УДК 004.056

Афанасьева Наталья Сергеевна, старший преподаватель
Елизаров Дмитрий Александрович, доцент, к.т.н.
Разумов Илья Васильевич, аспирант
(ОмГУПС, г. Омск)
Natalia S. Afanaseva, senior lecturer
Dmitry A. Elizarov, associate professor, Ph.D. (Eng),
Ilya V. Razumov, graduate student
(OSTU, Omsk)

КРОСС-ДЕВАЙСНАЯ УСТОЙЧИВОСТЬ СИСТЕМ НЕПРЕРЫВНОЙ АУТЕНТИФИКАЦИИ ПО ДИНАМИКЕ ДВИЖЕНИЯ МЫШИ

DEVICE-INVARIANT CONTINUOUS AUTHENTICATION SYSTEMS USING MOUSE DYNAMICS

В статье исследуется актуальная проблема кросс-девайсной устойчивости систем непрерывной аутентификации пользователей на основе анализа динамики движений мыши. Эффективность традиционных биометрических моделей часто снижается, когда пользователь меняет устройство ввода из-за различий в аппаратных характеристиках сенсоров (DPI, частота опроса). В работе проведена экспериментальная оценка устойчивости алгоритмов верификации с использованием пяти различных моделей мышей (включая офисные и игровые устройства). Авторами проанализировано влияние смены манипулятора на метрики точности системы (FAR, FRR, EER).

The article investigates the pressing issue of cross-device robustness in continuous user authentication systems based on mouse movement dynamics. The effectiveness of traditional biometric models often declines when a user switches input devices due to differences in hardware sensor specifications (such as DPI and polling rate). The study presents an experimental evaluation of verification algorithm robustness using five different mouse models, including both office and gaming devices. The authors analyze the impact of changing the input device on system accuracy metrics (FAR, FRR, and EER).

Движение компьютерной мыши является одним из наиболее информативных источников поведенческих биометрических данных [1 – 4]. В процессе работы за компьютером пользователь постоянно взаимодействует с графическим интерфейсом операционной системы и программных приложений посредством перемещения курсора, выбора

объектов, выполнения кликов и других действий. Для описания траектории движения компьютерной определен расширенный набор признаков, представляющий совокупность кинетических, статистических и фрактально-энтропийных мер, позволяющий аппроксимировать поведенческий паттерн как многомерный хаотический процесс.

Эффективность традиционных биометрических моделей часто снижается, когда пользователь меняет устройство ввода из-за различий в аппаратных характеристиках сенсоров (DPI, частота опроса). В работе проведена экспериментальная оценка устойчивости алгоритмов верификации с использованием пяти различных моделей мышей (Acer OMR401, Acer OMW134, A4Tech Bloody L65 Max, Defender Classic MB-230 и Defender Whisper GM-209). Основные характеристики выбранных устройств представлены в таблице 1.

Таблица 1 – Характеристики компьютерных мышей

Идентификатор в датасете	Тип подключения	DPI (Режимы)	Частота опроса	Ускорение	Скорость (IPS)
acer_OMR401	Проводная / Радио (10м) / Bluetooth	600 / 800 / 1600 / 3200 / 6400 / 12000	1000 Гц	35 G	300 IPS (7.62 м/с)
acer_OMW134	Проводная USB (1.5 м)	800 / 1600 / 2400 / 3200	125 Гц	15 G	Не указана
bloody_L65	Проводная USB (1.8 м)	1000 / 1200 / 1600 / 2000 / 1200	125 / 250 / 500 / 1000 / 2000 Гц	35 G	250 IPS
def_MB-230	Проводная USB (1.5 м)	500 / 800 / 1000 / 1600	125 Гц	4 G	Не указана
whisper_GM-209	Проводная / Радио (10м) / Bluetooth	800 / 1200 / 1600 / 2400 / 4800 / 7200	125 / 250 / 500 / 1000 Гц	10 G	30 IPS

Для проверки устойчивости системы верификации к смене модели компьютерной мыши был собран набор данных, состоящий из 125 сессий (по 25 сессий на каждое из 5 тестируемых устройств). Для формирования характерных движений курсора пользователю необходимо последовательно наводить указатель на случайным образом расположенные цели (мишени) и выполнять по ним щелчок мышью.

