УДК 004.056

ПОДХОД К ОБНАРУЖЕНИЮ АНОМАЛИЙ В ЛОКАЛЬНОМ СЕТЕВОМ ТРАФИКЕ НА ОСНОВЕ АНАЛИЗА СТАТИСТИЧЕСКИХ ХАРАКТЕРИСТИК ПОТОКОВ

Автор – Шабала Егор Евгеньевич (Университет ИТМО)

Научный руководитель - к.т.н. Попов Илья Юрьевич (Университет ИТМО)

Введение. Не смотря на использование современных средств защиты во многих случаях обнаружение целевых атак происходит через длительный период времени после первоначального проникновения злоумышленника в защищаемую систему. Одним из возможных подходов к решению данной проблемы является применение в общем контуре системы обеспечения ИБ - систем обнаружения аномалий в сетевом трафике. Основная задача данных систем – сформировать паттерн нормального трафика на основе анализа выбранных его характеристик, выявлять отклонения от паттерна – аномалии, и их классифицировать. При этом в большинстве случаев для работы данных систем необходим доступ к полезной нагрузке трафика, что безусловно сужает потенциально возможный перечень мест их применения.

Иным подходом для формирования паттернов нормального трафика является анализ статистических характеристик потоков, на основе которых для каждого пользователя системы формируется индивидуальная поведенческая метрика, при этом не требуется использования полезной нагрузки трафика, что соответственно исключает возникновение дополнительных векторов атак для злоумышленников. Основной сложностью при данном подходе является определение специфичных для пользователя статистических характеристик - значимых признаков для применения в алгоритмах МО.

Цель работы. Целью данной работы является разработка подхода к обнаружению аномалий в локальном сетевом трафике на основе анализа статистических характеристик потоков, определение перечня статистических характеристик потоков специфичных для выбранного пользователя для формирования его цифровой метрики, сравнение результатов применения данного подхода с использованием различных методов машинного обучения с целью максимизации установленных в работе метрик качества.

Основные результаты. В работе предложен подход, в котором для определенных пользователей и устройств на основе их трафика возможно составить метрику эталонного поведения, описанную статистическими характеристиками, извлеченными из TCP потоков между ними, а именно особенностями, которые характерны для используемых пользователями программных и аппаратных средств, их расположением в топологии сети, маршрутам трафика. Осуществлено тестирование данного подхода на основе собранных в

имитированной сети данных, и сформированных паттернов нормального поведения, с применением нескольких алгоритмов МО. На основе полученных результатов сделан вывод о целесообразности предлагаемого подхода, возможности его реализации в виде комплексного программного решения, оценены результаты применения различных алгоритмов МО и проведено их сравнение, определены значимые статистические признаки и признаки, вызывающие гиперкорреляцию. Определены дальнейшие направления исследования в данной области.

Автор _______ Шабала Е.Е.

Научный руководитель _____ Попов И.Ю.