# УПРАВЛЕНИЕ ДОСТУПОМ

УДК 004.056.53

## Различия подходов к пошаговому контролю целостности: TPM и IMA/ EVM или ПАК СЗИ НСД

*А. М. Каннер*
Закрытое акционерное общество "ОКБ САПР", Москва, Россия

*Рассматриваются существующие подходы к пошаговому контролю целостности в отечественных и зарубежных средствах защиты информации, проводится анализ их различий. Приводится сравнение функциональных и технических характеристик программно-аппаратных комплексов средств защиты информации от несанкционированного доступа и решений, использующих trusted platform module в качестве основы для дальнейшего контроля целостности и создания корня доверия, делаются выводы о целесообразности использования тех или иных средств защиты данных.*

*Ключевые слова:* пошаговый контроль целостности, аппаратный модуль доверенной загрузки, trusted platform module.

В конце XX в. ученые и специалисты в области защиты информации пришли к мнению, что для гарантированной защиты данных от несанкционированного доступа (НСД) необходимо использовать так называемый принцип пошагового контроля целостности. Данный принцип заключается в выполнении взаимосвязанных последовательных шагов по контролю целостности аппаратных, а затем и программных компонентов средства вычислительной техники (СВТ). При этом на раннем этапе активизации СВТ (включение питания, работа базовой подсистемы ввода/вывода) в системе должен присутствовать резидентный компонент безопасности, целостность встроенного ПО которого обеспечивается технологически [1]. Данный модуль позволяет на раннем этапе активизации СВТ проводить аппаратный контроль целостности и тем самым обеспечивает неизменность и дальнейшую активизацию программных средств статического/динамического контроля целостности и разграничения доступа, а те в конечном итоге обеспечивают конфиденциальность и целостность непосредственно защищаемых данных, компонентов подсистемы управления доступом, критически важных компонентов операционной системы (ОС) и программной среды пользователя СВТ.

**Каннер Андрей Михайлович**, программист группы программирования ПО для СЗИ отдела программирования СЗИ.
E-mail: kanner@okbsapr.ru

*Статья поступила в редакцию 11 мая 2018 г.*



Принцип пошагового контроля целостности впервые был предложен в работах А. Ю. Щербакова и В. А. Конявского, посвященных теории доверенных вычислительных систем и защищенного субъектно-объектного взаимодействия в них. Данный принцип позволил обосновать формальную модель безопасности, гарантирующую невозможность изменения действующей в компьютерной системе политики управления доступом [2], впервые рассматривавшей подсистему защиты в виде сущности системы, которую необходимо защищать, как и сами данные.

Созданные на базе результатов научных работ указанных авторов реализации резидентного компонента безопасности получили название аппаратных модулей доверенной загрузки (АМДЗ). Они активно используются на IBM-совместимых СВТ архитектуры x86/x86_64. Чуть позже о необходимости создания подобных средств задумались и за рубежом, предложив спецификацию модуля для доверенных вычислений (Trusted Platform Module, TPM) [3]. Однако набор реализуемых TPM функций безопасности отличается от функций АМДЗ, и цели, с которыми эти два средства используют, не идентичны.

После рассмотренных резидентных компонентов безопасности как логическое продолжение идеи принципа пошагового контроля целостности были созданы средства, позволяющие осуществлять динамический и статический контроль целостности уже в процессе работы ОС. В Российской Федерации такие средства, как правило, входят в состав программно-аппаратных комплексов средств защиты информации от НСД (ПАК СЗИ

НСД), а иностранные средства обычно интегрированы в конкретные ОС. Цели использования этих средств несколько отличаются, как и в случае с АМДЗ и TPM.

Проанализируем отличие в подходах к пошаговому контролю целостности современных иностранных средств защиты информации от отечественных. Рассмотрим такие средства защиты, как TPM совместно с технологиями Integrity Measurement Architecture (IMA) [4], Extended Verification Module (EVM) [5] операционной системы GNU/Linux и АМДЗ со специальным ПО "Аккорд-X" [6]. Подробное описание подхода к пошаговому контролю целостности с помощью АМДЗ и "Аккорд-X" приведено в [7].

### Особенности технологий TPM и IMA/EVM

TPM изначально разрабатывался как встроенный модуль с поддержкой криптографических операций и возможностью хранения ключей для защиты данных СВТ. TPM состоит из:

- аппаратного генератора случайных чисел;
- криптографического процессора (блоков генерации ключей RSA/AES и хэшей SHA-1/SHA-256/HMAC, блока шифрования-дешифрования-подписи данных);
- хранилища ключевой информации (постоянная и универсальная память).

