

ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00060-05 92 03–ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«ВАЛИДАТА CSP» ВЕРСИЯ 5.0

ПРОГРАММА КОНТРОЛЯ ЦЕЛОСТНОСТИ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

ВАМБ.00060-05 92 03

2016

Аннотация

Программа контроля целостности **hashfile.exe** из состава ПО СКЗИ «Валидата CSP» предназначена для контроля за составом и целостностью системного программного обеспечения (ПО), прикладного ПО, а также для контроля целостности СКЗИ «Валидата CSP».

ПО контроля целостности предназначено для использования в 32- битных и 64-битных версиях операционных систем (ОС) Microsoft Windows XP/Server 2003/Vista/Server 2008/7/Server 2008 R2/8/8.1/Server 2012/Server 2012 R2.

Контроль целостности обеспечивается за счёт использования криптографических функций, а именно, вычисления хэш-функций по алгоритмам ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012.

Для обеспечения контроля предусматривается создание списка контролируемых файлов с вычисленными значениями хэш-функции для каждого файла и последующая проверка значений хэш-функции для всех файлов из списка.

Содержание

1 СОСТАВ И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ	4
2 СОЗДАНИЕ СПИСКА КОНТРОЛЯ ЦЕЛОСТНОСТИ	5
3 АВТОМАТИЧЕСКАЯ ПРОВЕРКА КОНТРОЛЯ ЦЕЛОСТНОСТИ	7
4 КОНТРОЛЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПО СПИСКУ	9
5 РЕГЛАМЕНТ ПРИМЕНЕНИЯ	10
6 КОДЫ ВОЗВРАТА	11
ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	11
ПЕРЕЧЕНЬ ТАБЛИЦ	13

1 СОСТАВ И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

В состав ПО СКЗИ «Валидата CSP» входит программный исполняемый модуль **hashfile.exe** (далее по тексту - программа **hashfile.exe**) контроля целостности ПО, работающий под ОС Windows (как консольное приложение).

Программа **hashfile.exe** запускается из командной строки со следующими параметрами:

hashfile.exe [-p] -Command Infile OutFile [/S] [/m|/M] [/G]

Описание параметров:

-**p** - необязательный параметр, требующий выдачи на экран терминала информации о работе программы. При отсутствии этого параметра программа **hashfile.exe** ничего не выдаёт на экран терминала;

- **<Command>** - обязательный параметр, устанавливающий тип выполняемой операции. Данный параметр может иметь два значения:

-**F** - создание файла, содержащего список контроля целостности ПО;

-**T** - выполнение контроля целостности ПО на основе списка контроля целостности;

-**C** - вычисление контрольной суммы файла и запись ее в список контроля целостности, хранящийся в реестре ОС Windows;

-**V** - выполнение контроля целостности ПО на основе списка контроля целостности, хранящегося в реестре ОС Windows;

- **Infile** - для типа операции **-F** - имя входного файла, содержащего список контролируемого ПО; для типа операции **-T** - имя входного файла, содержащего список контроля целостности ПО; для типа операции **-C** - имя входного файла, для которого следует вычислить контрольную сумму;

- **Outfile** - для типа операции **-F** - имя выходного файла, содержащего список контроля целостности ПО; для типов операции **-T** и **-V** - имя выходного файла, содержащего протокол проверки целостности ПО;

- **/S** - прекратить проверку файлов при возникновении ошибки;

- **/G** - использовать алгоритм хэширования по ГОСТ Р 34.11-2012;

- **/m** - не закрывать окно при возникновении ошибки;

- **/M** - не закрывать окно при возникновении ошибки и выдать диалоговое окно.

2 СОЗДАНИЕ СПИСКА КОНТРОЛЯ ЦЕЛОСТНОСТИ

Для создания списка контроля целостности ПО необходимо предварительно подготовить список контролируемого ПО. Список контролируемого ПО представляет собой текстовый файл, содержащий в каждой строке по одному имени файла контролируемого ПО.

