УДК 004.7

МЕТОД ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ НА ОСНОВЕ УСТРАНЕНИЯ ИЗБЫТОЧНОЙ СВЯЗНОСТИ

Бондарева А.Д. (Университет ИТМО**, г. Санкт-Петербург**)
Научный руководитель – к.т.н., доцент Кузнецов А.Ю.
(Университет ИТМО, г. Санкт-Петербург)

Введение. Одним из наиболее серьезных недостатков в организации информационной инфраструктуры является отсутствие логической сегментации. Проектирование сетей в большинстве случаев осуществляется без учета требований безопасности. Особенно актуальной данная проблема становится в условиях организации удаленной работы. Сетевое разграничение доступа является одним из немногих действенных методов защиты: у потенциального злоумышленника отсутствует возможность для компрометации сервиса при отсутствии доступа к этому сервису. Большинство современных решений основаны на программной сегментации сети, при которой реализуется виртуальная сетевая инфраструктура поверх существующей сети [1]. Недостатки данных решений определяют проблематику разграничения сетевого доступа имеющимися средствами без необходимости внедрения дорогостоящих решений.

Основная часть. Разработана модель сетевых взаимодействий. Для представленной модели описан метод автоматического определения правил межсетевого экранирования. Он направлен на минимизацию показателя критичности путей между субъектами и объектами доступа в условиях ограниченности ресурсов и наличия дополнительного требования, направленного на равномерное распределение правил фильтрации трафика по межсетевым экранам. Последнее правило направлено на защиту от ряда атак, направленных на отказ в обслуживании средств маршрутизации и межсетевого экранирования вследствие наличия чрезмерно большого количества правил. Исходя из степени подверженности сети атакам, была поставлена задача нелинейного программирования. Данная задача была решена с использованием метода ветвей и границ [2]. При решении задачи было наложено ограничение на удаление путей, необходимых для легитимного доступа субъектов к объектам. В результате формируется множество путей для установления запрещающих правил межсетевого экранирования, и, как следствие. устранения избыточной сетевой связности.

Выводы. В данной работе рассмотрена аналитическая модель сетевой инфраструктуры, предназначенная для решения задачи сегментации сетевой инфраструктуры, а также метод сегментации сети с использованием этой модели. Данный метод предназначен для обеспечения сегментации сети в соответствии с принципом минимизации количества правил межсетевого экранирования.

Список использованных источников:

1. Бондарева А.Д. Проблематика обеспечения безопасности сетевой инфраструктуры посредством сегментации сети. Сборник трудов X Конгресса молодых ученых (Санкт-Петербург, 14-17 апреля 2021 г.). 2021. Т. 1. С. 31-35.
2. Мельников, Б. Ф., & Мельникова, Е. А. (2021). О классической версии метода ветвей и границ. Компьютерные инструменты в образовании, (1), 21-44. https://doi.org/10.32603/2071-2340-2021-1-21-45