

Средство защиты информации от несанкционированного доступа
«Блокхост-Сеть 3»

Руководство администратора безопасности. Приложение 2

1 Особенности работы с жесткими и символьными ссылками объектов при настройке дискреционного механизма разграничения доступа

В файловой системе NTFS существует технология привязки (*link*), позволяющая одному и тому же файлу существовать в нескольких каталогах, иногда под разными именами (т.е. два разных имени файла указывают на одну и ту же внутреннюю структуру данных). Подобная привязка называется жесткой связью или жесткой ссылкой (*hard link*). Жесткие ссылки могут быть созданы только для файлов в пределах одного логического диска.

Другим вариантом привязки файлов является символьная ссылка. В файловой системе NTFS существует два вида символьных ссылок: «*junction point*» и «*symlink*». *Junction point* (точка соединения NTFS) позволяет отображать указанную папку или логический диск, как папку на другом логическом диске, либо в другой папке. *Symlink* представляет собой небольших размеров файл, содержащий путь к исходному файлу (папке). При запуске файла, являющегося символьной ссылкой, по содержащемуся в нем пути происходит обращение к исходному (оригинальному) файлу (папке).

Junction point могут быть созданы для каталогов на диске и/или логического диска целиком. *Symlink* могут быть созданы для файлов и каталогов, при этом они могут пересекать границы логических дисков, а также указывать на имена файлов, находящихся на удаленных компьютерах.

Создать *junction point* возможно средствами ОС Windows 7/2008R2/8.1/2012/2012R2/10.2016/2019.

Для того чтобы установить дискреционное разграничение доступа для объекта, имеющего жесткие и/или символьные ссылки, администратору безопасности необходимо:

- 1) Проверить наличие жестких и символьных ссылок, относящихся к контролируемым объектам. Методика проверки наличия жестких и символьных ссылок и работы с ними приведены ниже.
- 2) В настройках дискреционного механизма консоли администрирования СЗИ вместе с контролируемыми объектами добавить на контроль жесткие ссылки, относящиеся к ним, с правами доступа исходных (оригинальных) объектов.
- 3) Для объектов, имеющих символьные ссылки, необходимо убедиться, что в

настройках дискреционного механизма консоли администрирования СЗИ на контроль добавлены исходные (оригинальные) файлы, а не их символьные ссылки. Методика проверки наличия символьных ссылок и работы с ними приведены ниже. Установленные в СЗИ права доступа для оригинального файла будут действовать при попытках доступа к нему по символьной ссылке.

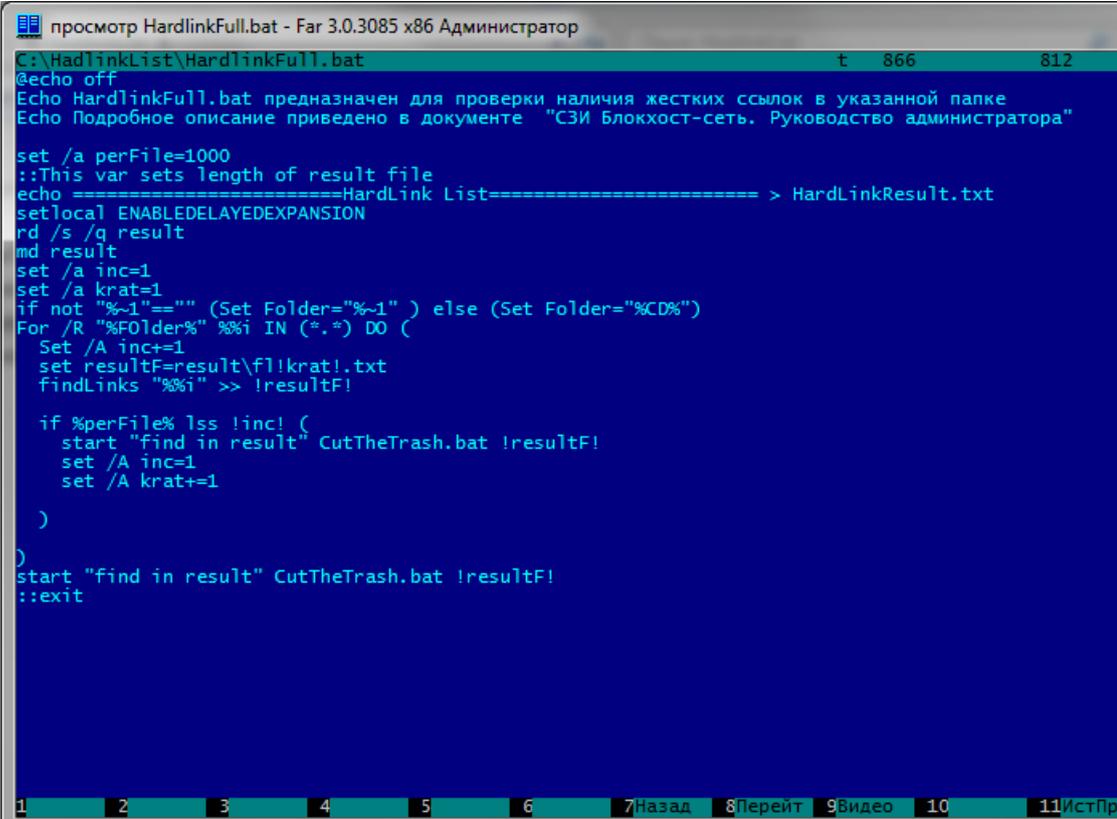
1.1 Особенности работы с жесткими ссылками