Датасет включает в себя информацию о положении курсора и временных интервалах выполнения задач по поражению мишеней.

Собранные данные проходили стадию извлечения признаков. Для классификации был применен ансамблевый подход, состоящий из трех различных архитектур (Random Forest, Gradient Boosting и Convolutional Neural Network).

Для количественной оценки эффективности моделей использовались специальные показатели качества, позволяющие определить, насколько успешно алгоритм справляется с поставленной задачей, а также сравнить результаты различных моделей между собой. Метрика Accuracy показывает долю объектов, для которых модель определила класс правильно, относительно общего количества объектов тестовой выборки. Высокое значение метрики Accuracy свидетельствует о хорошей способности модели различать классы пользователей. Для более детального анализа также были определены показатели Precision, Recall и F1-мера. Показатель Precision характеризует долю правильно классифицированных объектов среди всех объектов, отнесенных моделью к определенному классу. Чем выше значение Precision, тем меньше количество ложных срабатываний. Показатель Recall отражает способность модели обнаруживать объекты конкретного класса среди всех реально существующих объектов данного класса. Высокое значение Recall указывает на низкое количество пропущенных объектов. F1-мера представляет собой гармоническое среднее между Precision и Recall и позволяет комплексно оценить качество классификации.

Для визуального анализа результатов для каждой модели была построена матрица ошибок. Она показывает количество правильно и неправильно классифицированных объектов тренировочной выборки для каждого класса и позволяет определить, между какими пользователями модель допускает наибольшее количество ошибок.

Матрица ошибок модели Random Forest (рисунок 1а) демонстрирует высокую точность классификации пяти профилей мышей. Модель определила 5 из 5 сессий для устройств acer_OMR401, bloody_L65, def_MB-230 и whisper_GM-209. Единственная ошибка алгоритма – ложная классификация одной сессии acer_OMW134 как def_MB-230 (остальные 4 сессии определены верно).

Согласно матрице ошибок модели Gradient Boosting (рисунок 1б), профили bloody_L65, def_MB-230 и whisper_GM-209 распознаны без ошибок – по пять корректных предсказаний для каждого. В матрице ошибок модели зафиксированы три ошибки классификации: одна сессия профиля acer_OMR401 была ошибочно отнесена к классу acer_OMW134, а две сессии acer_OMW134 – к классу def_MB-230.

Матрица ошибок модели Convolutional Neural Network (рисунок 1в) демонстрирует невысокую точность. Предсказания заметно «разбросаны»

между разными классами, что говорит о слабой способности четко разделять профили.