Например, файл со списком контролируемого ПО может выглядеть так:

```
c:\test\test1.txt
e:\test\util\file.exe
lib.dll
```

Для создания списка контроля целостности необходимо выполнить программу **hashfile.exe** со следующими параметрами:

```
hashfile.exe -p -F list.txt hash.out
```

или

```
hashfile.exe -F list.txt hash.out
```

В первом случае программа будет выдавать на консоль информацию о процедуре обработки, а во втором случае информация на экран пользователя выдаваться не будет.

list.txt - это файл, содержащий список контролируемого ПО;

hash.out - это имя создаваемого программой файла, в который будет записан список контроля целостности ПО, т.е. список файлов (перечисленных в **list.txt**), их длины и их контрольные суммы (хэш-функции содержимого файлов).

В результате работы программы формируется файл списка с указанным именем и расширением, имеющий (пример) следующую структуру:

```
gdbm.dll
000033103910F6A96340C73188AB2D6D603696682AD081C1A0246E0D5097B71A4F1B208C
init.dll
00006000EBFB6FB7D8914D3AC11751040090A4448EB969A4564690868DABAE0F870B1B47
intl3.dll
00001D10D3A09A52D10A38EA88E89E770412B71B67B2724E40BE8893FC946B203281971E
spki.dbg
0006F48C1A3AF83C45B5F4CAB1D7942738E6AEAE042F9ED490459BFE3B285C8540038B6C
```

Примечания

1 Если в имени файла, входящего в список контроля целостности, встречаются символы кириллицы, имя файла в списке должно быть записано в кодировке Windows-1251.

2 Программа (**hashfile.exe**) не предназначена для контроля целостности самого исполняемого модуля **hashfile.exe** и списка контроля целостности ПО. Способы контроля целостности этих файлов описаны в документе ВАНБ.00060-05 93 02. «СКЗИ «Валидата CSP» версия 5.0. Программа контроля целостности. Руководство администратора информационной безопасности».

При работе программы с параметром **-p** на дисплей, например, выводится следующая информация:

Программа верификации файлов v1.12.02

Обработан файл: gdbm.dll

Статус завершения: 0

Обработан файл: init.dll

Статус завершения: 0

Обработан файл: intl3.dll

Статус завершения: 0

Обработан файл: spki.dbg

Статус завершения: 0

Необходимо отметить, что 32-битная программа **hashfile.exe**, запускаемая на платформе x64, при обращении к файлу, расположенному в системном каталоге **%WINDIR%\System32**, в действительности будет обращаться к файлу с таким же именем, но расположенному в системном каталоге **%WINDIR%\SysWOW64**. Из-за этой особенности, в общем случае, на платформе x64 следует запускать 64-битную программу **hashfile.exe** для контроля целостности исполняемых модулей.

3 АВТОМАТИЧЕСКАЯ ПРОВЕРКА КОНТРОЛЯ ЦЕЛОСТНОСТИ

Программа **hashfile.exe** получила новые сервисные возможности: при инсталляции установочного пакета в реестре Windows создаётся список исполняемых файлов, содержащихся в этом установочном пакете и подлежащих автоматическому контролю целостности, причём для каждого файла указывается его контрольная сумма (хэш). При каждом запуске пользовательского сеанса Windows программа **hashfile.exe** запускается автоматически с параметром **-V**, что приводит к проверке контрольных сумм всех файлов, находящихся в списке. В случае несовпадения контрольных сумм на экран выдаётся сообщение (Рисунок 1).