Для проверки наличия жестких ссылок (*hardlink*), относящихся к контролируемым объектам, администратору безопасности необходимо:

- 1) выполнить подготовительные операции – на жестком диске создать папку с именем **HardlinkList** со следующими файлами *HardlinkFull.bat*, *CutTheTrash.bat*, *FindLinks.exe*.

Содержимое командных файлов *HardlinkFull.bat* и *CutTheTrash.bat* приведено на рисунках П2.1 и П2.2 соответственно. Данные командные файлы можно также скопировать из каталога *GIS\Documents\Linklist\HardlinkList* дистрибутивного диска.

Программа *FindLinks.exe* доступна на официальном сайте компании Microsoft (<https://docs.microsoft.com/en-us/sysinternals/downloads/findlinks>).



```
просмотр HardlinkFull.bat - Far 3.0.3085 x86 Администратор
C:\HardlinkList\HardlinkFull.bat t 866 812
@echo off
Echo HardlinkFull.bat предназначен для проверки наличия жестких ссылок в указанной папке
Echo Подробное описание приведено в документе "СЗИ Блокхост-сеть. Руководство администратора"

set /a perFile=1000
::This var sets length of result file
echo =====HardLink List===== > HardLinkResult.txt
setlocal ENABLEDELAYEDEXPANSION
rd /s /q result
md result
set /a inc=1
set /a krat=1
if not "%~1"==" (Set Folder="%~1" ) else (Set Folder="%CD%")
For /R "%Folder%" %%i IN (*.*) DO (
  Set /A inc+=1
  set resultF=result\fl\krat!.txt
  findlinks "%%i" >> !resultF!

  if %perFile% lss !inc! (
    start "find in result" CutTheTrash.bat !resultF!
    set /A inc=1
    set /A krat+=1
  )
)
start "find in result" CutTheTrash.bat !resultF!
::exit
```

Рисунок П2.1 – Содержимое файла *HardlinkFull.bat*

2) проверить наличие жестких ссылок (в отдельной папке или целиком на жестком диске). Для этого в командной строке (cmd.exe) необходимо выполнить команду *HardlinkFull.bat* <Полный путь до проверяемой папки>. Вызываемый командный файл *HardlinkFull.bat* запускает программу *FindLinks.exe* для проверки наличия жестких ссылок по указанному пути.

Пример:

- *C:\HardlinkList\HardlinkFull.bat C:* (проверяется наличие жестких ссылок на диске C:\);
- *C:\HardlinkList\HardlinkFull.bat C:\user1* (проверяется наличие жестких ссылок в папке C:\user1\).



Если в наименовании пути к проверяемой папке содержатся пробелы или русские буквы, имена папок и файлов необходимо указывать в формате 8.3 (например, *Docume~1*);

В качестве промежуточного результата в папке запуска командного файла *HardlinkFull.bat* создается папка *result* с перечнем всех файлов по указанному адресу, независимо от наличия у них жестких ссылок.

