УДК 004.056.53 Вестник УрФО № 4(18) / 2015, стр. 12–15

Скурлаев С. В., Соколов А. Н.

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ WINDOWS TO GO В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ КЛАССОВ 2А И 3А С СЕРТИФИЦИРОВАННЫМИ СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ

Предложена альтернатива использованию съёмного системного жёсткого диска с использованием устройства Mobile Rack в виде внешнего жёсткого диска или USB-флэш накопителя (USB-накопителя). Поставлен эксперимент, позволяющий выяснить работоспособность предложенного решения. Описаны основные трудности, возникшие в ходе эксперимента, и способы их преодоления. Сделаны предложения для улучшения совместимости работы USB-накопителя с используемым средством защиты информации.

Ключевые слова: *автоматизированная система (АС), контроль целостности (КЦ), несанкционированный доступ (НСД), операционная система (ОС), основные технические средства и системы (ОТСС), средство защиты информации (СЗИ).*

Skurlaev S. V., Sokolov A. N.

TECHNICAL SOLUTIONS USED FOR 3A/2A CLASS SYSTEMS TO PROTECT AGAINST UNAUTHORIZED ACCESS

Use of USB-drive (USB-flash pendrive or USB-harddrive) suggested as an alternative for removable hard drive with use of Mobile Rack mount. Perfomed an experiment that allows to research compatibility of the proposed solution. Described main difficulties encountered in the course of the experiment, and ways to overcome them. Made suggestions for improving the compatibility of use USB-drive with means of information protection.

Keyword: *automated system (AS), integrity control (IC), unauthorized access (UA), operating system (OS), primary technical means and systems (PTMS), means of protecting information from unauthorized access.*

В случае обработки информации в автоматизированных системах классов 3А, 2А и выше нормативными документами требуется либо обеспечить условия хранения обрабатываемой информации в помещении с основными техническими средствами и системами (ОТСС), либо осуществить отчуждаемость носителей информации от этих средств для хранения их в другом оборудованном для этих целей помещении. В том случае, когда в организации есть несколько помещений с расположенными в них ОТСС, как правило, выбирается и оборудуется только одно из них для целей хранения защищаемой информации, а в другом помещении, где предусмотрена лишь обработка, требуется обеспечить отчуждаемость накопителей информации от ОТСС, в том числе и основного жёсткого диска с установленной на нём операционной системой (ОС). В некоторых организациях внутренними нормативными документами обеспечить отчуждаемость накопителей требуется в любом случае с целью дальнейшего их хранения в сейфах или металлических шкафах. Основной и де-факто единственный возможный способ до последнего времени предполагал размещение жёсткого диска в устройстве Mobile Rack (салазки) (рис. 1) в корпусе системного блока, что негативно сказывалось на продолжительности работы и производительности устройства.

Для осуществления отчуждаемого жёсткого диска можно прибегнуть к нескольким способам:

1. Обычным решением является использование устройства Mobile Rack в корпусе системного блока для удобного извлечения жёсткого диска после завершения работы.

2. Альтернативным решением является использование внешнего накопителя, подключающегося через USB-разъём. Он может быть как обычным жёстким диском, который располагается в разборном или неразборном корпусе, так и USB-флэш накопителем.

Первый способ является более распространённым на данный момент. Устройства Mobile Rack занимают отсек 5.25 в корпусе системного блока, в отделяющуюся часть помещается жёсткий диск. При этом Mobile Rack редко обеспечивает необходимый для жёстких дисков температурный режим, а ежедневное подключение и отключение устройства также способствует снижению срока его жизни.

В качестве альтернативы предлагается использовать технологию переносимой операционной системы, установленной на USB-накопитель. Чтобы проверить работоспособность механизмов СЗИ, описанных в предыдущей статье [1], поставлен эксперимент: в качестве целевой ОС выбрана Windows 8.1, поскольку технология Windows To Go появилась начиная с Windows 8, а в качестве СЗИ выбран Secret Net 7, поскольку является сертифицированным средством для выбранной ОС. Поставленный эксперимент основывается на рекомендуемых в статье Microsoft2 шагах и заключается в последовательной установке на USB-накопитель ОС, пакета прикладных программ, СЗИ, с дальнейшей настройкой и тестовой эксплуатацией.

