3. Средства доверенной загрузки (ФСТЭК МД 30.12.2013)

Доверенная загрузка — это загрузка различных операционных систем только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и аппаратной идентификации / аутентификации пользователя.

Доверенная загрузка обычно включает в себя:

* Аутентификацию;
* Контроль устройства, с которого BIOS начинает загрузку ОС (чаще, жёсткий диск компьютера, но это также может быть устройство чтения съёмный носителя, загрузки по сети и т.п.);
* Контроль целостности и достоверности загрузочного сектора устройства и системных файлов запускаемой ОС;
* Шифрование/расшифрование загрузочного сектора, системных файлов ОС, либо шифрование всех данных устройства (опционально).
* Аутентификация, шифрование и хранение секретных данных, таких как ключи, контрольные суммы и хэш-суммы, выполняются на базе аппаратных средств.

Аутентификация пользователя может производиться различными способами и на разных этапах загрузки компьютера.

Для подтверждения личности запускающего компьютер могут требоваться различные факторы:

* Секретный логин и пароль пользователя;
* Дискета, компакт-диск, флэш-карта с секретной аутентификационной информацией;
* Аппаратный ключ, подключаемый к компьютеру через USB, последовательный или параллельный порты;
* Аппаратный ключ, либо биометрическая информация, считываемые в компьютер с помощью отдельно выполненного аппаратного модуля.

Аутентификация может быть многофакторной. Также аутентификация может быть многопользовательской с разделением прав доступа к компьютеру. Так, один пользователь сможет только запустить операционную систему с жёсткого диска, в то время как другому будет доступно изменение конфигурации CMOS и выбор загрузочного устройства.

Аутентификация может происходить:

* Во время выполнения микропрограммы BIOS;
* Перед загрузкой главной загрузочной записи (MBR) либо загрузочного сектора операционной системы;
* Во время выполнения программы загрузочного сектора.

На различных этапах загрузки компьютера доверенная загрузка может быть выполнена различными средствами, и, следовательно, будет обладать различной функциональностью.

**Выполнение микропрограммы BIOS**. На этом этапе могут быть реализованы: проверка целостности микропрограммы BIOS, проверка целостности и подлинности настроек CMOS, аутентификация (защита от запуска компьютера в целом, либо только от изменения конфигурации CMOS или выбора загрузочного устройства), контроль выбора загрузочного устройства. Этот этап загрузки должен быть полностью выполнен в микропрограмме BIOS производителем материнской платы;

**Передача управления загрузочному устройству**. На этом этапе BIOS, вместо продолжения загрузки, может передать управление аппаратному модулю доверенной загрузки. Аппаратный модуль может выполнить аутентификацию, выбор загрузочного устройства, дешифрование и проверку целостности и достоверности загрузочных секторов и системных файлов операционной системы. При этом дешифрование загрузочного сектора операционной системы может быть выполнено только на этом этапе. Микропрограмма BIOS должна поддерживать передачу управления аппаратному модулю, либо аппаратный модуль должен эмулировать отдельное загрузочное устройство, выполненного в виде жёсткого диска, сменного носителя либо устройства загрузки по сети;

**Выполнение загрузочного сектора операционной системы**. На этом этапе также может быть выполнена проверка целостности, достоверности загрузчика, системных файлов операционной системы и аутентификация. Однако исполняемый код загрузочного сектора ограничен в функциональности вследствие того, что имеет ограничение на размер и размещение кода, а также выполняется до запуска драйверов операционной системы.

Доверенная загрузка должна обеспечивать:

* блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;
* контроль доступа пользователей к процессу загрузки операционной системы;
* контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.

В соответствии с Информационным сообщением ФСТЭК России №240/24405 от 06.02.2014 г.

«Об утверждении Требований к средствам доверенной загрузки», а также собственно Приказом ФСТЭК России № 119 от 27.09.2013 г., рассматриваемый класс средств защиты информации подразделяется на три типа:

* Средства доверенной загрузки уровня базовой системы ввода-вывода;
* Средства доверенной загрузки уровня платы расширения;
* Средства доверенной загрузки уровня загрузочной записи.

Первая группа средств - уровня BIOS - это, как правило, многокомпонентные программные средства, один из модулей которых встраивается непосредственно в микропрограмму материнской платы. Примерами таких средств доверенной загрузки являются «МДЗ-Эшелон» компании НПО «Эшелон» и Altell Trust производства компании Altell. Для функционирования таких средств не требуется установка плат PCI/PCI-E, что существенно упрощает и ускоряет ввод СЗИ в эксплуатацию [6, 7].

Средства доверенной загрузки уровня платы расширения всегда программно-аппаратные. Это самый широкий сегмент рынка средств доверенной загрузки. В качестве примера можно привести ПАК «Соболь» компании «Код Безопасности», Максим-М1 НПО «РусБИТех», АПМДЗ «Щит-ЭЦП» Концерна «Системпром» и др. [8, 9]

Наконец, механизм функционирования средств доверенной загрузки уровня загрузочной записи основан на модификации boot-секторов логических разделов жестких дисков. Содержимое загрузочных секторов шифруются, что позволяет скрыть информацию о логических разделах при несанкционированной загрузке компьютера. Примером может служить Trusted Boot Loader компании «Код Безопасности» (поддержка которого, к сожалению, прекращена, а срок действия сертификата истек в прошлом году).