Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056

Бобков
Олег Владиславович

Система обеспечения информационной безопасности центра обработки данных

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-98 80 01 "Методы и системы защиты информации, информационная безопасность"

Научный руководитель
Пулко Татьяна Александровна
кандидат технических наук, доцент

Минск 2016

ВВЕДЕНИЕ

С целью оптимизации структуры, расширения числа сервисов и удовлетворения растущих потребностей пользователей, происходят процессы объединения информационных ресурсов предприятий в единую систему, к развитию новых критически важных приложений, к модернизации серверных парков. Учитывая, что ЦОД часто используют крупные организации энергетического и банковского сектора, операторы связи и компании, сдающие ресурсы ЦОД в аренду, то возрастают требования по обеспечению их надежной работы и устойчивости к внешним воздействиям со стороны сторонних пользователей и организаций.

В Республике Беларуси в данный момент существует два основных государственных стандартов регулирующие правовые аспекты проектирования и эксплуатации ЦОД: СТБ П 2227-2011 “Центры обработки данных. Общие правила проектирования”, СТБ П 2236-2011 “Информационные технологии. Требования к показателям качества интернет-услуг”.

Эти стандарты описывают ряд потенциальных угроз работы ЦОД, указывают на необходимость постоянного мониторинга сетевого и серверного оборудования, гибкость в управлении инфраструктуры, определяют место технологий виртуализации в информационной защите.

Данная работа посвящена разработке системы мер, формирования безопасных центров обработки данных и виртуализация безопасных процессов для локальной и магистральной инфраструктуры предприятия, реализующей основные положения названных нормативных документов.

Система обеспечения безопасности ЦОД должна обеспечивать гибкость, комплексную защиту инфраструктуры предприятий, предлагать средства для защиты важных приложений и конфиденциальных данных, и быстро создавать новые безопасные среды для работы приложений, обеспечивающих поддержку новых производственных процессов. А система защиты ЦОД должна давать возможность предприятиям внедрять новые технологии коммутации, хранения данных и программного обеспечения, которые позволят наращивать функциональность, увеличивать производительность, соответствуя растущим технологическим и требованиям предприятий.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи исследования

Цель настоящей диссертационной работы состоит в разработке концепции формирования безопасных центров обработки данных и виртуализация безопасных процессов для локальной и магистральной инфраструктуры предприятия.

Для достижения поставленной цели потребовалось решение следующих задач:

1. Провести анализ и обоснование существующих концепций проектирования центров обработки данных.
2. Реализовать механизмы обеспечения безопасной инфраструктуры, исследуемого центра обработки данных предприятия.
3. Выполнить виртуализацию разработанных механизмов безопасности центра обработки данных по выбранным направлениям исследования.

В качестве объекта исследования рассматривался центр обработки данных.

Предметом исследований являлись технологии виртуализации сети предприятия, которые позволяют организовать защиту и увеличивает контроль над сетями.

Личный вклад соискателя

Содержание диссертации отражает личный вклад соискателя. В работах, выполненных в соавторстве, автор принимал участие в определении целей, задач исследований, а также в проведении самих исследований и обработке полученных результатов.

Апробация и опубликованность результатов

Основные полученные результаты диссертационной работы докладывались и обсуждались на международной научно-технической конференции «Информационные технологии и системы 2015 (ИТС 2015» (Минск, Республика Беларусь, 2015 г.) и XIII Белорусско-российской научно-технической конференции «Технические средства защиты информации» (Минск, Республика Беларусь, 2014 г.). – сюда вставьте свои публикации.

По результатам исследований, представленных в диссертации, опубликовано 2 работы, в том числе 1 статья в сборнике материалов конференций, 1 статья в научном журнале.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, четырех глав, заключения и библиографического списка. Полный объем диссертации составляет 84 страницы машинописного текста. Диссертация содержит 21 рисунков на 17 страницах. Библиографический список занимает 3 страниц и состоит из 32 наименования использованных источников и списка собственных публикаций соискателя из двух наименований на одной странице.

Связь с приоритетными научными направлениями

В работе рассматриваются вопросы разработки средств технической и криптографической защиты, соответствующие приоритетным направлениям научно-технической деятельности в Республике Беларусь по направлению информационно-коммуникационных и аэрокосмических технологий.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении приводится оценка значимости центров обработки данных в современном информационном обществе, рассматриваются основные стандарты Республики Беларусь защиты центров обработки данных, формулируются решаемые в магистерской диссертации задачи.

В первой главе приводится описание понятия центр обработки данных, его структура. Анализируются проблемы обеспечения информационной безопасности ЦОД и наиболее распространенные виды угроз и атак, которым они подвергаются. Приводиться обзор работ и публикаций последних лет по тематике обеспечения информационной безопасности сетевого, серверного оборудования и центров обработки данных в целом. Обосновывается актуальность темы магистерской диссертации.

Во второй главе приводится обзор технологий, которые позволяют обеспечить мониторинг, безопасность оборудования и передачу трафика с помощью технологий VPN, AAA, NTP, ACL и др. Рассмотрены принципы работы систем обнаружения и предотвращения вторжений (Cisco IPS/IDS), а также брандмауэр CISCO ASA.

В третьей главе рассматриваться наиболее популярные средства виртуализации, симуляторы и эмуляторы сетей. Приводиться тестовый стенд, настроенный в GNS3, который реализует концепцию многоуровневой защиты серверов, на основе комплексного применения набора различных технологий.

В четвертой главе приводятся примеры реализации различных технологий защиты центров обработки данных, на основе оборудования Cisco в приложении GNS3.

В заключении приводятся основные результаты, полученные в ходе выполненных исследований.

ЗАКЛЮЧЕНИЕ

В данной работе были определены наиболее распространенные и критические угрозы, которым подвергаются центры обработки данных. Проведен анализ работ, посвященных решению задачам защиты ЦОД, на основании которых был проведен анализ потенциальных угроз.

Исходя, из обозначенных угроз были рассмотрены технологии и методы, которые позволяют сформировать многоуровневую архитектуру защиты современных приложений, сделать комплексную защиту магистральной инфраструктуру и управления. Выделены принципы работы, сильные и слабые стороны применения каждой технологии.

Рассмотрены методы и технологии позволяют с помощью виртуализации смоделировать инфраструктуру любой сложности, и выявить все уязвимые места в инфраструктуре центров обработки данных.

Все выше изложенные подходы описывают концепцию системы защиты, при совместном их использовании обеспечивается полная защита всех компонентов и инфраструктуры.

Данная концепция позволят обеспечивать непрерывную защиту, несмотря на возможность масштабируемости инфраструктуры центров обработки данных и внедрения новых технологий.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. А.О. Хмельницкий, О.В. Бобков, Т.А. Пулко, “Защита динамических веб-сайтов с помощью продукции компании CheckPoint на примере межсетевого экрана CheckPoint R77”, XIII Белорусско-российской научно–технической конференции, с.50, г. Минск, БГУИР 4–5 июня 2015 г.

2-А. О.В. Бобков, А.О. Хмельницкий, Т.А. Пулко, “Использование системы управления конфигурациями Ansible как инструмента для управления несколькими WEB-серверами”, с. 26 – 27, Международная научная конференция «Информационные технологии и системы 2015 (ИТС 2015)», БГУИР, Минск, Беларусь, 28 октября 2015