Командный файл *CutTheTrash.bat* выбирает из общего перечня файлы, которые имеют жесткие ссылки.

В результате в папке **...\HardlinkList** (в папке запуска командного файла *HardlinkFull.bat*) создается итоговый файл *HardlinkResult.txt*, содержащий перечень файлов и их жестких ссылок (рис. П2.3).

```

C:\HadlinkList\CutTheTrash.bat t 1251
@echo off
setlocal ENABLEDELAYEDEXPANSION
Set FilePath=%~1
set resultToCopy=0
set /A FileNameToCopy=0
Set /a resultToCopy=0
For /F "tokens=* delims=" %%x IN ('type "%FilePath%") DO (
  IF /I "%%x" EQU "Linking file:" (
    set /A resultToCopy=1
  ) ELSE (
    rem NothingElseMatters
  )
)
  IF /I "%%x" EQU "Linking files:" (
    set /A resultToCopy=1
  ) ELSE (
    rem NothingElseMatters
  )
)
  IF /I "%%x" EQU "Sysinternals - www.sysinternals.com" (
    set /A FileNameToCopy=1
  ) Else (
    rem NothingElseMatters
  )
)
  IF Not "!FileNameToCopy!"=="0" (
    set /A FileNameToCopy+=1
    If "!FileNameToCopy!"=="3" (
      set /a FileNameToCopy=0
      Set HardlinkFile=%%x
    )
  )
  IF Not "!resultToCopy!"=="0" (
    set /a resultToCopy+=1
    If /I "%%x" EQU "FindLinks v1.0 - Locate file hard links" (
      set /a resultToCopy=0
    ) ELSE (
      IF "2"=="!resultToCopy!" (
        Echo ===== >> HardLinkResult.txt
        echo !HardlinkFile! >> HardLinkResult.txt
      ) ELSE (
        echo %%x >> HardLinkResult.txt
      )
    )
  )
)
)
)
exit
  
```

Рисунок П2.2 – Содержимое файла *CutTheTrash.bat* при создании жестких ссылок

```

=====HardLink List=====
c:\qt\qt5.0.1\vcredist\test.exe
c:\Qt\Qt5.0.1\vcredist\vcredist_sp1_x86.exe
=====
c:\qt\qt5.0.1\vcredist\vcredist_sp1_x86.exe
c:\Qt\Qt5.0.1\vcredist\test.exe
  
```

Рисунок П2.3 – Пример содержимого файла *HardlinkResult.txt*

В консоли администрирования СЗИ настройки разграничения доступа к объектам должны быть продублированы и для их жестких ссылок.



При удалении файла с жесткого диска существующие жесткие ссылки, относящиеся к данному файлу, остаются. Доступ к файлу будет возможен, пока в системе существует хотя бы одна жесткая ссылка на него, даже если исходный файл был удален.

Пример:

Для выбранного администратором безопасности пользователя необходимо установить дискреционное разграничение доступа для папок `e:\tests\BHS\test1-RW`, `e:\tests\BHS\test2-R`, `e:\tests\BHS\test3-W`, `e:\tests\BHS\test4-` в соответствии с таблицей П2.1.

Таблица П2.1 – Пример дискреционного разграничение доступа для папок при работе с жесткими ссылками

	Права доступа
<code>e:\tests\BHS\test1-RW</code>	RW
<code>e:\tests\BHS\test2-R</code>	R
<code>e:\tests\BHS\test3-W</code>	W
<code>e:\tests\BHS\test4-</code>	-

В этих папках следует проверить наличие файлов, имеющих жесткие ссылки. Это можно сделать с помощью команды:

```
C:\hardlinkList\HardlinkFull.bat e:\tests\BHS\
```

В результате в папке `C:\hardlinkList\` создается файл `HardlinkResult.txt`, содержащий список файлов и жестких ссылок (рис. П2.4).

