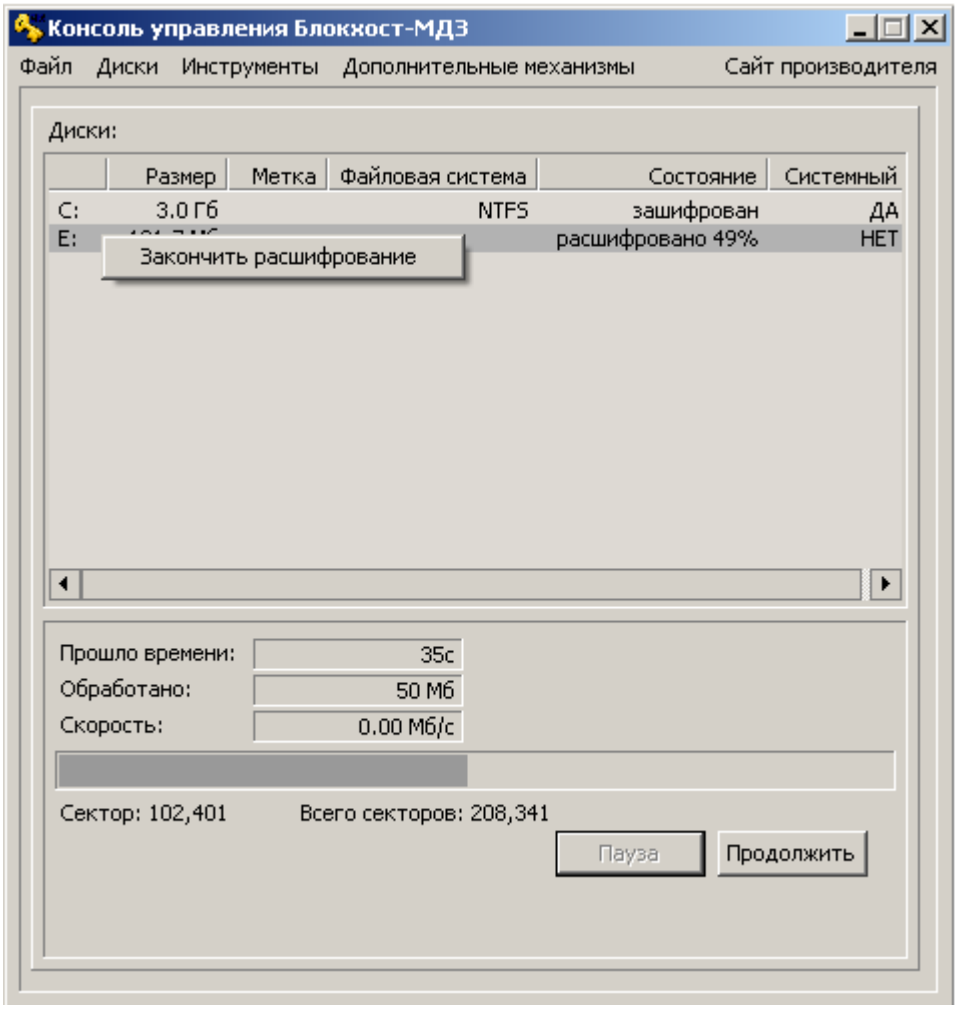

Рисунок 4.2.4.1.2 – Выбор пункта «Закончить расшифрование» в контекстном меню

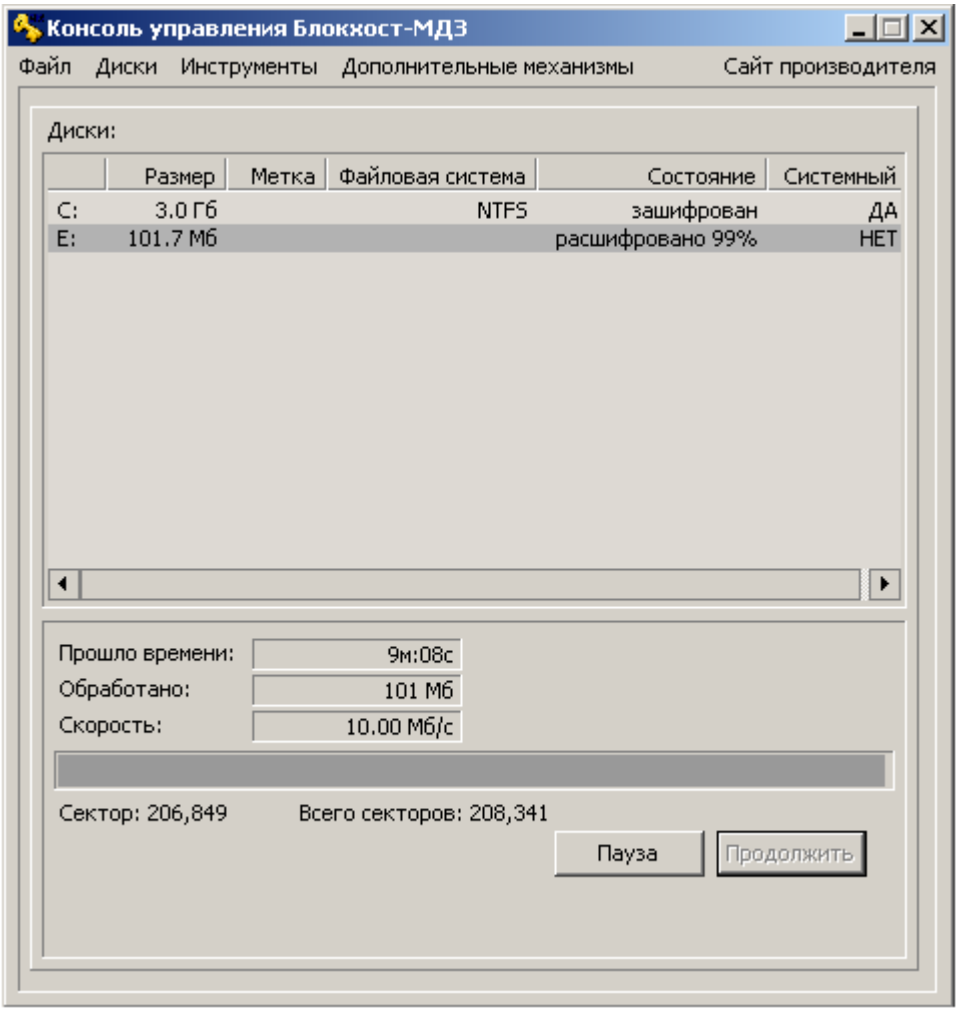

Рисунок 4.2.4.1.3 – Отображение процесса расшифровывания пользовательского диска

О том, что процесс расшифровывания активен, свидетельствует строка «расшифровано» с указанием количества процентов готовности в поле «Состояние».

Когда диск полностью расшифрован и готов к работе, поле «Состояние» принимает значение «Не зашифрован».

4.2.5 Отключение зашифрованных дисков

Все зашифрованные диски (кроме системного зашифрованного диска) отключаются при закрытии сеанса пользователя.

Для того чтобы отключить один или несколько зашифрованных дисков, не закрывая сеанса пользователя, необходимо выполнить следующие операции:

1. Закрыть все приложения, обращающиеся к диску. Для корректного отключения зашифрованного диска на нём не должно быть ни одного открытого документа.
2. Запустить консоль управления ПАК «Блокхост-МДЗ».
3. Выбрать зашифрованный диск, который необходимо отключить.
4. Щёлкнуть правой кнопкой мыши на данном диске, и в открывшемся контекстном меню выбрать пункт «Отключить» (Рисунок 4.2.5.1).

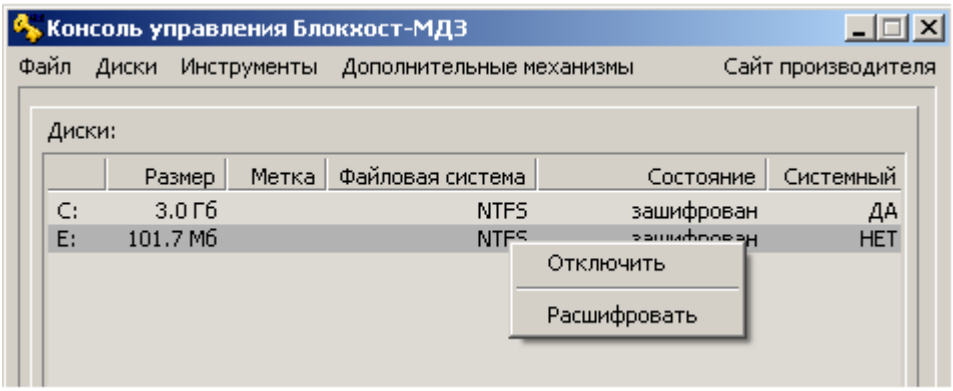

Рисунок 4.2.5.1 – Отключение зашифрованных дисков

5. В появившемся окне запроса (Рисунок 4.2.5.2) нажать кнопку «Да».

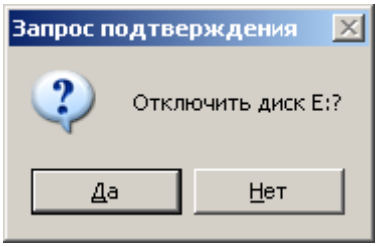

Рисунок 4.2.5.2 – Запрос подтверждения отключения диска

Если отключаемый диск занят, на экране появится диалоговое окно (Рисунок 4.2.5.3) с запросом на принудительно отключение диска. Если не надо в данный момент отключать диск, нажмите «Нет», иначе нажмите «Да».

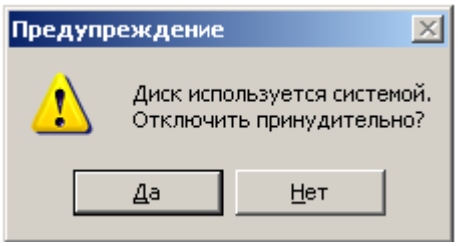

Рисунок 4.2.5.3 – Запрос на принудительное отключение диска

В случае успешного отключения диска (дисков) поле «Состояние» изменит своё значение с «зашифрован» на «отключен», а поле «Файловая система» не определено.

