GIS ГАЗИНФОРМ СЕРВИС

Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4»

Руководство администратора безопасности

Часть 5. Подсистема гарантированного удаления по требованию

Санкт-Петербург, 2021

Аннотация

Настоящий документ содержит описание применения подсистемы гарантированного удаления по требованию средства защиты информации от несанкционированного доступа «Блокхост-Сеть 4» (далее по тексту – СЗИ от НСД «Блокхост-Сеть 4», СЗИ или средство).

В документе также приводится описание инсталляции и деинсталляции подсистемы гарантированного удаления по требованию.

Содержание

Введение

СЗИ от НСД «Блокхост-Сеть 4» является программным средством защиты информации от несанкционированного доступа к информации, предназначенным для комплексной и многофункциональной защиты информационно-программных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах на базе персональных компьютеров под управлением операционных систем (ОС) Microsoft Windows 2008R2/7/8.1/2012/2012R2/10/2016/2019.

СЗИ от НСД «Блокхост-Сеть 4» состоит из клиентской части, которая устанавливается на рабочие станции в сети, и серверной части, которая устанавливается на серверы безопасности и к которой обращаются администраторы безопасности для централизованного управления подчиненными серверами, группами и рабочими станциями в сети.

Степени важности примечаний:

Важная информация
Указания, требующие особого внимания.

Дополнительная информация
Указания, позволяющие упростить работу с подсистемой.

1 Назначение подсистемы гарантированного удаления по требованию

Подсистема гарантированного удаления по требованию (далее подсистема ГУПТ) предназначена для осуществления гарантированного удаления выбранных объектов файловой системы с носителя информации (за исключением оптических дисков) без возможности их дальнейшего восстановления. Удаление выбранных файлов происходит троекратным затиранием содержимого кластеров носителя информации по специальному алгоритму, исключающему считывание остаточной информации на диске после их удаления.

Подсистема гарантированного удаления по требованию может применяться как в составе СЗИ от НСД «Блокхост-Сеть 4», так и отдельно от него.

2 Инсталляция подсистемы ГУПТ

2.1 Локальная инсталляция подсистемы ГУПТ

Консоль управления подсистемы ГУПТ имеет графический интерфейс. Установка подсистемы производится с компакт-диска или другого носителя. Дистрибутив подсистемы поставляется в виде файла инсталлятора Microsoft Windows Installer:

- *GIS.WipeFiles<№_версии>.msi (для 32-bit ОС);*
- *GIS.WipeFiles<№_версии>x64.msi (для 64-bit ОС).*

Для установки подсистемы ГУПТ на рабочую станцию необходимо войти в ОС под учетной записью с правами администратора и запустить файл инсталлятора (*GIS.WipeFiles<№_версии>.msi* или *GIS.WipeFiles<№_версии>x64.msi*), дважды щелкнув по нему левой клавишей мыши. На экране монитора появится диалоговое окно приветствия мастера установки (Рисунок 2.1), в котором необходимо нажать кнопку ***Далее***.

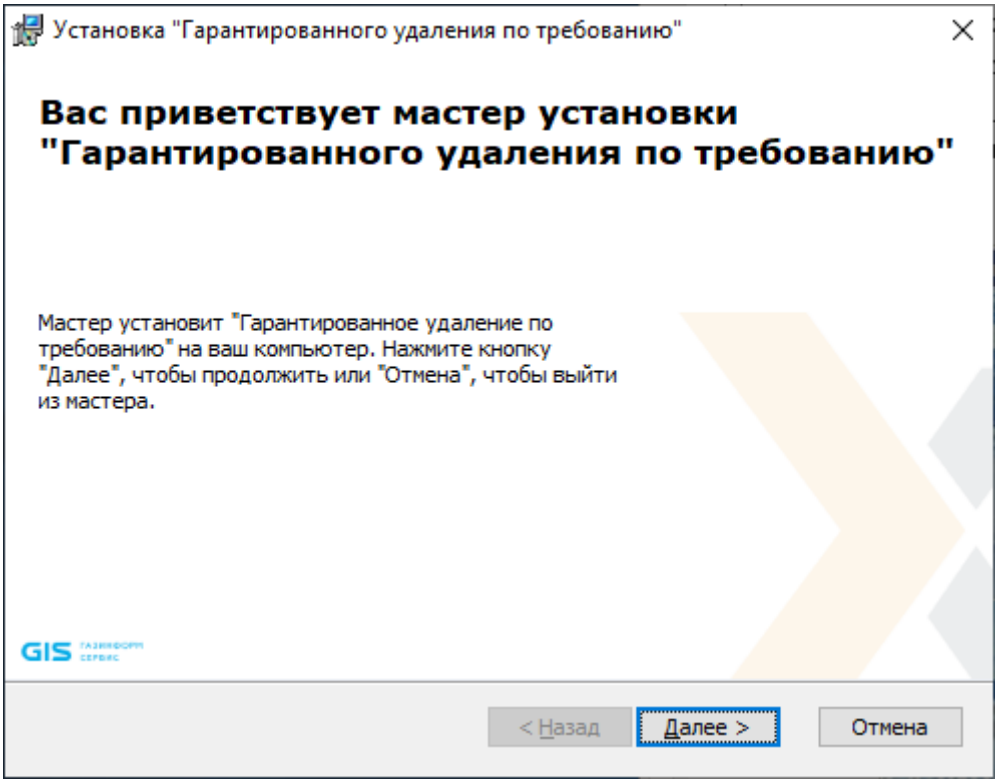

Рисунок 2.1 – Окно установки подсистемы

Для прекращения установки подсистемы ГУПТ можно в любой момент работы мастера установки нажать кнопку ***Отмена***, после чего появится окно, показанное на Рисунок 2.2. При нажатии на кнопку ***Да*** работа мастера установки будет прервана, при нажатии ***Нет*** – продолжена.

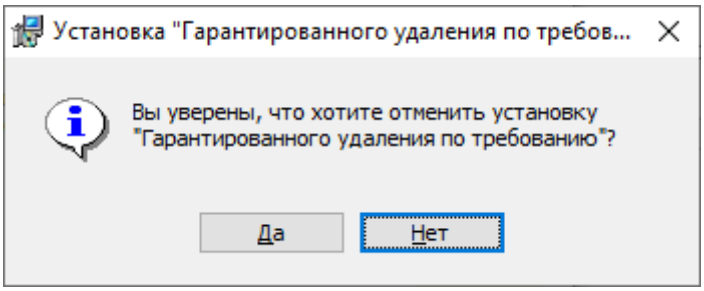

Рисунок 2.2 – Диалоговое окно отмены установки

На следующем этапе работы мастера установки на экране монитора появится окно выбора каталога установки подсистемы ГУПТ (Рисунок 2.3). Можно согласиться с каталогом установки, указанным по умолчанию (*C:\Program Files (x86)\GIS\Гарантированное удаление по требованию*), или выбрать иной. После выбора каталога установки следует нажать кнопку ***Далее***.

