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

УДК 004.56:621.395

Петрученя
Евгений Юрьевич

Разработка комплексной системы защиты информации в центрах обработки данных на примере РУП «Белтелеком»

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

Научный руководитель
Першин Виктор Тихонович
канд. техн. наук, доцент

Минск 2016

ВВЕДЕНИЕ

В современном понимании центр обработки данных – это комплексное организационно-техническое решение, предназначенное для создания высокопроизводительной и отказоустойчивой информационной инфраструктуры.

Учитывая современные тенденции развития центров обработки данных, их технологическое совершенствование, усложнение инфраструктуры и появление многоуровневой архитектуры, необходимо уделять пристальное внимание обеспечению безопасности хранимой, передаваемой и обрабатываемой информации на всех этапах жизненного цикла. Важно понимать, что в современном мире угрозы информационной безопасности носят комплексный характер.

Комплексный характер угроз нарушения конфиденциальности, целостности и доступности информации в ЦОД приводит к необходимости её комплексной защиты от подобного рода угроз. Это, в свою очередь, ставит крайне остро вопросы методического обеспечения мер комплексной защиты информации в ЦОД для направлений её совершенствования.

Целевая комплексность механизмов защиты информации в ЦОД предполагает реализацию механизмов обеспечения информационной безопасности и всей совокупности факторов, влияющих на нее. Это означает, что механизмы защиты информации должны строиться для достижения целевой функции защиты – обеспечение конфиденциальности, целостности и доступности хранимой, обрабатываемой и используемой информации.

Структурная комплексность предполагает использование при реализации единых целей защиты информации в ЦОД различных средств защиты.

В качестве отдельного вида средств защиты информации выделяются криптографические средства, реализуемые в виде технических, программных и программно-аппаратных средств.

Данная диссертационная работа посвящена решению вопросов информационной безопасности дата-центра РУП «Белтелеком». Таким образом, целевой установкой является соотнесение мировых тенденций развития систем защиты информации с ситуацией в непосредственно рассматриваемом центре обработке данных. Учитывая несовершенство применяемых средств защиты информации, а также отсутствие комплексности в построении системы защиты, необходимо представить рекомендации и выстроить концепции повышения уровня защищенности информации на всех этапах жизненного цикла.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью диссертационной работы является исследование и выбор средств для комплексной защиты информации центра обработки данных РУП «Белтелеком».

Для достижения данной цели необходимо решить следующие задачи:

1. Провести анализ инфраструктуры центров обработки данных.
2. Провести анализ угроз информационной безопасности центров обработки данных и разработать модель угроз безопасности дата-центра РУП «Белтелеком».
3. Разработать комплексную системы защиты информации центра обработки данных РУП «Белтелеком».
4. Разработать систему мониторинга и управления событиями информационной безопасности центра обработки данных РУП «Белтелеком».

Связь с приоритетными направлениями научных исследований и запросами реального сектора экономики

Тема диссертационной работы соответствует подразделам 5.2 «Системные решения, архитектура, методологическое и аппаратно-программное обеспечение высокопроизводительных параллельных и распределенных информационно-коммуникационных процессов, сетей и систем, их информационная безопасность» и 5.5 «Методы, средства и технологии обеспечения информационной безопасности при обработке, хранении и передаче данных с использованием криптографии, квантово-криптографические системы» приоритетных направлений фундаментальных и прикладных научных исследований Республики Беларусь на 2011–2015 гг., утвержденных Постановлением Совета Министров Республики Беларусь 19.04.2010 г., № 585.

В данной работе разработана система мониторинга и управления событиями информационной безопасности на примере центра обработки данных РУП «Белтелеком» с использованием бесплатной программной платформы, что имеет экономическую целесообразность.

Апробация диссертации и информация об использовании ее результатов

Основные положения и результаты исследований докладывались и обсуждались на 51 СНТК БГУИР (Минск, 13.04.2015 – 17.04.2015).