Примечание

Для отключения всех пользовательских дисков существует групповая операция «Отключить Все диски», доступная через пункт главного меню «Диски» → «Отключить Все диски», а также через иконку в панели задач. Отключить системный (загрузочный) диск нельзя.

4.2.6 Подключение зашифрованных дисков

Зашифрованный диск можно подключать, только если он является пользовательским.

Для того чтобы подключить зашифрованный диск, необходимо выполнить следующие операции:

1. Запустить консоль управления подсистемы шифрования ПАК «Блокхост-МДЗ».
2. Выбрать зашифрованный диск, который необходимо подключить.

3. Щелкнуть по выбранному диску правой кнопкой мыши и в открывшемся контекстном меню выбрать пункт «Подключить» (Рисунок 4.2.6.1).

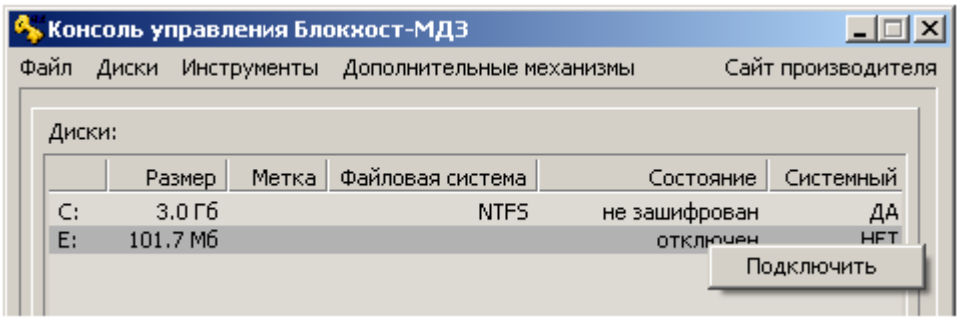

Рисунок 4.2.6.1 – Подключение зашифрованного диска

4. При необходимости указать имя виртуального карт-ридера, к которому подключен электронный идентификатор, на основе которого был зашифрован диск, и ввести пароль к выбранному идентификатору (Рисунок 4.2.6.2).

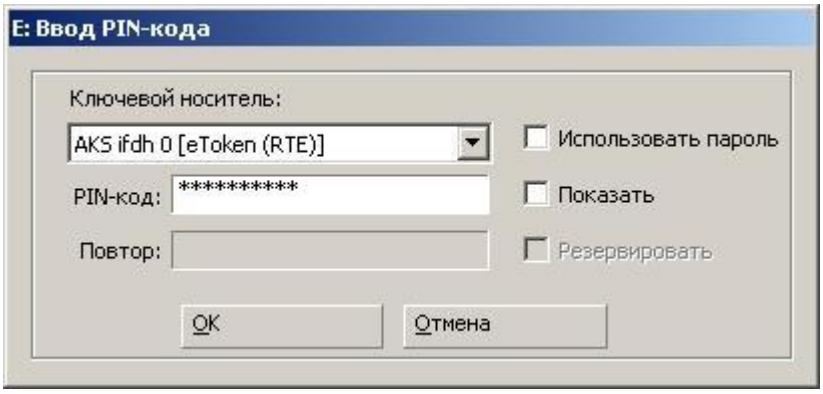

Рисунок 4.2.6.2 – Ввод пароля доступа к диску

В случае успешного подключения зашифрованного диска (дисков) поле «Состояние» изменит своё значение с «не зашифрован» на «зашифрован» (Рисунок 4.2.6.3).

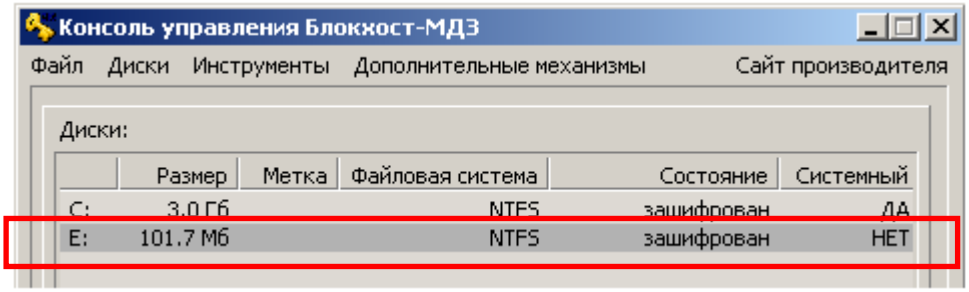

Рисунок 4.2.6.3 – Изменение статуса диска

Примечание

Для подключения всех пользовательских дисков существует групповая операция «Подключить Все диски», доступная через пункт главного меню «Диски» → «Подключить Все диски», а также через иконку в панели задач.

4.2.7 Смена носителя ключевой информации к пользовательскому разделу

Для того чтобы сменить носитель ключевой информации к пользовательскому разделу, необходимо выполнить следующие операции:

1. Запустить консоль управления подсистемы шифрования ПАК «Блокхост-МДЗ».

2. Если пользовательский раздел отключен, подключить его в соответствии с п. 4.2.6. настоящего документа.

3. Выделить в списке разделов (дисков) зашифрованный пользовательский раздел (диск). Для такого раздела (диска) в поле «Системный» будет стоять значение «НЕТ», а в поле «Состояние» значение «зашифрован» (Рисунок 4.2.7.1).

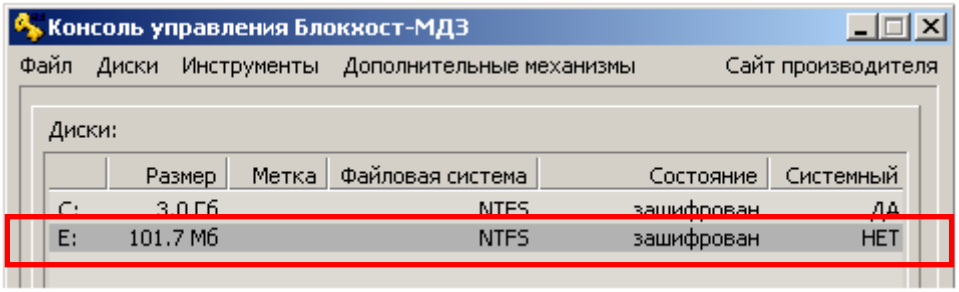

Рисунок 4.2.7.1 – Выбор подключенного зашифрованного пользовательского диска

4. Выбрать пункт меню «Инструменты» → «Сменить носитель».

5. В открывшемся диалоговом окне (Рисунок 4.2.7.2) необходимо:

- в выпадающем списке «Ключевой носитель» выбрать имя виртуального карт-ридера, к которому подключен электронный идентификатор, на который необходимо перенести ключевую информацию;
- в поле «PIN-код:» ввести пароль доступа к новому электронному идентификатору;
- в поле «Повтор:» осуществить повторный ввод пароля.

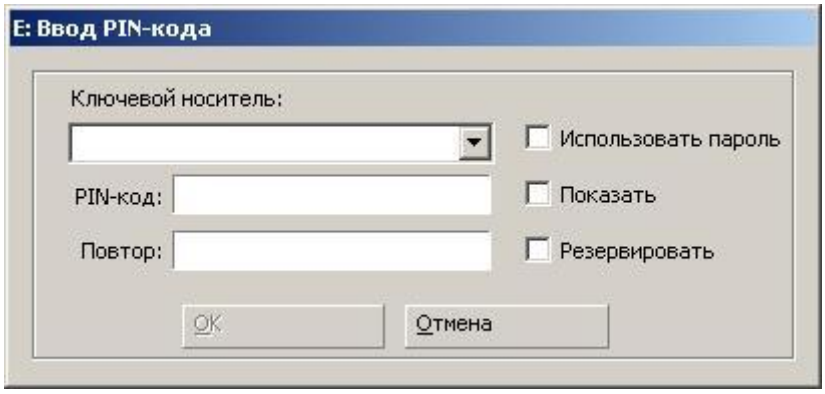

Рисунок 4.2.7.2 – Диалоговое окно ввода пароля

6. Нажать кнопку «OK». При следующей операции подключения пользовательского раздела потребуется ввести пароль и имя нового электронного идентификатора.

4.2.8 Загрузка ОС с зашифрованного системного раздела: аутентификация до загрузки ОС

Процедура аутентификации проводятся до загрузки операционной системы. Для того чтобы загрузка операционной системы произошла успешно, необходимо выполнить следующие операции:

1. Предъявить идентификатор eToken, на котором производилось шифрование системного раздела.

2. Ввести PIN-код.

4.3 Режимы работы подсистемы шифрования

Подсистема шифрования ПАК «Блокхост-МДЗ» в зависимости от требуемого уровня защищенности и ограничений, накладываемых программным и аппаратным обеспечением ПК, может работать в следующих режимах:

- Усиленная Доверенная загрузка ПК с предъявлением USB-ключа eToken;
- Усиленная Доверенная загрузка ПК по паролю;
- Базовая Доверенная загрузка ПК с предъявлением USB-ключа eToken;
- Базовая Доверенная загрузка ПК по паролю;
- Легкая Доверенная загрузка ПК с использованием USB-ключа eToken;
- Легкая Доверенная загрузка ПК по паролю.

В подсистеме шифрования при режимах базовой и легкой доверенной загрузки необходимо активировать режим «Замок». В режиме «Замок» осуществляется защита ПЭВМ от НСД к его ресурсам, предотвращая загрузку операционной системы для пользователей не прошедших аутентификацию. При включенном режиме «Замок» при включении или перезагрузке ПЭВМ подсистема требует предъявления персонального идентификатора с PIN-кодом или пароля, в зависимости от выбранного режима. В случае успешной аутентификации осуществляется загрузка ОС.

4.3.1 Усиленная Доверенная загрузка ПК

4.3.1.1 Усиленная Доверенная загрузка ПК с предъявлением USB-ключа eToken

Данный режим работы ПАК «Блокхост-МДЗ» обеспечивает максимальный уровень защищенности т.к. в нём активированы все механизмы защиты: двухфакторная аутентификация до загрузки ОС с использованием USB-ключей eToken; шифрование “на лету” системного и пользовательских разделов; включение и отключение пользовательских дисков; контроль целостности файловых объектов.