Из рисунка П2.3 видно, что были обнаружены попарно одинаковые объекты (например, при проверке файла `e:\tests\BHS\test1-RW\read.txt` был обнаружен файл с такой же структурой данных по адресу `e:\tests\bhs\temp\hardlink\test1.txt`). Таким образом, при настройке дискреционного механизма разграничения доступа на контроль необходимо устанавливать оба объекта с одними и теми же правами доступа согласно таблице П2.1 (рис. П2.5).

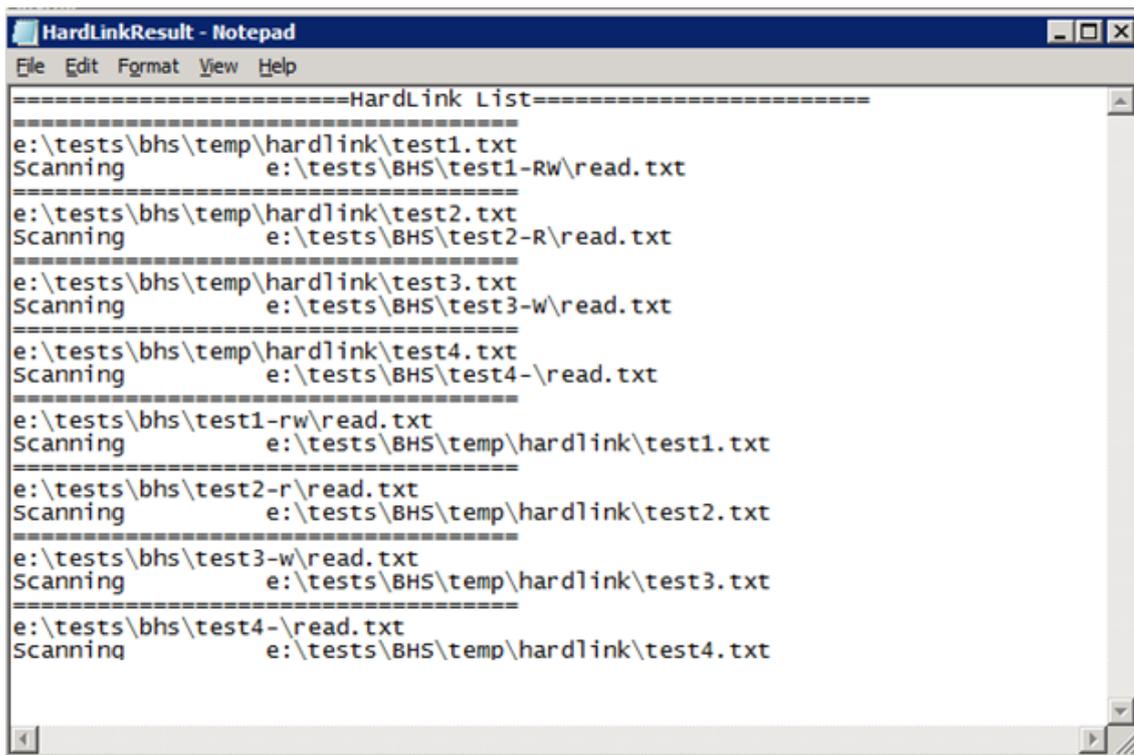


Рисунок П2.4 – Пример проверки наличия жестких ссылок

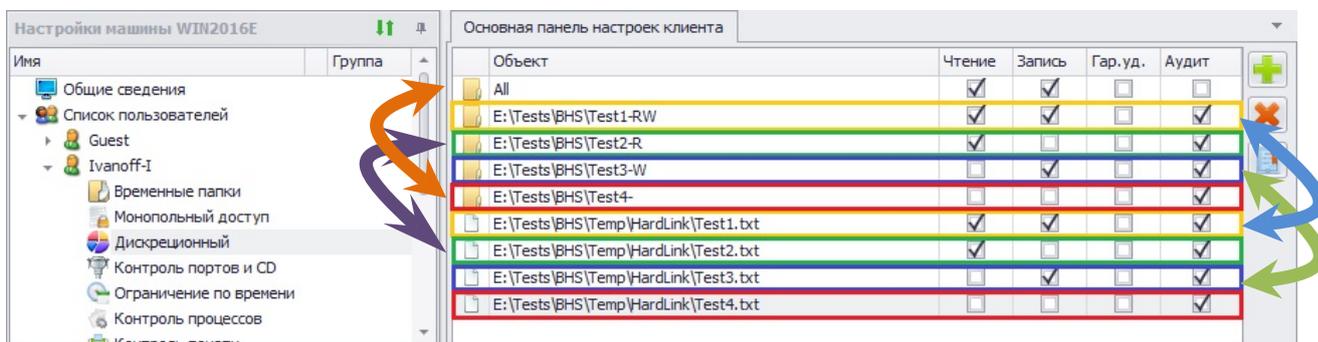


