

DOI: 10.55648/1998-6920-2026-3-20-3-15

Верификация личности оператора по динамике одиночных нажатий мыши в системе аттестации специалистов неразрушающего контроля

А. А. Попков, В. С. Выплавень, А. Ю. Коровченко

Сибирский государственный университет путей сообщения (СГУПС)

Аннотация. Процедура аттестации специалистов неразрушающего контроля влечёт правовые последствия, поэтому подлинность результата тестирования следует относить к задачам защиты информации. Парольная защита подтверждает подлинность субъекта только в момент входа и не контролирует, кто фактически отвечает на вопросы в течение сеанса. Устранить этот разрыв позволяет поведенческая биометрия, скрытая по способу сбора признаков. В работе оценивается надёжность подтверждения личности аттестуемого по динамике одиночных нажатий мыши и выявляются признаки с наибольшей различающей способностью. Источником данных послужил журнал действующей системы аттестации, накопленный с 2020 года и содержащий свыше 3,4 млн событий нажатия от 250 пользователей. Для каждого нажатия зафиксированы длительность удержания кнопки и относительные координаты точки нажатия. Предложен набор из шестнадцати сессионных признаков и схема верификации с открытым множеством, использующая в качестве базовой модели случайный лес. Интервальные оценки качества получены бутстрепом (методом размножения выборок) по пользователям. На тестовой выборке достигнута равная ошибка (EER) 18,3 % при оценке по одной сессии (95 %-й доверительный интервал [16,2; 19,5] %) и площадь под характеристической кривой 0,899. Объединение решений по нескольким сессиям снижает ошибку до долей процента (0,47 % при двенадцати сессиях), что ввиду статистической зависимости сессий одного пользователя следует понимать как оптимистическую границу. Наибольший вклад в различающую способность вносят пространственные признаки точки нажатия, дополняемые длительностью удержания кнопки. Показана применимость динамики нажатий как дополнительного, скрытно собираемого фактора подтверждения подлинности субъекта в системах тестирования без дополнительного оборудования.

Ключевые слова: поведенческая биометрия, динамика нажатий мыши, скрытая аутентификация, верификация личности, защита информации, аттестация персонала, неразрушающий контроль.

Для цитирования: Попков А. А., Выплавень В. С., Коровченко А. Ю. Верификация личности оператора по динамике одиночных нажатий мыши в системе аттестации специалистов неразрушающего контроля // Вестник СибГУТИ. 2026. Т. 20, № 3. С. 3–15 <https://doi.org/10.55648/1998-6920-2026-3-20-3-15>.



Контент доступен под лицензией

Creative Commons Attribution 4.0 License

© А. А. Попков, В. С. Выплавень, А. Ю. Коровченко, 2026

Статья поступила в редакцию 08.07.2026;
переработанный вариант – 22.08.2026;
принята к публикации 24.08.2026.

1. Введение

Аттестация специалистов неразрушающего контроля (НК) влечёт прямые правовые последствия. По её результатам выдаётся квалификационный сертификат на право контроля ответственных объектов. Поэтому подлинность результата тестирования относится к задачам защиты информации, а не к вопросам удобства процедуры. Если тест за аттестуемого проходит более подготовленное лицо, к работе допускается формально аттестованный, но фактически некомпетентный специалист, что создаёт прямую угрозу безопасности контролируемых объектов. Классическая защита входа по логину и паролю подтверждает подлинность субъекта однократно, в начале сеанса, и не показывает, кто фактически отвечал на вопросы на протяжении последующих полутора часов.

Устранить этот разрыв позволяет поведенческая биометрия, то есть анализ индивидуальной манеры работы с устройствами ввода. В отличие от паролей и токенов, поведенческие признаки существенно труднее воспроизвести или передать другому лицу вместе с учётной записью. Их регистрация не требует дополнительного оборудования и не вмешивается в ход тестирования [1]. Скрытность относится к способу сбора признаков. Незаметным остаётся механизм регистрации, тогда как сам факт контроля правомерно закрепляется в регламенте системы и доводится до пользователя. Среди поведенческих модальностей динамика мыши наиболее уместна там, где основное действие пользователя представляет собой выбор ответа нажатием. На нажатия приходится почти весь поток событий интерфейса тестирования [1; 2].

Целью работы является оценка надёжности подтверждения подлинности субъекта по динамике одиночных нажатий мыши и определение признаков журнала, обладающих наибольшей различающей способностью. В отличие от большинства известных работ, результат получен не на лабораторной выборке, а на массиве реальных эксплуатационных данных действующего аттестационного центра, что определяет практическую значимость установленных границ применимости метода.

Для достижения поставленной цели решается несколько задач. Первая задача состоит в формализации подтверждения подлинности оператора как задачи верификации с открытым множеством. Вторая задача заключается в формировании признакового пространства одиночных нажатий на основе длительности удержания кнопки и относительных координат точки нажатия. Третья задача предполагает экспериментальную оценку качества верификации по одной сессии и анализ информативности отдельных признаков. Четвёртая задача связана с оценкой эффекта объединения решений по нескольким сессиям и определением границ практической применимости метода.