Для работы в этом режиме необходимо:

1. Зашифровать системный диск с использованием USB-ключа eToken;
2. Зашифровать все пользовательские разделы;
3. Поставить на контроль целостности все необходимые файлы.

4.3.1.2 Усиленная Доверенная загрузка ПК по паролю

В данном режиме вместо двухфакторной аутентификации до загрузки ОС будет производиться однофакторная аутентификация. Этот режим работы предназначен для доверенной загрузки ПК, где по каким-либо причинам невозможно использовать USB-ключи eToken. Возможные причины: отсутствие на ПК USB-портов; для входа в ОС уже используется электронный идентификатор, отличный от USB-ключа eToken Pro\NG-FLASH\NG-OTP и др.

Примечание:
Для удобства работы пользователя можно назначить пароль, совпадающий с PIN-кодом электронного идентификатора, который используется для входа в ОС.

Для работы в данном режиме необходимо:

1. Зашифровать системный диск с использованием пароля;
2. Зашифровать все пользовательские разделы;
3. Поставить на контроль целостности все необходимые файлы.

4.3.2 Базовая Доверенная загрузка ПК

4.3.2.1 Базовая Доверенная загрузка ПК с предъявлением USB-ключа eToken

В базовом режиме ПАК «Блокхост-МДЗ» обеспечивает максимальную совместимость с аппаратным обеспечением ПК. В этом режиме ПАК «Блокхост-МДЗ» проводит двухфакторную аутентификацию до загрузки ОС, осуществляет шифрование пользовательских дисков и контролирует целостность файлов.

Для работы в данном режиме необходимо:

1. Активировать режим «Замок», указав тип входа: по USB-ключу eToken;
2. Зашифровать все пользовательские диски;
3. Поставить на контроль целостности все необходимые файлы.

4.3.2.2 Базовая Доверенная загрузка ПК по паролю

В базовом режиме ПАК «Блокхост-МДЗ» обеспечивает максимальную совместимость с аппаратным обеспечением ПК. В этом режиме ПАК «Блокхост-МДЗ» проводит однофакторную аутентификацию до загрузки ОС, осуществляет шифрование пользовательских дисков и контролирует целостность файлов.

Для работы в данном режиме необходимо:

1. Активировать режим «Замок», указав тип входа: по паролю;
2. Зашифровать все пользовательские диски;
3. Поставить на контроль целостности все необходимые файлы.

4.3.3 Легкая Доверенная загрузка ПК

4.3.3.1 Легкая Доверенная загрузка ПК с использованием USB-ключа eToken

Если нет потребности в шифровании дисков, ПАК «Блокхост-МДЗ» может проводить двухфакторную аутентификацию до загрузки ОС с использованием USB-ключей eToken и контролировать целостность всех необходимых файлов.

Для работы в данном режиме необходимо:

1. Активировать режим «Замок», указав тип входа: по USB-ключу eToken;
2. Поставить на контроль целостности все необходимые файлы.

4.3.3.2 Легкая Доверенная загрузка ПК по паролю

Если нет потребности в шифровании дисков и по каким-либо причинам невозможно использование USB-ключей eToken Pro\NG-FLASH\NG-OTP, ПАК «Блокхост-МДЗ» может проводить однофакторную аутентификацию до загрузки ОС и контролировать целостность всех необходимых файлов.

Для работы в данном режиме необходимо:

1. Активировать режим «Замок», указав тип входа: по паролю;
2. Поставить на контроль целостности все необходимые файлы.

5 Подсистема очистки памяти

Подсистема «Очистка памяти» контролирует определенные (критические) процессы, поставленные на контроль, и после их завершения осуществляет очистку освобождаемых областей оперативной памяти ПК, ранее использованных для хранения информации ограниченного доступа, путем записи маскирующей информации в память при ее освобождении (перераспределении).

Использование групповых политик домена позволяет централизованно выполнить установку подсистемы и загрузить список контролируемых процессов на удаленные рабочие станции.

5.1 Консоль управления подсистемы

Консоль управления подсистемы позволяет выполнять следующие действия:

- формировать список процессов, устанавливаемых на очистку памяти;
- фильтровать список процессов по заданным критериям;
- выполнять сортировку контролируемых процессов;
- осуществлять экспорт и импорт списка процессов.

Консоль управления подсистемы состоит из 5 частей (Рисунок 5.1.1):

1. Главное меню.
2. Список процессов, поставленных на очистку памяти.
3. Панель «Действия». Отображает последнее выполненное действие.
4. Панель «Команды».
5. Панель «Контроль».

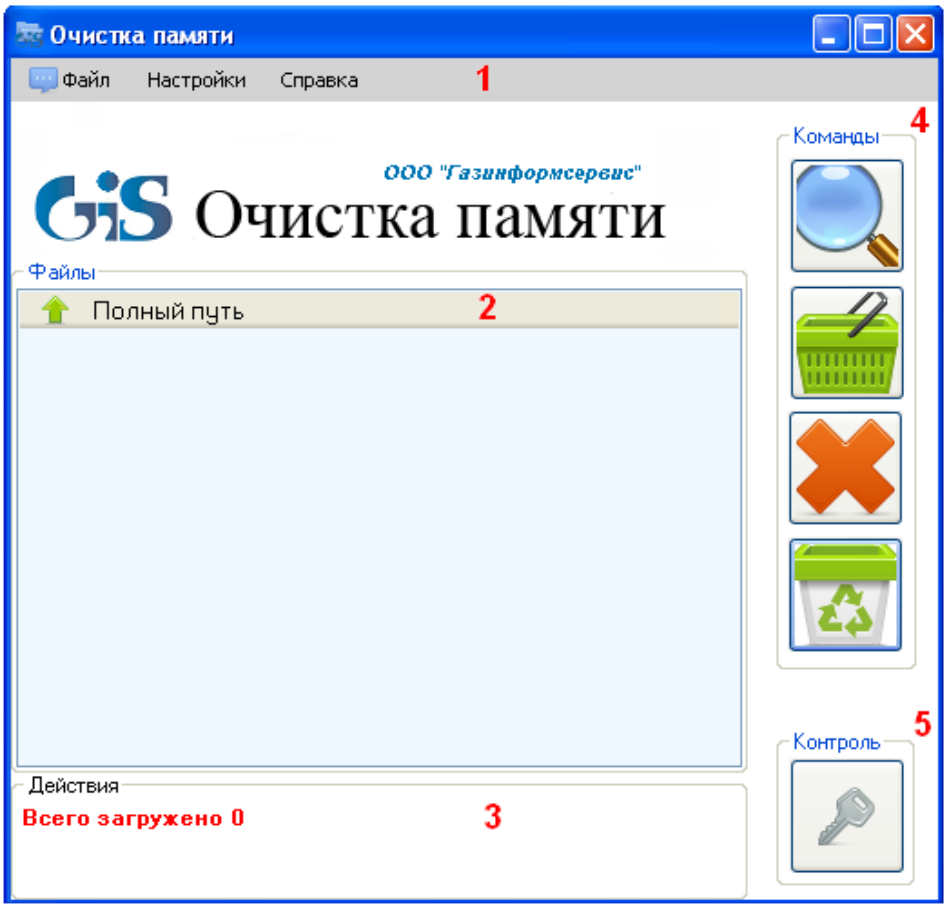

Рисунок 5.1.1 – Консоль управления подсистемы

5.1.1 Главное меню

Главное меню состоит из меню:

- Файл
- Настройки
- Справка

Меню **«Файл»** содержит следующие пункты:

- *Экспорт* – запись в текстовый файл списка имен выбранных процессов;
- *Импорт* – добавление процессов из подготовленного списка;
- *Обновить состояние* – проверка текущего состояния файлов, сравнение их с базой данных;
- *Инфо* – общая статистика по контролируемым подсистемой файлам.

В меню **«Настройки»** можно включить или отключить показ иконок, а также задать настройки протокола Syslog, и возможность получить отчет в формате .txt или .pdf. С отключенными иконками загрузка файлов и их обновление значительно ускоряется.

С помощью меню **«Справка»** → **«О программе»** можно получить информацию об организации-производителе и о версии продукта, а при вызове пункта **«Помощь»** открывается файл справки о функциях подсистемы.

5.1.2 Панель кнопок «Команды»

В главном окне подсистемы на панели «Команды» расположены следующие кнопки:

Кнопка «Добавить папку или файл». С её помощью можно поставить на очистку памяти отдельный исполняемый файл или всю папку целиком.

Буква «F» появляется в случае, когда активирован фильтр на добавление.

Кнопка «Фильтр». Позволяет сделать выборку исполняемых файлов в соответствии с заданными параметрами фильтрации (например, выбрать все файлы размером > 100 Кб).

Такой вид кнопка «Фильтр» принимает, если в настройках фильтрации заданы параметры.

Кнопка «Удалить выделенное». Используя эту функцию, можно удалить несколько выбранных файлов из списка.

Кнопка «Удалить все». Удаляет из списка все файлы, стоящие на очистке памяти.

5.1.3 Панель «Контроль»

На панели «Контроль» расположена кнопка «Статус контроля», которая имеет 2 состояния:

Состояние «включен». Это означает, что служба очистки памяти запущена. Контроль осуществляется.

Состояние «выключен». Данное состояние говорит о том, что служба очистки памяти выключена. Контроль не осуществляется.

5.2 Настройки подсистемы

5.2.1 Настройка Syslog-сервера

Для обеспечения централизованного сбора сообщений о произошедших на рабочих станциях нарушениях необходим Syslog-сервер. При обнаружении нарушения подсистема контроля целостности отправляет сообщения на Syslog-сервер.

В настройках подсистемы необходимо указать ip-адрес и порт Syslog-сервера (Рисунок 5.2.1.1):

Рисунок 5.2.1.1 – Настройка протокола Syslog

5.2.2 Получить отчет

Чтобы получить отчет о работе подсистемы необходимо выполнить следующие операции:

1. Выбрать меню «Настройки» → «Получить отчет» → «Формат файла отчета» (Рисунок 5.2.2.1).