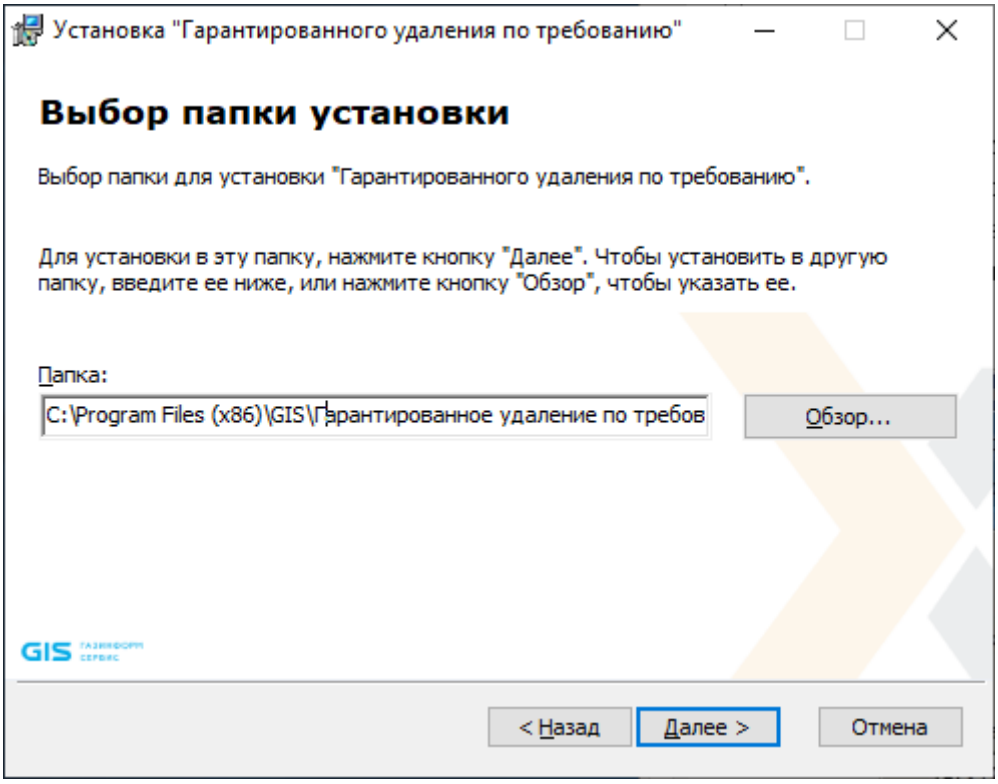

Рисунок 2.3 – Окно выбора каталога установки

На следующем шаге работы мастера установки откроется окно, сигнализирующее о готовности к установке (Рисунок 2.4). После нажатия на кнопку ***Установить*** начнется фактическая установка подсистемы ГУПТ на рабочую станцию.

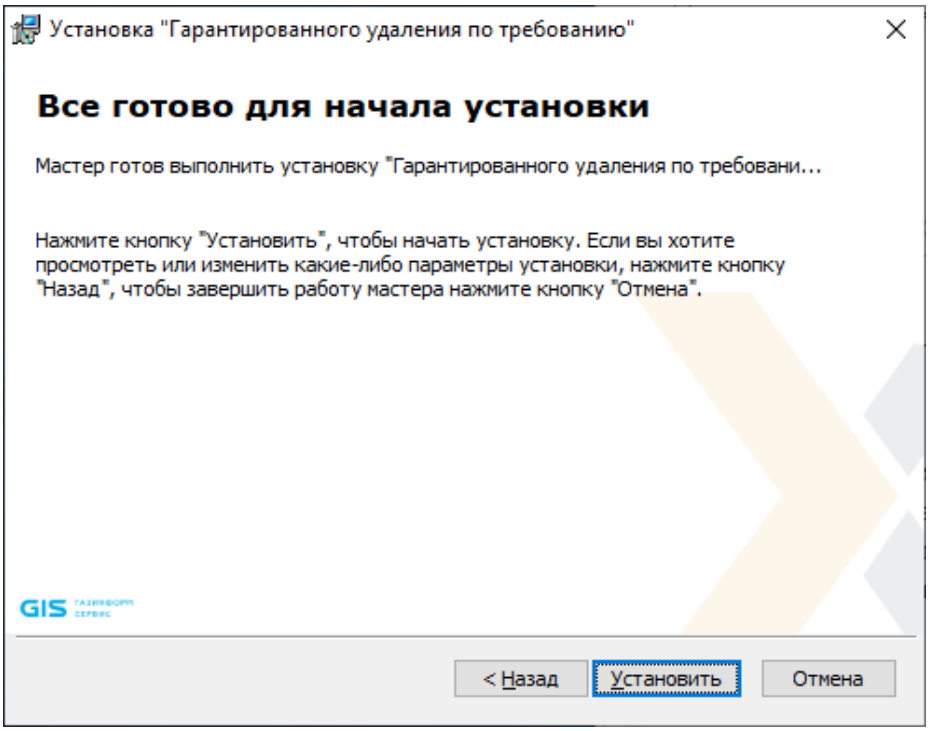

Рисунок 2.4 – Окно начала установки

По окончании процесса инсталляции для завершения работы мастера установки подсистемы необходимо нажать ***Готово*** (Рисунок 2.5). Если при этом установить указатель напротив пункта ***Запустить «Гарантированное удаление по требованию»***, то после нажатия кнопки ***Готово*** будет запущена консоль управления подсистемой ГУПТ.

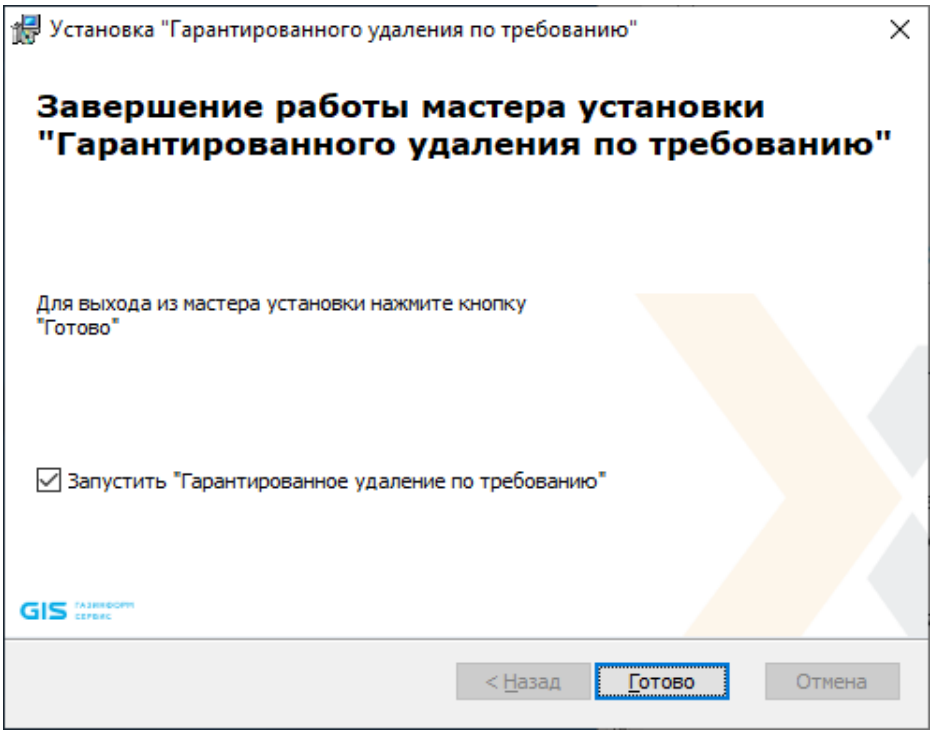

Рисунок 2.5 – Окно завершения работы мастера установки

В дальнейшем запустить консоль управления подсистемой гарантированного удаления по требованию можно, нажав на панели задач кнопку ***Пуск*** и выбрав пункт ***Гарантированное удаление по требованию***:

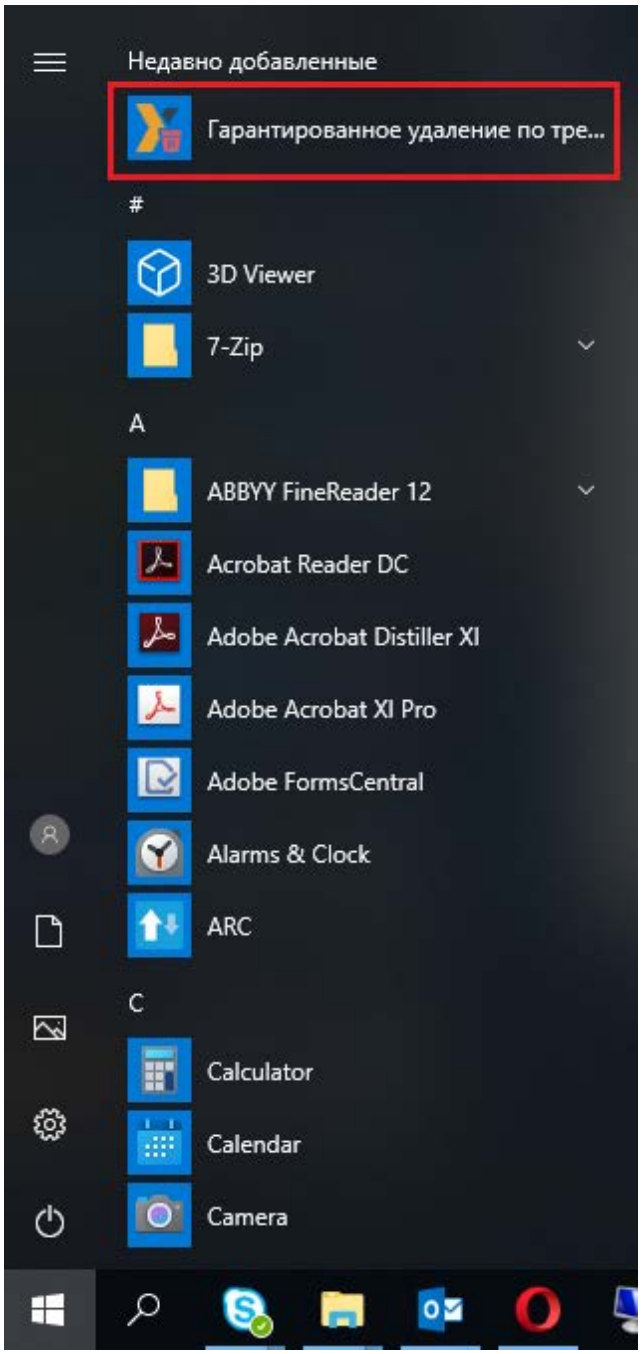

Рисунок 2.6 – Запуск консоли управления подсистемой ГУПТ

Также запустить программу можно при помощи ярлыков вызова программы на рабочем столе, которые создаются в процессе установки подсистемы ГУПТ на рабочую станцию:

 – ярлык запуска консоли подсистемы ГУПТ;

 – ярлык запуска функции гарантированного удаления файлов из корзины.

Одновременное использование подсистемы ГУПТ и модуля гарантированного удаления, работающего в активном режиме, в составе СЗИ от НСД «Блокхост-Сеть 4», является нецелесообразным.

2.2 Инсталляция подсистемы ГУПТ с помощью системы развертывания

Для установки подсистемы ГУПТ с помощью системы развертывания СЗИ от НСД «Блокхост-Сеть 4» на рабочие станции необходимо отредактировать параметры автоматически созданной в подсистеме развертывания задачи на установку подсистемы ГУПТ:

- сформировать список рабочих станций, на которые будет устанавливаться подсистемы ГУПТ;
- указать параметры расписания установки подсистемы ГУПТ на рабочие станции;
- указать параметры перезагрузки рабочей станции после окончания установки на нее подсистемы ГУПТ.

После редактирования выполнить запуск задачи по установке подсистемы ГУПТ, если в настройках задан запуск задачи вручную.

Подробная установка подсистемы ГУПТ с помощью системы развертывания описана в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит».

2.3 Структура файловой системы подсистемы ГУПТ

Подсистема ГУПТ СЗИ от НСД «Блокхост-Сеть 4» состоит из объектов файловой системы, представленных в Таблица 2.1.

Таблица 2.1 – Файлы подсистемы гарантированного удаления по требованию

№ п/п	Имя файла	Описание файла
1	GIS.WipeFile.exe	Модуль графического интерфейса подсистемы
2	GIS.MenuExt.dll	Библиотека, отвечающая за добавление контекстного меню

3 Деинсталляция подсистемы ГУПТ

Для удаления подсистемы ГУПТ с рабочей станции необходимо последовательно пройти через меню ***Пуск*** →***Панель управления*** → ***Программы и компоненты***, выбрать программу «Гарантированное удаление по требованию» и нажать кнопку ***Удалить***. Появится запрос подтверждения удаления:

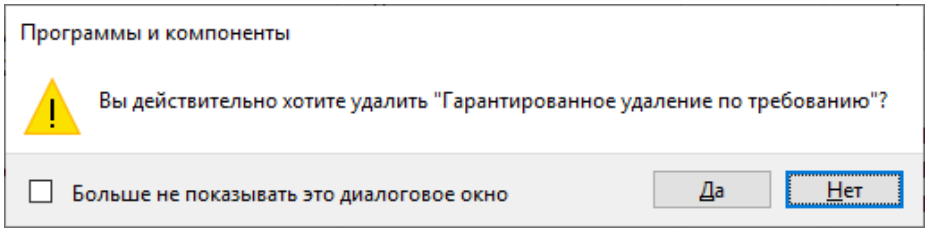

Рисунок 3.1 – Запрос подтверждения удаления

После подтверждения удаления начнется процесс удаления подсистемы (Рисунок 3.2). После его завершения подсистема ГУПТ будет удалена с рабочей станции.

