

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

Руководство администратора безопасности
Часть 1. Управление политиками
Приложение 1

Санкт-Петербург, 2021

1 Настройка жестких и символьных ссылок в дискреционном механизме 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 или каталогу. При запуске файла, являющегося символьной ссылкой, по содержащемуся в нем пути происходит обращение к исходному файлу или каталогу.

Junction point могут быть созданы для каталогов на диске и/или для 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 в разделах «**Особенности работы с жесткими ссылками**» и «**Особенности работы с символьными ссылками**».
- 2) В настройках дискреционного механизма консоли администрирования СЗИ вместе с контролируемыми объектами добавить на контроль жесткие ссылки, относящиеся к ним, с правами доступа исходных объектов.
- 3) Для объектов, имеющих символьные ссылки, необходимо убедиться, что в настройках дискреционного механизма на контроль добавлены исходные файлы, а

не их символьные ссылки. Установленные права доступа для оригинального файла будут действовать при попытках доступа к нему по символьной ссылке.

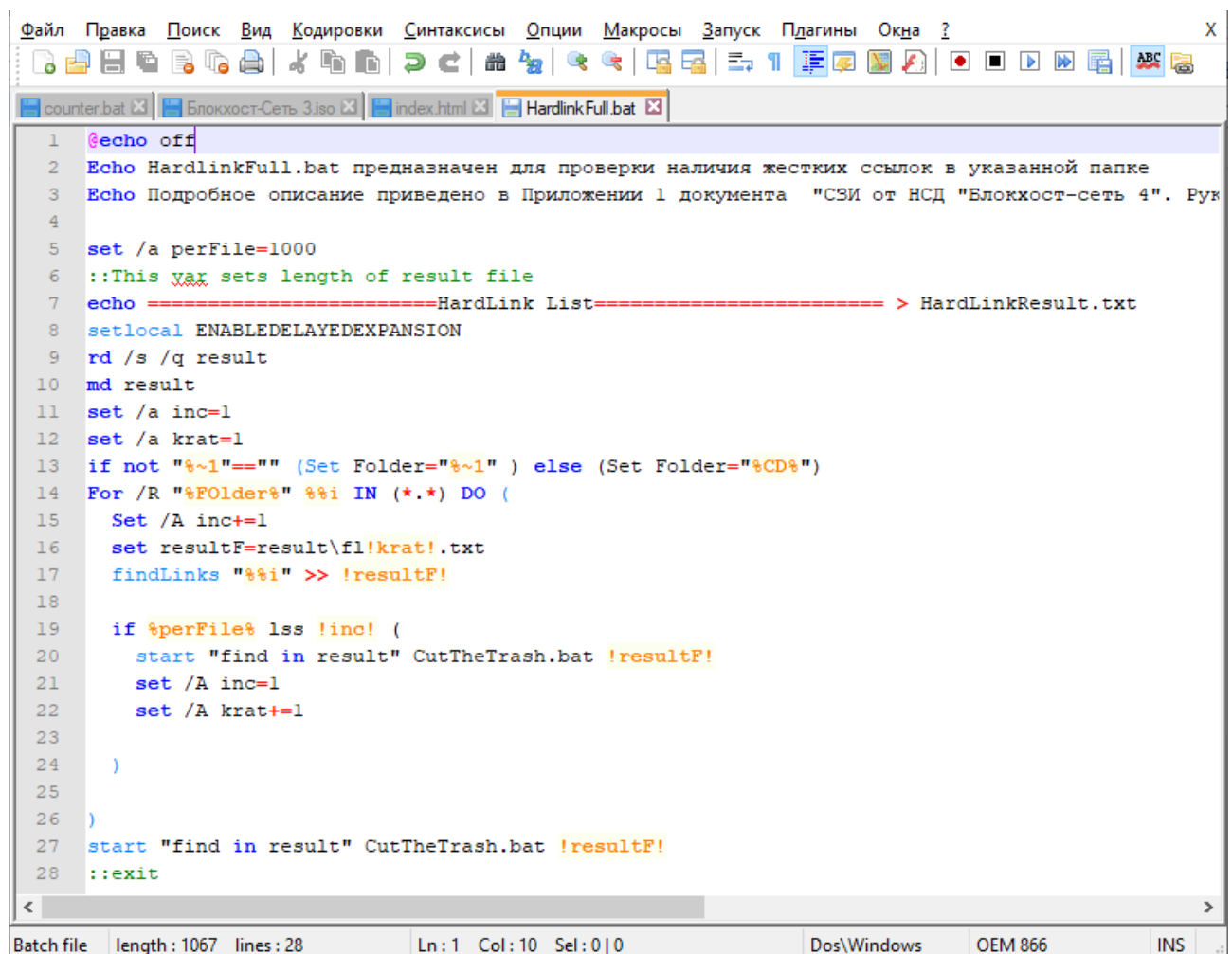
1.1 Особенности работы с жесткими ссылками