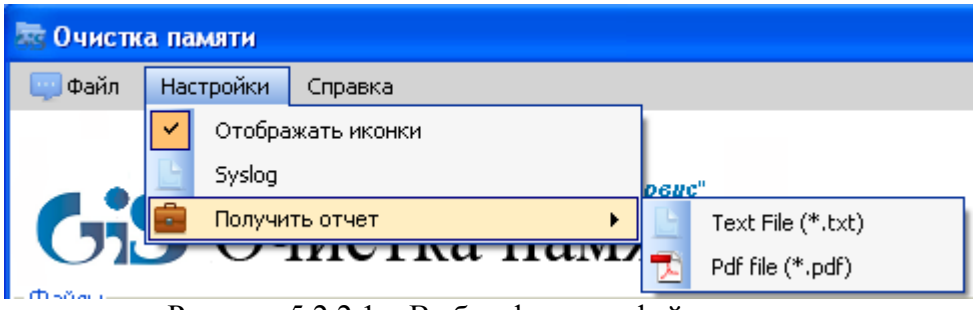

Рисунок 5.2.2.1 – Выбор формата файла отчета

2. В открывшемся окне «Сохранить как…» указать имя файла отчета и его расположение на диске, нажать кнопку «Сохранить».

В указанном месте будет сохранен файл отчета выбранного формата. Пример отчета в формате *.txt представлен на рисунке 5.2.2.2.

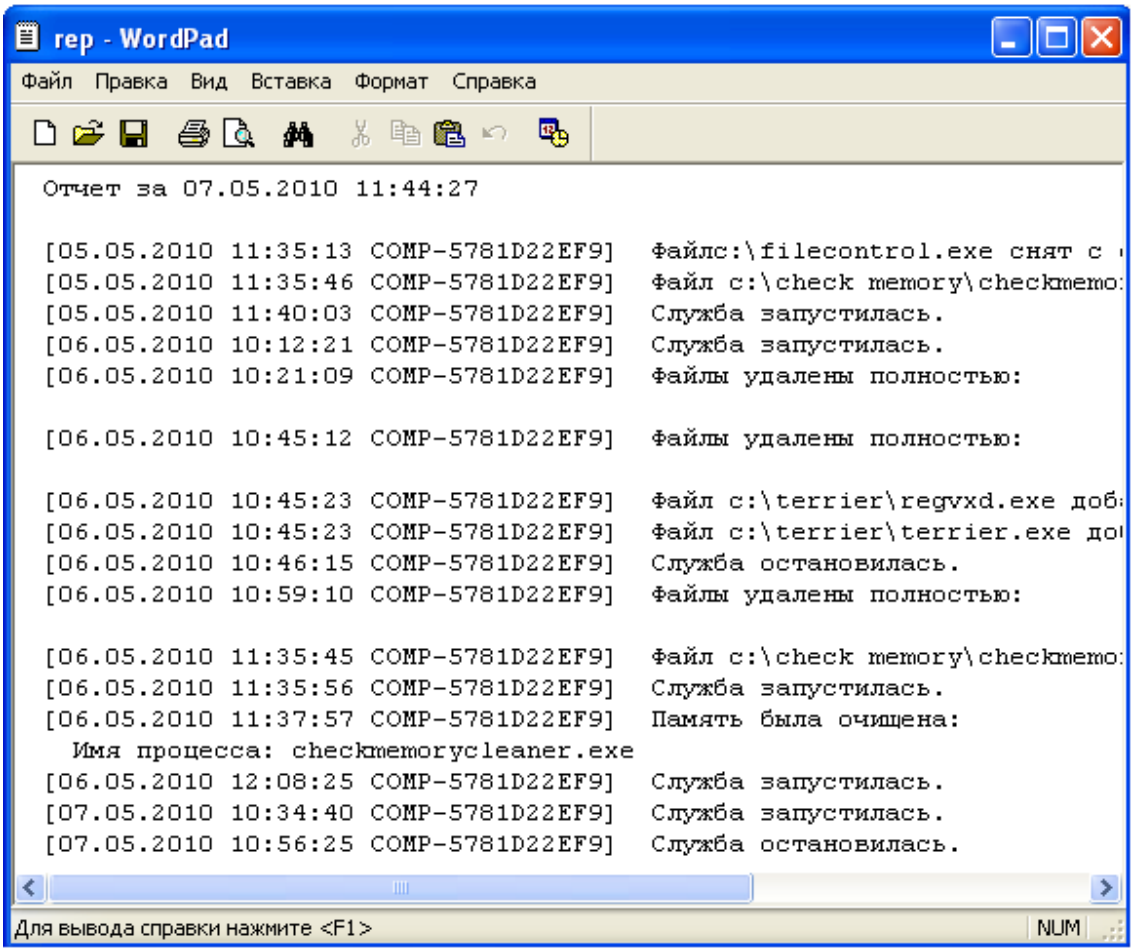

Рисунок 5.2.2.2 – Отчет о работе подсистемы очистки памяти

5.3 Работа со списком контролируемых объектов

Работа со списком подразумевает такие операции как:

- Добавление файлов и каталогов.
- Импорт.
- Экспорт.
- Удаление файлов.
- Фильтрация списка.
- Работа с использованием командной строки.

А также операции с самими файлами, вызываемые из контекстного меню (Рисунок 5.3.1):

- Показать в папке – в проводнике открывается каталог, в котором расположен выбранный файл.
- Свойства – открывается стандартное окно свойств выбранного файла.

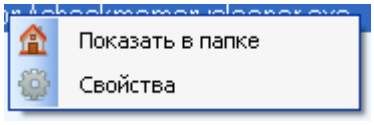

Рисунок 5.3.1 – Команды для файлов

5.3.1 Добавление файлов (каталогов)

В подсистеме «Очистки памяти» существует возможность добавлять как отдельные файлы, так и целые папки.

Добавление файлов выполняется следующими способами:

- Добавление файлов через консоль управления.
- Импорт подготовленного списка файлов (см. п. 5.3.2)
- Добавление файлов с помощью командной строки (см. п. 5.3.6)

Для добавления через консоль управления отдельного файла необходимо:

1. Нажать на кнопку **«Добавить папку или файл».**
2. В появившемся окне выбрать объект **«Файл»** (Рисунок 5.3.1.1).
3. Выбрать необходимый исполняемый файл на диске.

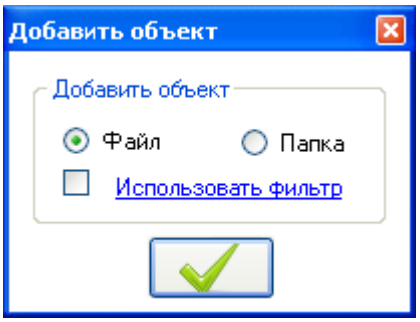

Рисунок 5.3.1.1 – Добавление файла

Добавление на контроль папки выполняется аналогично действиям при добавлении файлов.

Функция **«Использовать фильтр»** используется для того, чтобы выбрать только те файлы, которые соответствуют заданным параметрам фильтра. Чтобы выбор файлов производился с учетом фильтра, для этого необходимо включить эту функцию в окне добавления объекта (Рисунок 5.3.1.2) и нажать кнопку согласия:

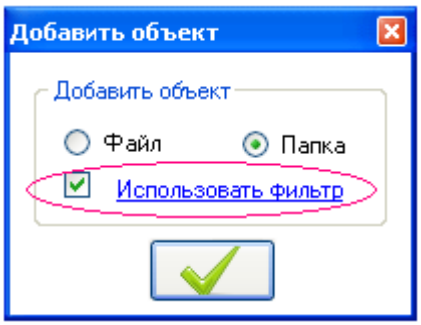

Рисунок 5.3.1.2 – Включение фильтра

Настроить фильтр можно следующим образом:

1. В диалоговом окне «Добавить объект» (Рисунок 5.3.1.1) выбрать объект «Папка» и нажать на ссылку «Использовать фильтр».
2. В открывшемся окне (Рисунок 5.3.1.3) задать параметры фильтра.

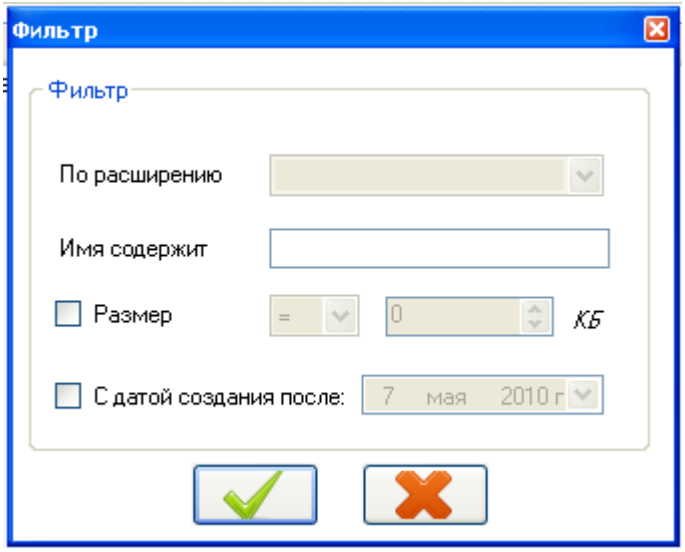

Рисунок 5.3.1.3 – Настройки фильтра

5.3.2 Импорт

Функция **«Импорт»** создана для того, чтобы исполняемые файлы, имена которых записаны в текстовом файле, были поставлены на очистку памяти. Чтобы импортировать файлы, необходимо:

1. Выбрать пункт «**Импорт**» в меню «**Файл**» или нажать сочетание клавиш Alt+I.
2. В открывшемся окне (Рисунок 5.3.2.1) ввести имена всех файлов с указанием их полного пути через точку с запятой (;) или же, нажав на кнопку «**Импорт из файла**», выбрать необходимый файл со списком добавляемых файлов.

