УДК 004.056.2

ПОИСК СРЕДСТВ АВТОМАТИЗАЦИИ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ

Носков Д.Е. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Научный руководитель – к.т.н., Балакшин П.В.

(федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

В данной работе рассматривается способ обнаружения различных средств автоматизации, угрожающих целостности данных в различных системах. Предложенное решение сфокусировано на долговременную работу и выявление подозрительной активности, кроме того, его можно использовать в новой области.

Введение. С развитием процесса цифровизации в современном мире все более активной становится опосредованная работа пользователей с различными информационными системами. Таким образом происходит распространение разнообразных специально разработанных средств автоматизации. Данные средства позволяют обеспечить ускоренную обработку данных, исключить человеческий фактор, который может порождать ошибки внесения, систематизации и хранения данных, вплоть до полной автоматизации процесса. В качестве примера позитивного автоматизированного сервиса можно привести поисковые системы, которые способны выполнять как простой поиск, так и сложные поисковые запросы: мультимедийные (аудио, видео, изображения), с ограничивающими условиями (фильтрация по сайтам, формату страницы и т. п.).

В то же время некоторые информационные системы нацелены на работу исключительно с живым пользователем, поэтому влияние на них автоматизации может негативно сказаться на итоговом результате работы этих систем в целом. Такие информационные системы имеют потребность к отказу в обслуживании пользователей, использующих средства автоматизации.

Основная часть. В целях улучшения качества поиска средств автоматизации предлагается сформировать отдельные решения для каждого типа систем из-за различных угроз.

В частности, для защиты онлайн игр от средств автоматизации предлагается механизм журналирования действий пользователя с последующим анализом периодов активности пользователя с целью выявления поведенческих аномалий. Данный механизм позволит обнаружить средства автоматизации, нацеленные на длительное использование, кроме того, позволит отобрать наиболее подозрительные аккаунты для дополнительной проверки.

Для защиты систем компьютерного тестирования предлагается использовать механизм журналирования времени, затраченного тестируемым на каждый вопрос, а также общего времени тестирования. После окончания проведения теста собранные данные анализируются на предмет поиска временных аномалий, что позволит выявить случаи нечестного выполнения тестирования и/или некорректно сформулированных вопросов.

Выводы. Использование предложенных методов за счет простоты реализации и быстроты внедрения может применяться организациями для повышения уровня информационной безопасности.

Носков Д.Е. (автор) Подпись

Балакшин П.В. (научный руководитель) Подпись