УДК 004.33

Механизм обновления защищенных микрокомпьютеров МКТ

А. Ю. Батраков
Закрытое акционерное общество "ОКБ САПР", Москва, Россия

Описаны два метода обновления защищенных микрокомпьютеров: с изменением и без изменения состояния ПЗУ.

Ключевые слова: защищенный компьютер, микрокомпьютер, обновление.

Защищенные микрокомпьютеры МКТ обладают простым, но надежным механизмом обеспечения целостности операционной системы. Вся внутренняя память данных микрокомпьютеров физически переводится в режим "только чтение" [1—7]. Это гарантирует, что никакие вредные данные не могут быть записаны в МКТ и никакие предустановленные средства разграничения доступа не могут быть удалены или выключены [8].

Однако, средство, которое нельзя изменить, не может быть удобным и безопасным.

Во-первых, огромное количество обнаруженных за последнее время уязвимых мест показывает, что бывают необходимы обновления системных библиотек и программного обеспечения. В качестве примера можно привести печально знаменитый Heartbleed. Во-вторых, постоянно появляются новые модели принтеров, сканеров и другой техники. Для них могут понадобиться новые драйвера. В-третьих, не стоит забывать, что может обновляться и пользовательское программное обеспечение, например с целью расширения функционала.

Таким образом, становится очевидно: удобное и безопасное средство должно иметь возможность обновления. Вместе с тем память МКТ физически находится в режиме "только чтение". Один из возможных способов обновления здесь очевиден: передать устройство в сервисный центр, где будут произведены все технологические операции для перезаписи памяти. Однако этот способ требует доставки всех обновляемых устройств в сервисные центры, а также ненулевого времени на проведение обновления.

Для проведения быстрого и удобного обновления была разработана специальная технология. В микрокомпьютерах МК имеется посадочное место для MicroSD карты. На эту карту может быть записан образ обновления. Образ содержит в себе информацию обо всех изменениях: какой файл заменить, какой удалить, какой добавить.

Образ обновления не может принести вреда, поскольку он распространяется только совместно с электронной подписью. Неизменная операционная система содержит в себе сертификат, на котором подпись может быть проверена. При каждой загрузке неизменная операционная система проверяет подпись под образом обновления. Если подпись верна, обновление применяется к файловой системе прямо в оперативной памяти. Если же проверка подписи закончилась ошибкой, загрузка будет прервана.

Таким образом, с одной стороны, операционная система осталась неизменной, а с другой стороны, она обновлена.

Разумеется, у этой технологии есть и свои минусы. Так как при каждом старте операционной системы (даже после перезагрузки!) необходимо проверить подпись под образом, загрузка несколько замедляется. Замедляется она несильно: примерно на 10 с при размере образа обновления в 100 Мегабайт (100 Мегабайт — это довольно много; в них одновременно может содержаться сразу несколько новых библиотек, несколько дополнительных драйверов). Однако обновления со временем накапливаются, а образ разрастается. Особенно быстро образ растет при обновлении версии операционной системы, когда он может легко увеличиться до гигабайта и более. Понятно, что с таким образом обновления работать неудобно. В таком случае предлагается все же передать устройства в сервисный центр, где после проведения необходимых технологических процедур все обновления будут применены к основной операционной системе. Это позволит резко сократить время загрузки и начать собирать новые обновления.

Имеется несколько вариантов того, как подписанный образ обновления должен попасть на MicroSD-карту. Самый простой из них состоит в том, что администратор извлекает карту из МКТ, записывает на нее образ и возвращает карту на

Батраков Антон Юрьевич, начальник отдела программирования.
E-mail: abatrakov@okbsapr.ru

Статья поступила в редакцию 26 июня 2016 г.

© Батраков А. Ю., 2016

место. Этот способ пригоден, если количество используемых МКТ невелико.

Более удобный способ — централизованная передача обновлений по сети. Для этого устанавливается простейший сервер. Микрокомпьютеры по регламенту или по команде запрашивают обновления у сервера. Если обновление есть, оно закачивается на карту памяти, и уже при следующей перезагрузке будет применено.

Поскольку можно при каждом включении забирать образ обновления с сервера по сети, закачивать обновление на карту памяти не обязательно. О соответствующей технологии можно прочитать в статье "Центр-Т на защищенных микрокомпьютерах МКТ".

Литература

1. Компьютер типа "тонкий клиент" с аппаратной защитой данных. Патент на полезную модель № 118773. 27.07.12, бюл. № 21.

2. Компьютер с аппаратной защитой данных от несанкционированного изменения. Патент на полезную модель № 137626. 20.02.2014, бюл. № 5.

3. Мобильный компьютер с аппаратной защитой доверенной операционной системы. Патент на полезную модель № 138562. 20.03.2014, бюл. № 8.

4. Мобильный компьютер с аппаратной защитой доверенной операционной системы от несанкционированных изменений. Патент на полезную модель № 139532. 20.04.2014, бюл. № 11.

5. Мобильный компьютер с аппаратной защитой доверенной операционной системы. Патент на полезную модель № 147527. 10.11.2014, бюл. № 31.

6. Мобильный компьютер с аппаратной защитой доверенной операционной системы от несанкционированных изменений. Патент на полезную модель № 151264. 27.03.2015, бюл. № 9.

7. Рабочая станция с аппаратной защитой данных для компьютерных сетей с клиент-серверной или терминальной архитектурой. Патент на полезную модель № 153044. 27.06.2015, бюл. № 18.

8. *Конявский В. А.* Компьютер с вирусным иммунитетом // Информационные ресурсы России. 2015. № 6. С. 31—34.

Mechanism of updating for protected microcomputers MKT

A. Yu. Batrakov
Closed Joint Stock Company "OKB SAPR", Moscow, Russia

The article describes two methods of protected microcomputers updating: with change of state of the ROM and without change.

Keywords: protected computer, microcomputer, update.

Bibliography — 8 references. *Received June 26, 2016*