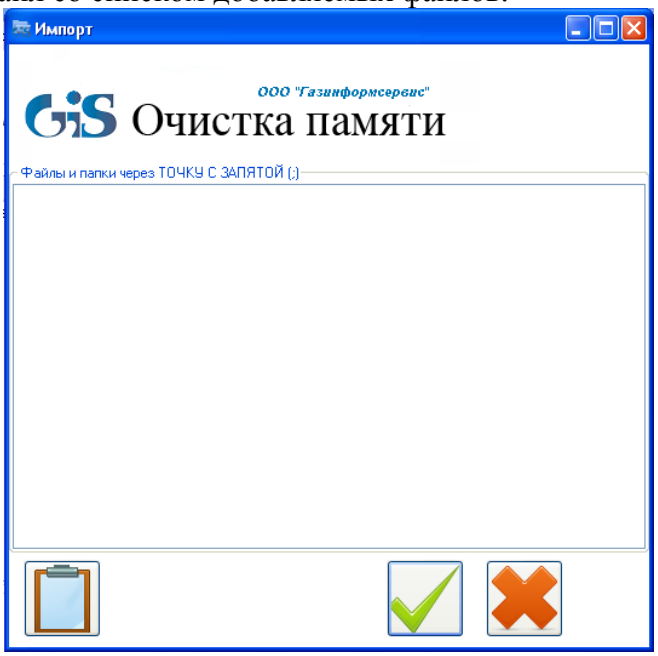

Рисунок 5.3.2.1 – Окно «Импорт»

3. Если все действия выполнены верно, в главном окне подсистемы появится список импортированных файлов.

5.3.3 Экспорт

Под экспортом понимается запись в текстовый файл списка имен выбранных файлов. Для

экспорта необходимо:

1. Выбрать пункт **«Экспорт»** в меню **«Файл»** или нажать сочетание клавиш ***Alt+E***.
2. В открывшемся окне **«Сохранить как»** указать имя и месторасположение файла.
3. Нажать кнопку **«Сохранить»**.
4. Если все действия были выполнены верно, в указанном месторасположении будет находиться файл формата *.txt, содержащий список экспортируемых файлов с указанием их полных путей через точку с запятой.

5.3.4 Удаление файлов

Удалить файлы можно несколькими способами. Пользователь может сам решить, какой способ удобнее для него.

- **Удаление одного файла:**
  Выделите файл и нажмите на клавишу **«Delete»** или на кнопку **«Удалить выбранное»**. Подтвердите удаление.
- **Удаление нескольких файлов:**
  Удерживая нажатой клавишу **«Ctrl»**, выберите необходимые файлы. Нажмите на клавишу **«Delete»** или на кнопку **«Удалить выбранное».** Подтвердите удаление.
- **Удаление всех файлов:**
  На панели нажмите на кнопку **«Удалить все»**. Подтвердите удаление.
- **Удаление файлов с использованием командной строки.**
  См. п. 5.3.6.

5.3.5 Фильтрация списка

Фильтрация списка файлов, поставленных на очистку памяти, осуществляется при помощи кнопки **«Фильтр»**, расположенной на консоли управления подсистемы. Для фильтрации списка необходимо выполнить следующие операции:

1. В главном окне подсистемы нажать на кнопку **«Фильтр»**.
2. В открывшемся окне (Рисунок 5.3.5.1) задать параметры и нажать кнопку согласия.

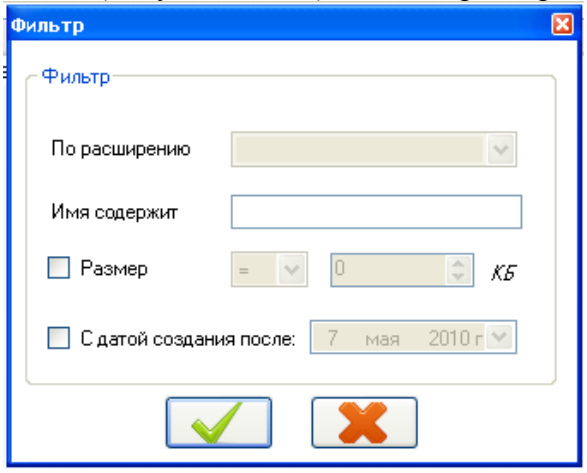

Рисунок 5.3.5.1 – Параметры фильтра

3. В главном окне подсистемы отобразятся только те файлы, которые подходят по всем заданным параметрам фильтра.

5.3.6 Использование командной строки

Использование командной строки позволяет работать со списком контролируемых объектов без использования консоли управления подсистемы.

Поддерживаются переменные окружения операционной системы.

Команды для работы с командной строкой:

- **«-process»** - включает режимы работы с очисткой памяти

- **«-add»** - добавление файлов\папок\переменных окружения (если имя файла или директории содержит пробел, то он пишется в кавычках (“”). Если требуется добавить несколько объектов, их имена пишутся через точку с запятой (;).

  Например:
  fileControl.exe -process -add c:\temp
  fileControl.exe -process -add %systemdrive%\temp

- **«-clear»** - удаление всех объектов из списка;

  Например:
  FileControl.exe -process –clear

- **«-del»** - удаление выбранных файлов\папок\переменных окружения;

  Например:
  fileControl.exe –process -del c:\temp; c:\1.xml
  fileControl.exe –process -del %systemdrive%\temp; %systemdrive%\1.xml

- **«-file»** - эта команда выполняет операции, прописанные в текстовом файле. Например, в документе прописана команда «-add;» и имена файлов. Это означает, что файл с этим именем будет добавлен на очистку памяти. Если в том же документе будет прописана команда «-del;» - то файлы, к которым она относится, будут удалены.

  В файле могут быть использованы все допустимые переменные окружения операционной системы, например %systemdrive%, %windir% и т.д.

  Например:
  fileControl.exe -process-file c:\exp.txt

- **«-filter»** - включение режима фильтрации при добавлении: **«-name»** - фильтрация по имени

  Например:
  FileControl.exe -process-file c:\exportList.txt -filter -name 1

- **«-help»** - помощь по работе с командной строкой

  Например:
  FileControl.exe -help

6 Подсистема контроля целостности

Подсистема «Контроль целостности» предназначена для периодического контроля целостности файлов и содержимого каталогов на рабочей станции.

Использование групповых политик домена позволяет централизованно выполнить установку подсистемы и загрузить список контролируемых файлов на удаленные рабочие станции.

6.1 Консоль управления подсистемы

Консоль управления подсистемы позволяет выполнять следующие действия:

- формировать список файлов и каталогов, устанавливаемых на контроль;
- отслеживать текущее состояние файлов и каталогов;
- фильтровать файлы по заданным критериям;
- выполнять сортировку контролируемых файлов;
- осуществлять экспорт и импорт списка файлов;
- просматривать общую статистику по контролируемым файлам и каталогам.

Консоль управления подсистемы состоит из 5 частей (Рисунок 6.1.1):

1. Главное меню.
2. Список файлов и каталогов, поставленных на контроль.
3. Панель «Действия». Отображает последнее выполненное действие.
4. Панель кнопок «Команды».
5. Панель «Контроль».

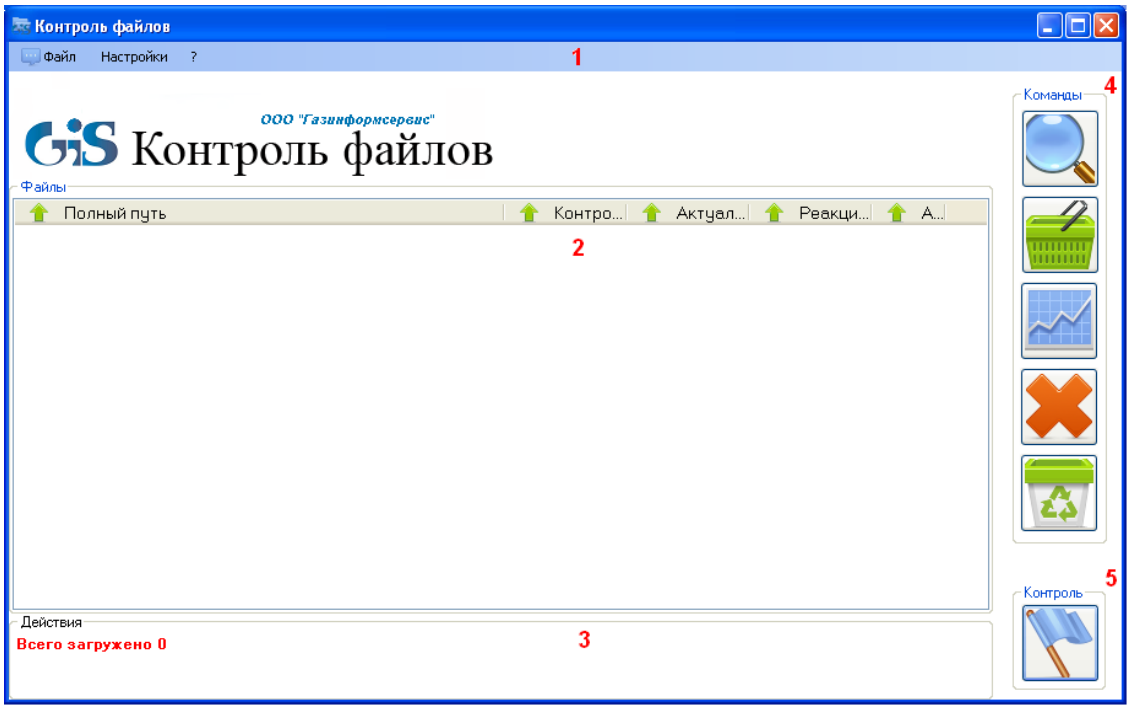

Рисунок 6.1.1 – Консоль управления подсистемы

6.1.1 Главное меню

Главное меню состоит из меню:

- Файл
- Настройки

- Справка

Меню **«Файл»** содержит следующие пункты:

- *Экспорт* – запись в текстовый файл списка имен выбранных файлов;
- *Импорт* – добавление файлов из подготовленного списка;
- *Обновить состояние* – проверка текущего состояния файлов, сравнение их с базой данных;
- *Инфо* – общая статистика по контролируемым подсистемой файлам.

В меню **«Настройки»** можно выбрать алгоритм подсчёта контрольных сумм (CRC32 или MD5)**,** включить или отключить показ иконок, а также задать настройки протокола Syslog и периодичность контроля целостности файлов. С отключенными иконками загрузка файлов и их обновление значительно ускоряется.