2. Обзор литературы

Поведенческая аутентификация по динамике мыши развивается с середины 2000-х годов. В работе [2] впервые показано, что пользователей можно различать по характеристикам перемещения курсора и нажатий, и предложен набор признаков на основе скоростей и углов движения. В [1] выполнен переход к верификации на фиксированном задании, а статистические признаки дополнены процедурными, описывающими ход отдельного действия мышью, что заметно повысило точность. В [3] систематизирована статическая аутентификация по мыши и отмечено её ключевое ограничение, а именно малый объём данных в момент входа, что определяет интерес к анализу поведения в ходе сеанса.

Различают два режима применения модальности. Идентификация состоит в поиске «один из многих», а верификация означает подтверждение заявленной личности сравнением «один к одному» [4]. Ранние системы верификации по перемещениям курсора [5] и последующие работы по классификации сессий [6; 7] показали устойчивую индивидуальность манеры работы с мышью, однако достигаемая по короткому наблюдению равная ошибка остаётся, как правило, на уровне от единиц до десятков процентов и существенно зависит от объёма наблюдаемого материала. Современное состояние области систематизировано в обзоре [4], где сопоставлены модальности, признаковые пространства, классификаторы, общедоступные наборы данных и метрики качества и отмечена общая тенденция перехода от ручного конструирования признаков к моделям машинного и глубокого обучения [8].

Отдельную линию образуют работы, анализирующие не непрерывную траекторию, а поток дискретных событий-нажатий. В [9] профиль пользователя строится по сегментам действий мыши методом случайного леса, что близко к представлению данных настоящей работы. Для сравнения методов широко используются открытые наборы Balabit [10] и наборы, рассмотренные в [11], содержащие данные порядка десяти пользователей. Устойчивость поведенческих систем к целенаправленной имитации чужого почерка изучается отдельно и в общем случае снижает наблюдаемое качество [8; 12]. В настоящей работе рассматривается неимитирующий нарушитель.

Большинство опубликованных результатов получено в лабораторных условиях, на десятках испытуемых и специально организованных заданиях. Промышленных журналов, накопленных штатной системой за годы эксплуатации и привязанных к содержательно значимой процедуре сертификации, в открытом доступе практически нет. Настоящая работа восполняет этот пробел, опираясь на массив данных действующего аттестационного центра [13] и намеренно обеднённый набор признаков, включающий только одиночные нажатия, что позволяет оценить нижнюю границу информативности акта прицельного нажатия.

3. Постановка задачи и модель угроз

Объектом исследования является программное обеспечение учебного и экзаменационного тестирования аттестационного центра, развёрнутого на базе Сибирского государственного университета путей сообщения (г. Новосибирск) [13; 14]. Сеанс тестирования включает 40 вопросов с одиночным или множественным выбором ответа. Продолжительность сеанса не превышает 90 минут. Каждое содержательное действие пользователя представляет собой нажатие левой кнопки мыши на элементе интерфейса. Встроенный модуль регистрации сохраняет для каждого нажатия длительность удержания и координаты, что и образует исходный поток данных.

Задача ставится как верификация подлинности субъекта, то есть сравнение «один к одному», и отделяется от идентификации (поиска «один из многих») и от аутентификации в широком смысле как подтверждения личности по совокупности факторов. В рассматриваемой постановке динамика нажатий выступает дополнительным фактором. Система проверяет гипотезу о том, что сеанс выполняет заявленный субъект доступа, и не устанавливает его личность среди прочих. Для каждой проверяемой сессии вычисляется оценка соответствия заявленной личности, после чего решение принимается сравнением оценки с порогом θ . Качество проверки описывается вероятностями ложного пропуска чужого

(FAR) и ложного отказа своему (FRR). Сводными характеристиками служат рабочая характеристика (ROC) и равная ошибка (EER), при которой FAR и FRR совпадают в общей рабочей точке θ^* [15].

$$EER = FAR(\theta^*) = FRR(\theta^*) \quad (1)$$

Защищаемым активом выступает достоверность результата аттестации, то есть соответствие между лицом, фактически выполнившим тестирование, и субъектом, на чьё имя оформляется сертификат. Нарушителем выступает более подготовленное лицо, проходящее тест вместо аттестуемого по его учётным данным. Предполагается, что нарушитель располагает действительными реквизитами доступа (логином и паролем) и имеет физический доступ к рабочему месту, однако не контролирует встроенный модуль регистрации нажатий и не получает обратной связи о работе средств контроля подлинности. Парольная защита в этих условиях преодолевается штатно, поэтому подтверждение подлинности возлагается на поведенческий фактор.

Самостоятельным фактором идентификации может выступать цифровой отпечаток компьютерного устройства, формируемый по параметрам его аппаратной и программной конфигурации [16]. Однако в рассматриваемой модели угроз подменяющее лицо использует то же рабочее место, поэтому такой отпечаток идентифицирует устройство, но не позволяет выявить замену оператора, что обосновывает применение поведенческих признаков.

Принимается допущение о неимитирующем нарушителе. Подменяющее лицо работает с мышью в естественной для себя манере и не предпринимает целенаправленных попыток воспроизвести моторику заявленного субъекта. Устойчивость метода к осознанному подражанию составляет отдельную задачу [12] и выходит за рамки настоящей работы. При этих допущениях задача сводится к верификации подлинности субъекта по совокупности сессий.