В ходе эксперимента использовались штатные средства Windows 8.1. Эксперимент выполнен поэтапно:

1. Выбраны такие накопители, у которых не установлен флаг удаляемого устройства (removable bit): он сообщает ОС, что данное устройство может быть извлечено во время работы компьютера; по умолчанию флаг «removable bit» у USB-флэш накопителей находится в состоянии «1» (установлен), а у внешних жёстких дисков в состоянии «0» (не установлен).

2. Для создания рабочей среды Windows To Go ёмкость накопителя разбита на разделы с использованием скрипта, предложенного Microsoft [2]:

Рис. 1. Устройство Mobile Rack

```
   # The following command will set $Disk to all USB drives with >20 GB of
storage
   $Disk = Get-Disk | Where-Object {$_.Path -match «USBSTOR» -and $_.Size
-gt 20Gb -and -not $_.IsBoot }
   #Clear the disk. This will delete any data on the disk. (and will fail
if the disk is not yet initialized. If that happens, simply continue with
'New-Partition…) Validate that this is the correct disk that you want to
completely erase.
   # To skip the confirmation prompt, append –confirm:$False
   Clear-Disk –InputObject $Disk[0] -RemoveData –confirm:$False
   # This command initializes a new MBR disk
   Initialize-Disk –InputObject $Disk[0] -PartitionStyle MBR
   # This command creates a 350 MB system partition
   $SystemPartition = New-Partition –InputObject $Disk[0] -Size (350MB)
-IsActive
   # This formats the volume with a FAT32 Filesystem
   # To skip the confirmation dialog, append –Confirm:$False
   Format-Volume -NewFileSystemLabel «UFD-System» -FileSystem FAT32 `
   -Partition $SystemPartition –Confirm:$False
   # This command creates the Windows volume using the maximum space
available on the drive. The Windows To Go drive should not be used for other
file storage.
   $OSPartition = New-Partition –InputObject $Disk[0] -UseMaximumSize
   Format-Volume -NewFileSystemLabel «UFD-Windows» -FileSystem NTFS `
   -Partition $OSPartition –Confirm:$False
   # This command assigns drive letters to the new drive, the drive letters
chosen should not already be in use.
   Set-Partition -InputObject $SystemPartition -NewDriveLetter «S»
   Set-Partition -InputObject $OSPartition -NewDriveLetter «W»
   # This command sets the NODEFAULTDRIVELETTER flag on the partition which
prevents drive letters being assigned to either partition when inserted into
a different computer.
   Set-Partition -InputObject $OSPartition -NoDefaultDriveLetter $TRUE
```

После окончания работы скрипта ёмкость USB-накопителя разделена на два раздела, ниже приведена таблица разделов для USB-флэш накопителя:

```
PS C:\Windows\system32> Get-Volume -DriveLetter S,W
DriveLetter  FileSystemLabel  FileSystem  DriveType  HealthStatus  SizeRemaining  Size
-----------  --------------  ----------  ---------  ------------  -------------  ----
S            UFD-Windows     NTFS        Fixed      Healthy       334.51 MB    350 MB
W            UFD-Windows     NTFS        Fixed      Healthy       117.42 GB  117.53GB
```

3. Для эксперимента использован образ install.wim из установочного дистрибутива ОС Windows 8.1 Pro. Распаковка выполнена с помощью командлета и его параметров:

```
   Expand-WindowsImage –ImagePath
F:\sources\install.wim –Index 1 –
ApplyPath W:\
```

4. ОС установлена, загружена с USB-накопителя и обновлена с учётом всех выпущенных исправлений и обновлений.

5. С целью тестового применения установлен пакет офисных программ LibreOffice 5.

6. Завершающим этапом является установки и настройка СЗИ.

По итогам эксперимента стало ясно, что предложенный Microsoft способ установки не является оптимальным для ОС с СЗИ. Прежде чем удалось достичь последнего шага, эксперимент начинался заново ввиду нестабильности ОС в работе. При использовании USB-флэш накопителя ОС не могла установить все исправления, перестав корректно загружаться после обновления драйверов. Время отклика дисковой подсистемы (storage latency) под нагрузкой составляла около 3000 мс для основных процессов, на рис. 2 приведён скриншот отчёта монитора ресурсов при установке обновлений.

При использовании внешнего жёсткого диска ситуация становилась приближенной к использованию обычного внутреннего накопителя, но ОС после установки и тестовой эксплуатации СЗИ перестала корректно загружаться.