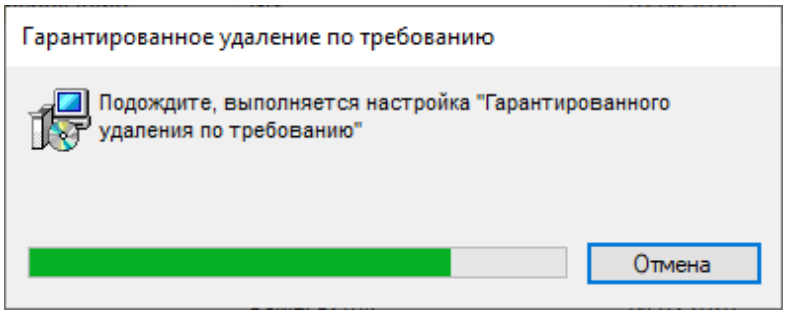

Рисунок 3.2 – Ход удаления подсистемы ГУПТ

4 Работа с консолью управления подсистемы ГУПТ

4.1 Запуск консоли управления подсистемы

Управление подсистемой ГУПТ осуществляется через консоль управления. Запустить консоль управления может только пользователь, учетная запись которого включена в группу Администраторы локального компьютера.

Для запуска консоли управления необходимо нажать на панели задач кнопку ***Пуск*** и выбрать пункт ***Гарантированное удаление по требованию***:

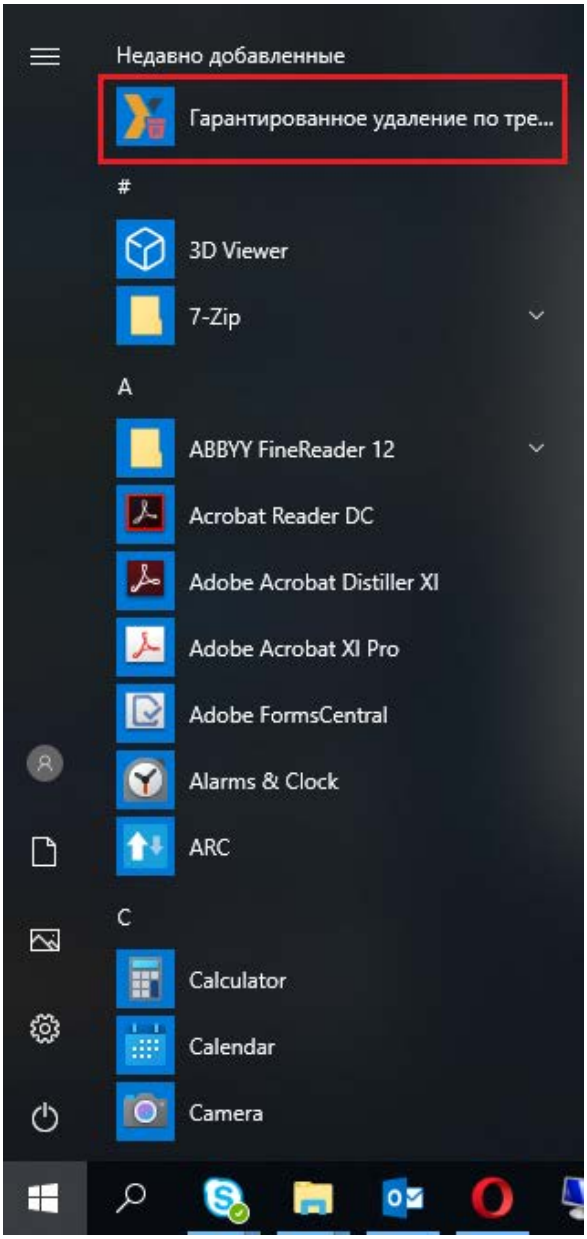

Рисунок 4.1 – Запуск консоли управления подсистемой

Запустить консоль управления подсистемой ГУПТ можно также при помощи ярлыка вызова программы  , расположенном на рабочем столе.

4.2 Внешний вид консоли управления подсистемы

Консоль управления подсистемы позволяет выполнять следующие действия:

- формировать список файлов и папок, подлежащих гарантированному удалению;
- определять размер псевдослучайной последовательности символов, которыми будут заполняться кластеры носителей информации при выполнении гарантированного удаления;
- гарантированно удалять выбранные файлы и папки;
- гарантированно очищать (заполнять псевдослучайной последовательностью символов) свободное пространство разделов жестких дисков.

Внешний вид консоли управления подсистемы представлен на Рисунок 4.2.

Консоль управления подсистемы состоит из 4 областей:

1 – Главное меню;

2 – Область данных (содержит список файлов и папок, устанавливаемых на гарантированное удаление);

3 – Область программных кнопок;

4 – Строка прогресса.