4. Экспериментальные данные и признаковое пространство

Источником данных послужил журнал действующей системы аттестации, накопленный с мая 2020 года. Исходная таблица нажатий содержит 3 466 600 записей, относящихся к 250 уникальным пользователям. Каждая запись включает идентификатор пользователя, идентификатор вопроса, длительность удержания кнопки (мс), относительные координаты точки нажатия и метку времени с точностью до миллисекунды. Координаты отсчитываются от левого верхнего угла нажимаемого элемента, поэтому сопоставимы между сеансами независимо от положения элемента на экране.

Перед анализом данные очищались. Удалялись записи с нулевой и аномально большой (свыше 2000 мс) длительностью удержания. Такие записи соответствуют ситуациям, когда кнопка оставалась нажатой при отвлечении пользователя, и не отражают двигательного акта. Удалялись также нажатия с отрицательными координатами, регистрируемые при срабатывании вне границ элемента. После очистки сохранено 3 353 528 записей, что составляет 96,7 % исходного объёма. Доля отброшенных артефактов невелика и не вносит заметного смещения в оценки.

Поток нажатий каждого пользователя разбивался на сессии. Новая сессия открывалась, если интервал между соседними нажатиями превышал 90 минут, что соответствует

регламентной длительности прохождения теста. После разбиения и отбрасывания сессий короче десяти нажатий в анализ вошло 19 225 сессий. Распределение по пользователям неравномерно и охватывает от полутора десятков до нескольких сотен сессий на человека, что типично для эксплуатационных данных. В эксперимент включались пользователи, имеющие не менее шестнадцати сессий. Этого достаточно для разделения истории на обучающую и контрольную части.

Признаки вычислялись в пределах сессии и описывали поведение по трём группам наблюдаемых величин (табл. 1). Первую группу образуют статистики длительности удержания кнопки. Они характеризуют типичную скорость нажатия и её устойчивость. Вторую группу составляют характеристики координат точки нажатия, отражающие индивидуальную манеру наведения курсора на элемент. Третью группу образует межкликковый ритм, то есть статистики интервалов между нажатиями при отбрасывании пауз свыше пяти минут, относимых к обдумыванию. Состав признаков согласуется с практикой выделения статистических признаков в задачах динамики мыши [1; 9]. Итоговый вектор сессии включает шестнадцать признаков.

Таблица 1: Группы признаков динамики одиночных нажатий

Группа признаков	Состав признаков	Число
Длительность удержания кнопки	среднее, среднеквадратическое отклонение, медиана, 10-й и 90-й процентиля, межквартильный размах, коэффициент вариации	7
Координаты точки нажатия	средние и среднеквадратические отклонения по обеим осям, обобщённый разброс относительно среднего положения, коэффициент корреляции координат	6
Межкликковый ритм	медиана, среднеквадратическое отклонение и межквартильный размах интервалов между нажатиями	3

Перед обучением признаки стандартизировались по статистикам обучающей части, что исключает доминирование величин с большим масштабом. Параметры стандартизации применялись к контрольной части без пересчёта, что предотвращает утечку информации.

$$\tilde{x} = \frac{x - \mu_{train}}{\sigma_{train}} \quad (2)$$

В этой записи x обозначает исходное значение признака, $\tilde{x}$ обозначает стандартизованное значение, а величины μ_{train} и σ_{train} задают среднее и среднеквадратическое отклонение признака по обучающей части.

5. Методика верификации

Множество пользователей делилось на две части в соответствии с моделью открытого множества. Пятьдесят человек полностью исключались из обучения и выступали в роли посторонних. Их сессии не предъявлялись модели на этапе настройки и использовались только для имитации попытки постороннего выдать себя за зарегистрированного субъекта. Оставшиеся двести человек считались зарегистрированными. Их сессии упорядочивались по времени, более ранние 60 % направлялись на обучение, а поздние 40 %

оставлялись для контроля. Временное разбиение исключает одновременное попадание соседних во времени сессий одного человека в обучение и контроль и позволяет оценить устойчивость метода к естественному дрейфу почерка.

В качестве базовой модели использован случайный лес из 300 деревьев, то есть алгоритм, широко применяемый в задачах динамики мыши за устойчивость и интерпретируемость [9; 17]. Для контрольной сессии модель формирует распределение апостериорных вероятностей по зарегистрированным субъектам. Вероятность заявленного субъекта a принимается за оценку соответствия s .

$$s(z, a) = \hat{P}(a|z) \quad (3)$$

Здесь z обозначает вектор признаков контрольной сессии, a обозначает заявленного субъекта, а $\hat{P}(a|z)$ задаёт оценку апостериорной вероятности принадлежности сессии этому субъекту. Решение «свой» принимается, если оценка соответствия не меньше порога, то есть $s(z, a) \geq \theta$.

Подлинные попытки формировались предъявлением контрольной сессии под её истинным идентификатором. Попытки постороннего строились двумя способами. В закрытом сценарии контрольная сессия зарегистрированного пользователя предъявлялась под чужим, также зарегистрированным, идентификатором. В открытом сценарии сессия исключённого из обучения постороннего предъявлялась под идентификатором случайно выбранного зарегистрированного пользователя. Открытый сценарий ближе к реальной угрозе, при которой подменяющий субъект вообще отсутствует в системе. Интервальные оценки качества получены бутстрепом (методом размножения выборок) по пользователям, а не по сессиям, поскольку сессии одного человека статистически зависимы [18].