Первоначальная цель использования TPM состоит в обеспечении целостности платформы, т. е. в контроле того, что оборудование и ПО, участвующее в процессе загрузки СВТ, выполняет строго предопределенные действия до полной загрузки ОС. При этом ответственность за обеспечение целостности платформы лежит не на самом TPM (его роль является *пассивной*), а скорее, на внутреннем ПО аппаратного обеспечения СВТ или ОС. Например, подсистема ввода/вывода UEFI может использовать TPM для создания так называемого корня доверия (*root of trust*), используя предоставляемые TPM регистры PCR (*Platform Configuration Registers*) для защищенного хранения определенных метрик, описывающих изменения в конфигурации аппаратных компонентов СВТ, на основе которых можно принимать решение о целесообразности дальнейшей загрузки системы.

Создание корня доверия возможно с использованием двух подходов: SRTM (*Static Root of Trust for Measurements*) и DRTM (*Dynamic Root of Trust for Measurements*). SRTM выполняется только на самом раннем шаге загрузки СВТ. Сначала в загрузочном блоке BIOS/UEFI с использованием TPM и значения из нулевого PCR-регистра проверяется целостность самого BIOS/UEFI, затем — целостность опции PCI ROM (значение первого PCR-регистра), загрузчика и так далее. С помощью SRTM последовательно проверяется целостность всех компонентов, участвующих в загрузке СВТ, вплоть до ядра ОС. При этом на всех шагах инициировать проверку целостности должны именно компоненты СВТ, а не TPM (например, специальный загрузчик TrustedGrub). Другой подход к SRTM был реализован в устройствах Chromebook, в которых целостность первой части встроенного ПО базовой подсистемы ввода/вывода обеспечивается технологически (память доступна только для чтения), а целостность следующих компонентов, участвующих в процессе загрузки, контролируется с помощью кода и данных из первой части (с применением или без применения TPM).

DRTM выполняется в процессе работы СВТ и позволяет достичь доверенной среды из недоверенного начального состояния системы. Классическими примерами DRTM являются технология процессоров Intel под названием Trusted Execution Technology (TXT, ранее LaGrande Technology) и аналогичная технология AMD Secure Virtual Machine (SVM), которые используются для создания цепочки доверия (*chain of trust*). Технически на этапе работы BIOS/UEFI в определенный момент прерывается выполнение задач на всех, кроме одного, процессорах. Далее на оставшемся процессоре с помощью специальных инструкций последовательно загружаются с проверкой целостности в TPM компоненты, ответственные за дальнейшую реализацию DRTM (SINIT ACM, MLE, LCP). Все другие задачи физически не могут выполняться. Далее приостановленные процессоры активируются и с их помощью модуль MLE, представляющий собой очень маленькую ОС, последовательно проводит контроль целостности дополнительных компонентов (ядра ОС СВТ, критически важных конфигурационных файлов) по созданной последовательности запускаемых объектов в ходе загрузки ОС СВТ. Основной функцией DRTM является пошаговый контроль компонентов, участвующих в загрузке СВТ и ОС. При этом на первом этапе контроль целостности осуществляется на аппаратном уровне, а далее производится уже с использованием программных средств, целостность которых подтверждена. Дополнительной функцией технологии DRTM Intel TXT является возможность удаленно подтвердить, что на СВТ используется только предопределенное аппаратное и программное обеспечение. Не следует путать DRTM-технологию Intel TXT (или аналогичную AMD SVM) с более поздней технологией Secure Boot, которая используется в составе UEFI и применяется

для блокировки загрузки неподписанных ядра ОС, драйверов или загрузчиков. Secure Boot изначально не использует TPM даже в качестве ключевого хранилища информации.

Также TPM может применяться в системах полного шифрования носителей данных в целях хранения ключевой информации и обеспечения целостности процесса загрузки, включая целостность внутреннего ПО различного оборудования и загрузочных секторов. Кроме того, TPM можно использовать для хранения ключевой информации ОС (например, данных для аутентификации) или для защиты авторской информации DRM-систем. При этом в TPM существует встроенный механизм, ограничивающий возможность доступа к внутренним данным с помощью подбора и использования словарей.

Необходимо отметить, что по умолчанию в TPM присутствует лишь ограниченное число 160-битных PCR-регистров (минимум 16; зависит от конкретной реализации модуля TPM), однако в теории можно хранить намного больший объем метрик, чем общий объем памяти этих регистров. Для этого в новом значении PCR-регистра сохраняется хэш от новых данных и старого значения PCR-регистра:

$$PCR_{i\text{-}new\text{-}value} = hash(PCR_{i\text{-}old\text{-}value} \,||\, new\text{-}data).$$

Важно, что уже с 2006 г. (первоначально для ноутбуков) TPM постепенно встраивается в новые СВТ в виде платы расширения с интерфейсом SPI/LPC или интегрируется непосредственно в материнскую плату или чипсет. Таким образом, в скором времени в большинстве новых СВТ будут доступны все возможности TPM.