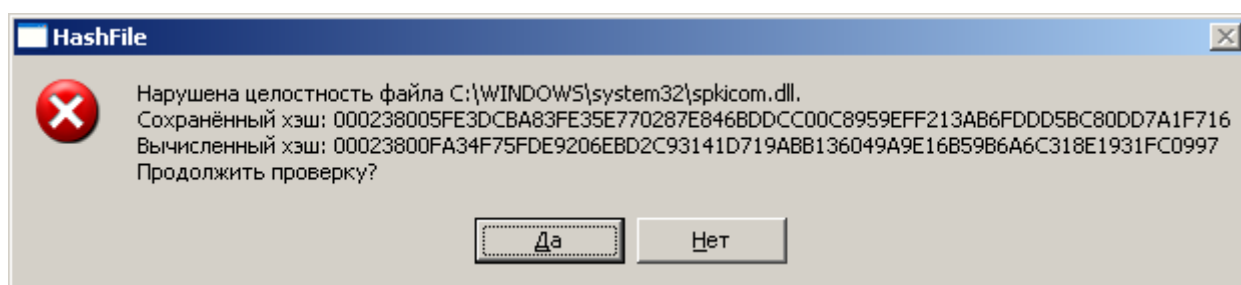


Рисунок 1 – Сообщение о нарушении целостности файла

Нажатие кнопки «Да» продолжит проверку целостности файлов, нажатие кнопки «Нет» - прекратит проверку. В любом случае, если в ходе проверки будет обнаружено нарушение целостности или отсутствие хотя бы одного файла из списка, в конце будет выдано сообщение (Рисунок 2).

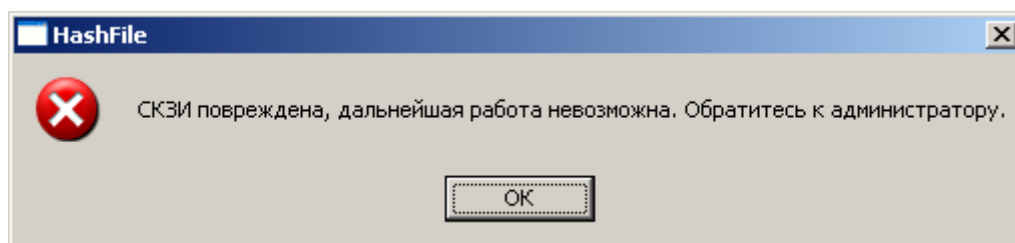


Рисунок 2 – Сообщение о нарушении целостности СКЗИ

В случае получения такого сообщения использование СКЗИ недопустимо.

При необходимости администратор может изменить эталонное значение контрольной суммы файла или добавить новый файл в список контроля целостности. Для этого необходимо запустить программу **hashfile.exe** с параметрами **-C <PathToHash>**, где **<PathToHash>** - полный путь к файлу, для которого вычисляется новая контрольная сумма, например:

hashfile.exe -C c:\windows\system32\spkicom.dll

Программа **hashfile.exe** также позволяет получить файл, содержащий информацию о размере, дате изменения и версии каждого из файлов, входящих в список контроля целостности. Для этого необходимо запустить программу **hashfile.exe** с параметрами **-V <LogFile>**, где **<LogFile>** - имя файла протокола, в который будет записана информация, например:

hashfile.exe -V c:\tmp\ver.log

Необходимо отметить, что 32-битная программа **hashfile.exe**, запускаемая на платформе x86, и 64-битная программа **hashfile.exe**, запускаемая на платформе x64, хранят список авто-

матического контроля в разделе **HKLM\Software\Validata\Hashfile** реестра Windows. Однако, 32-битная программа **hashfile.exe**, запускаемая на платформе x64, хранит список автоматического контроля в разделе **HKLM\Software\Wow6432Node\Validata\Hashfile** реестра Windows. Из-за этой особенности, в общем случае, на платформе x64 следует запускать 64-битную программу **hashfile.exe** для контроля целостности 64-битных исполняемых модулей, и запускать 32-битную программу **hashfile.exe** для контроля целостности 32-битных исполняемых модулей.

4 КОНТРОЛЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПО СПИСКУ

Программой **hashfile.exe** диагностируются следующие изменения файлов ПО:

- изменение размера каждого файла контролируемого ПО;
- изменение содержимого каждого файла контролируемого ПО на основе сравнения значений хэш-функций.