С помощью меню **«Справка» → «О программе»** можно получить информацию об организации-производителе и о версии продукта, а при вызове пункта **«Помощь»** открывается файл справки о функциях подсистемы.

6.1.2 Панель кнопок «Команды»

В главном окне подсистемы на панели «Команды» расположены следующие кнопки:

Кнопка «Добавить папку или файл». С её помощью можно поставить на контроль целостности отдельный файл или всю папку целиком.

Буква «F» появляется в случае, когда активирован фильтр на добавление.

Кнопка «Фильтр». Позволяет сделать выборку контролируемых файлов в соответствии с заданными параметрами фильтрации (например, выбрать все файлы с расширением *.exe или *.dll).

Такой вид кнопка «Фильтр» принимает, если в настройках фильтрации заданы параметры.

Кнопка «Показать нарушения». С помощью этой функции будут показываться файлы, целостность которых была нарушена.

Кнопка «Показать нарушения» принимает такой вид в том случае, когда в списке показаны только нарушения. Повторное нажатие приведет к тому, что в списке появятся все файлы.

Кнопка «Удалить выделенное». Используя эту функцию, можно удалить несколько выбранных файлов из списка.

Кнопка «Удалить все». Удаляет из списка все файлы, стоящие на контроле целостности.

6.1.3 Панель «Контроль»

На панели «Контроль» расположена кнопка «Статус контроля», которая имеет 2 состояния:

Состояние «включен». Это означает, что служба контроля целостности запущена. Контроль осуществляется.

Состояние «выключен». Данное состояние говорит о том, что служба контроля целостности выключена. Контроль не осуществляется.

6.2 Настройки подсистемы

6.2.1 Периодичность контроля

Пункт **«Периодичность контроля»** в меню **«Настройки»** позволяет настроить интервал времени, через который будет производиться проверка файлов, стоящих на контроле. По умолчанию устанавливается значение, равное 1 минуте; интервал не должен превышать 24 часов (Рисунок 6.2.1.1).

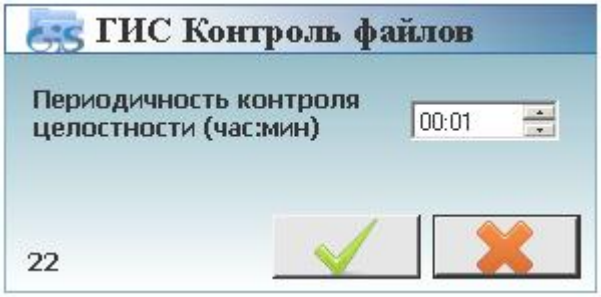

Рисунок 6.2.1.1 - Установка периода контроля целостности

Для применения настроек после изменения периодичности контроля целостности в консоли управления подсистемы контроля целостности необходимо выключить контроль и включить его заново (п. 6.1.3. настоящего документа).

6.2.2 Настройка Syslog-сервера

Для обеспечения централизованного сбора сообщений о произошедших на рабочих станциях нарушениях необходим Syslog-сервер. При обнаружении нарушения подсистема контроля целостности отправляет сообщения на Syslog-сервер.

В настройках подсистемы необходимо указать ip-адрес и порт Syslog-сервера (Рисунок 6.2.2.1):

Рисунок 6.2.2.1 – Настройка протокола Syslog

6.2.3 Получить отчет

Чтобы получить отчет о работе подсистемы необходимо выполнить следующие операции:

1. Выбрать меню «Настройки» → «Получить отчет» → «Формат файла отчета» (Рисунок 5.2.2.1).

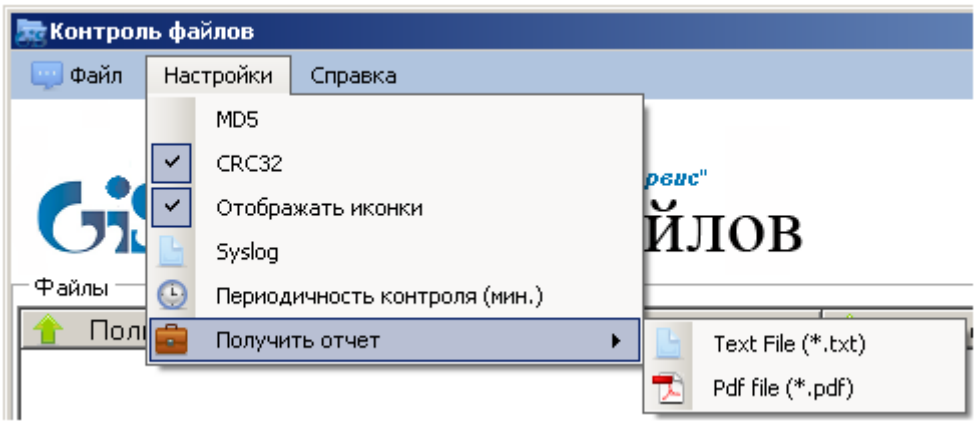

Рисунок 6.2.3.1 – Выбор формата файла отчета

2. В открывшемся окне «Сохранить как…» указать имя файла отчета и его расположение на диске, нажать кнопку «Сохранить».

В указанном месте будет сохранен файл отчета выбранного формата. Пример отчета в формате *.txt представлен на рисунке 6.2.3.2.

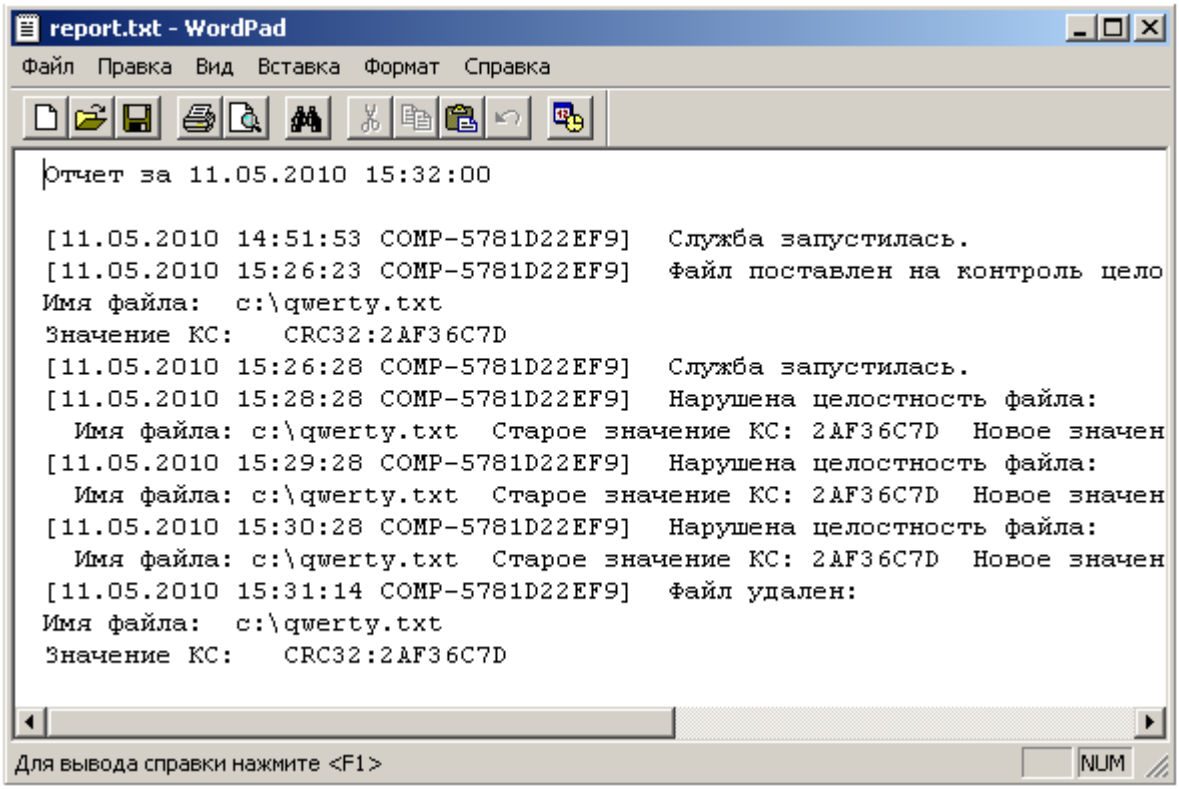

Рисунок 6.2.3.2 – Отчет о работе подсистемы очистки памяти

6.3 Работа со списком контролируемых объектов

Работа со списком подразумевает такие операции как:

- Добавление файлов и каталогов.
- Импорт.
- Экспорт.
- Удаление файлов.
- Фильтрация списка.
- Работа с использованием командной строки.

А также операции с самими файлами, вызываемые из контекстного меню (Рисунок 6.3.1):

- Пересчитать – пересчитывается контрольная сумма выбранного файла в соответствии с указанным в настройках алгоритмом.
- Показать в папке – в проводнике открывается каталог, в котором расположен выбранный файл.
- Свойства – открывается стандартное окно свойств выбранного файла.

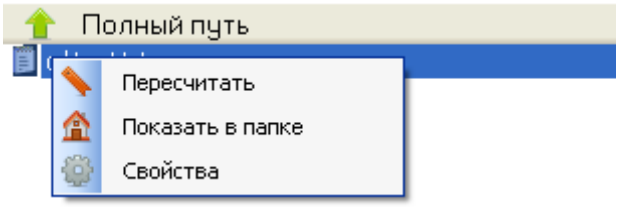

Рисунок 6.3.1 – Команды для файлов

6.3.1 Добавление файлов (каталогов)

В подсистеме «Контроль целостности» существует возможность добавлять как отдельные файлы, так и целые папки.

Добавление файлов выполняется следующими способами:

- Добавление файлов через консоль управления.
- Импорт подготовленного списка файлов (см. п. 6.3.2)
- Добавление файлов с помощью командной строки (см. п. 6.3.6)

Для добавления через консоль управления отдельного файла необходимо:

1. Нажать на кнопку **«Добавить папку или файл».**
2. В появившемся окне выбрать объект **«Файл»** (Рисунок 6.3.1.1).
3. Выбрать необходимый файл на диске.

