УДК 004.056

РАЗРАБОТКА СИСТЕМЫ МОДЕЛИРОВАНИЯ СЕТЕВЫХ АНОМАЛИЙ ДЛЯ ТЕСТИРОВАНИЯ И ОТЛАДКИ АЛГОРИТМОВ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

С.А.Кияшко
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, город Санкт-Петербург

Научный руководитель: к.т.н, доцент Гирик А.В.
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, город Санкт-Петербург

Введение. В современном мире сети передачи данных играют все большую роль в обеспечении жизнедеятельности человека. Однако, параллельно с увеличением масштабов компьютерных сетей наблюдается рост и количества информационных угроз и факторов, приводящих к нестабильному функционированию сетей передачи данных. В таких условиях разработка и совершенствование способов обнаружения информационных угроз в СПД приобретают большую важность. Одним из компонентов обеспечения информационной защиты сетей являются программные комплексы, предназначенные для обнаружения вредоносной или подозрительной активности.

Цель работы. Разработка системы моделирования сетевых аномалий для тестирования и отладки алгоритмов обнаружения сетевых атак.

Базовые положения. Для разработки системы моделирования сетевых аномалий были рассмотрены методы генерации тестовой выборки, на основании которой будет производиться поиск аномалий, а так же основные методы построения профиля нормального функционирования, необходимого для поиска заданных пользователем аномалий.

В ходе разработки были проанализированы различные способы и инструменты генерации, хранения тестовой выборки данных и поиска аномалий, заданных пользователем, в сгенерированных значениях.

Основные результаты, промежуточные результаты. Промежуточным результатом работы является тестовая версия системы. В ее функционал входят формирование тестовой выборки данных, в которой будет производиться поиск аномалий, на основании заданных пользователем параметров, и работа с этими данными через интерфейс системы. Программно реализовано внесение в сгенерированные данные аномальных значений, которые пользователь может добавить через интерфейс программы. Так же определены алгоритмы поиска аномалий.