УДК 004.056.52 Вестник УрФО № 3(61) / 2026, с. 5–18
DOI: 10.14529/secur260301

Афанасьева Н.С., Елизаров Д.А.

МАРКОВСКОЕ МОДЕЛИРОВАНИЕ ПОСЛЕДОВАТЕЛЬНОСТИ ДЕЙСТВИЙ КАК ИСТОЧНИК ДОПОЛНИТЕЛЬНЫХ ПРИЗНАКОВ ДЛЯ ДЕТЕКТИРОВАНИЯ АВТОМАТИЗИРОВАННЫХ СРЕДСТВ ПОДМЕНЫ ПОЛЬЗОВАТЕЛЯ

Afanaseva N.S., Elizarov D.A.

MARKOV MODELING OF ACTION SEQUENCES AS A SOURCE OF ADDITIONAL FEATURES FOR DETECTING AUTOMATED USER-SPOOFING TOOLS

Предложенное ранее автором признаковое пространство для детектирования автоматизированных средств подмены пользователя (ботов) описывает непрерывную геометрическую форму траектории движения мыши, но не рассматривает последовательность типов действий (перемещение, клик, прокрутка) как самостоятельный источник признаков. В настоящей работе последовательность действий смоделирована марковской цепью первого порядка. На ее основе построено отдельное признаковое пространство, сопоставленное с траекторным и их объединением. Показано, что признаки на основе действий сами по себе дают низкое качество классификации (F1-мера по классу «бот» – 0,319, у траекторных признаков – 0,837), однако их добавление к траекторным признакам дает прирост полноты (recall) с 0,937 до 0,947 и F1-меры с 0,837 до 0,844. При этом независимое ранжирование важности признаков методом SHAP в объединенном пространстве показывает, что верхние позиции занимают именно признаки на основе кликов, а не траекторные. Анализ параметров марковской цепи объясняет эту особенность – вероятность повторного клика подряд у скриптов на основе Selenium составляет 43,6–65,5%, когда у реальных пользователей и прежде изученных ботов это значение колеблется в пределах16,0–21,5%.

Ключевые слова: бот, вредоносный бот, детектор ботов, цепь Маркова, последовательность действий, классификация, движение курсора мыши, признаковое пространство.

The feature space previously proposed by the author for detecting automated user-substitution tools (bots) describes the continuous geometric shape of the mouse movement trajectory, but does not consider the sequence of action types (movement, click, scroll) as an independent source of features. In the present work, the sequence of actions is modeled as a first-order Markov chain. Based on this, a separate feature space is constructed and compared with the trajectory-based feature space and their combination. It is shown that action-based features alone yield low classification quality (F1-score for the "bot" class – 0,319, versus 0,837 for trajectory-based features); however, adding them to the trajectory-based features improves recall from 0,937 to 0,947 and F1-score from 0,837 to 0,844. At the same time, independent feature importance ranking using SHAP in the combined feature space shows that the top positions are occupied specifically by click-based features rather than trajectory-based ones. Analysis of the Markov chain parameters explains this pattern: the probability of a repeated consecutive click for Selenium-based scripts is 43,6 –65,5%, whereas for real users and previously studied bots this value ranges between 16,0–21,5%.

Keywords: bot, malicious bot, bot detector, Markov chain, action sequence, classification, mouse cursor movement, feature space.

Введение

Согласно ежегодному отчету Imperva о вредоносных ботах, в 2025 году автоматизированный трафик впервые превысил долю трафика реальных пользователей в сети Интернет, составив 53% от общего объема веб-трафика [1]. В отчете это связывается с распространением автономных программных агентов на основе искусственного интеллекта, действующих от имени пользователя через те же интерфейсы, что и человек. Такие продукты размывают границу между легитимным и автоматизированным трафиком и снижают эффективность существующих методов детектирования. По мере того как автоматизированный трафик растет в объеме и правдоподобности, методы детектирования, использующие в себе только один аспект для сравнения, могут устаревать быстрее, чем успевают распространиться в промышленную эксплуатацию.

