УДК 004.056

АНАЛИЗ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБМЕНЕ ИНФОРМАЦИЕЙ И УПРАВЛЕНИИ СРЕДОЙ ВИРТУАЛИЗАЦИИ УДАЛЕННЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

М.Б. Довгаленко, В.В. Семенов
(Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, г. Санкт-Петербург)
Научный руководитель – к.т.н. Будько М.Ю.
(Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, г. Санкт-Петербург)

Сегодняшний опыт организации центров обработки данных (ЦОД) позволяет выделить основные недостатки традиционных ЦОД, которые находятся на контролируемой зоне: высокая стоимость аппаратной части, сложность восстановления работоспособности системы после сбоев, проблема распределения вычислительных ресурсов между потребителями, низкая энергоэффективность. Использование виртуализации помогает обойти часть недостатков традиционных ЦОД, однако появляются новые уязвимости: возможность злоумышленника подключиться к каналу связи с ЦОД, возможность доступа к хранимым данным и вычислительным мощностям других пользователей в обход системы разграничения доступа, необходимость поддерживать устойчивый канал связи с вычислительной инфраструктурой.

Целью работы является анализ информационной безопасности при обмене информацией и управлении средой виртуализации удаленных центров обработки данных.

Базовые положения исследования. В исследовании были рассмотрены основные особенности организации работы удаленных центров обработки данных:

- Организация надежного канала связи с высокой пропускной способностью;
- Включение в систему ЦОД механизмов резервного копирования и восстановления работоспособности после сбоев;
- Наличие системы разграничения доступа к вычислительным ресурсам и хранимым данным между пользователями;
- Наличие механизма аутентификации для пользователей и администраторов ЦОД;
- Наличие механизма проверки легитимности управляющих команд, то есть необходимо достоверно определять, что инициатором изменений в работе системы является уполномоченное лицо, а не злоумышленник.

В результате анализа были выделены наиболее актуальные проблемы информационной безопасности при управлении средой виртуализации ЦОД: необходимость дополнительной проверки достоверности получаемых сервером команд, для этого необходимо помимо настройки разноуровневых прав на изменение дополнительно использовать заверение команд электронной подписью с последующей проверкой на стороне сервера. Настройка доступа и обмена информацией между виртуальными машинами, расположенными на одном сервере.

Результаты работы. Проведен анализ актуальных проблем информационной безопасности при управлении удаленными центрами обработки данных. Определены наиболее критичные уязвимости таких систем, предложены способы минимизации вероятности реализации данных угроз.