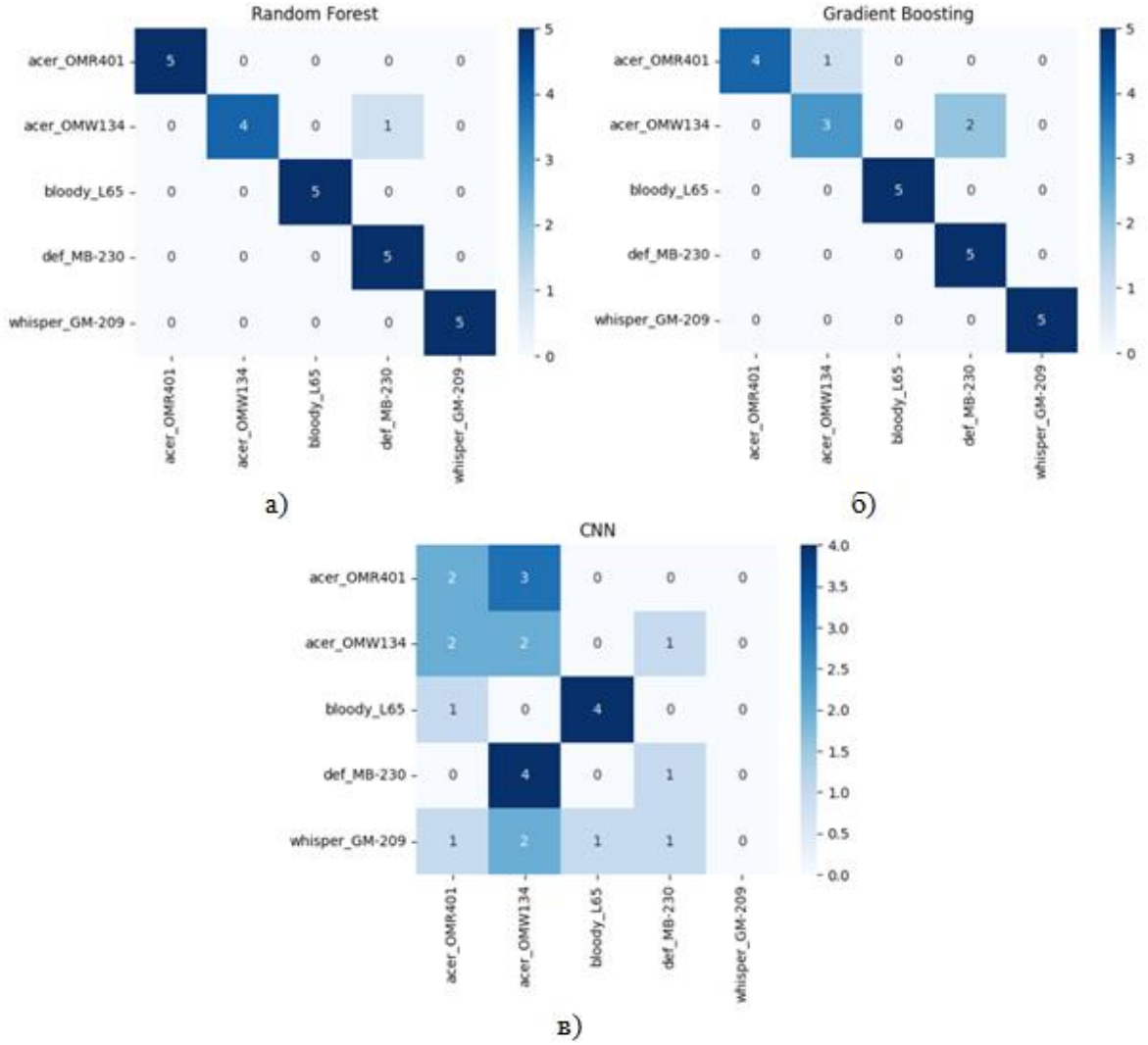

Рисунок 1 – Матрица ошибок а) модель Random Forest; б) модель Gradient Boosting;
в) модель Convolutional Neural Network

На следующем этапе тестирования система идентифицирует случайный профиль мыши, сопоставляя его с уже обученными образцами устройств. Сервис, реализованный на базе библиотеки Gradio, на входе принимает JSON-файл с сырыми данными о движении мыши, а на выходе предоставляет информацию о принадлежности устройства к конкретному классу. Результаты проверки для мыши acer_OMW134 показаны на рисунке 2, для мыши acer_OMR401 – на рисунке 3. Как видно из рисунков 2-3 профили мыши успешно прошли идентификацию.