Любое взаимодействие пользователя с графическим интерфейсом раскладывается на две во многом независимые составляющие. Непрерывная кинематическая сторона описывает как именно перемещается курсор между двумя точками (форма, скорость, ускорение), дискретная событийная сторона – то, какие типы действий совершаются и в каком порядке чередуются (перемещение, клик, прокрутка). Признаковое пространство, предложенное автором ранее для решения задачи детектирования ботов, описывает непрерывную геометрическую форму траектории движения мыши: базовый набор

кинематических параметров дополнен порядковыми статистиками скорости, ускорения, рывка и кривизны, признаками сравнения распределений конкретного трека с распределениями эталонных датасетов на основе критерия хи-квадрат, энтропийными характеристиками и угловыми характеристиками траектории [2]. Совокупность этих групп признаков характеризует форму отдельного, изолированно рассматриваемого перемещения курсора между двумя точками взаимодействия. Однако, данное пространство не рассматривает другую сторону взаимодействия пользователя с интерфейсом – последовательность типов совершаемых действий. Тогда как форма отдельного перемещения может быть имитирована автоматизированным скриптом, сам порядок чередования типов действий в сессии определяется логикой скрипта на более высоком уровне и потенциально несет самостоятельную информацию, не сводимую к геометрии отдельных перемещений.

Естественным математическим аппаратом для описания подобной последовательности дискретных состояний, сменяющих друг друга во времени, выступает марковская цепь. Она компактно описывает вероятностную структуру переходов между типами действий одним небольшим набором параметров (матрицей переходных вероятностей и вектором начального распределения), не требуя явного моделирования всей последовательности целиком, и при этом остается интерпретируемой [3]. Каждый параметр такой цепи имеет прямой содержательный смысл (например, вероятность того, что за кликом последует еще один клик, а не перемещение).

Целью настоящей работы является построение и эмпирическая оценка признакового пространства на основе марковской цепи первого порядка по типам действий, сопоставление его детектирующей способности с траекторным пространством и их объединением, а также анализ того, какую содержательную информацию о различии легитимного и автоматизированного трафика несут параметры такой цепи.

Использование марковских цепей для детектирования ботов

Марковские цепи ранее применялись для детектирования ботов в других постановках задачи. В работе [4] сетевой (не поведенческий) трафик бота моделируется марковской цепью по высокоуровневым признакам сетевых потоков (объем, направление, интервалы между пакетами), выступающим в роли состояний. Полученные параметры цепи использовались как признаки для классификатора Random Forest, что позволяло системе детектировать трафик ранее не встречавшихся семейств ботов с F-мерой 93,03%. Таким образом марковское представление в этой работе использовалось в первую очередь для повышения устойчивости детектора к новым, не участвовавшим в

обучении семействам, а не для описания поведения курсора. Настоящая работа переносит идею марковского моделирования последовательности состояний в область поведенческой биометрии движения мыши, где ранее она в явном виде не применялась, и использует в качестве состояний не сетевые характеристики, а непосредственно тип действия пользователя (перемещение, клик, прокрутка).

В области поведенческой биометрии подавляющее большинство работ решает задачу верификации или идентификации личности, а не бинарной классификации «человек/бот». В [5] и [6] строится модель нормального поведения конкретного пользователя, и оценивается отклонение новой сессии от нее. В работе [7] движения мыши используются в составе более широкой системы человеко-компьютерного взаимодействия для непрерывной аутентификации. Авторы [8] используют признаки движения мыши для идентификации пользователя в задаче веб-браузинга, в [9] для той же задачи идентификации применяются модели глубокого обучения. Во всех перечисленных работах типичными метриками качества выступают равный уровень ошибок (EER) и площадь под ROC-кривой (AUC), не тождественные метрикам точность (precision), полнота (recall) и F1-мера, используемым при решении задачи бинарной классификации «человек/бот».

Отдельная линия исследований посвящена непосредственно детектированию ботов: в [10] применяются методы глубокого обучения для детектирования веб-ботов по поведенческой биометрии, в [11] предложен метод синтетической генерации обучающих траекторий (BeCAPTCHA-Mouse) для обучения и тестирования детекторов, в [12] предложена облегченная по вычислительным затратам сетевая архитектура, ориентированная на промышленное применение. Ни в одной из перечисленных работ не рассматривалась последовательность типов действий как самостоятельный источник признаков, дополняющий геометрию траектории. Настоящая работа проверяет гипотезу о том, что построенное на основе такого расширения признаковое пространство способно повышать детектирующую способность детектора, ранее предложенного автором [13].

