УДК 004.056.53

Персональное устройство контроля целостности вычислительной среды

***А.А. Алтухов*[1,2,3],**

[1]Закрытое акционерное общество «ОКБ САПР», Москва, Россиия
[2]Московский физико-технический институт (государственный университет)
[3]Национальный исследовательский ядерный университет «МИФИ»

Концепция доверенной вычислительно среды (ДВС) на настоящий момент является основной парадигмой доверенных вычислений [1. С. 204]. В рамках этой концепции одной из основных задач обеспечения безопасности является обеспечение целостности вычислительной среды, где под целостностью вычислительной среды понимается стабильность работы в течение рассматриваемого периода времени в требуемом диапазоне состава объектов и процессов, их взаимосвязей и параметров функционирования [2. С. 142].

Для создания ДВС обязателен резидентный компонент безопасности (РКБ). Одной из возможных реализаций РКБ является аппаратный модуль доверенной загрузки (АМДЗ)[1].

Модули доверенной загрузки являются стационарными устройствами. Однако существуют сценарии, в рамках которых удобно и возможно применять модуль доверенной загрузки, который обладает свойством мобильности. Одним из возможных сценариев является использование одного устройства, в качестве средства доверенной загрузки (СДЗ) для нескольких средств вычислительной техники (СВТ), находящихся в одном помещении (серверные стойки) [3]. Более общий подход – это использование одного СДЗ на нескольких рабочих местах, объединённых общим признаком [Там же].

Было спроектировано и разработано устройство, решающее вышеописанные проблемы. «Модуль контроля целостности среды» (МУКЦ), можно использовать не для одной вычислительной среды, а для нескольких, что отличает данное устройство от существующих средств доверенной загрузки, в том числе работающих с шиной USB[4].

Физически устройство МУКЦ представляет собой автономно функционирующее высокозащищённое примитивное подключаемое к СВТ посредством интерфейса USB устройство, обладающее защищённой памятью, доступ которой осуществляется через активный элемент (контроллер).

Данное устройство реализует почти весь перечень функций безопасности, описанных в профиле защиты средства доверенной загрузки уровня платы расширения четвёртого класса[5]. В частности, функции контроля целостности технических средств компьютера, контроля целостности программных средств (файлов системного и прикладного ПО), контроль целостности загрузочных областей жёсткого диска, аутентификация пользователей, фиксация событий администрирования.

МУКЦ проектировался и создавался под одного пользователя, задача которого инициировать старт процедуры создания ДВС на нескольких СВТ, поэтому у него в отличие от много других СДЗ нет широких возможностей управления пользователями данного устройства. Отличительная особенность данного устройства заключается в возможности хранить базы контроля целостности для разных вычислительных сред (разных СВТ).

Любая система защиты информации — это комплекс не только технических мер, но и организационных. Для того, чтобы МУКЦ являлся полноценным СДЗ, должны соблюдаться и соответствующие организационные меры, которые немного отличаются от организационных мер, использующихся для более привычных СДЗ.

Литература.

1. *Конявский, В. А., Гадасин В. А. Основы понимания феномена электронного обмена информацией (Библиотека журнала «УЗИ»; Кн. 2). Мн.: «Беллитфонд», 2004. – 282 с.*
2. *Конявский В. А. Управление защитой информации на базе СЗИ НСД «Аккорд». М.: «Радио и связь», 1999. – 325 с.*
3. *Алтухов А. А. Концепция персонального устройства контроля целостности вычислительной среды // Вопросы защиты информации: Научно-практический журнал. ФГУП «ВИМИ», 2014. Вып. 4 (107). С. 12–14*
4. *СЗИ НСД "Аккорд-АМДЗ" [Электронный ресурс]. URL: http://www.accord.ru/accord-inaf.html (дата обращения: 28.09.2016)..*
5. *МЕТОДИЧЕСКИЙ ДОКУМЕНТ ПРОФИЛЬ ЗАЩИТЫ СРЕДСТВА ДОВЕРЕННОЙ ЗАГРУЗКИ УРОВНЯ ПЛАТЫ РАСШИРЕНИЯ ЧЕТВЕРТОГО КЛАССА ЗАЩИТЫ ИТ.СДЗ.ПР4.ПЗ [Электронный ресурс]. URLhttp://fstec.ru/component/attachments/download/661 (дата обращения: 10.04.2016).*