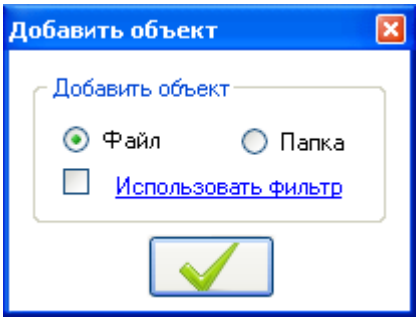

Рисунок 6.3.1.1 – Добавление файла

Добавление на контроль папки выполняется аналогично действиям при добавлении файлов.

Функция **«Использовать фильтр»** используется для того, чтобы выбрать только те файлы,

которые соответствуют заданным параметрам фильтра. Чтобы выбор файлов производился с учетом фильтра, для этого необходимо включить эту функцию в окне добавления объекта (Рисунок 6.3.1.2) и нажать кнопку согласия:

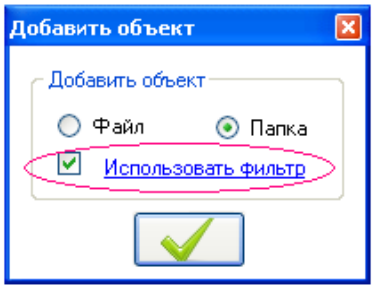

Рисунок 6.3.1.2 – Включение фильтра

Настроить фильтр можно следующим образом:

1. В диалоговом окне «Добавить объект» (Рисунок 6.3.1.1) выбрать объект «Папка» и нажать на ссылку «Использовать фильтр».
2. В открывшемся окне (Рисунок 6.3.1.3) задать параметры фильтра.

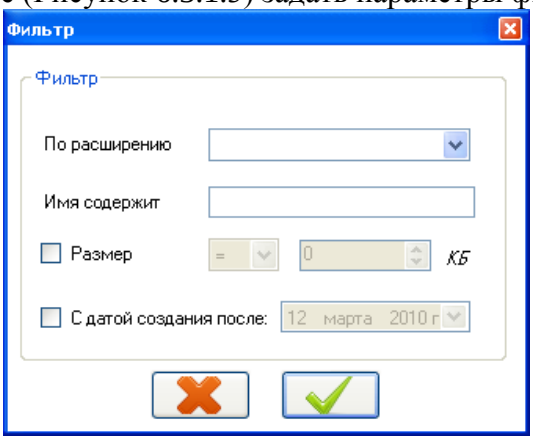

Рисунок 6.3.1.3 – Настройки фильтра

Чтобы выполнить фильтрацию по нескольким расширениям, необходимо в поле ввода **«По расширению»** ввести все необходимы расширения через точку с запятой.

6.3.2 Импорт

Функция **«Импорт»** создана для того, чтобы файлы, имена которых записаны в текстовом файле, были добавлены на контроль целостности. Чтобы импортировать файлы, необходимо:

1. Выбрать пункт «**Импорт**» в меню «**Файл**» или нажать сочетание клавиш Alt+I.
2. В открывшемся окне (Рисунок 6.3.2.1) ввести имена всех файлов с указанием их полного пути через точку с запятой (;) или же, нажав на кнопку «**Импорт из файла**», выбрать необходимый файл со списком добавляемых файлов.

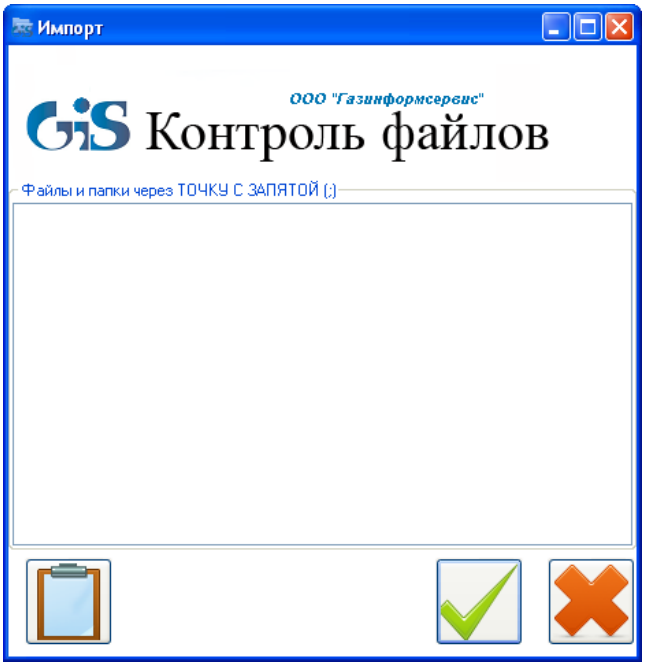

Рисунок 6.3.2.1 – Окно «Импорт»

3. Если все действия выполнены верно, в главном окне подсистемы появится список импортированных файлов.

6.3.3 Экспорт

Под экспортом понимается запись в текстовый файл списка имен выбранных файлов. Для экспорта необходимо:

1. Выбрать пункт **«Экспорт»** в меню **«Файл»** или нажать сочетание клавиш ***Alt+E***.
2. В открывшемся окне **«Сохранить как»** указать имя и месторасположение файла.
3. Нажать кнопку **«Сохранить».**
4. Если все действия были выполнены верно, в указанном месторасположении будет находиться файл формата *.txt, содержащий список экспортируемых файлов с указанием их полных путей через точку с запятой.

6.3.4 Удаление файлов

Удалить файлы (снять с контроля) можно несколькими способами. Пользователь может сам решить, какой способ удобнее для него.

- **Удаление одного файла:**
  Выделите файл и нажмите на клавишу **«Delete»** или на кнопку **«Удалить выбранное»**. Подтвердите удаление.
- **Удаление нескольких файлов:**
  Удерживая нажатой клавишу «**Ctrl**», выберите необходимые файлы. Нажмите на клавишу **«Delete»** или на кнопку **«Удалить выбранное».** Подтвердите удаление.
- **Удаление всех файлов:**
  На панели нажмите на кнопку **«Удалить все»**. Подтвердите удаление.
- **Удаление файлов с использованием командной строки.**
  См. п. 6.3.6.

6.3.5 Фильтрация списка

Фильтрация списка файлов, поставленных на контроль, осуществляется при помощи кнопки **«Фильтр»**, расположенной на консоли управления подсистемы. Для фильтрации списка необходимо выполнить следующие операции:

1. В главном окне подсистемы нажать на кнопку **«Фильтр»**.
2. В открывшемся окне (Рисунок 6.3.5.1) задать параметры и нажать кнопку согласия.

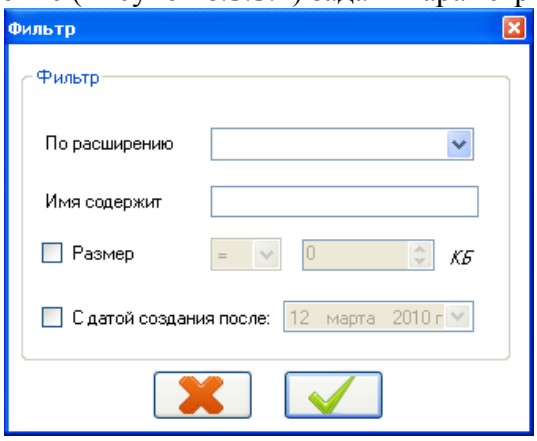

Рисунок 6.3.5.1 – Параметры фильтра

3. В главном окне подсистемы отобразятся только те файлы, которые подходят по всем заданным параметрам фильтра.

6.3.6 Использование командной строки

Работа со списком с использованием командной строки предназначена для оперативной обработки файлов, чтобы не открывать главное окно подсистемы «Контроль целостности».

Поддерживаются переменные окружения операционной системы.

Команды для работы с командной строкой:

- **«-add»** - добавление объекта (постановка на контроль целостности). Если требуется добавить несколько объектов, они пишутся через точку с запятой (;).
  Например:
  FileControl.exe –add c:\test.txt
  FileControl.exe -add %systemdrive%\temp
  FileControl.exe –add c:\test.txt; c:\text.doc
  FileControl.exe -add %systemdrive%\temp; %systemdrive%\1.xml

- **«-clear»** - удаление всех файлов из списка.
  Например:
  FileControl.exe –clear

- **«-del»** - удаление выбранных файлов.
  Например:
  FileControl.exe -del c:\temp; c:\1.xml
  FileControl.exe -del %systemdrive%\temp; %systemdrive%\1.xml

- **«-file»** - эта команда выполняет операции, прописанные в текстовом файле. Например, в документе прописана команда «-add» и имена файлов. Это означает, что файл с этим именем будет добавлен на контроль. Если в том же документе будет прописана команда «-del», то файлы, к которым она относится, будут удалены. В файле могут быть использованы все допустимые переменные окружения операционной системы, например %systemdrive%, %windir% и т.д.
  Например:
  FileControl.exe -file c:\exp.txt

- **«-filter»** - включение режима фильтрации при добавлении:

- **«-ext»** - фильтрация по расширениям
  Например:
  FileControl.exe -file c:\exportList.txt -filter -ext *.exe; *.dll
- **«-name»** - фильтрация по имени
  Например:
  FileControl.exe -file c:\exportList.txt -filter -name 1

- **«-hash»** - параметр определения типа контрольной суммы (1-MD5, 2-CRC32).
  Например:
  FileControl.exe -file c:\exp.txt -hash 2

- **«-reload»** - пересчет всех нарушенных контрольных сумм.
  Например:
  FileControl.exe –reload

- **«-interval»** - установка интервала проверки в секундах.
  Например:
  FileControl.exe -interval 3600

- **«-syslog»** - установка адреса Syslog-сервера.
  Например:
  FileControl.exe -syslog 192.168.0.1:514

- **«-help»** - помощь по работе с командной строкой.
  Например:
  FileControl.exe -help

6.4 Просмотр событий

6.4.1 Оповещение об инцидентах

Если в системе произошло событие, которое требует внимания пользователя/администратора, то пиктограмма ПАК «Блокхост-МДЗ» примет вид:  , и появится сообщение о произошедшем событии (Рисунок 6.4.1.1).