Датасеты и признаковые пространства, используемые для классификации

Для эксперимента используются данные из различных источников. user_BALABIT и user_BOGAZICI – эталонные публичные датасеты реальных пользователей, user_BROWSER – собственный датасет реальных пользователей, bot_BOT– ранее изученный генератор автоматизированного трафика, BROWSER_BOTS_E – браузерный бот с более сложной, вариативной

имитацией действий, E_line, E_teleport, E_move_to_element, E_b-spline interpolation – четыре датасета скриптов-скраперов на основе библиотеки Selenium. Методология формирования и разметки данных подробно описана в [13]. Итоговая тестовая выборка содержит 6071 наблюдение класса «бот» и 692102 наблюдения класса «пользователь».

Для сопоставления детектирующей способности построены три классификатора Random Forest [14] (n_estimators по умолчанию, max_depth = 10, class_weight = 'balanced') с идентичной архитектурой, обученные на трех разных подмножествах признаков («action», «trajectory», «action + trajectory») одной и той же объединенной выборки.

Пространство «action» включает три группы признаков, производных от марковской цепи и статистики по типам действий. Каждая точка сессии взаимодействия отнесена к одному из трех типов действия: перемещение курсора (MOUSE_MOVE), клик (MOUSE_CLICK) или прокрутка колеса мыши (MOUSE_WHEEL). Последовательность типов действий в пределах сессии моделируется цепью Маркова первого порядка. Для каждой сессии рассчитывается матрица A вероятностей перехода между типами действий (элемент A[i,j] – вероятность того, что за действием типа i непосредственно следует действие типа j) и вектор π стационарного (в данной реализации начального усредненного) распределения по типам действий. Помимо параметров самой цепи, данное признаковое пространство включает статистические характеристики распределения точек по типам действий и по временным интервалам между ними: число точек каждого типа действия, характеристики гистограмм длительности интервалов между последовательными действиями одного типа, а также отдельную группу признаков дублирования кликов (долю и число кликов, совпадающих по координатам с одним из предыдущих кликов в той же сессии).

Пространство «trajectory» включает 222 признака геометрической формы траектории: порядковые статистики параметров движения (квартили, межквартильный размах, медианы скорости, ускорения, рывка, кривизны и угловых характеристик), признаки сравнения распределения конкретного трека с распределениями эталонных датасетов на основе критерия хи-квадрат, энтропийные характеристики, угловые характеристики траектории в целом. Признаки данного пространства не зависят от того, к какому типу относится каждая отдельная точка (перемещение, клик или прокрутка), и рассчитываются по геометрии пути целиком.

Пространство «action + trajectory» образовано непосредственным объединением (конкатенацией) всех признаков обоих пространств без дополнитель-

ного отбора или преобразования, что позволяет классификатору самостоятельно определить относительный вклад каждой группы признаков в итоговое решение.

Для каждой модели рассчитаны precision, recall и F1-мера по классу «бот», а также доля треков, отнесенных к каждому классу, в разбивке по конкретным источникам данных.

Результаты эксперимента

Результаты классификации по классу «бот» в трех признаковых пространствах представлены на рис. 1 и в табл. 1.