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 П1.1 и П1.2 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>).



```
1 @echo off
2 Echo HardlinkFull.bat предназначен для проверки наличия жестких ссылок в указанной папке
3 Echo Подробное описание приведено в Приложении 1 документа "СЗИ от НСД "Блокхост-сеть 4". Рук
4
5 set /a perFile=1000
6 ::This var sets length of result file
7 echo =====HardLink List===== > HardLinkResult.txt
8 setlocal ENABLEDELAYEDEXPANSION
9 rd /s /q result
10 md result
11 set /a inc=1
12 set /a krat=1
13 if not "%~1"==" (Set Folder="%~1" ) else (Set Folder="%CD%")
14 For /R "%Folder%" %i IN (*.*) DO (
15     Set /A inc+=1
16     set resultF=result\fl!krat!.txt
17     findLinks "%i" >> !resultF!
18
19     if %perFile% lss !inc! (
20         start "find in result" CutTheTrash.bat !resultF!
21         set /A inc=1
22         set /A krat+=1
23     )
24 )
25 )
26 )
27 start "find in result" CutTheTrash.bat !resultF!
28 ::exit
```

Рисунок П1.1 – 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 каталогов 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 (рисунок П1.3).

```

1 @echo off
2 setlocal ENABLEDELAYEDEXPANSION
3 Set FilePath=%~1
4 set resultToCopy=0
5 set /A FileNameToCopy=0
6 Set /a resultToCopy=0
7 For /F "tokens=* delims=" %%x IN ('type "%FilePath%"') DO (
8     IF /I "%%x" EQU "Linking file:" (
9         set /A resultToCopy=1
10        ) ELSE (
11            rem NothingElseMatters
12        )
13    IF /I "%%x" EQU "Linking files:" (
14        set /A resultToCopy=1
15    ) ELSE (
16        rem NothingElseMatters
17    )
18
19    IF /I "%%x" EQU "Sysinternals - www.sysinternals.com" (
20        set /A FileNameToCopy=1
21    ) Else (
22        rem NothingElseMatters
23    )
24    IF Not "!FileNameToCopy!"=="0" (
25        set /A FileNameToCopy+=1
26    IF "!FileNameToCopy!"=="3" (
27        set /a FileNameToCopy=0
28        Set HardlinkFile=%%x
29    )
30    )
31    IF Not "!resultToCopy!"=="0" (
32        set /a resultToCopy+=1
33        IF /I "%%x" EQU "FindLinks v1.0 - Locate file hard links" (
34            set /a resultToCopy=0
35        ) ELSE (
36            IF "2"=="!resultToCopy!" (
37                Echo =====>> HardLinkResult.txt