Рисунок П2.5 – Установка разграничений доступа в СЗИ для файлов и их жестких ссылок

1.2 Особенности работы с символьными ссылками

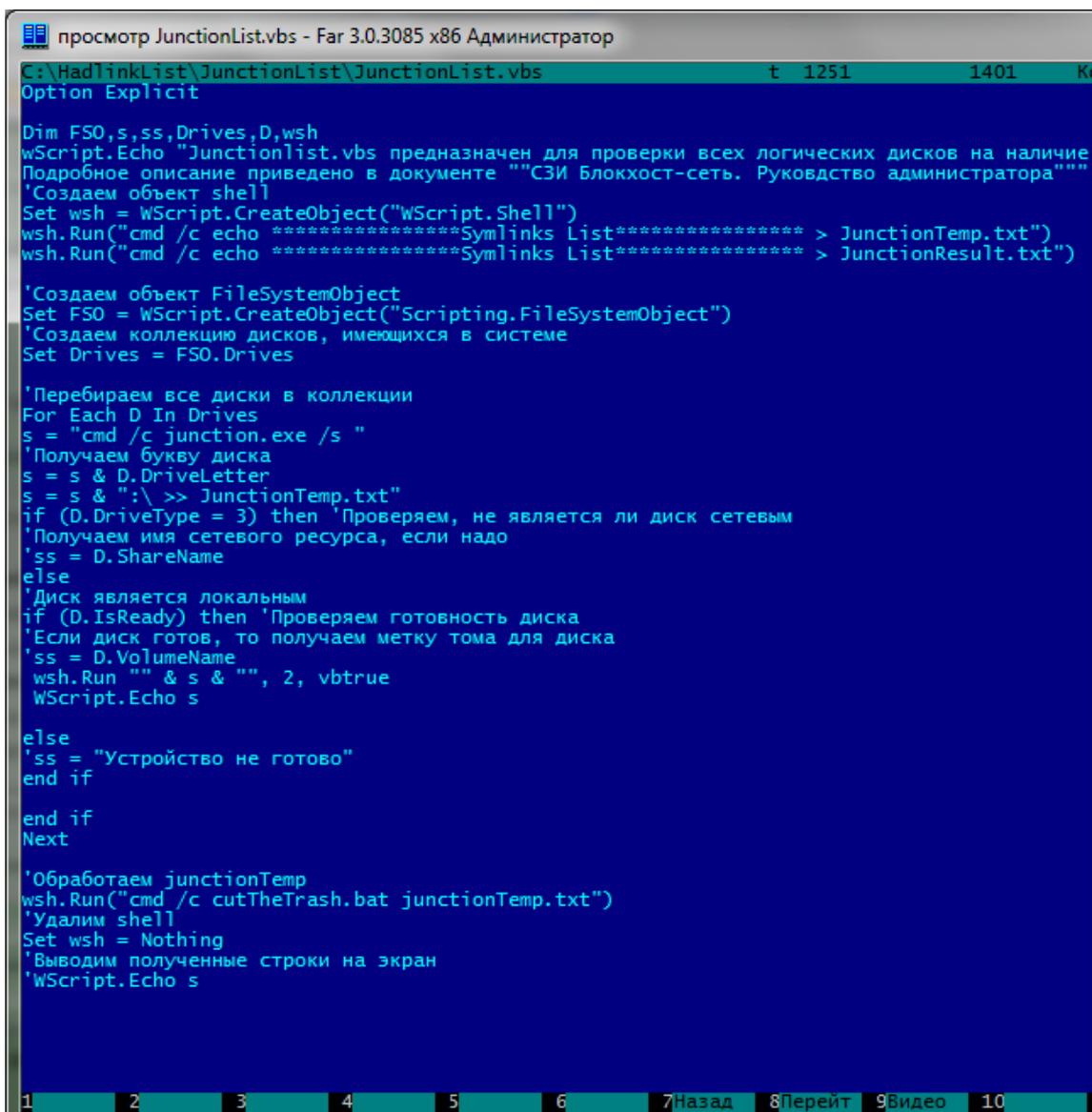
Основная особенность разграничения доступа к файлам (папкам), имеющим символьные ссылки, состоит в следующем – в консоли администрирования СЗИ права доступа должны быть настроены администратором безопасности обязательно для оригинального файла (оригинальной папки). В этом случае при попытке доступа к этому файлу (папке) через symlink (junction point) будет также осуществляться с учетом настроек СЗИ.