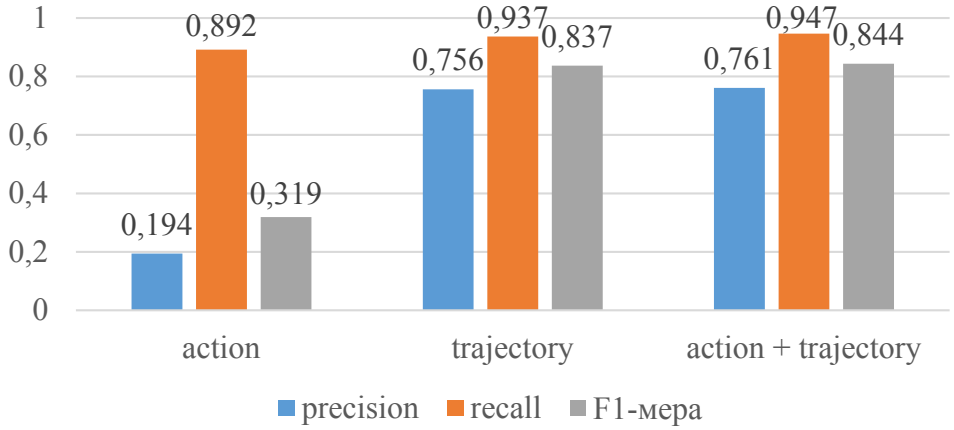


Рис. 1. Качество классификации в трех признаковых пространствах

Таблица 1

Качество классификации по классу «бот» в трех признаковых пространствах

Пространство	precision	recall	F1-мера	accuracy
action	0,194	0,892	0,319	0,967
trajectory	0,756	0,937	0,837	0,997
action + trajectory	0,761	0,947	0,844	0,997

Признаки на основе действий сами по себе дают заметно более низкое качество классификации, чем траекторные признаки. F1-мера по классу «бот» в пространстве действий составляет 0,319 против 0,837 у траекторных признаков, что обуславливается низкой точностью (precision 0,194 и 0,756 соответственно). Модель на основе действий существенно чаще ложно относит треки реальных пользователей к боту. При этом полнота (recall) в пространстве действий оказывается на высоком уровне и составляет 0,892, то есть эти признаки способны улавливать значительную часть ботов, но ценой большого числа ложных срабатываний. Объединение двух пространств дает небольшой, но устойчивый прирост метрик относительно чистой траектории (полнота с 0,937 до 0,947, F1-мера с 0,837 до 0,844).

Разбивка доли треков, отнесенных к классу «бот», по конкретным источникам данных (табл. 2) показывает, что добавление признаков действий к траекторным затрагивает источники неравномерно.

Таблица 2

Доля треков, отнесенных к классу «бот», по источникам и пространствам, %

Источник	action	trajectory	action + trajectory
bot_BOT	70,07	77,07	80,54
E_b-spline	88,54	99,62	99,61
E_ line	99,17	99,92	99,90
E_move_to_element	99,70	99,89	99,89
E_teleport	99,39	99,83	99,89
user_BALABIT (ложноположж.)	19,03	2,29	2,21
user_BOGAZICI (ложноположж.)	3,11	0,04	0,08
user_BROWSER (ложноположж.)	2,89	0,32	0,23

Для ботов расширение признакового пространства путем добавления действий к траектории почти везде улучшает или сохраняет долю верно распознанных треков: для bot_BOT – с 77,07% до 80,54%, для E-скраперов рост либо отсутствует, либо укладывается в десятые доли процента. Для реального пользователя BALABIT ложноположительная доля при объединении пространств уменьшается 2,29% до 2,21%, тогда как для BOGAZICI направление изменения обратное (рост с 0,04% до 0,08%). Это указывает на то, что выигрыш от добавления признаков действий не является для всех источников безусловно положительным и должен оцениваться на конкретной, представительной для эксплуатации выборке легитимных пользователей.

Стационарное распределение по типам действий (вектор π) различается между источниками. Доля кликов колеблется от 1,47% (BROWSER_ BOTS_E) до 12,28% (E_move_to_element), доля прокрутки – от 0% (user_ BOGAZICI, где события прокрутки в данных отсутствуют) до 10,81% (BROWSER_BOTS_E). Полное стационарное распределение по трем типам действий (вектор π) для всех рассмотренных источников приведено в табл. 3.

Таблица 3

Стационарное распределение по типам действий (вектор π), %

Источник	Перемещение	Клик	Прокрутка
user_BALABIT	96,57	2,85	0,59
user_BOGAZICI	93,31	6,69	0,00
user_BROWSER	89,62	1,47	8,91
bot_BOT	98,14	1,73	0,13
BROWSER_BOTS_E	87,71	1,47	10,81
E_line	83,36	10,90	5,74

Окончание табл. 3

E_teleport	83,00	11,20	5,80
E_move_to_element	80,78	12,28	6,94
E_b-spline	83,94	10,52	5,54

Дополнительно рассчитана вероятность перехода из состояния «клик» обратно в состояние «клик» (диагональный элемент матрицы переходов), то есть вероятность того, что за одним кликом непосредственно последует еще один клик без промежуточного перемещения (рис. 2).

