4. Biometrics and Authentication in Elearning wiki. URL: http://biometrics.pbworks.com (дата обращения: 12.12.2012).
5. Voice Biometrics Group. Authenticating the Identity of Distance Learning Students. Voice Biometrics Group (VBG) Vocal-ID™ Service Assures Identity. URL: www.voicebiogroup.com (дата обращения: 29.11.2012).
6. *Levey S., Ed. D.* Associate Vice Chancellor, Jeff Maynard B.Sc., CEO and Founder. Identity Proofing for Online Student ID Verification: Report of Pilot with Houston Community College, January 17, 2011.
7. *Takamizawa H., Kaijiri K.* Reliable Authentication Method by Using Cellular Phones in WBT. Faculty of Engineering, Shinshu University. Japan, 2006.

В. И. Королев, В. Ю. Статьев

СОЗДАНИЕ ДОВЕРЕННОЙ ВИРТУАЛЬНОЙ СРЕДЫ

Опыт создания автоматизированных систем показывает, что информатизация охватывает различные процессы и проблемно-тематические области деятельности организаций, все чаще порождает новые вызовы, связанные с нерешенными проблемами.

Современный этап информатизации требует создания автоматизированных систем в защищенном исполнении (АСЗИ), включающих в свой состав информационно-вычислительные комплексы различного уровня функциональной и архитектурной сложности, которые связаны между собой единой информационной моделью и единой телекоммуникационной средой.

Разработчики создаваемых АСЗИ сталкиваются с рядом серьезных проблем, которые не позволяют обеспечить требуемую ритмичность проектирования систем и уровень качества информатизации, что приводит к удорожанию конечного продукта проектирования.

Основными из таких проблем являются:

1. Концептуальные идеи обеспечения информационной безопасности ИТ-систем, нормативная база, регламентирующая вопросы создания АСЗИ, и процесс ее развития отстают от динамики модернизации и совершенствования современного аппаратного, программного и информационного обеспечения автоматизированных систем, от появления новых образцов изделий ИКТ и применения новых подходов к архитектурному построению ИТ-систем.

2. Существующее доверенное общесистемное программное обеспечение (операционные системы, системы управления базами данных, системы управления ресурсами и т. д.), как правило, не соответствует требованиям по созданию АСЗИ необходимого класса защищенности, предъявляемым в соответствии с актуальной в момент создания системы нормативной базой.

3. Для реализации целевых функций информатизации отсутствует доверенное прикладное программное обеспечение с требуемыми тактико-техническими характеристиками применения.

4. Допустимые к использованию технологии и средства защиты информации, степень развития которых напрямую связана с уровнем развития доверенных аппаратных и программных платформ, как правило, отстают по своим функциональным и техническим возможностям, которые требуются в создаваемых АСЗИ.

Имеет место ряд объективных факторов, которые влияют на решение указанных проблем. Значимыми факторами являются большие затраты временных, финансовых и людских ресурсов на выявление недекларированных возможностей в программных продуктах и аппаратных средствах, определение скрытых каналов мониторинга и управления информационными процессами. Это, прежде всего, относится к изделиям производителя, не имеющего доверенного статуса.

На практике полное выявление подобных возможностей и каналов является крайне трудоемкой, дорогостоящей и иногда весьма сложной технической задачей. В ряде случаев эта задача вообще не имеет решения.

Представляется, что эти проблемы могут быть в определенной мере решены, если рассматривать в совокупности доверенную платформу виртуализации как технологическую основу защиты информации от НСД в АСЗИ и процессно-ролевую модель разграничения доступа.

При этом под *доверенной платформой виртуализации* понимается платформа, которая представляет собой доверенную среду виртуализации, позволяющую разворачивать в ней виртуальные машины, обладающие свойством «инкапсуляции», под управлением любой недоверенной «гостевой» ОС. Свойство «инкапсуляции» виртуальных машин означает, что любое устанавливаемое ПО, включая и недоверенное, в пределах доверенной среды виртуализации не сможет:

- оказать какое-либо негативное влияние на другую виртуальную машину, развернутую в доверенной среде виртуализации, в том числе и на установленное в ней программное обеспечение;
- повлиять на функции безопасности доверенной среды виртуализации, обеспечивающей взаимную изоляцию машин и их свойство «инкапсуляции».

Виртуализация может быть обеспечена путем применения гипервизорной модели виртуализации. При этом гипервизор является монитором виртуальных машин, обеспечивающим одновременное, параллельное выполнение нескольких операционных систем на одном и том же хост-компьютере, а также обеспечивает изоляцию операционных систем друг от друга, разделение ресурсов между различными запущенными ОС и управление ресурсами.

В основе реализации механизмов защиты информации и разграничения доступа лежит *процессно-ролевая модель*, в рамках которой конкретная функциональность и семантика информации ассоциируются с определенной ролью, выполняемой группой специалистов в ходе конкретного процесса реализации своих профессиональных обязанностей.

Применяя эти схемы функционирования, можно организовать процессное управление, в котором обязательно имеются точка доверенного входа в процесс, точки доверенного контроля процесса и возможны недоверенные точки процесса.

В состав доверенной платформы виртуализации должны входить:

- аппаратная платформа, включая доверенный BIOS;
- доверенный гипервизор;
- доверенная базовая операционная система.

В качестве объектов виртуализации могут выступать:

- серверные компоненты АСЗИ;
- автоматизированные рабочие места пользователей АСЗИ;
- приложения/сервисы АСЗИ;
- сетевые компоненты АСЗИ;
- средства хранения данных;
- аппаратное обеспечение.

В рамках рассматриваемого подхода из известной совокупности характеристик безопасности информации акцент делается, прежде всего, на такую характеристику, как «конфиденциальность». Другие характеристики безопасности информации могут быть обеспечены методами, которые в данной статье не рассматриваются.

Для каждого объекта виртуализации в рамках доверенной платформы виртуализации определяются метки безопасности. Виртуальный объект (например, виртуальная машина) соотносится с одной или несколькими ролями, доступ к нему равноправный для всех субъектов этих ролей.

Технология виртуализации естественным образом поддерживает процессно-ролевую модель организации разграничения доступа, так как сама в своей основе имеет фрагментацию функциональных элементов АСЗИ в виде виртуальных машин и процессную модель организации вычислительного процесса.

Таким образом, основными характеристиками подхода являются:

- соотнесение одной виртуальной машины с одной или несколькими ролями, причём доступ к виртуальной машине равноправный для всех субъектов этих ролей;
- использование доверенной операционной среды, обеспечивающей управление процессами виртуализации;
- инкапсуляция виртуальных машин по отношению к другим виртуальным машинам, обеспечивающая невозможность несанкционированного взаимодействия между ними;
- наличие меток безопасности у виртуальных машин.

Основными достоинствами рассматриваемой архитектуры АСЗИ и технологии организации доступа являются:

- учет установленных требований безопасности информации в условиях использования недоверенного программного обеспечения;
- высокая надежность АСЗИ, которая обуславливается тем, что в случае выхода из строя отдельного терминального сервера, сервера базы данных или приложений остальные виртуальные машины, развернутые в рамках доверенной среды виртуализации, сохранят свою работоспособность благодаря изоляции виртуальных машин друг от друга;
- высокая масштабируемость АСЗИ, связанная с тем, что в случае необходимости развертывания дополнительной роли пользователя эта задача решается путем развертывания в рамках доверенной среды виртуализации дополнительной виртуальной машины с соответствующим программным обеспечением.

Предложенный подход прошел практическую апробацию, включая нагрузочные испытания, и показал прагматическую эффективность своего применения.