УДК 004.7

РАЗРАБОТКА МЕТОДА ОБНАРУЖЕНИЯ АНОМАЛИЙ В СТРУКТУРЕ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ НА ОСНОВЕ АНАЛИЗА ТОПОЛОГИИ

М.А. Пятов
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург
maxs.pyatov36@gmail.com
Научный руководитель - к. т. н., А.В. Гирик
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург

В современном мире с развитием Интернета происходит укрупнение и усложнение сетей, а также рост объемов информации, которая передается по ним. Вместе с этим становится все труднее обеспечивать безопасность сетевой инфраструктуры и информационных потоков. Одним из способов обеспечения безопасности вычислительных сетей является мониторинг целостности их структуры и оперативного обнаружения нарушений структуры сети на физическом и логическом уровне, а также на уровне распределенных потоков данных.

Целью работы является разработка метода обнаружения аномалий в структуре вычислительной сети на основе анализа ее топологии.

Объектом исследования выступают вычислительные сети в процессе их функционирования. Предметом исследования является поиск решения по мониторингу состояния сети в целях обнаружения аномалий, возникающих в ее структуре, путем анализа топологии данной сети и отслеживания изменений в ней.

Основной задачей работы является выявление наилучшего способа сканирования топологии функционирующей сети и дальнейшего поиска аномалий в ее структуре, что будет являться возможной угрозой для безопасности вычислительной сети. Следующая задача работы - реализовать программное средство обнаружения данных аномалий, основывающееся на полученном на предыдущем шаге способе.

В ходе работы были рассмотрены следующие способы реализации сбора информации о топологии сети:

1. Обращение к каждому коммутатору исследуемой сети через консольный интерфейс по протоколу SSH без использования средств протокола LLDP [1];
2. Обращение к каждому коммутатору исследуемой сети через консольный интерфейс по протоколу SSH с использованием средств протокола LLDP;
3. Опрос коммутаторов по протоколу SNMP [2] без использования средств протокола LLDP.
4. Опрос коммутаторов по протоколу SNMP с использованием средств протокола LLDP.

В ходе изучения данных способов были выявлены плюсы и минусы их использования. Для программной реализации был выбран третий способ.

Программное средство было реализовано на языке Python версии 3.

Работа программы заключалась в опросе коммутаторов сети, сборе данных о ее реальной топологии и сравнении полученных данных с задокументированными.

В ходе разработки проводилось тестирование программного средства. Заключительное тестирование показало эффективность и корректность работы программы.

Практическим результатом исследования является выявленный метод обнаружения аномалий в структуре вычислительной на основе анализа топологии и программное средство, реализующее этот метод. Данный метод может стать основой для разработки

комплексных программных средств по мониторингу состояния структуры сети и выявления неисправностей.

Список литературы

1. A. Bierman Request for Comments: 2922. Physical Topology MIB [Электронный ресурс] / K. Jones. - Электрон. текстовые дан. - 2000. - Режим доступа: https://tools.ietf.org/html/rfc2922, __ свободный.
2. J. Case Request for Comments: 1157. A Simple Network Management Protocol (SNMP) [Электронный ресурс] / M. Fedor, M. Schoffstall, J. Davin - Электрон. текстовые дан. - 1990. - Режим доступа: https://tools.ietf.org/html/rfc1157, свободный.

Автор М.А. Пятов

Научный руководитель А.В. Гирик

Декан факультета БИТ Д.А. Заколдаев