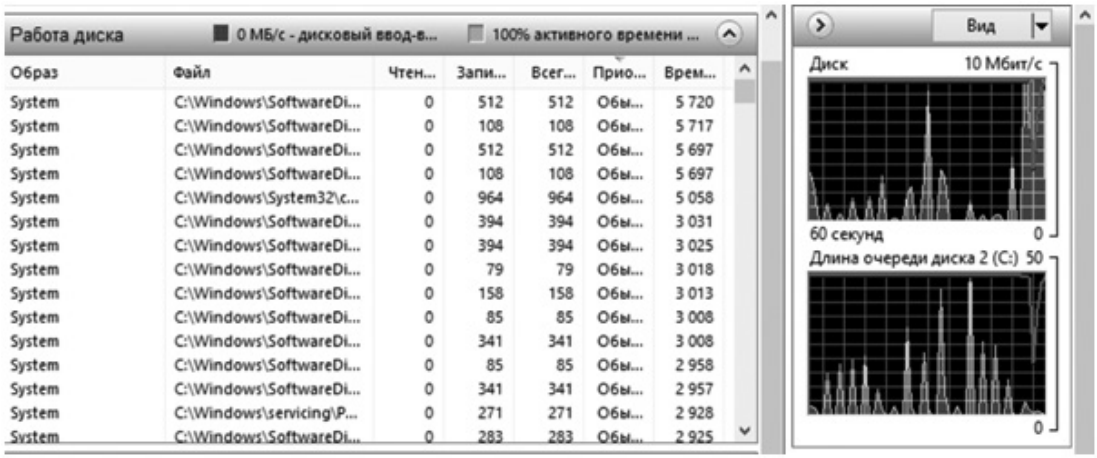

Рис. 2. Время отклика дисковой подсистемы при установке обновлений

Из приведённого выше следует, что условия эксперимента требуется изменить, чтобы достичь поставленной цели. Для этого предлагается использовать не стандартный образ из дистрибутива ОС Windows 8.1, а модифицированный, где уже будут предустановлены необходимые программы и СЗИ. Также возможно применение других способов и средств контроля целостности, рассмотренных в предыдущей статье [3] и в статье Microsoft [4]. После достижения положительных результатов с использованием предложенных модификаций работоспособность решения необходимо протестировать при типовой нагрузке для указанных классов АС, а также с помощью алгоритма, описанного в предыдущей статье [5].

Примечания

1. Скурлаев С. В., Соколов А. Н. Технические решения, применяемые для защиты от несанкционированного доступа в системах классов 3А и 2А //Вестник УрФО. Безопасность в информационной сфере. – Челябинск : Изд. центр ЮУрГУ, 2014. – №1 (11). – С. 21–26.

2. Deploy Windows To Go in Your Organization. URL: https://technet.microsoft.com/ru-ru/library/JJ721578.aspx (дата обращения 20.11.2015).

3. Скурлаев С. В., Соколов А. Н. Проблема неизменности доверенной базы при защите системного и прикладного программного обеспечения от несанкционированного доступа // Безопасность информационного пространства : сборник трудов XIII Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных. — Челябинск : Изд. центр ЮУрГУ, 2015. – С. 140–143.

4. Availability and description of the File Checksum Integrity Verifier utility. URL: http://support.microsoft.com/kb/841290 (дата обращения 10.11.2014).

5. Скурлаев С. В., Соколов А. Н. Исследование системы разграничения доступа на основе поведенческой модели пользователя //Информационное противодействие угрозам терроризма: научно-практический журнал. Материалы XIV научно-практической конференции «Информационная безопасность – 2015». Таганрог, 4–7 июня 2015 г. – Таганрог : Изд. Южного федерального университета, 2015. – № 24. – С. 98–102.

Скурлаев Сергей Вадимович, аспирант кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет), специалист по защите информации ООО «Стратегия безопасности», г. Челябинск. E-mail: sch1081024@mail.ru

Соколов Александр Николаевич, кандидат технических наук, доцент, зав. кафедрой безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет), г. Челябинск. E-mail: ANSokolov@inbox.ru

Sergey Skurlaev, postgraduate Department of Information Systems Security "South Ural State University", security engineer of the LLC "Strategy of security", Chelyabinsk. E-mail: sch1081024@mail.ru

Alexander Sokolov, a. M. N., Associate Professor, Head. the Department of Information Systems Security "South Ural State University", Chelyabinsk. E-mail: ANSokolov@inbox.ru