По результатам исследований, представленных в диссертации, опубликована 1 работа.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении и общей характеристике работы обосновывается актуальность выбранной темы, даётся краткая характеристика её разработанности, определяются цель и задачи, указывается теоретико-методологическая основа, отмечены элементы научной новизны, формулируются основные положения диссертации, выносимые на защиту.

Первая глава носит теоретический характер, состоит из 2 разделов. Она посвящена современным подходам к обеспечению защиты информации центров обработки данных. Также приводится обзор нормативных документов РУП «Белтелеком», регламентирующих вопросы защиты информации на предприятии.

Вторая глава носит теоретический характер, состоит из 3 разделов. В ней дается определение и характеристика центров данных, определяются основные услуги, предоставляемые центрами обработки данных. Анализируется структура дата-центров для формирования списка компонентов, наиболее подверженных информационным или физическим атакам злоумышленников. Изучение и анализ данного аспекта позволил определить угрозы информационной безопасности центров обработки данных относительно их составляющих компонентов и разработать модель угроз информационной безопасности центра обработки данных РУП «Белтелеком».

Третья глава носит практико-ориентированный характер, состоит из 2 разделов. В ней формулируется определение комплексной системы защиты информации исходя из системного представления процесса защиты информации. Глава посвящена разработке комплексной системы защиты информации центра обработки данных РУП «Белтелеком», посредствам предоставления рекомендаций по внедрению и использованию средств организационной и технической защиты информации относительно IT-инфраструктуры, инженерных систем и систем физической безопасности.

Четвертая глава носит практико-ориентированный характер, состоит из 6 разделов. Она посвящена разработке системы мониторинга и управления событиями информационной безопасности центра обработки данных РУП «Белтелеком» на основне рекомендации, выданных в третьей главе. Представлено общее описание и задачи разрабатываемой системы. В главе приводятся основные конфигурации средств мониторинга и управления событиями информационной безопасности различных систем и модулей центра обработки данных (ОС Microsoft Windows Server, Unix-подобных ОС, сетевой инфраструктуры, физической среды помещений). В результате разработки описывается основной функционал системы, приводятся рисунки, иллюстрирующий визуальные сводки, отчеты, журналы событий.

В приложении представлен сконфигурированный шаблон для мониторинга событий информационной безопасности физической среды

помещений центра обработки данных.

ЗАКЛЮЧЕНИЕ

В работе получены следующие основные результаты.

Определено, что с точки зрения информационной безопасности основным компонентом центров обработки данных является совокупность систем мониторинга, управления и диспетчеризации дата-центров, обеспечивающая оповещение об аварийных событиях, протоколирование работы модулей центров обработки данных: IT-инфраструктуры, инженерных систем и систем физической безопасности.

Осуществлена классификация угроз информационной безопасности центра обработки данных РУП «Белтелеком» для его основных компонентов (IT-инфраструктуры, инженерных систем и систем физической безопасности) на основе модели конфиденциальности, целостности и доступности.

Разработана система защита информации центра обработки данных РУП «Белтелеком», основанная на использовании организационных и технических средств защиты сетей хранения данных, сетевой инфраструктуры, серверной инфраструктуры и виртуальной среды, систем электропитания и кондиционирования, систем защиты физической среды и помещений центра обработки данных.

В качестве базовой платформы для разработки системы мониторинга и управления событиями информационной безопасности выбрана свободная система мониторинга Zabbix, позволяющая максимально автоматизировать процессы обнаружения и устранения уязвимостей. Автоматический мониторинг информационной безопасности позволяет повысить уровень защищенности информации, хранимой и обрабатываемой дата-центром РУП «Белтелеком» при минимальной затрате материальных средств. Возможность получать максимально достоверную картину защищенности инфраструктуры ЦОД обеспечивается при помощи разработанных карт сетей, отчетов и журналов событий.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Петрученя, Е.Ю. Разработка комплексной системы защиты информации центров обработки данных на примере РУП «Белтелеком» / Е.Ю. Петрученя // 51 СНТК БГУИР: материалы 51 научной конференции аспирантов, магистрантов и студентов. Минск, 13-17 апреля 2015 г. – Минск, 2015 – с. 373-376.