6. Результаты и обсуждение

В обучении участвовало 9351 сессия двухсот зарегистрированных пользователей, а в контроле участвовало 6367 сессий. В режиме закрытой идентификации, когда сессия относилась к одному из 200 пользователей, доля правильных решений первого ранга составила 33,7 %, а попадание истинного пользователя в первую пятёрку составило 57,5 %. Эти значения многократно превышают случайный уровень (0,5 %) и показывают, что поток нажатий несёт устойчивую индивидуальную составляющую. Вместе с тем одной сессии недостаточно для однозначной идентификации среди сотен пользователей, что согласуется с выбором верификации в качестве основной постановки.

Эксплуатационные данные получены при выполнении описанных в разделе 3 учебных и экзаменационных тестов. Использование координат относительно нажимаемого элемента исключает прямое влияние его абсолютного положения на экране, поэтому изменение размера окна и порядка следования вопросов или вариантов ответа само по себе не изменяет начало системы координат. Вместе с тем координаты не нормировались на текущие размеры элемента. Масштабирование интерфейса, изменение ширины области ответа и перенос текста могут влиять на распределение пространственных признаков. Полученные оценки относятся к использованным эксплуатационным конфигурациям. Для применения метода при других масштабах и компоновках интерфейса требуется нормирование координат и дополнительная проверка устойчивости модели.

Для задачи верификации распределения оценок подлинных попыток и попыток посторо-

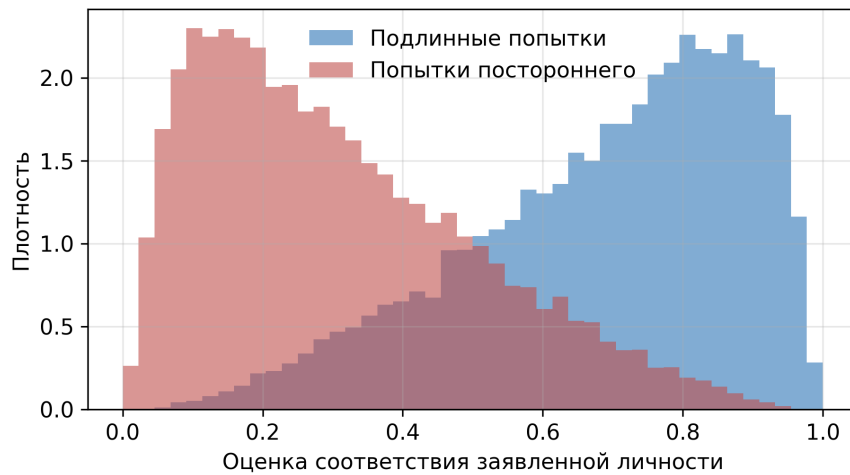


Рис. 1: Распределения оценки соответствия для подлинных попыток и попыток постороннего (открытое множество)

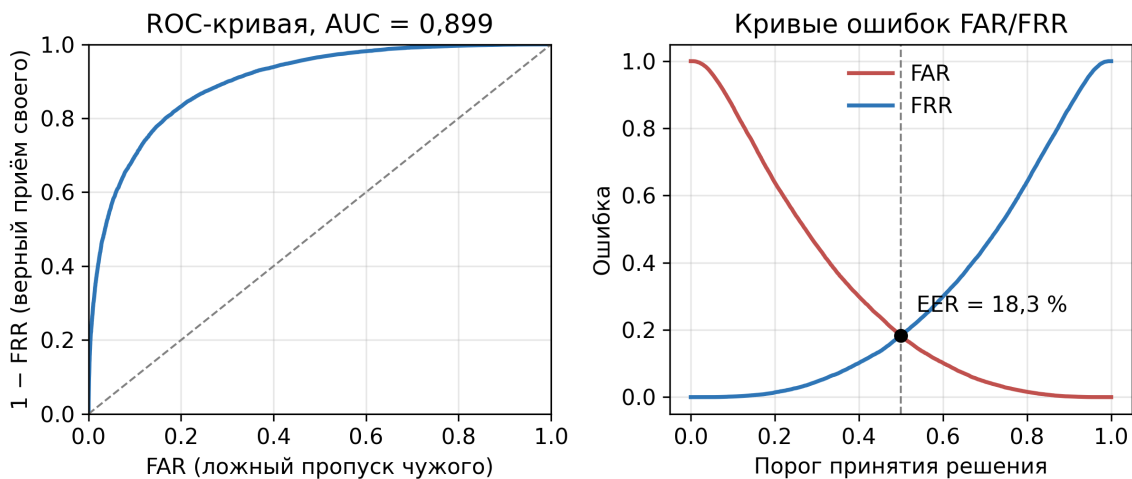


Рис. 2: Рабочая характеристика (слева) и кривые ошибок FAR/FRR с точкой равной ошибки $EER = 18,3 \%$ (справа)

ронного приведены на рис. 1. Эти распределения заметно смещены, но перекрываются, чем и определяется уровень ошибки. Соответствующая рабочая характеристика (рис. 2) имеет площадь под ROC-кривой 0,899. Равная ошибка составила 18,3 % в открытом сценарии и 17,7 % в закрытом. Близость значений показывает, что посторонний из числа незнакомых системе людей распознаётся не хуже, чем зарегистрированный пользователь под чужим именем. Бутстреп по пользователям (1000 повторных выборок) дал для AUC 95 %-й доверительный интервал [0,877; 0,902], а для равной ошибки в открытом сценарии интервал [16,2; 19,5] %. Ширина интервалов отражает разброс индивидуальных профилей и должна учитываться при сопоставлении с опубликованными результатами.