Технология Linux IMA была представлена в 2009 г. Она позволяет в дополнение к SRTM и созданию корня доверия вычислять контрольные суммы загружаемых в память бинарных данных (исполняемых файлов, разделяемых библиотек, модулей ядра) для дальнейшей удаленной аттестации системы с TPM, т. е. удостоверения того, что только доверенное ПО было запущено с момента загрузки СВТ. Контрольные суммы, вычисляемые с помощью IMA, могут подписываться уникальным ключом TPM.

Дополнительно к IMA с 2012 г. доступно применение технологии EVM, с помощью которой возможны локальная аттестация системы и проверка целостности объектов (не только бинарных данных) в соответствии со значениями расширенных файловых атрибутов. Также EVM позволяет защищать такие расширенные атрибуты от несанкционированного изменения с помощью электронной подписи и автоматически обновлять контрольные суммы при санкционированном изменении (когда изначально контрольные суммы совпали). Необходимо отметить, что технология IMA, в отличие от IMA/EVM, изначально не предполагала блокировку загрузки бинарных данных, а использовалась только для дальнейшей аттестации системы, т. е. была пассивным средством защиты информации.

Технологии IMA/EVM не требуют наличия TPM, хотя без него и невозможно гарантировать неизменность эталонных контрольных сумм или ключей подписи, и могут применяться на широком спектре устройств: от IBM-совместимых СВТ с архитектурой x86/x86_64 до носимой электроники и мобильных устройств на базе Android, Tizen и других систем, основанных на ядре Linux.

### Отличия подходов к пошаговому контролю целостности

На основе представленной информации и [7] проанализируем отличия в подходах к пошаговому контролю целостности современных иностранных средств защиты информации от отечественных.

Аппаратный компонент, который используется в качестве основы для пошагового контроля целостности в иностранных средствах защиты (TPM), в отличие от отечественных (АМДЗ), выполняет не активную, а пассивную функцию. Из-за этого для реализации пошагового контроля целостности с применением TPM необходимо использовать соответствующие адаптированные компоненты СВТ (UEFI, TrustedGrub и т. д.), которые будут играть активную роль. Таким образом, TPM на данном этапе развития представляет собой, по сути, небольшую плату, позволяющую хранить в своей защищенной памяти некоторые метрики/хэш-значения. АМДЗ представляет собой активный компонент, который принудительно перехватывает загрузку СВТ для проведения контрольных процедур и который не зависит от прочих компонентов СВТ.

Кроме того, TPM обычно представляет собой интегрированное решение, которое в большинстве случаев встраивается в СВТ на этапе производства, и его в общем случае нельзя использовать на другом СВТ. К тому же, существуют две спецификации TPM (v1.2 и v2.0), которые не во всех аспектах совместимы между собой. АМДЗ представляет собой встраиваемое универсальное (в рамках поддерживаемой архитектуры) решение, которое потенциально можно использовать на другом СВТ. Важным отличием в этом плане TPM от АМДЗ является то, что на большинстве старых СВТ нельзя использовать TPM и соответствующие технологии SRTM/DRTM, а АМДЗ использовать можно. Это

справедливо и для технологии IMA/EVM, которую можно использовать, начиная с определенной версии ядра Linux, и нельзя использовать на предыдущих его версиях. Необходимо отметить, что эти проблемы со временем сойдут на нет, но на данный момент являются очень актуальными.

Кроме очевидных технических отличий АМДЗ и TPM, необходимо отметить отличия в целях их использования и реализуемых функциях. У TPM более богатый функционал, который превосходит потребности пошагового контроля целостности. В АМДЗ вообще невозможно использовать какие-либо новые функции безопасности, весь функционал жестко фиксирован. АМДЗ является специализированным устройством, а TPM — более универсальным.

TPM часто используют не для хранения ключей/хэш-значений для личного пользования, а для хранения валидных сертификатов, что зачастую требует разворачивать целую инфраструктуру PKI/сети доверия и реализации механизмов проверки отозванных сертификатов в TPM. Также в отличие от АМДЗ TPM позволяет на основе сертификатов блокировать принципиальную возможность запуска на СВТ неподписанных бинарных данных. Разница TPM и АМДЗ заключается еще и в том, для кого конкретно реализуются защитные функции: в интересах производителя СВТ или конечного владельца. Владелец СВТ должен иметь возможность беспрепятственно запускать на нем любое ПО. Однако некоторые технологии, использующие TPM, лишают или ограничивают владельца в этой возможности.