```

Рисунок П1.2 – Содержимое файла *CutTheTrash.bat* при создании жестких ссылок

```

HardLinkResult.txt — Блокнот
Файл  Правка  Формат  Вид  Справка
=====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 П1.3 – 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 C:\Tests\BHS\Test1-RW, C:\Tests\BHS\Test2-R, C:\Tests\BHS\Test3-W, C:\Tests\BHS\test4- в соответствии с таблицей П1.1.

Таблица П1.1 – Пример дискреционного разграничения доступа для каталогов при работе с жесткими ссылками

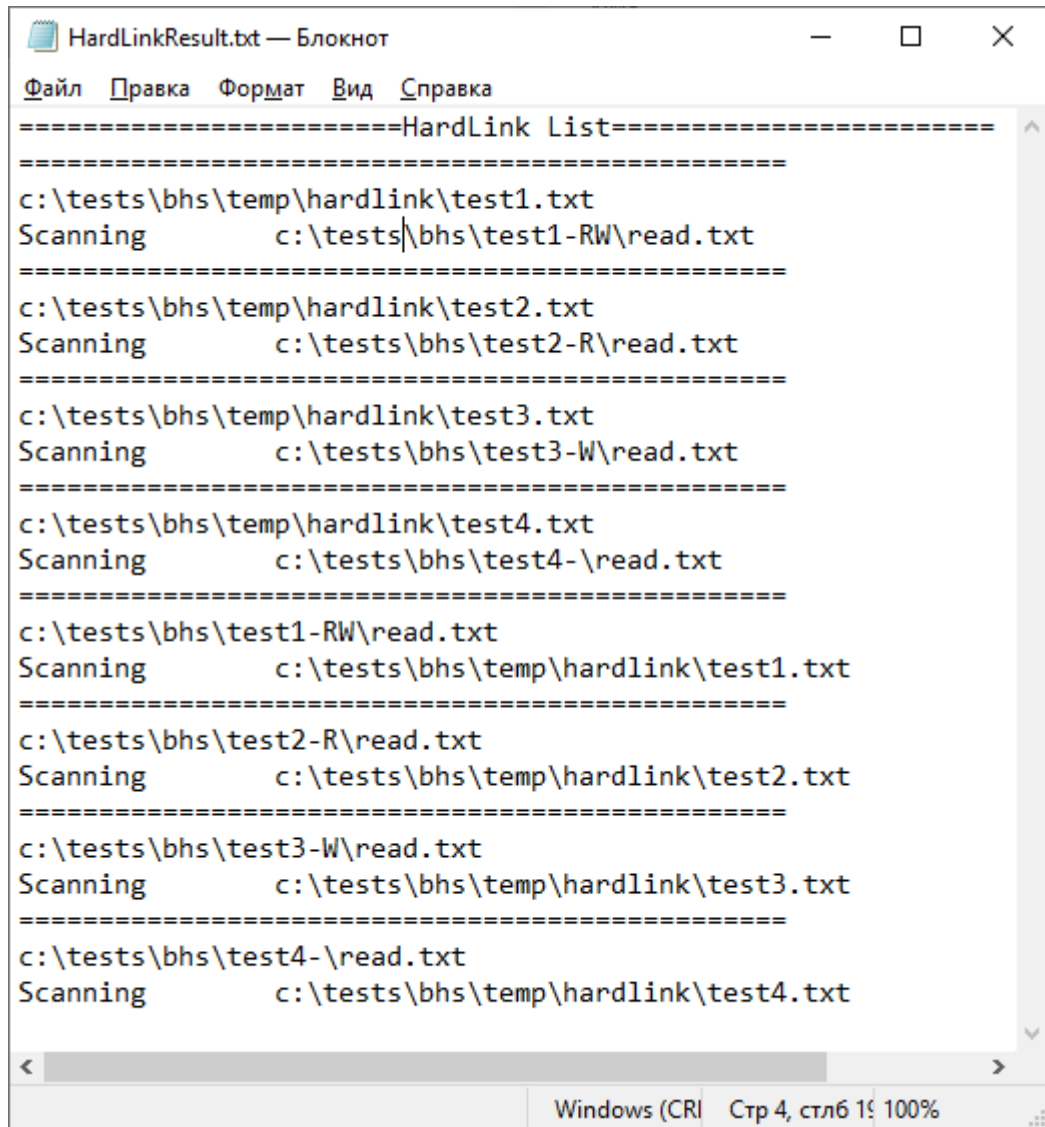
	Права доступа
C:\Tests\BHS\Test1-RW	RW
C:\Tests\BHS\Test2-R	R
C:\Tests\BHS\Test3-W	W
C:\Tests\BHS\Test4-	-

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