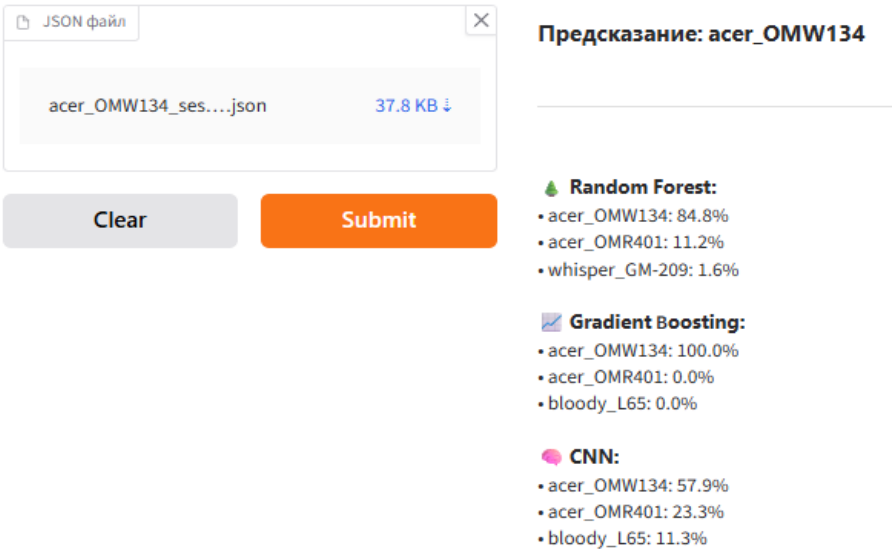

Рисунок 2 – Проверка мыши acer_OMW134

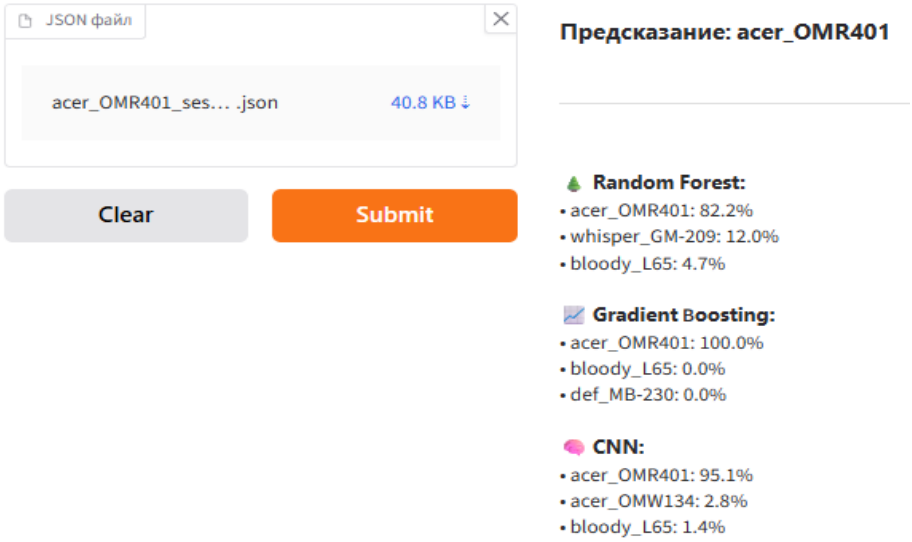

Рисунок 3 – Проверка мыши acer_OMR401

На заключительном этапе тестирования был интегрирован модуль «живой» верификации (Live-проверка). Пользователю предлагается пройти короткий тест с мишенями, после чего система анализирует его движения в реальном времени. Если итоговая уверенность ансамбля превышает заданный порог, устройство считается подтвержденным. Результат проверки мыши whisper_GM-209 представлен на рисунке 4. Модели Random Forest и Gradient Boosting показали хорошие результаты.

При анализе метрик тестовой выборки выявляется существенное превосходство ансамблевых древовидных алгоритмов над нейросетевым подходом в задаче классификации аппаратных профилей. Модель Random Forest продемонстрировала наивысшую стабильность классификации (таблица 2). Устройства bloody_L65 и whisper_GM-209 определяются со стопроцентной точностью (Precision 100%, Recall 100%). Наибольшую

сложность для алгоритма составило распознавание acer_OMW134 (Recall 80%), однако итоговое значение метрики F1-score для всех классов не опускается ниже 88.89%.