Анализ важности признаков (рис. 3) выявил ведущую роль пространственных характеристик точки нажатия, прежде всего среднего положения по обеим осям и разброса по вертикали. За ними следуют признаки длительности удержания, а именно нижний процентиль и медиана. Результат согласуется с физическим смыслом. Индивидуальная манера наведения курсора на элемент устойчивее во времени, чем темп нажатий, зави-

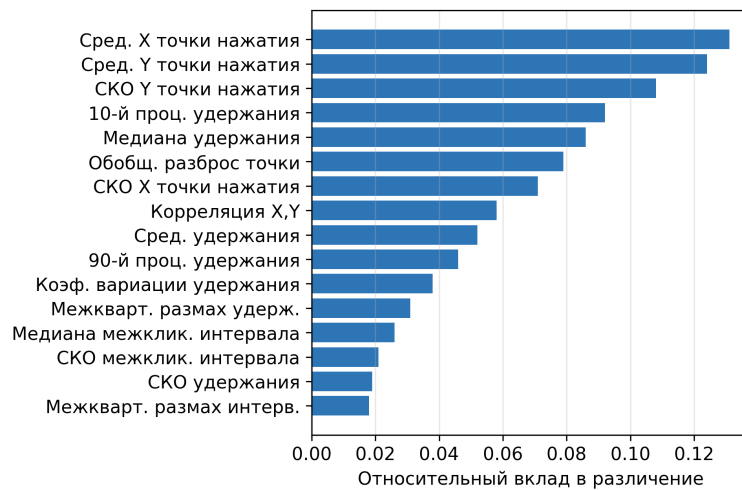


Рис. 3: Вклад признаков в различение пользователей (классификатор «случайный лес»)

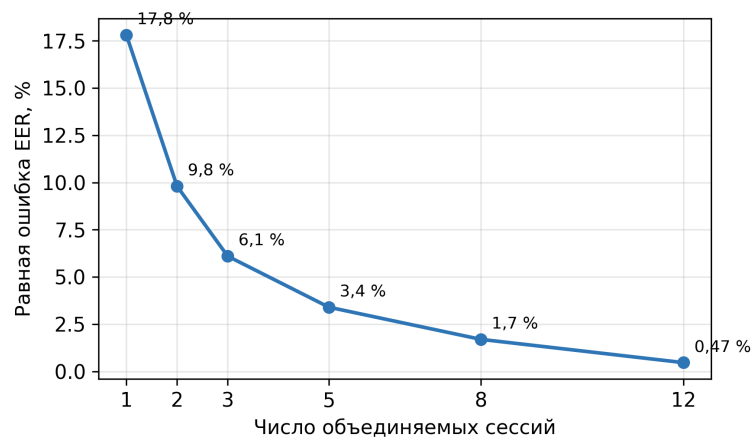


Рис. 4: Снижение равной ошибки при объединении решений по нескольким сессиям

сящий от сложности конкретного вопроса. Наименее информативным оказался межклик-овый ритм, что объясняется его зависимостью от времени обдумывания, не связанного с моторикой субъекта. Координаты точки касания относительно элемента образуют подпись зрительно-моторной координации пользователя, слабо поддающуюся сознательному контролю и потому ценную как биометрический признак [2; 6]. Длительность удержания дополняет её временной составляющей.

Уровень ошибки 18,3 % по одной сессии отражает умеренную, но отличную от нуля различающую способность ограниченного набора признаков. В условиях эксплуатации система аттестации наблюдает пользователя многократно, что позволяет объединять решения по нескольким сессиям простым усреднением оценок соответствия.

$$\bar{s}(a) = \frac{1}{k} \sum_{j=1}^k s(z_j, a) \quad (4)$$

Здесь k обозначает число объединяемых сессий, z_j обозначает вектор признаков j -й сессии, а $\bar{s}(a)$ задаёт усреднённую оценку соответствия заявленному субъекту.

Зависимость равной ошибки от числа объединяемых сессий приведена на рис. 4. С ро-

стом числа сессий равная ошибка быстро уменьшается. Для двух сессий равная ошибка составляет 9,8 %, для трёх сессий составляет 6,1 %, для пяти сессий составляет 3,4 %, для восьми сессий составляет 1,7 %, для двенадцати сессий составляет 0,47 %. Доверительные интервалы, полученные тем же бутстрепом по пользователям, с ростом k быстро расширяются из-за уменьшения числа независимых наблюдений. Для $k = 2$ интервал составляет [8,1; 11,6] %, для $k = 5$ интервал составляет [2,0; 5,1] %, для $k = 12$ интервал составляет [0,0; 1,9] %. Формула усреднения предполагает условную независимость ошибок по сессиям одного пользователя. На эксплуатационных данных это допущение нарушается. Сессии выполняются на одном рабочем месте, с устойчивым оборудованием и в близких условиях, поэтому их ошибки коррелированы. Значения равной ошибки при больших k следует поэтому трактовать как оптимистическую (нижнюю) границу достижимого качества, а не как точечный прогноз. Реальный выигрыш от объединения скромнее, хотя и остаётся существенным.