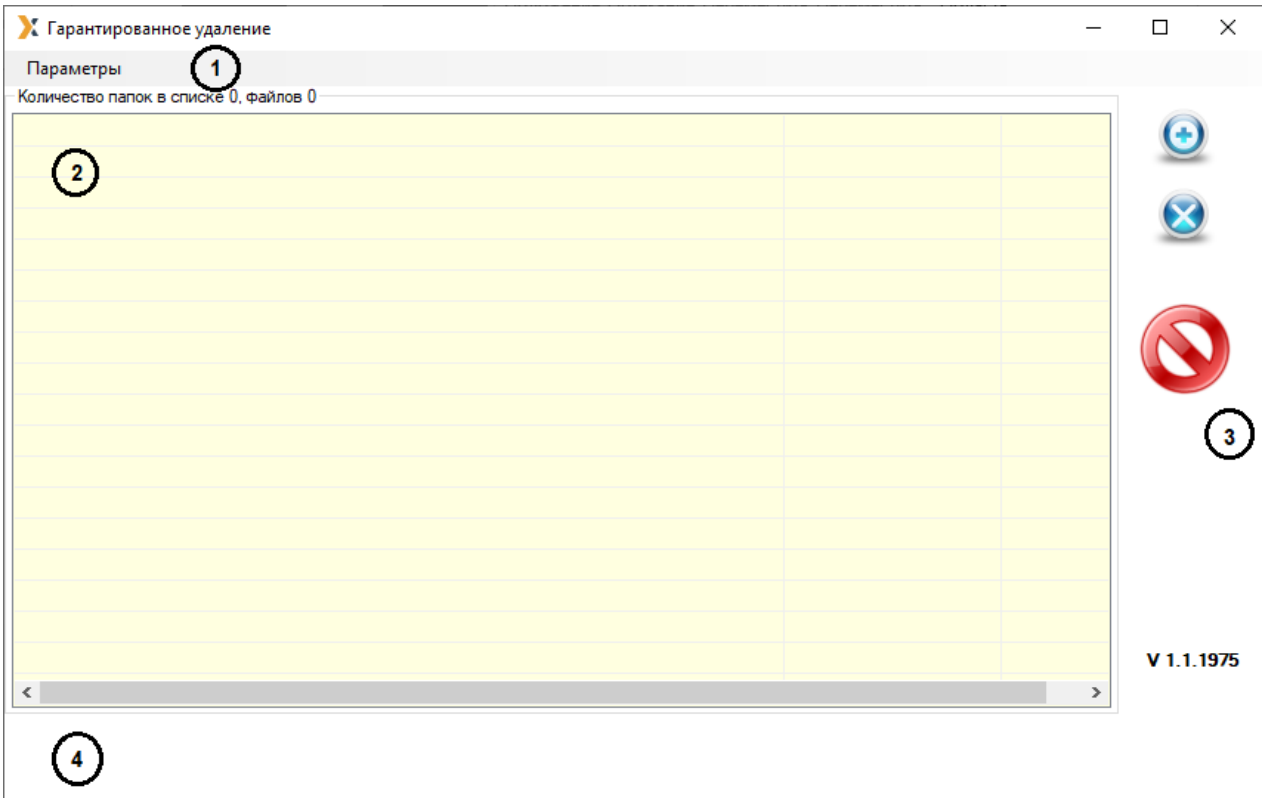

Рисунок 4.2 – Главное меню консоли управления

4.3 Формирование списка объектов, предназначенных для гарантированного удаления

Работа со списком объектов, предназначенных для гарантированного удаления, подразумевает такие операции как:

- добавление файлов и папок в список;
- добавление в список разделов жестких дисков и съемных накопителей;
- добавление в список свободной области устройств хранения информации (разделов жестких дисков, флэшек, дискет);
- фильтрация файлов и папок в списке;
- удаление файлов и папок из списка.

В подсистеме ГУПТ недоступно гарантированное удаление по требованию файлов, находящихся на SSD и USB-носителях.
Для полной очистки SSD и USB-носителей возможно использование операции очистки свободного пространства данных накопителей информации (раздел **4.3.3 «Добавление свободных областей в список удаляемых объектов»**).

Также доступны операции с самими файлами и папками, вызываемые из контекстного меню консоли управления. Контекстное меню появляется по щелчку правой кнопкой мыши на соответствующем объекте (файле или папке) в списке. Контекстное меню для файлов (Рисунок 4.3) содержит пункты:

- ***Показать в папке*** – открывается каталог расположения выбранного файла в стандартном Проводнике Windows;
- ***Открыть*** – происходит открытие файла соответствующей программой, если выбран исполняемый файл, то происходит его запуск.

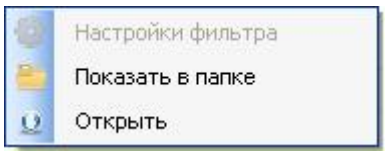

Рисунок 4.3 – Контекстное меню для файлов

Вид контекстного меню для папок зависит от того, уставлен ли фильтр для объектов данной папки. Контекстное меню для папок без установленного фильтра (Рисунок 4.4) содержит пункты:

- ***Задать фильтр*** – открывается окно настройки параметров фильтра (Рисунок 4.8);
- ***Показать в папке*** – открывается каталог расположения выбранной папки в стандартном Проводнике Windows;
- ***Открыть*** – в стандартном Проводнике Windows открывается содержимое выбранного каталога.

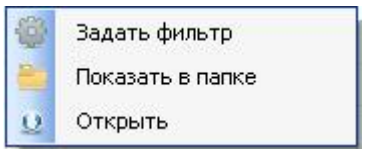

Рисунок 4.4 – Контекстное меню для папок без установленного фильтра

Контекстное меню для папок с установленным фильтром (Рисунок 4.5) включает пункты:

- ***Настройки фильтра*** – открывается окно настройки параметров фильтра (Рисунок 4.8);
- ***Показать в папке*** – открывается каталог расположения выбранной папки в стандартном Проводнике Windows;
- ***Открыть*** – в стандартном Проводнике Windows открывается содержимое выбранного каталога;
- ***Сбросить фильтр*** – для выбранного каталога отменяется функция

Использовать фильтр.

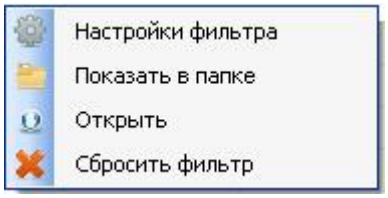

Рисунок 4.5 – Контекстное меню для папок с установленным фильтром

4.3.1 Добавление файловых объектов в список удаляемых объектов

Для того, чтобы добавить в список консоли управления файловый объект для его гарантированного удаления, необходимо нажать кнопку ***Добавить*** . В открывшемся окне добавления объектов (Рисунок 4.6) отметить необходимый тип объекта (***Файл*** или ***Каталог***) и нажать кнопку согласия. В результате откроется стандартное окно Windows ***«Открыть»*** в котором необходимо указать удаляемый объект.

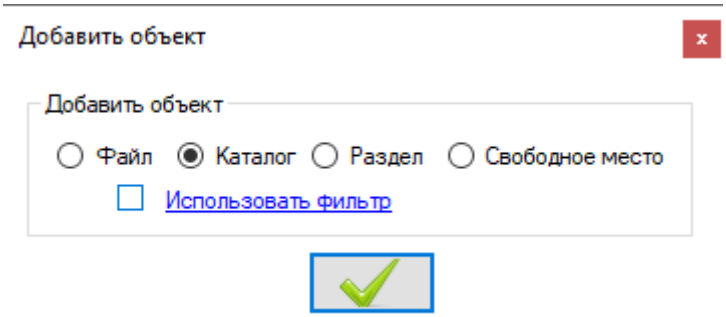

Рисунок 4.6 – Выбор типа добавляемого объекта

Если в качестве удаляемого типа объекта отмечен параметр ***Каталог***, то в окне ***«Добавить объект»*** появляется параметр ***Использовать фильтр***. Фильтр используется для того, чтобы выбрать для гарантированного удаления из указанного каталога только те файлы, которые соответствуют заданным параметрам. Чтобы выбор файлов производился с учетом фильтра, необходимо отметить этот параметр в окне добавления объекта (Рисунок 4.7) и нажать кнопку согласия:

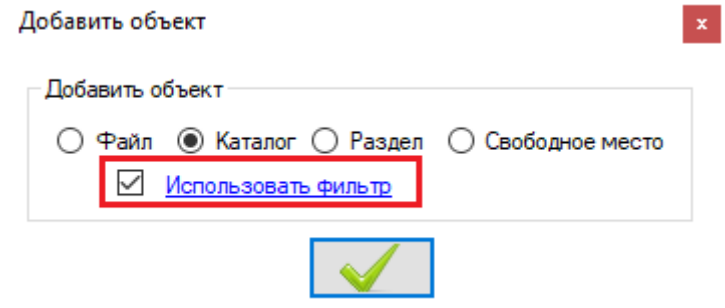

Рисунок 4.7 – Включение фильтра

Для настройки параметров фильтра необходимо нажать на ссылку ***Использовать***

фильтр и задать в открывшемся окне (Рисунок 4.8) параметры фильтра:

- расширение файла (при перечислении нескольких расширений необходимо указывать их через точку с запятой, например: ****.exe;*.db;*.doc***);
- маску имени файла (в поле ***Имя содержит*** можно ввести только одну маску – часть имени файла, без использования символов звездочки «*»);
- размер файла (больше, меньше или равен введенному в поле ввода числу) в килобайтах;
- дату, после которой был создан файл, добавляемый в консоль гарантированного удаления.

