СПИСОК ЛИТЕРАТУРЫ:

1. *Барбашов В. М., Трушкин Н. С.* Прогнозирование безопасности микропрограммных БИС в условиях возникновения информационных сбоев // Безопасность информационных технологий. 2008. Вып. 2. С. 61–64.
2. *Барбашов В. М., Трушкин Н. С.* Функционально-логическое моделирование качества функционирования ИС при воздействии радиационных и электромагнитных излучений // Микроэлектроника. 2009. Т. 38. № 1. С. 34–47.

Е. А. Беляева

КОМПЛЕКСНАЯ ОЦЕНКА ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ АППАРАТНО-ПРОГРАММНЫХ МОДУЛЕЙ ДОВЕРЕННОЙ ЗАГРУЗКИ

Расширение функциональных возможностей аппаратно-программных модулей доверенной загрузки (АПМДЗ) и создание на их основе многофункциональных аппаратно-программных средств защиты информации обуславливают необходимость проведения дополнительных исследований подобных устройств на предмет оценивания корректности и надежности реализации дополнительных функциональных возможностей АМПДЗ в свете влияния их на функциональную безопасность автоматизированной системы в защищенном исполнении (АС ЗИ) в целом [1].

Применительно к заданным условиям оценивания АПМДЗ разработана методика, обеспечивающая научно обоснованную оценку функциональных возможностей АПМДЗ в сфере их влияния на защищенность обрабатываемых данных от НСД с целью выявления аппаратно-программного средства с наилучшими характеристиками.

Задача комплексного оценивания функциональных возможностей АПМДЗ рассматривается как задача получения значений частных показателей функциональных возможностей АПМДЗ и численного показателя $E(A)$ эффективности защиты от НСД, обеспечиваемой модулем А, зависимого от наборов функциональных возможностей $OF\ (A)$ и $DF\ (A)$

В качестве математического аппарата для получения оценки эффективности АПМДЗ выбран метод экспертных оценок, обладающий следующими преимуществами:

– суммарная информация об АПМДЗ, которой обладают все члены группы экспертов, не меньше информации, располагаемой каждым из них. При правильном подборе группы экспертов суммарная информация, располагаемая ею, гораздо больше информации любого из участников группы экспертов;

– ранжирование функциональных возможностей, а также ввод и применение понятия «вес экспертного мнения» позволяют компенсировать полярность экспертных мнений, что способствует получению более точной комплексной оценки функциональных возможностей АПМДЗ [2].

В качестве процедуры экспертных измерений выбран метод Черчмена – Акоффа (последовательное сравнение) [2]. Согласно методу Черчмена – Акоффа, функциональные возможности ранжируются по предпочтительности.

В результате получена формула вычисления комплексной оценки функциональных возможностей АПМДЗ:

$$E(A) = \frac{\sum_{i=1}^{n}\sum_{z=1}^{m}\sum_{j=1}^{t}\psi(G_i) * k_{ij} * \varphi(FV_{ij}) * E_z}{\sum_{z=1}^{m} E_z},$$

где E_z — вес, приписываемый оценке z-го эксперта; FV — функциональная возможность (основная или дополнительная); φ *(VF)* — ранг функциональной возможности; k — оценка функциональной возможности; ψ *(G)*— ранг группы функциональных возможностей.

Разработанная методика комплексной оценки функциональных возможностей АПМДЗ обеспечивает оценивание уровня функциональной безопасности всего устройства в зависимости от архитектуры построения функциональных подсистем и параметров их настроек.

Для выбора устройства АПМДЗ, предлагаемого к применению в АС ЗИ, будут проводиться испытания на основании разработанной методики, по итогам которых будет выбран показавший наилучшую результативность модуль.

СПИСОК ЛИТЕРАТУРЫ:

1. *Беляева Е. А.* Разработка методики комплексного тестирования многофункциональных аппаратно-программных средств защиты информации // XIV Международная телекоммуникационная конференция студентов и молодых ученых «Молодежь и наука». Тезисы докладов. Ч. 3. М.: НИЯУ МИФИ, 2010. – С. 223.
2. Системный анализ и принятие решений: словарь-справочник: учеб. пособие для вузов / Под ред. В. Н. Волковой, В. Н. Козлова. М.: Высш. шк., 2004. – 616 с.

И. С. Боридько, А. А. Забелинский, Ю. И. Коваленко

DLP-СИСТЕМЫ: ЗАЩИТА ОТ ИНСАЙДЕРОВ

Современные информационные системы позволяют оперативно собирать информацию, систематизировать и группировать ее, ускоряя процессы принятия управленческих решений и обеспечивая прозрачность деятельности организации и для руководства, и для сотрудников.

Становится очевидным, что большое количество стратегических данных конфиденциального характера является важным информационным ресурсом организации и последствия потенциальной утечки этой информации скажутся на эффективности деятельности организации.

Традиционные средства обеспечения информационной безопасности, такие как системы обнаружения атак, межсетевые экраны, антивирусные программы, выполняют функции защиты информационных активов от внешних угроз, но не обеспечивают защиту информационных ресурсов от утечки, искажения или уничтожения внутренним злоумышленником (инсайдером). Поэтому задача защиты конфиденциальных данных становится одной из актуальных на сегодняшний день [1].

Решить проблему случайных и умышленных утечек конфиденциальных данных позволяют DLP-системы (*Data Leak Prevention System*), или системы предотвращения утечек [2,3].

DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При обнаружении в исходящем потоке конфиденциальной информации срабатывает DLP-система, и передача сообщения (пакета, потока, сессии) блокируется.

DLP-система реализуется путем использования технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также за счет применения технических устройств (программных или программно-аппаратных) для предотвращения утечек. Защита конфиденциальной информации осуществляется DLP-системой при помощи следующих