Полученные значения сопоставимы с опубликованными для динамики мыши, где равная ошибка по короткому наблюдению обычно лежит в диапазоне от единиц до двух-трёх десятков процентов и существенно зависит от объёма наблюдаемого материала [1; 7; 9]. Прямое сравнение абсолютных значений затруднено различием протоколов и данных. В большинстве работ используются открытые наборы примерно из десяти пользователей и богатые признаки траекторий движения, тогда как здесь рассматриваются 250 пользователей промышленного журнала и обеднённый набор признаков, включающий длительность и координаты одиночных нажатий без характеристик перемещения курсора. Уверенное различие даже на таком наборе указывает на высокую информативность самого акта прицельного нажатия.

Результаты следует трактовать с учётом ряда ограничений. Во-первых, метки в журнале соответствуют заявленному, а не достоверно подтверждённому пользователю. Независимой проверки присутствия система не проводит, поэтому обучающие данные в принципе могут содержать ранее не выявленные подмены. Такой эффект снижает, а не завышает наблюдаемую различающую способность. Во-вторых, оценки объединения по нескольким сессиям получены в предположении независимости ошибок, которое на эксплуатационных данных не выполняется, поэтому соответствующие значения являются оптимистической границей. В-третьих, рассмотрен неимитирующий нарушитель. Устойчивость метода к целенаправленному подражанию моторике заявленного субъекта составляет отдельную задачу. В-четвёртых, в журнале не фиксируются параметры оборудования (тип манипулятора, разрешение экрана), влияющие на динамику, и их учёт способен повысить устойчивость метода. Наконец, модель и набор признаков намеренно выбраны простыми ради воспроизводимой опорной оценки. Применение последовательностных моделей и признаков траекторий [8] может улучшить результат.

Заключение

На массиве реальных эксплуатационных данных действующей системы аттестации специалистов неразрушающего контроля установлено, что подлинность субъекта тестирования может быть верифицирована по динамике одиночных нажатий мыши. По одной сессии достигнута равная ошибка 18,3 % (95 %-й доверительный интервал [16,2; 19,5] %) при площади под характеристической кривой 0,899. Объединение решений по нескольким сессиям снижает ошибку до долей процента, причём ввиду статистической зависимости

сессий одного пользователя эти значения следует понимать как оптимистическую границу. Наибольшую различающую способность несут пространственные признаки точки нажатия, дополняемые длительностью удержания кнопки. Полученные оценки обосновывают применение динамики нажатий как дополнительного, скрытого по способу сбора фактора подтверждения подлинности субъекта в системах сертификации без дополнительного оборудования и определяют границы его практической применимости. Перспективным направлением дальнейших исследований является переход от посессионной верификации к контролю подлинности в пределах сеанса.

Литература

1. User authentication through mouse dynamics / C. Shen [et al.] // IEEE Transactions on Information Forensics and Security. Vol. 8. — 2013. — P. 16–30. — DOI: 10.1109/TIFS.2012.2223677.
2. *Ahmed A. A. E., Traore I.* A new biometric technology based on mouse dynamics // IEEE Transactions on Dependable and Secure Computing. Vol. 4. — 2007. — P. 165–179. — DOI: 10.1109/TDSC.2007.70207.
3. *Jorgensen Z., Yu T.* On mouse dynamics as a behavioral biometric for authentication // Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS). — 2011. — P. 476–482. — DOI: 10.1145/1966913.1966983.
4. Mouse dynamics behavioral biometrics: a survey / S. Khan [et al.] // ACM Computing Surveys. — 2024. — Vol. 56, no. 6. — P. 1–33. — DOI: 10.1145/3640311.
5. *Zheng N., Paloski A., Wang H.* An efficient user verification system via mouse movements // Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS). — 2011. — P. 139–150. — DOI: 10.1145/2046707.2046725.
6. User identity verification via mouse dynamics / C. Feher [et al.] // Information Sciences. — 2012. — Vol. 201. — P. 19–36. — DOI: 10.1016/j.ins.2012.02.066.
7. Performance evaluation of anomaly-detection algorithms for mouse dynamics / C. Shen [et al.] // Computers & Security. — 2014. — Vol. 45. — P. 156–171. — DOI: 10.1016/j.cose.2014.05.002.
8. *Chong P., Elovici Y., Binder A.* User authentication based on mouse dynamics using deep neural networks: a comprehensive study // IEEE Transactions on Information Forensics and Security. Vol. 15. — 2020. — P. 1086–1101. — DOI: 10.1109/TIFS.2019.2930429.
9. *Almalki S., Assery N., Roy K.* An empirical evaluation of online continuous authentication and anomaly detection using mouse clickstream data analysis // Applied Sciences. — 2021. — Vol. 11, no. 13. — P. 6083. — DOI: 10.3390/app11136083.
10. Balabit Mouse Dynamics Challenge data set / Á. Fülöp [et al.]. — 2016. — URL: <https://github.com> (visited on 07/02/2026).
11. *Antal M., Dénes-Fazakas L.* User verification based on mouse dynamics: a comparison of public data sets // Proceedings of the IEEE 15th International Symposium on Applied Computational Intelligence and Informatics (SACI). — 2021. — P. 000155–000160. — DOI: 10.1109/SACI51354.2021.9465583.