Для проверки наличия символьных ссылок (symbolic links и/или junction points) необходимо:

1) выполнить подготовительные операции – на жестком диске создать папку с именем *JunctionList* со следующими файлами: *Junctionlist.vbs*, *CutTheTrash.bat*, *Junction.exe*.

Содержимое командных файлов *Junctionlist.vbs* и *CutTheTrash.bat* приведено на рисунках П2.6 и П2.7. Данные командные файлы также можно скопировать из каталога *GIS\Documents\LinkList\JunctionList* дистрибутивного диска СЗИ.

Программа *Junction.exe* доступна на официальном сайте компании Microsoft (<https://docs.microsoft.com/ru-ru/sysinternals/downloads/junction>).



```
просмотр JunctionList.vbs - Far 3.0.3085 x86 Администратор
C:\HadlinkList\JunctionList\JunctionList.vbs t 1251 1401 K
Option Explicit

Dim FSO,s,ss,Drives,D,wsh
wScript.Echo "Junctionlist.vbs предназначен для проверки всех логических дисков на наличие
Подробное описание приведено в документе ""СЗИ Блокхост-сеть. Руководство администратора""
'Создаем объект shell
Set wsh = WScript.CreateObject("WScript.Shell")
wsh.Run("cmd /c echo *****Symlinks List***** > JunctionTemp.txt")
wsh.Run("cmd /c echo *****Symlinks List***** > JunctionResult.txt")

'Создаем объект FileSystemObject
Set FSO = WScript.CreateObject("Scripting.FileSystemObject")
'Создаем коллекцию дисков, имеющихся в системе
Set Drives = FSO.Drives

'Перебираем все диски в коллекции
For Each D In Drives
s = "cmd /c junction.exe /s "
'Получаем букву диска
s = s & D.DriveLetter
s = s & ":\ >> JunctionTemp.txt"
if (D.DriveType = 3) then 'Проверяем, не является ли диск сетевым
'Получаем имя сетевого ресурса, если надо
'ss = D.ShareName
else
'Диск является локальным
if (D.IsReady) then 'Проверяем готовность диска
'Если диск готов, то получаем метку тома для диска
'ss = D.VolumeName
wsh.Run "" & s & """, 2, vbtrue
WScript.Echo s

else
'ss = "Устройство не готово"
end if

end if
Next

'Обработаем junctionTemp
wsh.Run("cmd /c cutTheTrash.bat junctionTemp.txt")
'Удалим shell
Set wsh = Nothing
'Выводим полученные строки на экран
WScript.Echo s
```

