УДК 004.43 Вестник УрФО № 2(20) / 2016, с. 15–18

Скурлаев С. В., Соколов А. Н.

УСТАНОВКА ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВ WINDOWS И LINUX СО СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ НА ОТЧУЖДАЕМЫЙ НАКОПИТЕЛЬ

Рассмотрены особенности установки операционной системы специального назначения «ASTRA Linux Special Edition» (релиз «Смоленск») на отчуждаемый USB-накопитель. Проведено сравнение с установкой на отчуждаемый USB-НЖМД накопитель рабочей среды WindowsToGo и средства защиты информации SecretNet 7. Проанализированы преимущества и недостатки каждой из рассмотренных инсталляций и особенности сценариев их применимости для реализации методов доверенной загрузки.

Ключевые слова: *автоматизированная система (АС), несанкционированный доступ (НСД), операционная система (ОС), операционная система специального назначения (ОССН), средство защиты информации (СЗИ).*

Skurlaev S. V., Sokolov A. N.

INSTALLING OPERATING SYSTEMS FROM WINDOWS AND LINUX FAMILIES WITH MEANS OF PROTECTING INFORMATION ON A REMOVABLE DEVICE

The article discusscertain checkpoints of setting up an operating system of special meaning (ASTRA Linux «Smolensk» Release) on a removable USB-device. Compares installing Windows To Go environment with mean of protecting information Secret Net 7 on a USB-HDD. Analyzedadvantages and disadvantages of each of the considered installations and especially their application scenarios for implementing trusted boot methods.

Keywords: *automated system (AS), unauthorized access (UA), operating system (OS), operating system of special meaning (OSSM), means of protecting information from unauthorized access.*

В [1] описано применение технологии WindowsToGo и сертифицированного средства защиты информации SecretNet 7 с целью реализации установки операционной системы на отчуждаемыйнакопитель.Проанализируем возможности и особенности установки на внешний USB-Flash накопитель сертифицированной операционной системы «ASTRA Linux Special Edition» (релиз «Смоленск») (далее операционная система специального назначения, ОССН), а также особенности функционирования, преимущества и недостатки каждой из представленных инсталляций.

Установка ОССН на USB-Flashнакопитель проведена в штатном режиме:

Компьютер загружен с оптического диска с инсталляционным дистрибутивом ОССН.

Все ответы на запросы мастера установкиданы стандартно, на вопросе выбора системного диска указан подключенный USB-Flashнакопитель. На рис. 1 приведён вывод утилиты fdisk, показывающий существующие разделы на используемом в эксперименте USB-Flashнакопителе Kinston Data Traveler Hyper X 3.0 128 Gb. На рис. 2 приведён вывод мастера установки после выбора используемого накопителя в качестве основного системного диска для установки ОССН.На приведённых рисунках видно, что отчуждаемый накопитель определяется как стандартное блочное устройство (/dev/sda) и ничем не отличается для мастера установки от фиксированного накопителя, например, накопителя на жёстких магнитных дисках (НЖМД), напрямую подключенного к материнской плате компьютера.

Получено сообщение «Установка завершена».

```
~ # fdisk -l /dev/sda

Disk /dev/sda: 126.6 GB, 126567317504 bytes
255 heads, 63 sectors/track, 15387 cylinders, total 247201792 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00028fa6

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     1953791      975872   83  Linux
/dev/sda2         1955838   247199743   122621953    5  Extended
/dev/sda5         1955840    15626239     6835200   83  Linux
/dev/sda6        15628288    19531775     1951744   83  Linux
/dev/sda7        19533824    27918335     4192256   82  Linux swap / Solaris
/dev/sda8        27920384    28698623      389120   83  Linux
/dev/sda9        28700672   152928255    62113792    7  HPFS/NTFS/exFAT
~ # _
```

Рис. 1. Вывод утилиты fdisk, отражающий существующие разделы на используемом накопителе.