```
C:\hardlinkList\HardlinkFull.bat C:\Tests\BHS\
```

В результате в папке C:\hardlinkList\ создается файл *HardlinkResult.txt*, содержащий список файлов и жестких ссылок (рисунок П1.4).

Из рисунка П1.3 видно, что были обнаружены попарно одинаковые объекты (например, при проверке файла C:\Tests\BHS\Test1-RW\Read.txt был обнаружен файл с такой же структурой данных по адресу C:\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 П1.1 (рисунок П1.5).



```
HardLinkResult.txt — Блокнот
Файл  Правка  Формат  Вид  Справка
=====HardLink List=====
c:\tests\bhs\temp\hardlink\test1.txt
Scanning      c:\tests\bhs\test1-RW\read.txt
c:\tests\bhs\temp\hardlink\test2.txt
Scanning      c:\tests\bhs\test2-R\read.txt
c:\tests\bhs\temp\hardlink\test3.txt
Scanning      c:\tests\bhs\test3-W\read.txt
c:\tests\bhs\temp\hardlink\test4.txt
Scanning      c:\tests\bhs\test4-\read.txt
c:\tests\bhs\test1-RW\read.txt
Scanning      c:\tests\bhs\temp\hardlink\test1.txt
c:\tests\bhs\test2-R\read.txt