После определения параметров фильтра гарантированному удалению будут подвергаться только те файлы из добавленного каталога, которые соответствуют установленным параметрам фильтра.

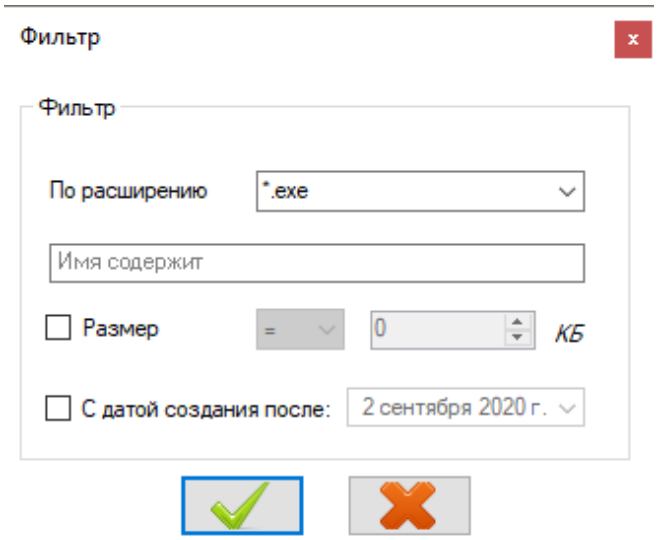

Рисунок 4.8 – Параметры фильтра

Добавлять файлы и папки в список консоли управления подсистемой ГУПТ можно также путем их перетаскивания мышью в область данных консоли из окна любого файлового менеджера.

Следует быть внимательным при добавлении в список объектов для гарантированного удаления системных каталогов ОС Windows (например, *C:\Program Files*; *C:\Windows*) – при гарантированном удалении файлов из таких каталогов может быть нарушена работа установленных программ или всей операционной системы.

После добавления файловых объектов, в области данных консоли управления отобразится список выбранных файлов и папок:

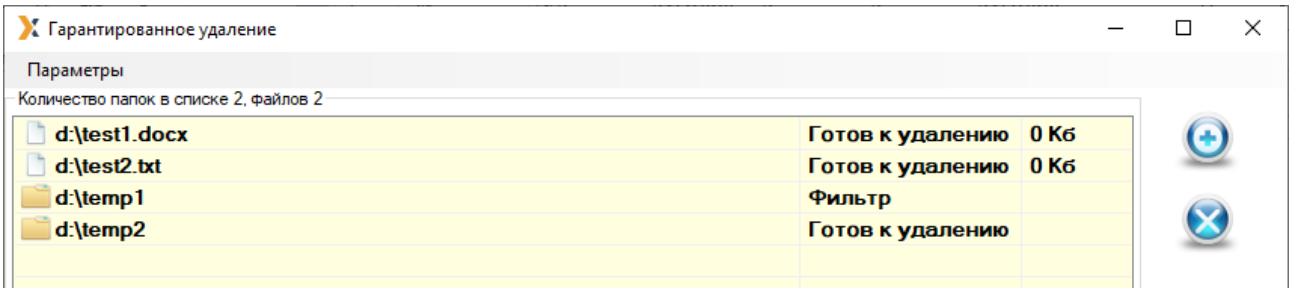

Рисунок 4.9 – Файлы и папки, добавленные в список гарантированного удаления

4.3.2 Добавление разделов в список удаляемых объектов

В подсистеме ГУПТ существует возможность полной очистки пользовательских разделов жестких дисков и/или съемных накопителей. При этом существующие на очищаемом разделе данные будут гарантированно уничтожены, а свободная область перезаписана по специальному алгоритму.

Для добавления в список консоли управления раздела жесткого диска или съемного носителя для очистки его содержимого необходимо в окне ***«Добавить объект»*** (Рисунок 4.6) выбрать параметр ***Раздел*** и нажать кнопку согласия.

В открывшемся окне выбора устройств выделить один или несколько разделов (с помощью клавиш ***<Ctrl>*** или ***<Shift>***), содержимое которых необходимо гарантированно удалить и нажать кнопку согласия (Рисунок 4.10).

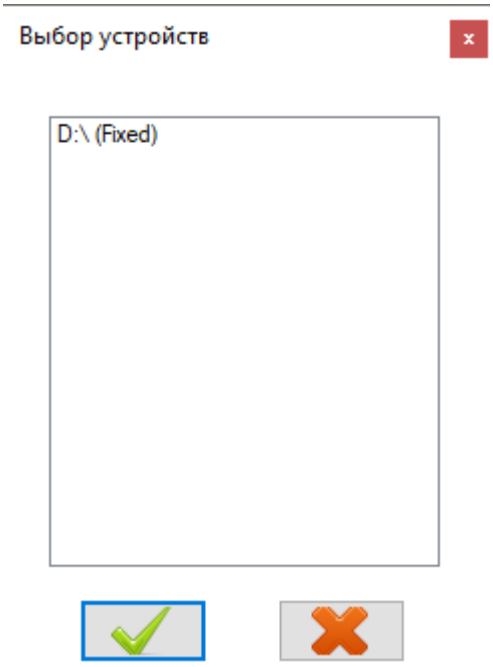

Рисунок 4.10 – Выбор раздела для очистки

В результате в списке объектов для гарантированного удаления отобразится строка ***содержимое и свободное место раздела < раздел>*** и размер выбранного для полной

очистки пользовательского раздела или съемного носителя (Рисунок 4.11).

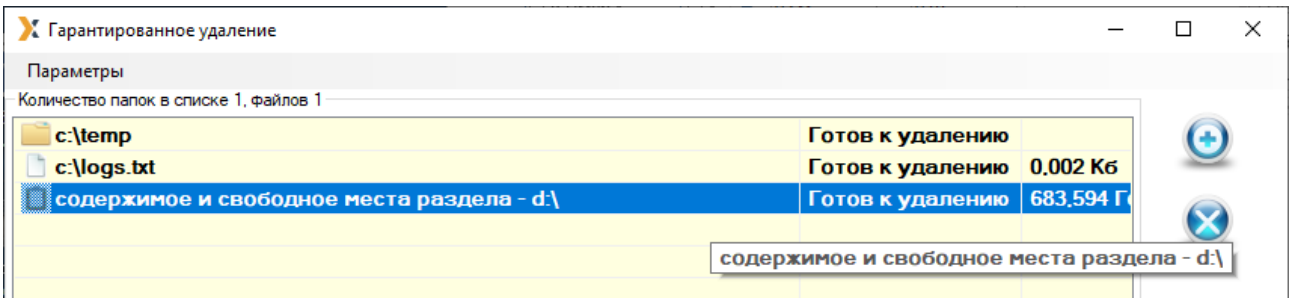

Рисунок 4.11 – Пользовательский раздел, добавленный в список гарантированного удаления

В список объектов для гарантированного удаления по требованию нельзя добавить системный раздел (раздел, на котором установлена ОС Windows). Такой раздел будет отсутствовать в окне выбора устройств (Рисунок 4.10).