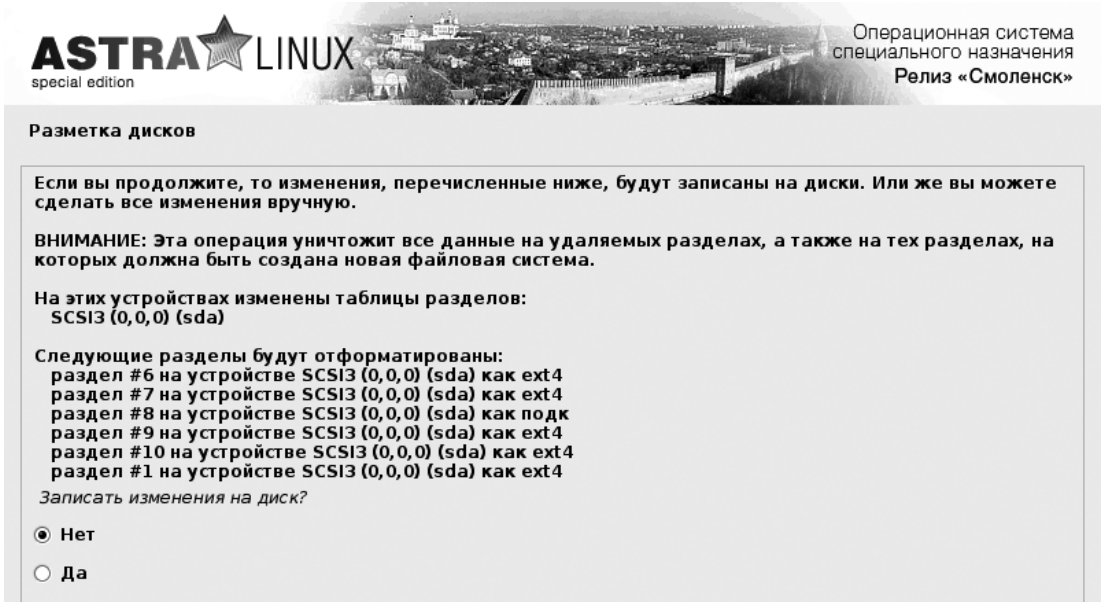

Рис. 2. Вывод мастера установки после выбора используемого накопителя в качестве основного диска для установки ОССН.

Таблица 1. Сравнение применимости инсталляций решений на базе операционных систем семейств Windows и Linux со средствами защиты на отчуждаемый накопитель

Сравниваемые аспекты	**Рабочая среда Windows To Go с установленным SecretNet 7**	**ОССН ASTRALinux версия «Смоленск»**
Применимые USB-накопители	USB-HDD (НЖМД); при использовании USB-Flash-накопителя возникают проблемы с откликом файловой системы, что не является строгим ограничением, но сильно затрудняет использование системы	USB-Flash или USB-HDD: возможно оптимально использовать оба типа накопителей
Масштабируемость ПО	Возможность установки любого прикладного ПО, работающего под управлением ОС Windows	Возможность и спользования ПО из официальных репозиториев, а также скомпилированного средствами ОССН; есть сертификационные ограничения, например, нельзя пересобирать ядро и системные библиотеки
Ограничения в применении	Полностью подходит только для АС классов 3А и ниже; для класса АС 2А требуется применение дополнительных организационных мер [1]	Установка на отчуждаемый накопитель не накладывает ограничений на использование
Переносимость инсталляции с фиксированного диска	Возможность переноса всего окружения Windows с внутреннего НЖМД компьютера с предварительным созданием на базе этого окружения шаблона установки (возможность развертывания этого шаблона на отчуждаемый накопитель)	Возможность переноса домашних каталогов и файлов конфигураций сервисов с внутреннего НЖМД компьютера на отчуждаемый накопитель после установки ОССН

После перезагрузки компьютер загружен с USB-Flash-накопителя, указаны реквизиты созданного во время установки пользователя, вход в систему осуществлен успешно.

Проведен тест работоспособности установленного по умолчанию программного обеспечения (ПО) (из инсталляционного дистрибутива на оптическом диске) путем его запуска. Тест прошел успешно.