Scanning      c:\tests\bhs\temp\hardlink\test2.txt
c:\tests\bhs\test3-W\read.txt
Scanning      c:\tests\bhs\temp\hardlink\test3.txt
c:\tests\bhs\test4-\read.txt
Scanning      c:\tests\bhs\temp\hardlink\test4.txt
Windows (CRI)  Стр 4, стлб 1 100%
```

Рисунок П1.4 – Пример проверки наличия жестких ссылок

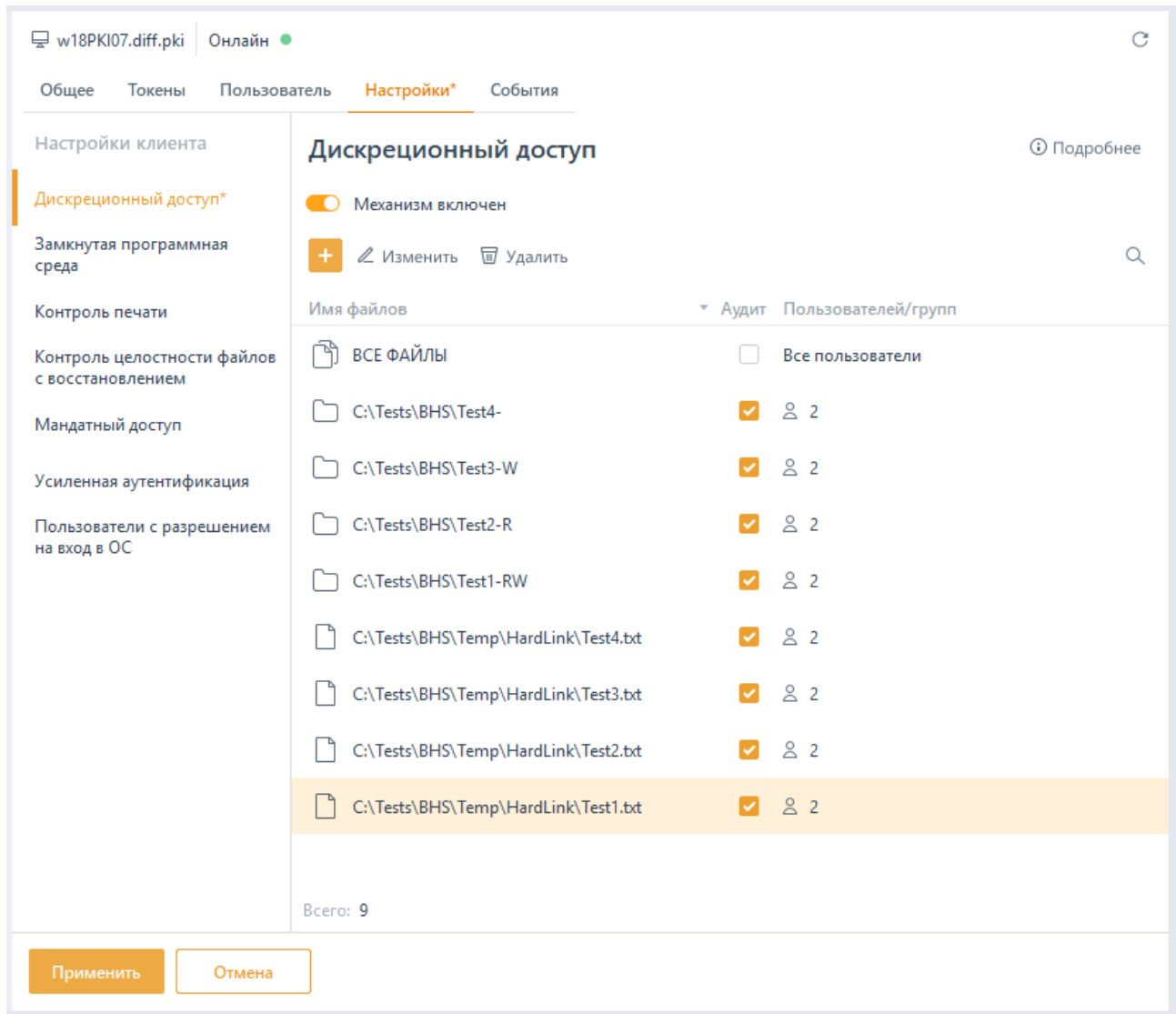


Рисунок П1.5 – Установка разграничений доступа в СЗИ для файлов и их жестких ссылок

1.2 Особенности работы с символьными ссылками

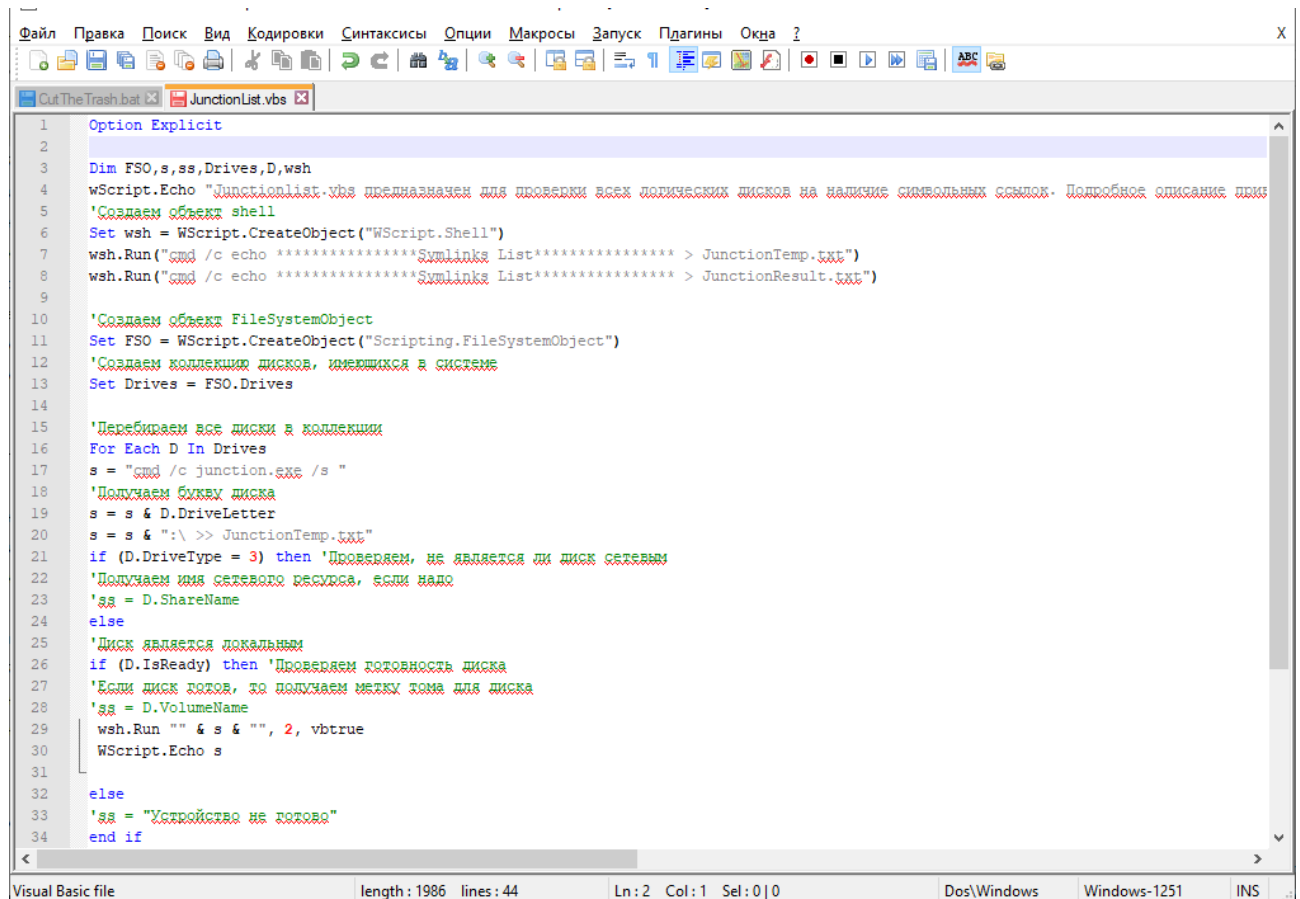
Основная особенность разграничения доступа к файлам или каталогам, имеющим символьные ссылки, состоит в следующем – в консоли администрирования СЗИ права доступа должны быть настроены администратором безопасности обязательно для оригинального файла (оригинального каталога). В этом случае попытка доступа к этому файлу или каталогу 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 П1.6 и П1.7. 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>).



