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

УДК 004.056:004.7

ПИНЧУК
Станислав Сергеевич

СРЕДСТВА МОНИТОРИНГА И ПРЕДОТВРАЩЕНИЕ УГРОЗ В КОМПЬЮТЕРНЫХ СЕТЯХ

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

Научный руководитель
Рыбак Виктор Александрович
Кандидат технических наук, доцент

Минск 2017

ВВЕДЕНИЕ

В последние годы с ростом уровня автоматизации, проникновения информационных технологий во все сферы деятельности человека и значительным повышением требований отказоустойчивости и надежности к информационным системам важное значение приобретают вопросы разработки эффективных средств мониторинга и диагностики информационных систем. В связи с повсеместным использованием вычислительных сетей и сетей передачи данных для организации взаимодействия как между отдельными рабочими станциями для передачи информации прикладного характера (например, при работе в глобальной сети Интернет), так и взаимодействия внутри замкнутых вычислительных кластеров, информационно-вычислительных комплексов обработки данных, корпоративных сетей и иных распределенных систем, основанных на использовании вычислительных сетей, остро встают вопросы мониторинга состояния подобных систем.

Кроме того, актуальными проблемами разработки систем сетевого мониторинга являются увеличение точности анализа состояния входящих в состав вычислительных сетей узлов. В связи с изложенным задачи исследования и разработки методов мониторинга и диагностики вычислительных сетей и распределенных систем, а также систем мониторинга на их основе в настоящее время являются актуальными.

В данной диссертации будут рассмотрены вопросы организации мониторинга и анализа данных. Цель исследования – разработка системы мониторинга трафика компьютерных сетей с целью выявления угроз.

Актуальность темы обосновывается необходимостью развития мониторинга компьютерных сетей по причине возросшего количества сетевых атак.

Практическая значимость работы заключается в возможности применения разработанной системы мониторинга для наблюдения и анализа сетевого трафика различных предприятий с целью выявления потенциальных угроз, подвергающих сетевую инфраструктуру предприятия вероятности утери работоспособности либо утечек информации.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016–2020 гг., утверждённых Постановлением Совета Министров Республики Беларусь 12 марта 2015 г., № 190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в разработке системы мониторинга компьютерных сетей с целью предотвращения атак. Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Проанализировать угрозы информационной безопасности компьютерных сетей.
2. Проанализировать существующие системы мониторинга.
3. Разработать программное обеспечение, осуществляющее перехват пакетов сетевого трафика. Осуществить обработку полученной информации с помощью системы мониторинга.

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликована 1 работа, в том числе 1 статья в научном журнале Общества Науки и Творчества «Научное знание современности»

Структура и объем диссертации

Структура диссертационной работы обусловлена целью, задачами и логикой исследования. Работа состоит из введения, трех глав и заключения, библиографического списка и приложений. Общий объем диссертации — 72 страницы, работа содержит 24 рисунка, 3 таблицы, библиографический список включает 30 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении рассмотрено состояние проблемы необходимости осуществления мониторинга компьютерных вычислительных сетей, определены основные направления исследований, а также дается обоснование актуальности темы диссертационной работы.

В общей характеристике работы сформулированы ее цель и задачи, показана связь с приоритетными направлениями научных исследований, приведена опубликованность результатов диссертации.

В первой главе рассматриваются проанализированы принципы построения компьютерных сетей; осуществлен обзор существующих решений в области мониторинга трафика компьютерных сетей, осуществлен обзор наиболее распространенных сценариев сетевых атак и методы их предотвращения.

Во второй главе приведен анализ и обоснование выбора программной базы для дальнейшей разработки программного обеспечения, описан процесс создания перехватчика пакетов, осуществлен выбор платформы хранения и визуализации данных.

В третей главе представлены результаты построения системы мониторинга трафика компьютерной сети, показан процесс атаки на наблюдаемый сервер, обнаружения угрозы и ее предотвращения. В приложениях приведен графический материал для защиты магистерской диссертации.

ЗАКЛЮЧЕНИЕ

1. Проведена систематизация знаний для понимания структуры, особенностей построения компьютерных сетей, обозначены основные функции системы мониторинга безопасности компьютерной сети, а также проведен обзор законодательной базы Республики Беларусь.

2. Проведено исследование и обзор существующих решений в сфере мониторинга компьютерных сетей, выявлены основные преимущества и недостатки. Разобраны основные сценарии и типы сетевых атак, а также предложены способы их предотвращения.

3. Разработано программное обеспечение, позволяющее перехватывать пакеты сетевого трафика основных протоколов и хранить на локальном дисковом хранилище.

4. Разработан комплекс мониторинга и анализа входящего и исходящего трафика.

5. Произведена пробная сетевая атака против наблюдаемого участка сети, угроза успешно выявлена и устранена, что позволяет утверждать о работоспособности и пользе разработанного решения.

Практическая значимость работы заключается в возможности применения разработанной системы мониторинга для наблюдения и анализа сетевого трафика различных предприятий с целью выявления потенциальных угроз, подвергающих сетевую инфраструктуру предприятия вероятности утери работоспособности либо утечек информации.

Результаты данной диссертационной работы могут быть использованы с целью построения системы мониторинга компьютерной сети любой организации, для которой важно сохранение целостности, работоспособности компьютерной сети, сетевого оборудования, а также рабочих машин конечных пользователей.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Пинчук, С.С. Система мониторинга компьютерных сетей / С.С.Пинчук // Международный электронный научный журнал Общества Науки и Творчества «Научное знание современности». - 2017 г. – № 6. – С. 30-36