Настроены основные механизмы согласно руководству [2]. Проведены тесты работоспособности механизмов защиты согласно руководству [3], а также путем реализации экспертным методом модели, рассмотренной в [4]. Сделан вывод о полной работоспособности встроенных механизмов защиты.

В табл. 1 приведены результаты сравнения решения на базе рабочей среды Windows To Go с установленным СЗИ SecretNet 7 и решения на базе ОССН ASTRA Linux версия «Смоленск», установленной на отчуждаемый USB-Flash-накопитель.

По результатам сравнения можно сделать следующие выводы:

1. Несмотря на то что нет технических ограничений на использование рабочей среды Windows To Go с USB-Flash накопителем, сопутствующая задержка операций ввода-вывода файловой системы существенно сказывается на удобстве работы с данной ОС. Отчуждаемые накопители типа USB-HDD или USB-SSD не имеют подобного недостатка. В случае использования ОССН ASTRA Linuxтип отчуждаемого накопителя не играет особой роли.

2. Под масштабируемостью здесь понимается возможность установки прикладного ПО без нарушений требований руководящих документов. На Windows To Go возможна установка любого прикладного ПО, разработанного для использования в ОС семейства Windows. В случае использования ОС вместе с СЗИ количество операций ввода-вывода значительно увеличивается, что приводит к задержкам при работе с компьютером, но данное утверждение справедливо не только для отчуждаемых накопителей. В случае использования ОССН ASTRA Linux возможно пользоваться стандартными возможностями

для дистрибутивов GNU/Linux на основе Debian: использование официальных репозиториев (разработчиков ОССН), компиляция собственных программ из исходных текстов. Ограничения, которые касаются невозможности компиляции новых системных модулей, например, последних версий ядра с сайта kernel.org или последних версий системных библиотек и другого ПО из текстов, не размещенных в официальных репозиториях ОССН, диктуется целесообразностью ненарушения функциональных возможностей продукта по защите информации и сохранению сертификационных требований.

3. Ввиду особенностей реализации средства защиты информации SecretNet 7 функционирование некоторых защитных механизмов на данный момент невозможно без нарушения работоспособности всей рабочей среды Windows To Go, что требует применения дополнительных организационных мер для восполнения этого недостатка. Защитные механизмы ОССН могут работать в штатном режиме и в случае установки на отчуждаемый накопитель это никак не сказывается на работоспособности предлагаемого решения.

4. Перенести все рабочее окружение с внутреннего НЖМД на отчуждаемый накопитель возможно в рамках любого из предложенных решений. В случае Windows To Go потребуется создать шаблон-образ с установленной системы, который после будет использован для реализации рабочего окружения Windows To Go. В случае использования ОССН ASTRA Linux потребуется скопировать на отчуждаемый накопитель домашние каталоги пользователей и конфигурационные файлы сервисов с предварительной установкой и воссозданием списков пользователей, а также установленного ПО.

Перечисленные преимущества и ограничения являются техническими. Стоит также отметить, что на применимость того или иного решения в конкретном сценарии влияют и другие характеристики. Например, ОССН ASTRA Linux возможно использовать в тех АС, где технологический процесс предполагает использование СУБД и клиента базы данных, которые присутствуют в официальных репозиториях, или где пользователи обучены правилам работы в подобных ОС. Вариант с использованием Windows To Go не повлечет необходимость дополнительного обучения пользователей, не ограничит в выборе прикладного ПО, но потребует применения дополнительных организационных мер.

Примечания

1. Скурлаев С. В., Соколов А. Н. Применение технологии Windows To Go в автоматизированных системах классов 2А и 3А с сертифицированными средствами защиты информации // Вестник УрФО. Безопасность в информационной сфере. Челябинск : Изд. центр ЮУрГУ, 2015. – № 4 (18).– С. 12–15.

2. «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1» РУСБ.10015-01 97 01-1-2012.

3. «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 2» РУСБ.10015-01 97 01-2-2012.

4. 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