```
1 Option Explicit
2
3 Dim FSO,s,ss,Drives,D,wsh
4 wScript.Echo "Junctionlist.vbs предназначена для проверки всех логических дисков на наличие символьных ссылок. Подробное описание программы
5 'Создаем объект shell
6 Set wsh = WScript.CreateObject("WScript.Shell")
7 wsh.Run("cmd /c echo *****Svmlinks List***** > JunctionTemp.txt")
8 wsh.Run("cmd /c echo *****Svmlinks List***** > JunctionResult.txt")
9
10 'Создаем объект FileSystemObject
11 Set FSO = WScript.CreateObject("Scripting.FileSystemObject")
12 'Создаем коллекцию дисков, имеющихся в системе
13 Set Drives = FSO.Drives
14
15 'Перебираем все диски в коллекции
16 For Each D In Drives
17 s = "cmd /c junction.exe /s "
18 'Получаем букву диска
19 s = s & D.DriveLetter
20 s = s & ":\ >> JunctionTemp.txt"
21 if (D.DriveType = 3) then 'Проверяем, не является ли диск сетевым
22 'Получаем имя сетевого ресурса, если надо
23 'ss = D.ShareName
24 else
25 'Диск является локальным
26 if (D.IsReady) then 'Проверяем готовность диска
27 'Если диск готов, то получаем метку тома для диска
28 'ss = D.VolumeName
29 wsh.Run "" & s & "" , 2, vbtrue
30 WScript.Echo s
31
32 else
33 'ss = "Устройство не готово"
34 end if
```

Рисунок П1.6 – 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* (рисунок П1.8), в котором нужно нажать кнопку подтверждения. Результатом работы скрипта *Junctionlist.vbs* является файл *JunctionResult.txt* с перечнем файлов и символьных ссылок на них (рисунок П1.10). После окончания проверки каждого логического диска появится окно, приведенное на рисунке П1.9.
- *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*.

