УДК 004.056.53

ПОДХОД К ПРИМЕНЕНИЮ АНСАМБЛЯ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК

Асадуллин А.Я., Менисов А.Б. (Военно-космическая академия А.Ф. Можайского)
Научный руководитель – к.т.н. Менисов А.Б.
(Военно-космическая академия А.Ф. Можайского)

В докладе представлено описание программного модуля, в основе которого положен новый подход к обнаружению компьютерных атак на объекты информационной инфраструктуры. Инновационность разработанного подхода заключается в использовании ансамбля объединенных моделей машинного обучения, что позволяет повысить результативность выявления и определения вида компьютерных атаки.

Введение. Внедрение информационных технологий с каждым годом оказывает все большее влияние на развитие информационной инфраструктуры - информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, что требует создания современных средств реагирования и предупреждения информационных угроз, ориентированных на анализ сетевого трафика, данных хоста и действий пользователей (например, файлы системного журнала и загрузки). Существенно увеличить качество работы систем обнаружения компьютерных атак и защищаемых ими объектов информационной инфраструктуры позволит использование ансамбля моделей машинного обучения.

Основная часть. Программный модуль обнаружения компьютерных атак на объекты информационной инфраструктуры с использованием ансамбля моделей машинного обучения включает в себя следующие процессы: предварительная обработка данных, отбор признаков, выбор алгоритмов машинного обучения, настройка гиперпараметров алгоритмов, и выбор показателей качества. Конечной целью выявления компьютерных атак на объекты информационной инфраструктуры является некоторый вывод о свойствах любых действий пользователей в сети. Выработка решения всегда осуществляется в условиях неопределенности, обусловленной неполнотой информации об исследуемом процессе, помехами как естественного, так и искусственного характера и т.п. В связи с этим определяемые характеристики, факты и т.д. носят статистический характер, а принимаемые решения являются статистическими. Основой для принятия решения является работа разработанного ансамбля моделей машинного обучения.

Выводы. В результате исследования был разработан программный модуль обнаружения компьютерных атак на объекты информационной инфраструктуры с использованием методов машинного обучения. Кроме того, предложенный программный модуль позволяет обнаруживать ранее неизвестные угрозы. Программный модуль возможно использовать при разработке новых технических решений информационной безопасности.