УДК 004.942

РАЗРАБОТКА МЕТОДА ОБНАРУЖЕНИЯ АНОМАЛИЙ НА ОСНОВЕ ДАННЫХ О ПРОЦЕССАХ В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS

Ванюков А.К. (Университет ИТМО), **Попов И.Ю.** (Университет ИТМО)
Научный руководитель – к.т.н., доцент Попов И.Ю.
(Университет ИТМО)

В данной работе представлен метод обнаружения аномалий действий пользователя в операционной системе Windows. Метод основан на комбинировании методов обнаружения на основе анализа статических и динамических модулей и данных о ресурсах процессов.

Введение. В последнее время все большее число сотрудников в компаниях переходят с офисного режима работы на удаленный, в связи с чем понижается контроль за ними со стороны работодателя и, соответственно, увеличивается риск компрометации конфиденциальной информации, через АРМ сотрудников. Современные системы безопасности обычно предполагают авторизацию пользователя на начальном этапе входа в учетную запись и при некоторых особых действиях, что при компрометации пароля или получение злоумышленником доступа к информационной системе с актуальным ключом сессии может привести к утечке конфиденциальной информации.

Основная часть. Для решение этой проблемы в данной работе предлагается использовать метод обнаружения аномалий в поведении пользователя основанный на комбинации методов обнаружения по исполняемым файлам процессов, статических и динамических модулей, файлов и ресурсов процессов. Для этого была разработана программа для отслеживания необходимых данных о процессах с интервалом в 1 секунду, тем самым обеспечивая возможность ежесекундного поведения пользователя. С помощью данной программы были собраны данные для обучения моделей машинного обучения с 10 реальных и виртуальных машин с Windows.В итоге было собрано около 400000 записей о нормальном поведении и 260000 об аномальном. После обучения и сравнения нескольких моделей машинного обучения на основе этих данных была выбрана модель случайного леса, которая показала F1-score = 97.3% для обнаружения аномалий и 91% для многоклассовой классификации типа аномалий.

Выводы. В ходе проделанной работы были собраны 660000 записей, обучены и сравнены несколько моделей машинного обучения. В результате чего получена готовая система для ежесекундной оценки аномальности поведения пользователя в операционной системе Windows.

Ванюков А.К. (автор) Подпись

Попов И.Ю. (научный руководитель) Подпись