Также в список файловых объектов, подлежащих гарантированному удалению, можно добавить свободное пространство любого из подключенных к рабочей станции накопителей информации: разделов жестких дисков, дискет, USB-накопителей и т.д.

4.3.3 Добавление свободных областей в список удаляемых объектов

Для очистки свободного пространства накопителей информации необходимо в окне добавления объектов (Рисунок 4.6) отметить параметр ***Свободное место*** и нажать кнопку согласия.

В открывшемся окне выбора устройств (Рисунок 4.10) выделить один или несколько (с помощью клавиш ***<Ctrl>*** или ***<Shift>***) устройств (или разделов жестких дисков) и нажать кнопку согласия.

В результате в списке объектов для гарантированного удаления отобразится строка ***свободное место на устройстве <устройство>*** и размер очищаемого на выбранном носителе свободного пространства.

В случае, если выбранный диск находится в зашифрованном и отключенном состоянии, то такой диск не будет добавлен в список объектов для очистки свободного пространства – откроется окно с сообщением об ошибке доступа к диску.

4.3.4 Установка размера псевдослучайной последовательности символов

В консоли управления подсистемой ГУПТ существует возможность задать размер последовательности символов, генерируемых случайным образом, которыми будет заполняться дисковое пространство при гарантированном удалении файловых объектов или очистке носителей информации, подключенных к рабочей станции.

Для изменения длины псевдослучайной последовательности необходимо в консоли управления выбрать пункт главного меню ***Параметры →Длина псевдослучайной последовательности***, в открывшемся окне изменения размера псевдослучайной последовательности установить необходимое значение в байтах и нажать кнопку подтверждения внесенных изменений:

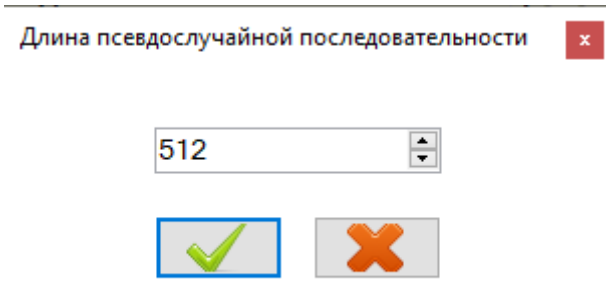

Рисунок 4.12 – Изменение размера псевдослучайной последовательности

Минимальный размер последовательности, который можно установить, равен 16 байт, максимальный – 10000000 байт. По умолчанию установлено значение 512 байт. При каждом запуске консоли управления длина псевдослучайной последовательности устанавливается в значение по умолчанию – 512 байт.

4.3.5 Удаление выбранных объектов из списка удаляемых

Для удаления объектов, предназначенных для гарантированного удаления, из списка в консоли управления необходимо выделить соответствующий объект и нажать кнопку ***Удалить из списка*** .

Можно выделить один элемент, щелкнув по нему левой кнопкой мыши, или при помощи клавиш ***<Ctrl>*** или ***<Shift>*** выделить сразу несколько элементов. Для выделения всех элементов можно использовать сочетание клавиш ***<Ctrl>+<A>***.

После подтверждения операции очистки списка в открывшемся окне (Рисунок 4.13) выбранные элементы будут удалены из сформированного списка консоли управления.

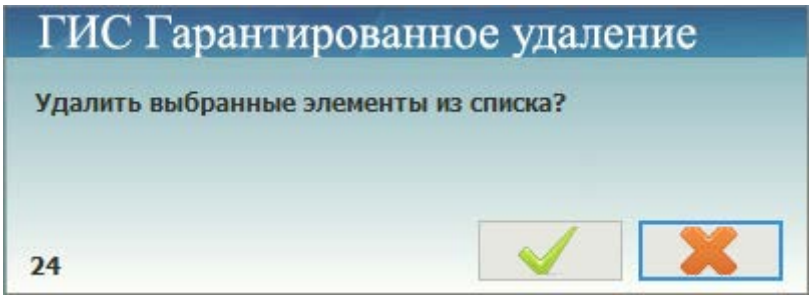

Рисунок 4.13 – Подтверждение удаления файлов из списка

Удалить выделенные элементы из списка консоли управления можно также при помощи клавиши ***<Delete>***.

4.4 Гарантированное удаление объектов

Для того, чтобы гарантированно удалить выбранные объекты с рабочей станции, необходимо выделить объекты, предназначенные для гарантированного удаления, в списке консоли управления и нажать кнопку ***Гарантированно удалить*** .

После подтверждения операции в диалоговом окне (Рисунок 4.14) начнется процесс гарантированного удаления.

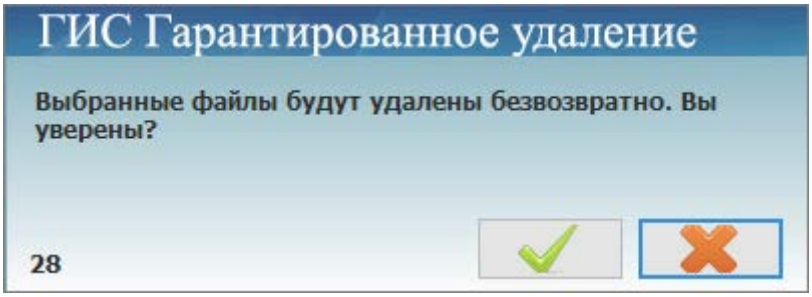

Рисунок 4.14 – Подтверждение гарантированного удаления файлов и папок

Ход процесса гарантированного удаления отображается в строке прогресса консоли управления (Рисунок 4.15):

Подготовка к удалению d:\temp2

Рисунок 4.15 – Отображение хода гарантированного удаления в строке прогресса

В результате объекты будут удалены без возможности их дальнейшего восстановления. В строке прогресса отображается соответствующая надпись (Рисунок 4.16), сопровождающаяся информационным сообщением (Рисунок 4.17).

Файл d:\test2.txt удален

Рисунок 4.16 – Подтверждение гарантированного удаления объектов в строке прогресса

Рисунок 4.17 – Сообщение об успешном завершении гарантированного удаления

В случае, если гарантированное удаление выбранного объекта невозможно (например, файл заблокирован системой или удален ранее стандартным способом), отображаются соответствующие сообщения об ошибке гарантированного удаления выбранного объекта (см. пример на Рисунок 4.18, Рисунок 4.19).