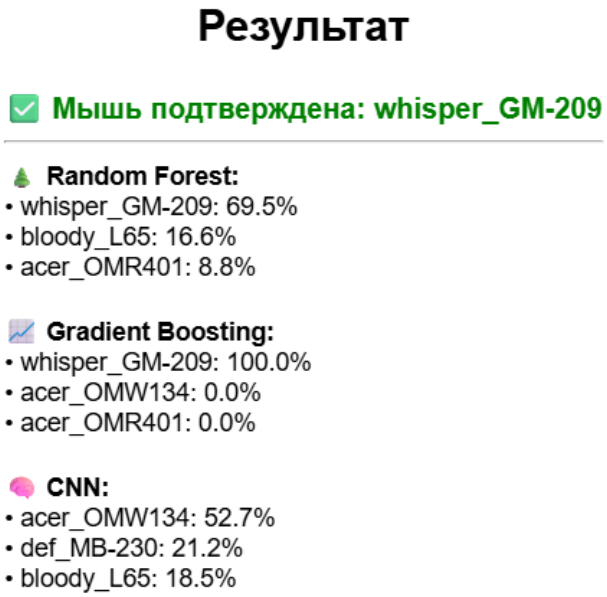

Рисунок 4 – Проверка Live-модуля на устройстве whisper_GM-209

Таблица 2 – Результаты модели Random Forest

Модель мыши	Precision (%)	Recall (%)	F1-score (%)
acer_OMR401	100.00	100.00	88.89
acer_OMW134	100.00	80.00	88.89
bloody_L65	100.00	100.00	100.00
def_MB-230	83.33	100.00	90.91
whisper_GM-209	100.00	100.00	100.00

Модель Gradient Boosting показала сопоставимые, но незначительно сниженные результаты (таблица 3). Профили bloody_L65 и whisper_GM-209 в ходе тестирования были классифицированы без ошибок. При этом для профиля acer_OMW134 зафиксировано снижение метрики Recall до 60 %, из-за чего итоговая метрика F1-score снизилась до 75 %.

Таблица 3 – Результаты модели Gradient Boosting

Модель мыши	Precision (%)	Recall (%)	F1-score (%)
acer_OMR401	83.33	100.00	90.91
acer_OMW134	100.00	60.00	75.00
bloody_L65	100.00	100.00	100.00
def_MB-230	83.33	100.00	90.91
whisper_GM-209	100.00	100.00	100.00

Согласно данным из таблицы 4, модель Convolutional Neural Network не справилась с задачей распознавания. Относительно успешная классификация зафиксирована только для профиля def_MB-230. Это свидетельствует о значительном числе как ложноположительных, так и ложноотрицательных срабатываний модели.

Таблица 4 – Результаты модели Convolutional Neural Network

Модель мыши	Precision (%)	Recall (%)	F1-score (%)
acer_OMR401	23.08	60.00	33.33
acer_OMW134	50.00	40.00	44.44
bloody_L65	40.00	40.00	40.00
def_MB-230	100.00	60.00	75.00
whisper_GM-209	0.00	0.00	0.00

В рамках проведенной работы проведена экспериментальная оценка устойчивости алгоритмов верификации при смене модели компьютерной мыши. Результаты испытаний подтвердили высокую эффективность предложенного подхода: несмотря на низкую точность и рассеивание предсказаний у модели Convolutional Neural Network, алгоритмы Random Forest и Gradient Boosting успешно компенсировали ее ошибки в итоговом голосовании. Ансамбль доказал свою жизнеспособность при проверках в режиме реального времени, позволяя надежно идентифицировать конкретное физическое устройство и выступать в качестве дополнительного фактора защиты в системах непрерывной аутентификации.

Список литературы

1. Yampolskiy R. Behavioural biometrics: a survey and classification // International Journal of Biometrics. – 2008. – С. 81–113.

2. Oduri S. Continuous authentication and behavioral biometrics: Enhancing cybersecurity in the digital era //International Journal of Innovative Research in Science Engineering and Technology. – 2024. – Т. 13. – № 7. – С. 13632-13640.

3. Динамическая аутентификация пользователей на основе анализа работы с компьютерной мышью / А. В. Березникер, М. А. Казачук, И. В. Машечкин [и др.] // Вестник Московского университета. Серия 15: Вычислительная математика и кибернетика. – 2021. – № 4. – С. 3-16.

4. Khan S. et al. Mouse dynamics behavioral biometrics: A survey //arXiv preprint arXiv:2208.09061. – 2022.