УДК 004.08

РАЗРАБОТКА МЕТОДА ПРОДОЛЖИТЕЛЬНОЙ АУТЕНТИФИКАЦИИ ПРИ РАБОТЕ В БАНКОВСКОМ ПРИЛОЖЕНИИ НА ОСНОВЕ АНАЛИЗА ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЯ

Веневцев И.В. (Университет ИТМО)
Научный руководитель – доцент, кандидат технических наук, Коржук В.М.
(Университет ИТМО)

Введение. Мошенничество в банковских приложениях является одной из актуальных проблем современного мира, связанной с развитием технологий и увеличением использования мобильного банкинга. Мошенники могут использовать различные методы для доступа к финансовым средствам пользователей, включая техники фишинга, создание поддельных мобильных приложений и информационный кражу. Кроме того, с развитием мобильных платежей и онлайн-банкинга риск мошенничества с использованием технологий, таких как компьютерная визуализация и искусственный интеллект, увеличивается [1].

Основная часть. Тема продолжительной аутентификации в банковских приложениях на основе анализа поведения пользователя является актуальной, так как она помогает повысить безопасность информации и снизить риск мошенничества. Этот метод аутентификации использует данные о поведении пользователя, такие как местоположение, способ ввода информации и историю транзакций, чтобы определить, является ли пользователь действительным владельцем учетной записи. Это позволяет снизить риск несанкционированного доступа к информации и увеличить уровень защиты для клиентов банка. В данном решении с помощью техник машинного обучения анализируются несколько открытых наборов данных, включающие в себя данные с акселерометра, гироскопа и магнитометра смартфона. С помощью этих данных создается модель пользователя. Обученная модель с помощью метода случайного леса выделяет аномальные действия пользователя, сравнивая с созданной моделью [2]. На основе данных о нормальности действий пользователя изменяется его уровень доверия, при достижении критического значения пользователь классифицируется как нелегитимный и должен пройти повторную аутентификацию. В данном решении оценка действий пользователя производится на основе текущего уровня доверия с повышающими и понижающими коэффициентам в результате чего увеличивается скорость определения мошенника, что является отличным от других подобных решений.

Выводы. Проведен анализ имеющихся решений и разработан метод продолжительной аутентификации пользователя.

Список использованных источников:

1. Stylios I. et al. Behavioral biometrics & continuous user authentication on mobile devices: A survey //Information Fusion. – 2021. – Т. 66. – С. 76-99.
2. Pang X. et al. Mineauth: Mining behavioural habits for continuous authentication on a smartphone //Australasian Conference on Information Security and Privacy. – Springer, Cham, 2019. – С. 533-551.

Веневцев И.В. (автор) Подпись

Коржук В.М. (научный руководитель) Подпись