УДК 004.056

АНАЛИЗ ТРЕБОВАНИЙ К НАБОРАМ ДАННЫХ ДЛЯ ВАЛИДАЦИИ МЕТОДОВ ОПРЕДЕЛЕНИЯ ГРУПП АТАКУЮЩИХ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Павлов А.В. (Университет ИТМО, г. Санкт-Петербург)
Научный руководитель – к.т.н., доцент Волошина Н.В.
(Университет ИТМО, г. Санкт-Петербург)

Выделение групп атакующих при анализе событий атак может позволить точнее определить уровень угрозы и применить адекватные ему меры. В работе рассматривается набор требований к наборам данных для подтверждения эффективности методов выявления групп атакующих.

Введение. Выделение групп атакующих при анализе событий атак может позволить точнее определить уровень угрозы и применить адекватные ему меры. Многие современные методы подтверждают свою эффективность на устаревших, закрытых или имеющих известные проблемы наборах данных. Поэтому для выбора надежного набора данных следует сформулировать набор требований к нему.

Основная часть. В рамках работы предложены требования по времени появления набора данных, требования к источнику данных, требуемых атрибутах, разнообразию типов атак в данных и достаточном их представлении и другие.

Выводы. В результате работы предложены требования к наборам данных, которые можно использовать для проверки эффективности методов выявления групп атакующих по данным систем защиты информации. Проведена первичная оценка соответствия существующих наборов данных требованиям. На основании полученного результата возможна разработка подходящего набора данных с использованием уже существующих.

Павлов А.В. (автор) Подпись

Волошина Н.В. (научный руководитель) Подпись