```

1 |echo off
2 |setlocal ENABLEDELAYEDEXPANSION
3 |Set FilePath=%~1
4 |set resultToCopy=0
5 |set stringPrevios=
6 |For /F "tokens=* delims=" %%x IN ('type "%FilePath%") DO (
7 |   set StringToCompare=%%x
8 |   IF /I "!StringToCompare:~0,19!" EQU " Print Name      :" (
9 |       |set /A resultToCopy=1
10 |       set ResultPathLink=!StringPrevios!
11 |       ) ELSE (
12 |       set StringPrevios=%%x
13 |       rem NothingElseMatters
14 |       )
15 |
16 | IF Not "!resultToCopy!"=="0" (
17 | set /a resultToCopy+=1
18 |
19 | IF "2"=="!resultToCopy!" (
20 |   Echo =====>>> JunctionResult.txt
21 |   echo !ResultPathLink! >> JunctionResult.txt
22 |   Echo %%x >> JunctionResult.txt
23 |   ) ELSE (
24 |   echo %%x >> JunctionResult.txt
25 |   set /a ResultToCopy=0
26 |   )
27 | )
28 | )
29 |
30 |exit
  
```

Batch file length: 842 lines: 30 Ln: 1 Col: 1 Sel: 0|0 Dos\Windows UTF-8 w/o BOM INS

Рисунок П1.7 – Содержимое файла *CutTheTrash.bat* при создании символьных ССЫЛОК



Рисунок П1.8 – Окно ознакомления с лицензией

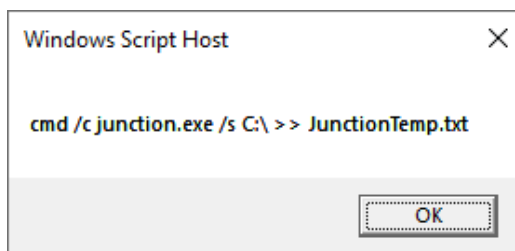
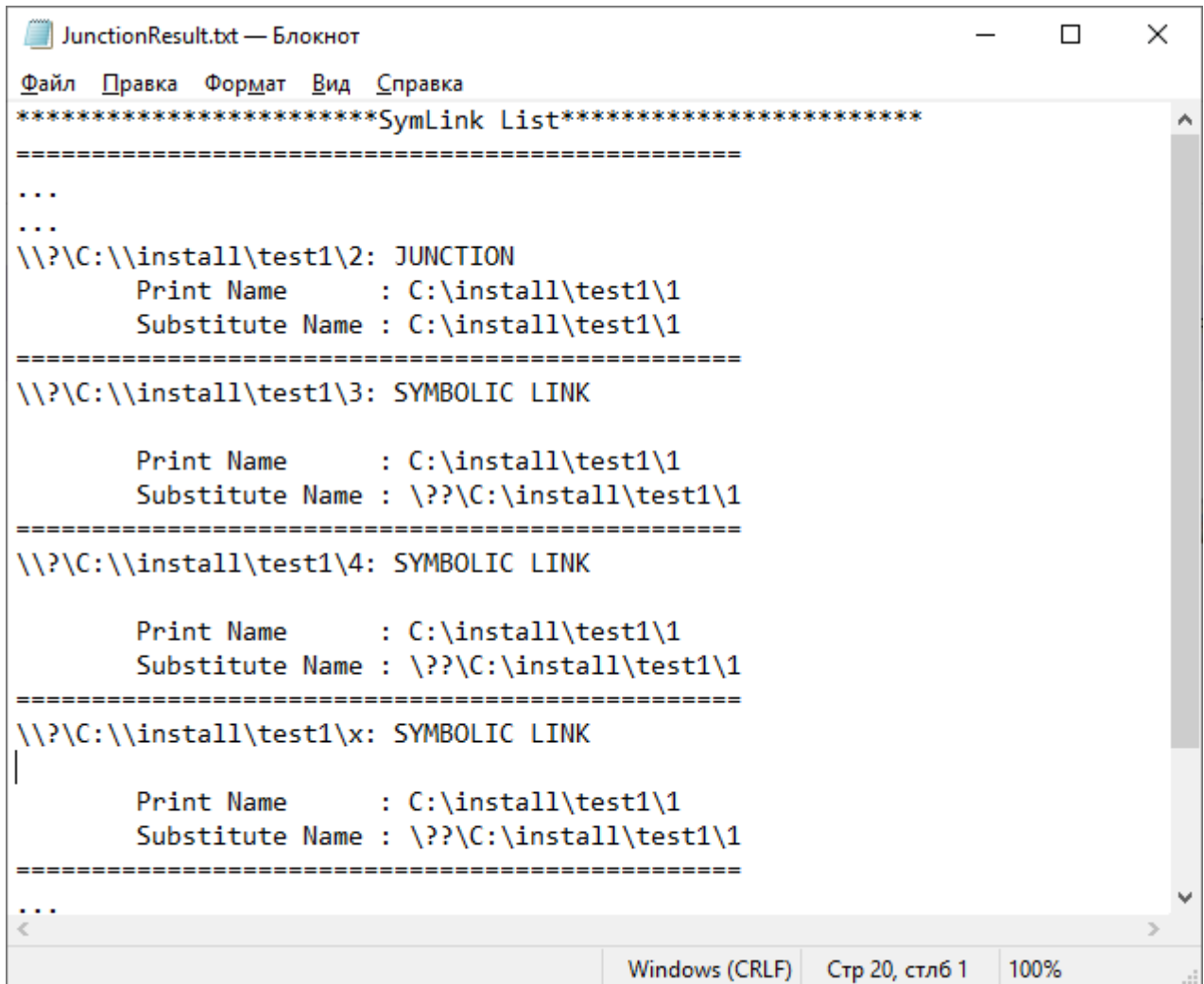


Рисунок П1.9 – Окно завершения проверки диска



