АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ И СРЕДСТВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ВИРТУАЛИЗАЦИИ В ВЫСШЕМ УЧЕБНОМ ЗАВЕДЕНИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Калиновская А. А., Савицкая Д. Г.

Кункевич Д. П. – канд.техн.наук, доцент

В данной работе рассмотрены основные принципы, которые необходимо учитывать при построении безопасных систем. Также рассмотрены основные способы и методы обеспечения безопасности информации, расположенной в виртуальной инфраструктуре, и обеспечение безопасности самой виртуальной инфраструктуры.

Основным устройством в системе образования для доступа к информационным ресурсам является персональный компьютер. Для обучения студентов используется большое количество компьютеров различной производительности, и иногда дисциплины образовательного процесса требуют широкого спектра информационных и программных ресурсов. Зачастую необходимые программные и технические возможности компьютеров несовместимы друг с другом, что может привести к еще большему увеличению числа компьютеров или необходимости их частой модернизации. Студентам необходим доступ к устройствам с прикладным программным обеспечением при проведении практических занятий, а количество компьютеров и их технические характеристики в разных классах могут не соответствовать требованиям. В то же время не всегда возможно установить на существующие компьютеры все приложения, необходимые для обеспечения учебного процесса из-за их недостаточной производительности. При этом важно обеспечить студентам и сотрудникам безопасный и надежный доступ к информационным ресурсам и приложениям.

Решение, которое отвечает всем этим требованиям, заключается в создании безопасного частного облака. Использование облачных технологий дает ряд преимуществ: экономия энергоресурсов, централизованное управление, компактность, мобильность, хранение информации в центре обработки данных, возможность работы с несколькими рабочими столами или несовместимым программным обеспечением. Облака объединяют различные аппаратные и программные технологии и в совокупности составляют сложную систему.

Ключевой технологией облачных сред является виртуализация. Виртуализация и облачные вычисления - это два термина, которые часто кажутся взаимозаменяемыми. Хотя эти две технологии похожи, они не одно и то же, и разница значительна. Виртуализация является фундаментальным элементом облачных вычислений и помогает повысить ценность облачных технологий. Облачные вычисления - это доставка общих вычислительных ресурсов и программного обеспечения. Технология виртуализации создает свободу, которая характеризует облака. Виртуализация позволяет эффективно распределять и настраивать несколько виртуальных машин на одном физическом хосте или перемещать одну виртуальную машину между разными хостами, также предлагает значительные преимущества с точки зрения изоляции, балансировки нагрузки с поддержкой динамической миграции, отказоустойчивости и более гибкого использования ресурсов.

Несмотря на все преимущества использования виртуализации, она создает новые уязвимости и угрозы в облачной системе. Виртуализация является целью злоумышленников. Злоумышленники могут скомпрометировать виртуальную инфраструктуру, получив доступ к виртуальным машинам и информации, хранящейся на них. Поэтому важно создать безопасную и надежную среду для работы студентов и сотрудников.

Можно выделить 2 типа проблем безопасности виртуализации, которые необходимо учесть: безопасность аппаратной части и безопасность информации. Обеспечение безопасности аппаратной части включает в себя физическую защиту всех устройств и предотвращение несанкционированного доступа к ним. Безопасность информации означает защиту хостов, виртуальных машин, а также информации, хранящейся в виртуальной инфраструктуре.

При построении безопасной инфраструктуры необходимо опираться на такие основополагающие принципы безопасности как конфиденциальность, целостность и доступность. Данные принципы определяют цели защиты виртуального пространства. Конфиденциальность препятствует передаче информации неавторизованным лицам, ресурсам или процессам. Целостность - это достоверность, согласованность и точность данных. Наконец, доступность гарантирует, что информация доступна авторизованным пользователям.

К основным методам обеспечения конфиденциальности информации можно отнести следующие:

- применение шифрования;

- стратегии управления доступом;
- маскирование данных.

К средствам обеспечения целостности относятся:
- алгоритмы хеширования;
- использование сертификатов и цифровых подписей.

Меры по обеспечению доступности:
- управление ресурсами;
- многоуровневая защита;
- резервирование;
- мониторинг;
- системы обнаружения вторжений;
- резервное копирование и аварийное восстановление.

Внедрение отдельного решения не может полностью обезопасить инфраструктуру от большого количества различных типов угроз. Поэтому средства и меры по обеспечению безопасности следует комплексно внедрять на нескольких уровнях.

Список использованных источников:

1. Security aspects of virtualization [Электронный ресурс]. – Режим доступа: https://www.enisa.europa.eu/publications/security-aspects-of-virtualization.

2. Virtualization Security [Электронный ресурс]. – Режим доступа: https://resources.infosecinstitute.com/virtualization-security-2/.