Рисунок П2.6 – Содержимое файла *Junctionlist.vbs*

- 2) проверить наличие символьных ссылок:
- *на всех логических дисках.* Для этого двойным щелчком левой кнопкой мыши вызвать файл *Junctionlist.vbs*. *Junctionlist.vbs* проверяет все логические диски на наличие символьных ссылок и при работе использует программу *Junction.exe*. При первом запуске *Junctionlist.vbs* появится окно ознакомления с лицензией программы *Junction.exe* (рис. П2.8), в котором нужно нажать кнопку подтверждения. Результатом работы скрипта *Junctionlist.vbs* является файл *JunctionResult.txt* с перечнем файлов и символьных ссылок на них (рис. П2.10). После окончания проверки каждого логического диска появится окно, приведенное на рисунке П2.9.
 - *в выбранной папке.* Для этого следует воспользоваться стандартной функциональностью программы *Junction.exe*. Например, вызов программы из командной строки с параметрами **junction.exe /s c:\test** позволит провести проверку на наличие символьных ссылок только папки *C:\test*.

```
просмотр CutTheTrash.Bat - Far 3.0.3085 x86 Администратор
C:\HadlinkList\JunctionList\CutTheTrash.Bat t 1251
@echo off
setlocal ENABLEDELAYEDEXPANSION
Set FilePath=%-1
set resultToCopy=0
set stringPrevios=
For /F "tokens=* delims=" %%x IN ('type "%FilePath%') DO (
  set StringToCompare=%%x
  IF /I "!StringToCompare:~0,19!" EQU " Print Name : " (
    set /A resultToCopy=1
    set ResultPathLink=!StringPrevios!
  ) ELSE (
    set StringPrevios=%%x
    rem NothingElseMatters
  )
)

IF Not "!resultToCopy!"=="0" (
  set /a resultToCopy+=1
  IF "2"=="!resultToCopy!" (
    Echo ===== >> JunctionResult.txt
    echo !ResultPathLink! >> JunctionResult.txt
    Echo %%x >> JunctionResult.txt
  ) ELSE (
    echo %%x >> JunctionResult.txt
    set /a ResultToCopy=0
  )
)
)
exit
```