```
JunctionResult.txt — Блокнот
Файл  Правка  Формат  Вид  Справка
*****Symlink List*****
=====
...
...
\\?\C:\\install\test1\2: JUNCTION
    Print Name      : C:\install\test1\1
    Substitute Name  : C:\install\test1\1
=====
\\?\C:\\install\test1\3: SYMBOLIC LINK
    Print Name      : C:\install\test1\1
    Substitute Name  : \\?\C:\install\test1\1
=====
\\?\C:\\install\test1\4: SYMBOLIC LINK
    Print Name      : C:\install\test1\1
    Substitute Name  : \\?\C:\install\test1\1
=====
\\?\C:\\install\test1\x: SYMBOLIC LINK
    Print Name      : C:\install\test1\1
    Substitute Name  : \\?\C:\install\test1\1
=====
...
Windows (CRLF)  Стр 20, стлб 1  100%
```

Рисунок П1.10 – Пример содержимого файла *JunctionResult.txt*

Первая строка на рисунке П1.10 показывает расположение символьной ссылки (*junction point* или *symlink*);

В строке *Substitute Name* на рисунке П1.10 показано расположение оригинального файла, для которого создана символьная ссылка.

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

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

2 Настройка жестких и символьных ссылок 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 **«Настройка жестких и символьных ссылок в дискреционном механизме 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 разделах **«Особенности работы с жесткими ссылками»** и **«Особенности работы с символьными ссылками»** настоящего приложения.
- 2) В настройках мандатного разграничения консоли администрирования СЗИ присвоить одинаковые мандатные метки контролируемым объектам (файлам и каталогам) и жестким ссылкам, относящимся к ним.
- 3) Для объектов, имеющих символьные ссылки необходимо убедиться, что в настройки мандатного механизма на контроль добавлены исходные файлы и каталоги, а не их символьные ссылки. Установленные права доступа для оригинального объекта (файла или каталога) будут действовать при попытках доступа к нему по символьной ссылке.