Рисунок 4.18 – Сообщение в строке прогресса о невозможности гарантированного удаления

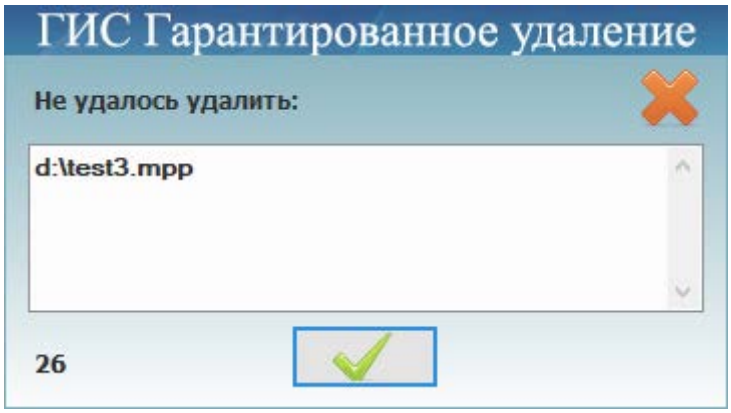

Рисунок 4.19 – Сообщение о невозможности произвести гарантированное удаление

Во время процесса удаления выбранных файловых объектов в консоли управления существует возможность приостановить на время процесс гарантированного удаления. Для этого необходимо нажать кнопку ***Остановить удаление*** и подтвердить остановку процесса в открывшемся окне:

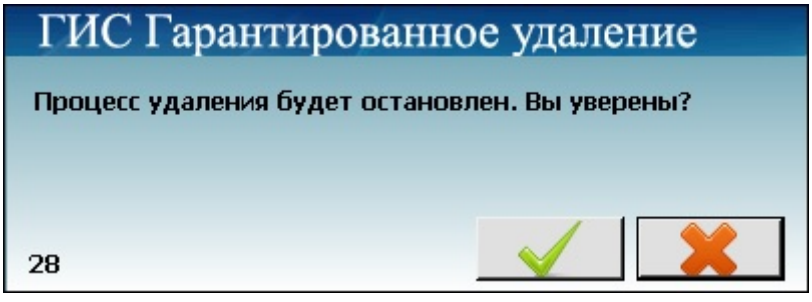

Рисунок 4.20 – Подтверждение остановки процесса гарантированного удаления файлов и папок

Для продолжения процесса гарантированного удаления файловых объектов из списка консоли управления необходимо нажать кнопку ***Гарантированно удалить*** и подтвердить выполнение операции в открывшемся диалоговом окне (Рисунок 4.14).

Произвести гарантированное удаление файла или папки возможно также и без открытия консоли управления подсистемы. Для этого необходимо щелкнуть по файлу или папке правой кнопкой мыши и в появившемся контекстном меню Windows выбрать пункт ***Гарантированное удаление →Удалить*** (Рисунок 4.21). В случае удачного завершения операции гарантированного удаления выбранного объекта появится сообщение, показанное на Рисунок 4.17.

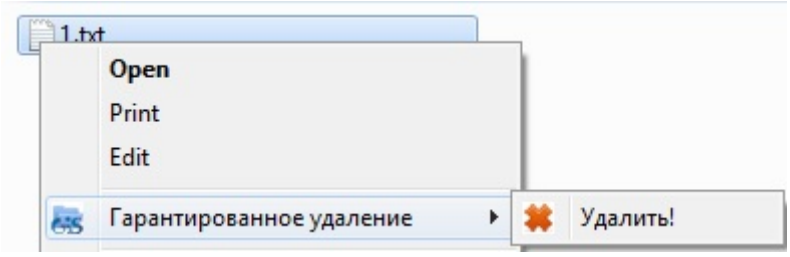

Рисунок 4.21 – Гарантированное удаление файла из контекстного меню Windows

4.5 Работа с подсистемой ГУПТ в режиме командной строки

Использование командной строки позволяет производить гарантированное удаление указанных файловых объектов без использования консоли управления подсистемы.

При работе с командной строкой поддерживаются переменные окружения операционной системы.

При работе с подсистемой ГУПТ из командной строки синтаксис команды имеет вид:

“c:\Program Files\GIS\GIS.WipeFiles\GIS.WipeFile.exe” <команда> <”полный путь к файлу(-ам)/папке(-кам)”>

или

“c:\Program Files\GIS\GIS.WipeFiles\GIS.WipeFile.exe” <команда> <”%наименование переменной окружения%\имя файла (папки)”>

Команды необходимо вводить с учетом регистра.
Одну команду можно применять сразу к нескольким объектам, указав их через точку с запятой ***«;»***.
Путь до объекта следует указывать в двойных кавычках (“”).

Команды для работы с командной строкой:

- **-wcur** – гарантированное удаление файлов/папок с выводом результата операции;

Например:

“c:\Program Files\GIS\GIS.WipeFiles\GIS.WipeFile.exe” –wcur c:\1.txt; c:\test1

“c:\Program Files\GIS\GIS.WipeFiles\GIS.WipeFile.exe” –wcur “%Systemdrive%%HOMEPATH%\Local Settings\Temp”; “%Systemdrive%%HOMEPATH%\Local Settings\Temporary Internet Files”; “%Systemdrive%\WINDOWS\Temp”

- **-wcur_no_msg** – гарантированное удаление файлов/папок без вывода результата операции;

Например:

“c:\Program Files\GIS\GIS.WipeFiles\GIS.WipeFile.exe” –wcur_ no_msg c:\1.xml; c:\temp

- **-wcur_files** – гарантированное удаление всех файлов из указанных папок без вывода результата операции. При наличии вложенных папок в указанной папке из них также будут удалены все файлы.

Например:

c:\Program Files\GIS\GIS.WipeFiles\GIS.WipeFile.exe –wcur_files c:\1

- **-wipeFile** – гарантированное удаление объектов, указанных в текстовом файле.

Например:

c:\Program Files\GIS\GIS.WipeFiles\GIS.WipeFile.exe –wipeFile c:\wipeFileList.txt

В текстовом файле пути до объектов указываются без кавычек. Содержание файла ***c:\wipeFileList.txt*** показано на Рисунок 4.22.

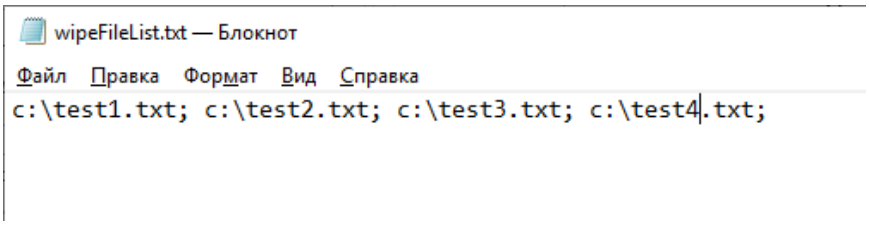

Рисунок 4.22 – Содержание файла ***c:\wipeFileList.txt***

- **-help, /?, ?** – помощь по работе с командной строкой.

Например:

c:\Program Files\GIS\GIS.WipeFiles\GIS.WipeFile.exe –help

Перечень сокращений

ГУПТ	–	Гарантированное удаление по требованию
НСД	–	Несанкционированный доступ
ОС	–	Операционная система
СЗИ	–	Средство защиты информации