УДК 004.891.3

МЕТОДИКА ВЫЯВЛЕНИЯ ВНУТРЕННЕГО НАРУШИТЕЛЯ НА ОСНОВЕ ОБРАБОТКИ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Странадкин Р.Н., Асадуллин А.Я., Шалькин Д.О. (Военно-космическая академия А.Ф. Можайского)

Научный руководитель – к.т.н. Менисов А.Б.

(Военно-космическая академия А.Ф. Можайского)

В докладе представлена новая методика выявления внутреннего нарушителя на основе обработки событий информационной безопасности. В основу формирования процесса выявления положено использование ансамбля моделей машинного обучения, объединенных для повышения эффективности определения типа внутреннего нарушителя.

Введение. В настоящее время при постоянной угрозе проведения различных типов атак злоумышленниками особую роль приобретают процессы организации информационной безопасности, особенно мониторинг и обнаружение событий информационной безопасности для обеспечения необходимого уровня конфиденциальности, целостности и доступности информации. Традиционно, наиболее используемой линией защиты информации и приложений являются системы обнаружения вторжений, ориентированные на анализ сетевого трафика, данных хоста и действий пользователей (например, файлы системного журнала и загрузки). В зависимости от процедуры обнаружения вторжений системы защиты обычно определяют аномальное поведение по сравнению с заранее заданными сигнатурами, то есть те события (цепочки событий), которые каким-то образом отклоняются от нормального поведения. Такая оценка традиционно выполняется с использованием смоделированных наборов данных с применением алгоритмов машинного обучения.

Основная часть. Методика выявления внутреннего нарушителя на основе обработки событий информационной безопасности включает в себя следующие этапы: предварительная обработка данных, отбор признаков, выбор алгоритмов машинного обучения, настройка гиперпараметров алгоритмов, и выбор показателей качества. Конечной целью выявления атак внутреннего нарушителя является некоторый вывод о свойствах любых действий пользователя в сети. Характер этих выводов может быть различен, и из множества выводов необходимо выбрать один, оптимальный, то есть принять решение. В рамках данного исследования, под решением будем понимать некоторое заключение, вывод о действии пользователя или его свойствах. 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: нейросетевая модель – для детектировки аномальности действий пользователя, Байесовский классификатор – для определения класса аномальности.

Выводы. Практическая значимость методики и программной реализации выявления внутреннего нарушителя на основе обработки событий информационной безопасности заключается в возможности применения при обосновании и разработке технических решений информационной безопасности.