Для выполнения процедуры проверки контроля целостности ПО необходимо иметь предварительно сформированный список контроля целостности ПО и исполняемый модуль программы **hashfile.exe** (записанные на внешнем носителе согласно документу ВАМБ.00060-05 93 02 «Программа контроля целостности. Руководство администратора информационной безопасности»). Запуск программы **hashfile.exe** производится в командной строке с параметрами, описываемыми ниже.

Выполнение проверки целостности ПО производится следующим образом:

hashfile.exe -p -T hash.out result.log

или

hashfile.exe -T hash.out result.log.

В первом случае программа будет выдавать на экран консоли информацию о процедуре проверки, а во втором случае информация на экран пользователя выдаваться не будет.

hash.out - это файл, содержащий список контроля целостности ПО.

result.log - это имя создаваемого программой файла, в который будет записан протокол проверки целостности ПО в текстовом виде.

Протокол проверки ведется для каждого файла в отдельности и имеет следующий вид:

Имя файла : test.txt

Хэш (записанный) : CE0D64F8 16EAA63B 710262E1 25E7BC1D 09FC2E17
A14C484A 012C7B8C 3837A2C6

Хэш (вычисленный) : CE0D64F8 16EAA63B 710262E1 25E7BC1D 09FC2E17
A14C484A 012C7B8C 3837A2C6

Размер файла (записанное) : 23486

Размер файла (вычисленное) : 23486

Статус завершения : Файл не изменен

Если при контроле ПО обнаруживается несколько ошибок в различных файлах, то на экран в качестве результирующей ошибки выдается сообщение:

Программа завершилась с ошибкой 1006.

Сообщение: Множественная ошибка.

При обнаружении нарушения целостности ПО необходимо принять меры в соответствии с рекомендациями, изложенными в ВАМБ.00060-05 93 02. «СКЗИ «Валидата CSP» версия 5.0. Программа контроля целостности. Руководство администратора информационной безопасности».

5 РЕГЛАМЕНТ ПРИМЕНЕНИЯ

Проверка целостности ПО любого автоматизированного рабочего места (АРМ), включающего в себя ПО, выполняющее криптографические преобразования, должна выполняться каждый раз перед запуском ПО АРМ.

Запуск ПО АРМ должен выполняться из командного файла, в состав которого необходимо включить следующий набор команд:

```
hashfile -p -T file.hsh file.log
if errorlevel 1 goto err
color 7
echo CHECK OK!
< Запуск ПО АРМ >
goto End
:err
color C
echo CHECK ERRORS!
< Нарушена целостность ПО АРМ >
:End
```

В данном примере **file.hsh** - это файл с контрольными хэш-функциями ПО АРМ, а **file.log** - это файл с протоколом проверки.

Данный набор команд не является обязательным, но его можно взять за основу при создании командного файла для запуска какого-либо ПО АРМ.

Если по завершению работы программы необходимо видеть результат проверки на экране монитора, то необходимо в командном файле запуска ПО АРМ выполнить команду «пауза». Например, следующим образом:

```
hashfile -p -T file.hsh file.log
pause
```

В данном случае после выполнения проверки командный файл остановит свою работу, и будет ждать нажатия любой клавиши на клавиатуре.

6 КОДЫ ВОЗВРАТА

Коды возврата, возвращаемые программой hashfile.exe, приведены ниже (Таблица 1).

Таблица 1 – Коды возврата, возвращаемые программой hashfile.exe

Код возврата	Описание
0	Нет ошибки. Программа выполнена успешно
2	Ошибка открытия файла
1000	Неверно заданы параметры командной строки
1001	Внутренняя ошибка программы
1002	Изменен размер файла
1004	Нарушена целостность файла. Не совпадает значение хэш-функции файла
1006	Множественная ошибка. Нарушена целостность нескольких файлов

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
СКЗИ	Средство криптографической защиты информации
ОС	Операционная система (Operating System)
ПО	Программное обеспечение

ПЕРЕЧЕНЬ ТАБЛИЦ

1	Коды возврата, возвращаемые программой hashfile.exe	11
---	---	----

[illegible][illegible]