УДК 004

Перспективы развития средств доверенной загрузки. Взгляд разработчика

Д. Ю. Счастный
Закрытое акционерное общество "ОКБ САПР", Москва, Россия

Развитие средств доверенной загрузки (СДЗ) идет в двух направлениях: они совершенствуются для архитектуры x86 и адаптируются для других архитектур. В статье рассматриваются эти процессы и описываются детали реализаций.

Ключевые слова: СДЗ, средства доверенной загрузки, доверенная загрузка.

СДЗ за последние несколько лет получили существенное развитие. Причин этому две: формализация требований к СДЗ со стороны регулятора (ФСТЭК России) и отказ от средств вычислительной техники на базе архитектуры в Государственных информационных системах (ГИС) в пользу "альтернативных" архитектур.

С 1 января 2014 г. сертификация средств защиты информации, реализующих функции доверенной загрузки, в системе сертификации ФСТЭК России проводится на соответствие Требованиям к средствам доверенной загрузки, утвержденным приказом ФСТЭК России от 27 сентября 2013 г. № 119 [1]. Кроме того, регулятор обязывает применять только сертифицированные средства при построении ГИС и обработке персональных данных [2, 3]. Таким образом, разработчики СДЗ получили некоторый формальный набор требований, соответствуя которому, они могут называть свой продукт СДЗ, заказчики — легально применять этот продукт, опираясь на формальное соответствие необходимому классу.

Вторым важным двигателем процесса развития СДЗ видится переход на "альтернативные" ×86 архитектуры СВТ в ГИС. В СМИ все чаще упоминаются реализованные проекты ГИС, построенные на Эльбрусах, Байкалах или "новой гарвардской архитектуре" [4]. По причине молодости этого рынка СДЗ для них пока очень мало, но создавать их, конечно, необходимо. При этом помимо требований Регулятора, о которых уже упоминалось, ключевым моментом, мотивирующим заказчиков ГИС применять СДЗ, должно быть основное предназначение СДЗ — обеспечение доверенной загрузки. Среди разработчиков и заказчиков подобных систем часто бытует мнение, что применение СДЗ у них не обязательно, так как "процессор доверенный, закладок не содержит, опасности нет". Однако даже самый проверенный процессор с не менее проверенным БИОСом, не содержащим закладок, не выполняет контроль целостности файлов и данных *до* старта операционной системы (ОС), не производит идентификацию/аутентификацию пользователей *до* старта ОС в целом не гарантирует доверенную загрузку ОС. У него другая задача. Именно по этой причине СДЗ нужно применять и на проверенных и доверенных процессорах.

В соответствии с указанными тенденциями можно выделить несколько направлений, по которым идет развитие СДЗ. Во-первых, продолжается развитие традиционных аппаратных СДЗ вслед за развитием средств вычислительной техники (СВТ). ОКБ САПР традиционно первым выпустил Аккорд-АМДЗ [5] для шины *m*.2 как ответ на увеличение доли компьютеров с этой новой перспективной шиной. В ближайшие несколько лет, очевидно, все разработчики аппаратных СДЗ будут работать над выпуском своих СДЗ для этой шины.

Вторым потенциальным направлением развития СДЗ может стать СДЗ для шины USB. Несмотря на то что СДЗ для этой шины разработан уже давно (продукт Инаф ОКБ САПР разработал пять лет назад [6]), в свете требований Регулятора у него появляется новая ниша. Имеется ряд СВТ (например, сервера, терминалы), у которых отсутствуют слоты с шинами расширения типа PCI (USB есть во всех современных СВТ всегда). Еще одним сценарием применения Инафа может стать встраивание в процесс загрузки "альтернативных" архитектур. Так как процесс загрузки процессоров не x86 достаточно подробно описан и существует возможность легально вносить в него санкционированные изменения, можно изменить этот про-

Счастный Дмитрий Юрьевич, заместитель генерального директора.
E-mail: DimaS@okbsapr.ru

Статья поступила в редакцию 5 июня 2017 г.

цесс таким образом, чтобы загрузка кода СДЗ с USB-устройства производилась в обязательном порядке.

Третье направление развития СДЗ связано с программными СДЗ. В приказе № 119 выделяются два типа потенциальных программных СДЗ: уровня базовой системы ввода—вывода и уровня загрузочной записи. СДЗ уровня загрузочной записи могут быть только низких классов и поэтому вряд ли получат широкое распространение в ближайшее время. СДЗ уровня базовой системы ввода—вывода потенциально могут использоваться в большинстве ГИС и в системах обработки персональных данных [7]. Внедрение подобных СДЗ в СВТ как архитектуры ×86, так и "альтернативных" архитектур достаточно хорошо специфицировано и документировано. В частности, для архитектуры ×86 есть стандарт UEFI, который поддерживается большинством современных СВТ этой архитектуры [8]. Способ встраивания в процесс загрузки "альтернативных" архитектур уже был описан. Он также не представляет особых сложностей. В настоящее время ОКБ САПР начало процесс сертификации СДЗ уровня базовой системы ввода—вывода (под названием Аккорд-МКТ) для процессора Rockchip 3288. Это СДЗ планируется использовать на различных устройствах, построенных на "новой гарвардской архитектуре". В первую очередь это будут защищенный терминал "МКТ-card long" и защищенный планшет "TrusTPad". Также завершаются работы по разработке аналогичного СДЗ для моно- блока "Таволга Терминал" на базе процессора Байкал-Т1. Ведутся работы по встраиванию СДЗ уровня базовой системы ввода—вывода в СВТ на базе процессора Эльбрус. Наряду с этим готовятся аналогичные СДЗ для UEFI. Работу планируется завершить эту к концу лета 2017 г.

Таким образом, по нашим оценкам, СДЗ имеют широкие перспективы развития.

Литература

1. Требования к средствам доверенной загрузки, утвержденные приказом ФСТЭК России от 27.09.2013 № 119.
2. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".
3. Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".
4. Мобильный компьютер с аппаратной защитой доверенной операционной системы. Патент на полезную модель № 138562. 20.03.2014. Бюл. № 8.
5. Способ защиты от несанкционированного доступа к информации, хранимой на персональной ЭВМ. Патент на изобретение № 2475823. 20.02.2013. Бюл. № 5.
6. *Счастный Д. Ю.* Привязка облака к земле // Вопросы защиты информации. 2015. № 1. С. 45—47.
7. *Авезова Я. Э., Фадин А. А.* Вопросы обеспечения доверенной загрузки в физических и виртуальных средах// Вопросы кибербезопасности. 2016. № 1(14). С. 24—30.
8. *Лыдин С. С.* О средствах доверенной загрузки для аппаратных платформ с UEFI BIOS// Вопросы защиты информации: Научно-практический журнал/ФГУП «ВИМИ», 2016. № 3. С. 45—50.

Trusted startup tools development perspective from the developer's aspect

D. Y. Schastny
Closed Joint Stock Company "OKB SAPR", Moscow, Russia

Trusted startup tools (TST) are developing according two main ways: perfecting (for x86) and adopting (for other different architectures). The article describes these processes and the details of particular realizations.

Keywords: TST, trusted startup tools, trusted startup.

Bibliography — 8 references. *Received June 5, 2017*