Е. А. Беляева, А. А. Модестов

КЛАССИФИКАЦИЯ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ АППАРАТНО-ПРОГРАММНЫХ МОДУЛЕЙ ДОВЕРЕННОЙ ЗАГРУЗКИ[1]

Для обеспечения защищенности информации от несанкционированного доступа (НСД) разрабатываются аппаратно-программные средства защиты информации, позволяющие применять современные технологии администрирования, аутентификации/идентификации пользователей и предоставления доступа, а также управления созданием и изменением учетных записей пользователей в автоматизированных системах (АС) [1].

В данной статье рассматривается наиболее широко применимый класс аппаратно-программных средств защиты информации — аппаратно-программные модули доверенной загрузки (АПМДЗ).

Основным назначением АПМДЗ является обеспечение защиты от НСД к информации путем реализации надежного контроля доступа пользователей к техническим средствам и загрузки доверенной операционной системы (ОС) [2, 3].

АПМДЗ обладают большим количеством функциональных возможностей в части защиты от НСД, которые можно классифицировать следующим образом:

- основные функциональные возможности, обязательные для реализации в АПМДЗ согласно требованиям руководящих документов по защите информации Российской Федерации;
- дополнительные функциональные возможности АПМДЗ, реализация которых не регламентирована руководящими документами, однако они позволяют повысить защищенность обрабатываемой информации от НСД.

Современные АПМДЗ реализуют большое количество основных и дополнительных функциональных возможностей для решения задач защиты данных от НСД, однако научно обоснованных методик оценивания их эффективности не существует. В связи с этим для эффективного обеспечения защиты информации от НСД с применением АПМДЗ необходимо создание научно обоснованного подхода к оцениванию эффективности реализации основных и дополнительных функциональных возможностей АПМДЗ.

Одной из научных задач в области оценивания эффективности реализации функциональных возможностей АПМДЗ является классификация основных и дополнительных функциональных возможностей АПМДЗ. Для решения указанной задачи анализировались следующие наиболее распространенные АПМДЗ [3]:

- программно-аппаратные комплексы (ПАК) семейства «Соболь» разработки группы компаний «Информзащита»;
- ПАК средств защиты информации от НСД семейства «Аккорд-АМДЗ» — ОКБ САПР;
- АПМДЗ семейства «Криптон-Замок» — фирмы «Анкад»;
- АПМДЗ «Максим» и «Максим-М1» — ОАО «НПО РусБИТех»;
- АПМДЗ семейства «Цезарь» — Всероссийского НИИ автоматизации управления в непромышленной сфере им. В. В. Соломатина.

На основании проведенного анализа АПМДЗ выявлены и классифицированы основные и дополнительные функциональные возможности в части защиты от НСД.

[1] Данная работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации в НИЯУ МИФИ в рамках проекта «Создание инженерно-технических решений для высокотехнологичного производства инновационных программно-аппаратных средств защиты информации на базе перспективных высокоскоростных интерфейсов информационного взаимодействия».

Для классификации основных функциональных возможностей АПМДЗ выделены следующие классификационные признаки (КП), характеризующие влияние функциональных возможностей на эффективность защиты информации от НСД.

КП1 – «Целостность программного обеспечения АПМДЗ и объектов, используемых операционной системой (ОС) и пользователями».

КП1 определяет состав основных функциональных возможностей АПМДЗ в части обеспечения целостности ПО АПМДЗ, целостности объектов, используемых АПМДЗ для загрузки ОС, а также объектов, используемых пользователями при работе с обрабатываемой информацией. По данному КП проверяется реализация следующих основных функциональных возможностей: контроль целостности внутренней памяти АПМДЗ, выбор контролируемых ячеек памяти АПМДЗ, контроль целостности оперативной памяти ЭВМ, выбор областей оперативной памяти ЭВМ для контроля и другие.

КП2 – «Программно-аппаратные возможности защиты информации».

КП2 определяет состав программных и аппаратных функциональных возможностей для реализации защиты информации, а именно: возможность очистки памяти ЭВМ, используемой АПМДЗ, наличие функций периодического самотестирования АПМДЗ для проверки работоспособности основных узлов и другие.

КП3 – «Аутентификация/идентификация пользователя».

КП3 определяет состав основных функциональных возможностей АПМДЗ в части реализации аутентификации/идентификации пользователя в системе. По данному КП проверяется реализация следующих основных функциональных возможностей: использование пароля как дополнительного фактора аутентификации; использование аутентифицирующего носителя пользователя в качестве фактора аутентификации; возможность смены пароля аутентификации; возможность генерации пароля аутентификации с помощью датчика случайных чисел и другие.

КП4 – «Контроль событий АПМДЗ».

КП4 определяет состав основных функциональных возможностей АПМДЗ по регистрации критических событий в части защиты обрабатываемой информации от НСД. Регистрация критических событий позволяет определять объект, с которым произошло критическое для защиты от НСД событие, пользователя и другие данные. По этому КП проверяется реализация следующих основных функциональных возможностей: регистрация попыток НСД к ресурсам системы; регистрация изменения настроек АПМДЗ; регистрация фактов смены пароля; регистрация событий контроля целостности и другие.

Для классификации дополнительных функциональных возможностей АПМДЗ предлагаются следующие КП, определяющие влияние функциональных возможностей на эффективность обеспечиваемой АПМДЗ защиты информации от НСД.

КП5 – «Проверка работоспособности платы АПМДЗ».

КП5 определяет состав дополнительных функциональных возможностей по проверке работоспособности АПМДЗ с целью выявления сбоев/отказов в работе АПМДЗ. К дополнительным функциональным возможностям, оцениваемым по данному КП, относятся: возможность тестирования АПМДЗ; наличие индикатора диагностики неисправностей АПМДЗ и другие.

КП6 – «Реализация удаленного управления».

КП6 определяет состав дополнительных функциональных возможностей в части реализации удаленного управления АПМДЗ, а именно: возможность удаленного администрирования АПМДЗ; возможность удаленного управления с любого рабочего места и другие.

КП7 – «Дополнительные функции контроля целостности».

КП7 определяет состав дополнительных функциональных возможностей в части реализации контроля целостности: автоматическое формирование списка программных модулей для контроля; возможность задания режима контроля журналов файловых систем и другие.

КП8 – «Дополнительные функции регистрации событий».

КП8 определяет состав дополнительных функциональных возможностей в части регистрации событий: фильтрация журналов регистрации событий и другие.

КП9 – «Обеспечение работы с ОС».

КП9 определяет состав дополнительных функциональных возможностей в части работы с ОС: поддерживаемые ОС; возможность принудительной загрузки ОС с определяемого администратором носителя информации и другие.

Полученные автором в результате анализа классификационные признаки функциональных возможностей АПМДЗ позволяют решить следующие задачи:

- провести сравнительный анализ АПМДЗ с основными и дополнительными функциональными возможностями;
- обеспечить получение исходных данных для оценивания АПМДЗ по степени эффективности защиты от НСД.

СПИСОК ЛИТЕРАТУРЫ:

1. *Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф.* Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина. 2-е изд., перераб. и доп. М.: Радио и связь, 2001. – 328 с.

2. *Варлатая С. К., Шаханова М. В.* Программно-аппаратная защита информации: учебн. пособие. Владивосток: Изд-во ДВГТУ, 2007. – 318 с.

3. *Зайцев А. П., Голубятников И. В., Мещеряков Р. В., Шелупанов А. А.* Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие. Издание 2-е, испр. и доп. М.: Машиностроение-1, 2006. – 260 с.