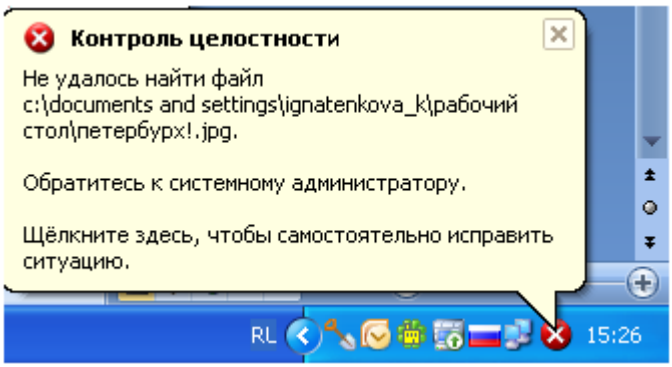

Рисунок 6.4.1.1 – Оповещение о нарушении

Чтобы посмотреть нарушение в консоли управления подсистемы необходимо щелкнуть по сообщению. В открывшемся окне **«Запуск от имени другого пользователя»** выбрать учетную запись администратора, ввести пароль и нажать кнопку **«ОК»**. В результате откроется консоль управления подсистемы, в которой отображаются все нарушения (см. п. 6.4.2).

6.4.2 Просмотр нарушений

Если нарушения произошли в ранее добавленном каталоге, то при открытии главного окна подсистемы в списке этот каталог будет выделен розовым цветом (Рисунок 6.4.2.1).

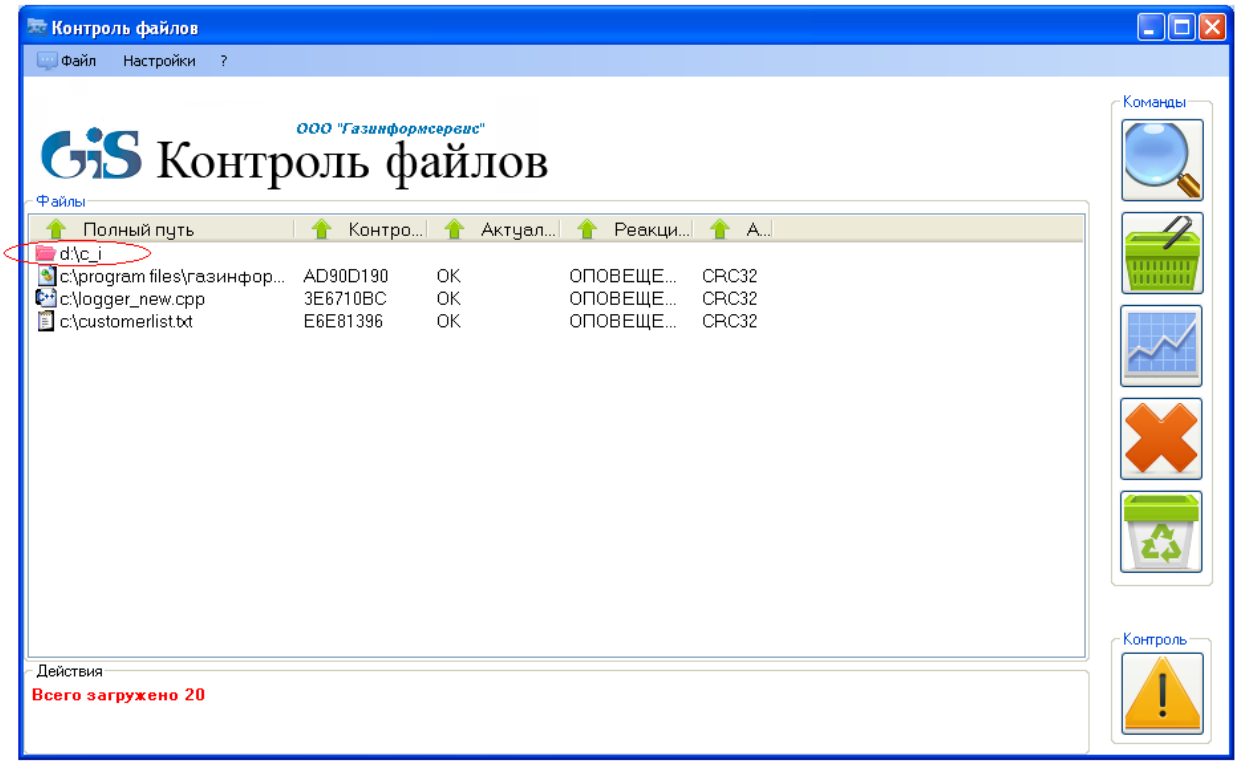

Рисунок 6.4.2.1 – Нарушения в каталоге

С помощью кнопки **«Показать нарушения»** можно осуществить поиск удаленных файлов, файлов, целостность которых была нарушена, и файлов, доступ к которым запрещен. В результате нажатия на кнопку **«Показать нарушения»** в списке будут скрыты файлы, которые не были изменены/удалены, и останутся только поврежденные и недоступные файлы (Рисунок 6.4.2.2). Строки могут быть подсвечены следующими цветами:

- Розовым – если файл удален.
- Красным – если файл изменен.
- Желтым – если доступ к файлу запрещен (например, файл занят другим приложением).

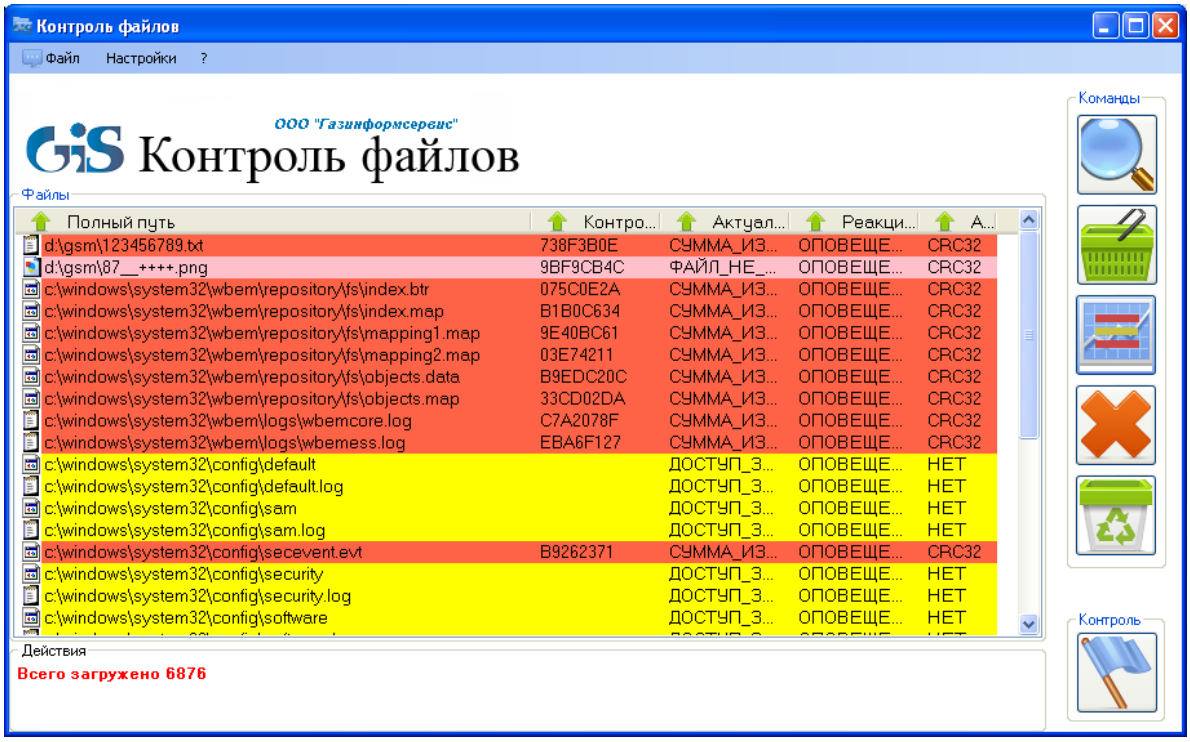

Рисунок 6.4.2.2 – Нарушения целостности файлов

7 Подсистема контроля целостности для Linux

Описание подсистемы контроля целосности для Linux приведено в документе «Программно-аппаратный комплекс доверенной загрузки «Блокхост-МДЗ». Подсистема контроля целостности для Linux. Описание применения».

8 Подсистема гарантированного удаления

Подсистема гарантированного удаления ПАК «Блокхост-МДЗ» состоит из двух отдельных модулей, устанавливаемых по выбору пользователя:

- модуль гарантированного удаления всех объектов файловой системы на ПЭВМ, удаляемых стандартным способом;
- модуль гарантированного удаления выбранных объектов файловой системы по требованию пользователя.

8.1 Подсистема гарантированного удаления, работающая в активном режиме

Подсистема гарантированного удаления ПАК «Блокхост-МДЗ» всегда активна и запрещает удаление файлов стандартным способом. Удаление файлов происходит трехкратным затиранием содержимого по специальному алгоритму, исключающему считывание остаточной информации на диске после удаления.

Работа подсистемы гарантированного удаления несовместима со стандартным мастером записи дисков ОС Windows, в случае, *если записываемые на CD данные находятся на системном диске* (например, на диске C:\). В связи с особенностями работы стандартного мастера записи дисков, информация, находящаяся на системном диске и записываемая на CD, «затирается».

Если файлы, которые требуется записать на CD-диск, находятся не на системном диске (например, на диске D:\), то конфликта не происходит.

В качестве рекомендации предлагается не использовать стандартную программу записи на CD-файлов непосредственно с системного диска. Если требуется записать на CD-диск файлы, расположенные на системном диске, то их необходимо предварительно скопировать на другой логический диск и с него уже можно осуществлять запись на CD стандартными средствами ОС Windows.

8.2 Подсистема гарантированного удаления по требованию

Описание подсистемы гарантированного удаления по требованию приведено в документе «Программно-аппаратный комплекс доверенной загрузки «Блокхост-МДЗ». Подсистема гарантированного удаления по требованию. Описание применения».