УДК 004.056

РАЗРАБОТКА СИСТЕМЫ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ТРАФИКА НА СЕТЕВОМ, ТРАНСПОРТНОМ И ПРИКЛАДНОМ УРОВНЯХ МОДЕЛИ TCP/IP С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Геннадьев Г. Д. (Санкт-Петербург, Университет ИТМО)
Научный руководитель – к.т.н., доцент Менщиков А. А.
(Санкт-Петербург, Университет ИТМО)

Аннотация. Значительная доля исследований в современной информационной безопасности уделяется анализу сетевого трафика, распознаванию в нем необычного, аномального поведения. В данной работе предложен алгоритм совмещения методов машинного обучения для обнаружения вредоносного трафика при анализе различных цифровых метрик транспортного и сетевого уровня, а также полезной нагрузки прикладного уровня модели TCP/IP. Приведен пример обработки уже существующих записей трафика.

Введение. В современных работах системы обнаружения вредоносного трафика с использованием машинного обучения анализируют только метрики сетевого и транспортного уровня, а полезную нагрузку прикладного уровня исследуют независимо с помощью различных шаблонов, которые пишутся вручную. Данный подход ухудшает результаты, получаемые системой, ввиду человеческого фактора, а также накладывает ограничения в виде постоянной доработки шаблонов.

Основная часть. Одним из недостатков существующих работ является анализ полезной нагрузки с помощью шаблонов, создаваемых человеком, что приводит к уменьшению количества детектируемых атак из-за их мутаций. Вторым недостатком является независимый анализ различных уровней модели TCP/IP. В данной работе предложен вариант анализа полезных нагрузок на прикладном уровне модели TCP/IP с помощью методов машинного обучения, а обучение модели производится с помощью шаблонов. Также для улучшения качества оценки предложено сопоставлять и совмещать результаты анализа различных уровней TCP/IP.

Выводы. Предложенный метод обладает более высокими качественными показателями обнаружения вредоносного трафика среди аналогов, а также большей гибкостью, что делает его перспективным вариантом для внедрения в современные системы обнаружения и предотвращения вторжений. В дальнейшем возможна доработка предлагаемого решения для учета большего количества параметров и метрик.

Геннадьев Г. Д. (автор) Подпись:_____

Менщиков А. А. (научный руководитель) Подпись:_____