12. *Antal M., Egyed-Zsigmond E.* Intrusion detection using mouse dynamics // IET Biometrics. — 2019. — Vol. 8, no. 5. — P. 285–294. — DOI: 10.1049/iet-bmt.2018.5126.
13. *Попков А. А., Школина Д. С.* Мониторинг и оценка результатов технической подготовки специалистов по неразрушающему контролю объектов железнодорожного транспорта // International Scientific Siberian Transport Forum TransSiberia 2021. Lecture Notes in Networks and Systems. Т. 403. — 2022. — С. 189–196. — DOI: 10.1007/978-3-030-96380-4_21.
14. *Выплавень В. С., Коломеец А. О., Попков А. А.* Обработка сигналов тензометрического контроля фильтром Калмана // Journal of Physics: Conference Series. — 2021. — Т. 2131, № 3. — С. 032015. — DOI: 10.1088/1742-6596/2131/3/032015.
15. *Fawcett T.* An introduction to ROC analysis // Pattern Recognition Letters. — 2006. — Vol. 27, no. 8. — P. 861–874. — DOI: 10.1016/j.patrec.2005.10.010.
16. *Вехов В. Б., Смушкин А. Б.* Криминалистическое исследование цифровых отпечатков компьютерных устройств // Всероссийский криминологический журнал. — 2024. — Т. 18, № 4. — С. 390–397. — DOI: 10.17150/2500-4255.2024.18(4).390-397.
17. *Breiman L.* Random forests // Machine Learning. — 2001. — Vol. 45, no. 1. — P. 5–32. — DOI: 10.1023/A:1010933404324.
18. *Efron B.* Bootstrap methods: another look at the jackknife // The Annals of Statistics. — 1979. — Vol. 7, no. 1. — P. 1–26. — DOI: 10.1214/aos/1176344552.

Попков Артём Антонович

кандидат технических наук, доцент кафедры «Информационные технологии транспорта», Сибирский государственный университет путей сообщения (СГУПС, 630049, г. Новосибирск, ул. Дуси Ковальчук, д. 191), тел. +7-999-468-5626, email: zabagy@gmail.com, ORCID: 0000-0002-8328-2415.

Выплавень Владимир Сергеевич

кандидат технических наук, доцент кафедры «Информационные технологии транспорта», Сибирский государственный университет путей сообщения (СГУПС, 630049, г. Новосибирск, ул. Дуси Ковальчук, д. 191), тел. +7-923-231-97-79, email: vladimir97927@gmail.com, ORCID: 0000-0002-9083-5882.

Коровченко Алексей Юрьевич

инженер-программист НИЛ «ФМК», Сибирский государственный университет путей сообщения (СГУПС, 630049, г. Новосибирск, ул. Дуси Ковальчук, д. 191), тел. +7-913-765-05-00, email: lecha3525@gmail.com, ORCID: 0009-0002-6388-2285.

Авторы прочитали и одобрили окончательный вариант рукописи.

Авторы заявляют об отсутствии конфликта интересов.

Вклад соавторов: Авторы внесли равный вклад в постановку задачи, обработку и анализ данных, интерпретацию результатов и подготовку рукописи.

Operator identity verification by single mouse-click dynamics in a certification system for non-destructive testing specialists

Artem A. Popkov, Vladimir S. Vyplaven, Alexey Yu. Korovchenko

Siberian Transport University (STU)

Abstract. Certification of non-destructive testing specialists entails legal consequences, so the authenticity of the test result should be treated as an information-security task. Password protection confirms the subject's identity only at login and does not control who actually answers the questions during the session. Behavioral biometrics, covert in the way features are collected, closes this gap. This paper assesses the reliability of confirming an examinee's identity by the dynamics of single mouse clicks and identifies the most discriminative features. The data source is the log of an operational certification system accumulated since 2020, containing over 3.4 million click events from 250 users. The hold duration and the relative coordinates of the click point are recorded for each click. A set of sixteen session-level features and an open-set verification scheme using a random forest as the baseline model are proposed. Interval quality estimates are obtained by user-level bootstrap. On the test set, an equal error rate (EER) of 18.3 % was achieved for single-session scoring (95 % confidence interval [16.2; 19.5] %) with an area under the characteristic curve of 0.899. Fusing decisions over several sessions reduces the error to fractions of a percent (0.47 % for twelve sessions), which, given the statistical dependence of one user's sessions, should be understood as an optimistic bound. The spatial features of the click point, complemented by the button hold duration, contribute most to discriminability. The applicability of click dynamics as an additional, covertly collected factor for confirming subject authenticity in certification systems without extra hardware is demonstrated.

Keywords: behavioral biometrics, mouse-click dynamics, covert authentication, identity verification, information security, personnel certification, non-destructive testing.

For citation: Popkov A. A., Vyplaven V. S., Korovchenko A. Yu. Verifikatsiya lichnosti operatora po dinamike odinochnykh nazhatii myshi v sisteme attestatsii spetsialistov nerazrushayushchego kontrolya [Operator identity verification by single mouse-click dynamics in a certification system for non-destructive testing specialists]. Vestnik SibGUTI, 2026, vol. 20, no. 3, pp. 3–15 <https://doi.org/10.55648/1998->



Content is available under the license

Creative Commons Attribution 4.0 License

© Popkov A. A., Vyplaven V. S., Korovchenko A. Yu., 2026

The article was submitted: 08.07.2026;
revised version – 22.08.2026;
accepted for publication: 24.08.2026.