Рисунок П2.7 – Содержимое файла *CutTheTrash.bat* при создании символьных ссылок

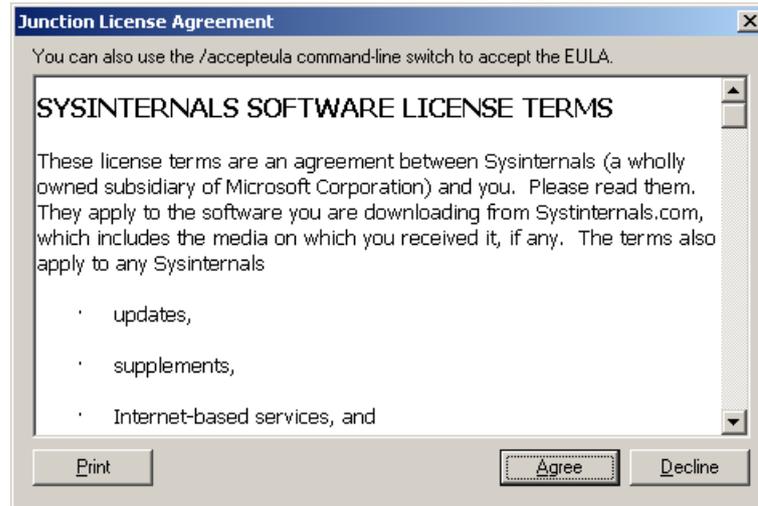


Рисунок П2.8 – Окно ознакомления с лицензией



Рисунок П2.9 – Окно завершения проверки диска

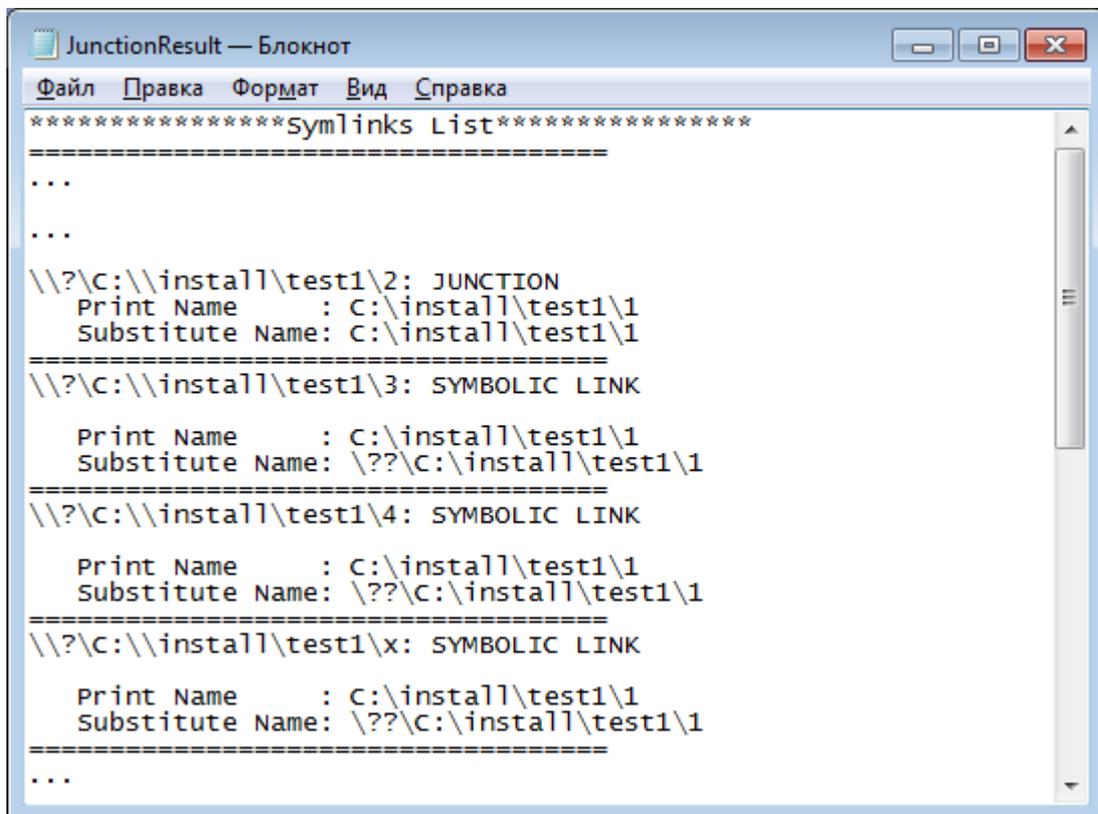


Рисунок П2.10 – Пример содержимого файла *JunctionResult.txt*

Первая строка на рисунке П2.10 показывает расположение символической ссылки (*junction point* или *symlink*);

В строке *Substitute Name* на рисунке П2.10 показано расположение оригинального файла, для которого создана символическая ссылка.

Установленные в СЗИ права доступа для оригинального файла будут действовать и при попытках доступа к нему по символической ссылке.



|| При удалении файла с жесткого диска существующие символические ссылки, относящиеся к данному файлу, остаются. Однако, в этом случае доступа к исходному файлу при обращении к нему по символической ссылке не будет.

2 Особенности работы с жесткими и символьными ссылками при настройке мандатного механизма разграничения доступа

В файловой системе NTFS существует технология привязки (*link*), позволяющая одному и тому же файлу существовать в нескольких каталогах, иногда под разными именами. Подобная привязка называется жесткой связью или жесткой ссылкой (*hard link*). Другим вариантом привязки файлов является символьная ссылка («*junction point*» и «*symlink*»). Более подробное описание жестких и символьных ссылок приведено в разделе 1 «Особенности работы с жесткими и символьными ссылками объектов при настройке дискреционного механизма разграничения доступа» настоящего приложения.

Для того, чтобы установить мандатное разграничение доступа для объекта, имеющего жесткие и символьные ссылки, администратору безопасности необходимо:

- 1) Проверить наличие жестких и символьных ссылок, относящихся к контролируемым объектам. Проверка проводится аналогично проверке наличия жестких и символьных ссылок при дискреционном разграничении доступа, описание которого приведено в разделе 1 «Особенности работы с жесткими и символьными ссылками объектов при настройке дискреционного механизма разграничения доступа» настоящего приложения.
- 2) В настройках консоли администрирования СЗИ присвоить одинаковые мандатные метки контролируемым объектам (файлам и папкам) и жестким ссылкам, относящимся к ним.
- 3) Для объектов, имеющих символьные ссылки необходимо убедиться, что в настройки консоли администрирования СЗИ на контроль добавлены исходные (оригинальные) файлы и папки, а не их символьные ссылки (см. подробнее раздел 1 «Особенности работы с жесткими и символьными ссылками объектов при настройке дискреционного механизма разграничения доступа» настоящего приложения). Установленные в СЗИ права доступа для оригинального объекта (файла или папки) будут действовать при попытках доступа к нему по символьной ссылке.