С этим же обстоятельством связана проблема доверия пользователя СВТ сертификатам производителей различных компонентов системы: у пользователя практически не существует способа настройки и администрирования решений, использующих TPM, и в соответствии с этим он обязан беспрекословно доверять подписанным компонентам без возможности самому принять решение. Так, например, в TPM на этапе производства создаются уникальные ключи RSA (*Endorsement Key*), которые в дальнейшем используются для создания корня доверия, однако нет никаких гарантий, что эти ключи недоступны производителю в дальнейшем после продажи СВТ, и он не сможет их использовать для компрометации системы. Таким образом, если у СВТ иностранный производитель (что для российской действительности практически всегда справедливо), актуальной является проблема национальной безопасности в вопросах защиты информации, так как на защищенность СВТ и использование TPM для защиты информации может повлиять кто-то из-за рубежа. В противоположность этому в АМДЗ абсолютно все критически важные данные создаются непосредственно пользователем (администратором) при первоначальной настройке комплекса, а в качестве источника энтропии используется аппаратный датчик случайных чисел.

В остальных аспектах пошаговый контроль целостности с помощью TPM (с хэш-значениями) и, например, IMA/EVM, не отличается от отечественных решений, использующих ПАК СЗИ НСД. Однако имеются зарубежные решения, которые не до конца друг с другом согласуются или дублируют часть своего функционала (Intel TXT, SecureBoot, IMA/EVM).

## Выводы

Таким образом, принцип пошагового контроля целостности в иностранных (в рамках SRTM) и отечественных средствах защиты информации в своей основе один и тот же: организуется последовательная проверка всех компонент, участвующих в загрузке СВТ. Так, использование TPM (без цифровых сертификатов) и решений, применяющих его для создания корня доверия (SRTM, IMA/EVM), аналогично использованию АМДЗ и ПАК СЗИ НСД. Однако рассмотренные средства имеют множество функциональных отличий. Например, АМДЗ является специализированным средством и не обладает таким богатым функционалом, как TPM. С другой стороны, АМДЗ является активным компонентом, тогда как TPM необходимо использовать только с другими специальными компонентами СВТ (UEFI, TrustedGrub).

Ряд иностранных решений (Intel TXT и AMD SVM) представляет собой принципиально новый уровень пошагового контроля целостности, позволяющий за счет возможностей новых чипсетов из недоверенной среды получить доверенную. Эти решения пока не получили широкого распространения, однако они имеют огромный потенциал.

Выбор конкретного решения для пошагового контроля целостности может зависеть как от необходимости определенного функционала (возможно, дополнительного), так и от степени доверия к тому или иному решению. Несмотря на широкие возможности TPM и основанных на нем решений, конечный пользователь не может полноценно их настраивать, также текущая реализация TPM предполагает создание уникальных ключей на этапе производства. Оба этих фактора при определенном стечении обстоятельств потенциально могут сделать из СВТ, принадлежащего некоторому владельцу, марионетку в руках производителя или того, в чьих интересах он может действовать.

**Литература**

1. *Конявский В. А.* Управление защитой информации на базе СЗИ НСД "Аккорд". — М.: Радио и связь, 1999. — 325 с.
2. *Щербаков А. Ю.* Методы и модели проектирования средств обеспечения безопасности в распределенных компьютерных системах на основе создания изолированной программной среды: автореф. дис. д-ра техн. наук. 05.13.12, 05.13.13. — М., 1997. — 35 с.
3. Trusted Computing Group. TPM Main Specification [Электронный ресурс]. URL: https://trustedcomputinggroup.org/tpm-main-specification/ (дата обращения: 12.03.2018 г.).
4. *Corbet J.* The Integrity Measurement Architecture [Электронный ресурс]. URL: https://lwn.net/Articles/137306/ (дата обращения: 12.03.2018 г.).
5. *Edge J.* The return of EVM [Электронный ресурс]. URL: https://lwn.net/Articles/394170/ (дата обращения: 12.03.2018 г.).
6. *Бажитов И. А.* Возможности ПАК СЗИ НСД "АККОРД-X" для ОС Linux: сб. мат. XVIII Межд. конф. "Комплексная защита информации". 19—22 мая 2009 г. — Могилев (Республика Беларусь), 2009. С. 26—27.
7. *Каннер А. М., Ухлинов Л. М.* Управление доступом в ОС GNU/Linux // Вопросы защиты информации. 2012. № 3. С. 35—38.

## Differences in approaches to step-by-step integrity control: TPM and IMA/EVM or HSC DST PUA

*A. M. Kanner*
Closed Joint Stock Company "OKB SAPR", Moscow, Russia

*The article considers the existing approaches to step-by-step integrity control in Russian domestic and foreign information security tools and analyzes their differences. The comparison of functional and technical characteristics of software and hardware complexes of data security tools against unauthorized access and solutions that use the trusted platform module as a basis for further measuring the integrity and creation of the root of trust is made, conclusions are made about the appropriateness of using certain data security tools.*

*Keywords*: step-by-step integrity control, trusted startup hardware module, trusted platform module.

Bibliography — 7 references. *Received May 11, 2018*