References

1. User authentication through mouse dynamics / C. Shen [et al.] // IEEE Transactions on Information Forensics and Security. Vol. 8. — 2013. — P. 16–30. — DOI: 10.1109/TIFS.2012.2223677.
2. Ahmed A. A. E., Traore I. A new biometric technology based on mouse dynamics // IEEE Transactions on Dependable and Secure Computing. Vol. 4. — 2007. — P. 165–179. — DOI: 10.1109/TDSC.2007.70207.
3. Jorgensen Z., Yu T. On mouse dynamics as a behavioral biometric for authentication // Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS). — 2011. — P. 476–482. — DOI: 10.1145/1966913.1966983.
4. Mouse dynamics behavioral biometrics: a survey / S. Khan [et al.] // ACM Computing Surveys. — 2024. — Vol. 56, no. 6. — P. 1–33. — DOI: 10.1145/3640311.
5. Zheng N., Paloski A., Wang H. An efficient user verification system via mouse movements // Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS). — 2011. — P. 139–150. — DOI: 10.1145/2046707.2046725.

6. User identity verification via mouse dynamics / C. Feher [et al.] // *Information Sciences*. — 2012. — Vol. 201. — P. 19–36. — DOI: 10.1016/j.ins.2012.02.066.
7. Performance evaluation of anomaly-detection algorithms for mouse dynamics / C. Shen [et al.] // *Computers & Security*. — 2014. — Vol. 45. — P. 156–171. — DOI: 10.1016/j.cose.2014.05.002.
8. *Chong P., Elovici Y., Binder A.* User authentication based on mouse dynamics using deep neural networks: a comprehensive study // *IEEE Transactions on Information Forensics and Security*. Vol. 15. — 2020. — P. 1086–1101. — DOI: 10.1109/TIFS.2019.2930429.
9. *Almalki S., Assery N., Roy K.* An empirical evaluation of online continuous authentication and anomaly detection using mouse clickstream data analysis // *Applied Sciences*. — 2021. — Vol. 11, no. 13. — P. 6083. — DOI: 10.3390/app11136083.
10. Balabit Mouse Dynamics Challenge data set / Á. Fülöp [et al.]. — 2016. — URL: <https://github.com> (visited on 07/02/2026).
11. *Antal M., Dénes-Fazakas L.* User verification based on mouse dynamics: a comparison of public data sets // *Proceedings of the IEEE 15th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. — 2021. — P. 000155–000160. — DOI: 10.1109/SACI51354.2021.9465583.
12. *Antal M., Egyed-Zsigmond E.* Intrusion detection using mouse dynamics // *IET Biometrics*. — 2019. — Vol. 8, no. 5. — P. 285–294. — DOI: 10.1049/iet-bmt.2018.5126.
13. *Popkov A. A., Shkolina D. S.* Monitoring and evaluation of the technical training results of non-destructive testing specialists for railway transport objects // *International Scientific Siberian Transport Forum TransSiberia 2021. Lecture Notes in Networks and Systems*. Vol. 403. — 2022. — P. 189–196. — DOI: 10.1007/978-3-030-96380-4_21.
14. *Vyplaven V. S., Kolomeets A. O., Popkov A. A.* Kalman-filter processing of strain-gauge testing signals // *Journal of Physics: Conference Series*. — 2021. — Vol. 2131, no. 3. — P. 032015. — DOI: 10.1088/1742-6596/2131/3/032015.
15. *Fawcett T.* An introduction to ROC analysis // *Pattern Recognition Letters*. — 2006. — Vol. 27, no. 8. — P. 861–874. — DOI: 10.1016/j.patrec.2005.10.010.
16. *Vekhov V. D., Smushkin A. B.* Kriminalisticheskoe issledovanie tsifrovyykh otpechatkov komp'yuternyykh ustroystv [Forensic investigation of digital fingerprints of computer devices] // *Vserossiiskii kriminologicheskii zhurnal*. — 2024. — Vol. 18, no. 4. — P. 390–397. — DOI: 10.17150/2500-4255.2024.18(4).390-397.
17. *Breiman L.* Random forests // *Machine Learning*. — 2001. — Vol. 45, no. 1. — P. 5–32. — DOI: 10.1023/A:1010933404324.
18. *Efron B.* Bootstrap methods: another look at the jackknife // *The Annals of Statistics*. — 1979. — Vol. 7, no. 1. — P. 1–26. — DOI: 10.1214/aos/1176344552.

Artem A. Popkov

PhD in Engineering, associate professor, Siberian Transport University (STU, 191 D. Kovalchuk St., Novosibirsk, 630049), e-mail: zabagy@gmail.com, ORCID ID: 0000-0002-8328-2415.

Vladimir S. Vyplaven

PhD in Engineering, associate professor, Siberian Transport University (STU, 191 D. Kovalchuk St., Novosibirsk, 630049), e-mail: vladimir97927@gmail.com, ORCID ID: 0000-0002-9083-5882.

Alexey Yu. Korovchenko

Software engineer, Siberian Transport University (STU, 191 D. Kovalchuk St., Novosibirsk, 630049), e-mail: lecha3525@gmail.com, ORCID ID: 0009-0002-6388-2285.