Реальные пользователи (BALABIT, BOGAZICI, user_BROWSER) и уже изученные боты (bot_BOT, BROWSER_BOTS_E) демонстрируют сопоставимо низкую вероятность повторного клика подряд, в диапазоне 16,0 – 21,5%. Все четыре скрипта на основе Selenium, напротив, показывают значительно более высокую вероятность – от 43,6% (line) до 65,5% (b-spline interpolation), то есть выше более чем в два – три раза. Такое поведение согласуется с логикой типового скрипта автоматизации, последовательно выполняющего несколько кликов по элементам страницы без промежуточных перемещений, характерных для человека или для более сложно имитирующего поведение бота.

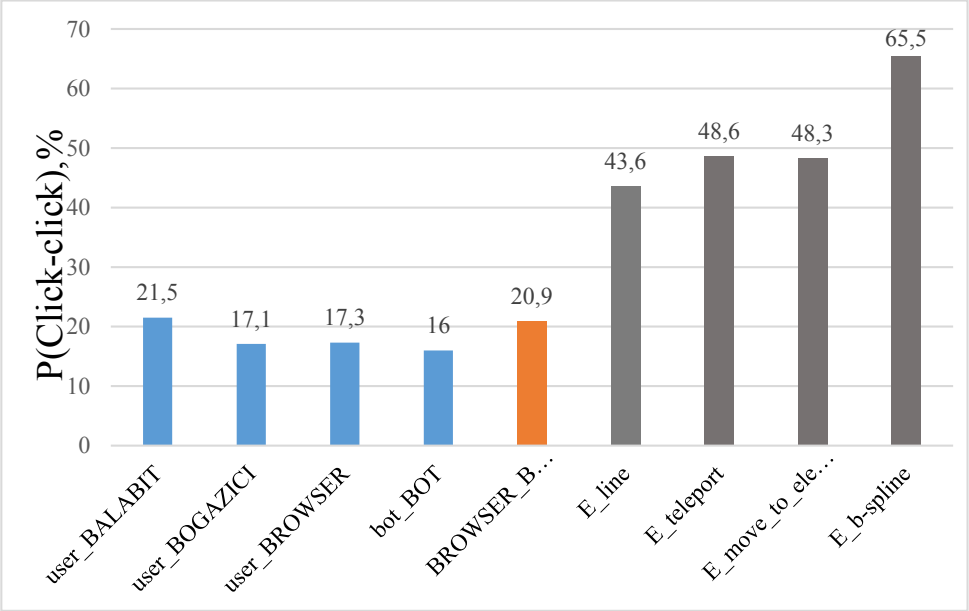


Рис. 2. Вероятность повторного клика подряд по источникам данных

Как видно из табл. 3, доля кликов у четырех Selenium-скраперов (10,52–12,28%) систематически выше, чем у реальных пользователей и ранее изученных ботов (1,47–6,69%), что дополняет информацию о повышенной вероятности повторного клика подряд. Скрипты-скраперы не только чаще кликают подряд, но и в целом отводят кликам большую долю от общего числа

действий. Доля прокрутки не дает столь же однозначной картины – она невелика и сопоставима у большинства источников (0–6,94%), однако заметно выше у BROWSER_BOTS_E (10,81%) и user_BROWSER (8,91%). Эти два источника не разделяются по данному признаку, что говорит об ограниченной самостоятельной различающей способности доли прокрутки в отрыве от остальных параметров цепи.

Независимым подтверждением значимости признаков на основе действий служит ранжирование важности признаков методом SHAP, рассчитанное для классификатора в объединенном пространстве «action + trajectory» (рис. 3). Верхние позиции ранжирования заняли признаки на основе кликов (доля и число повторяющихся по координатам кликов, распределение кликов по временным интервалам). Это согласуется с обнаруженным по параметрам марковской цепи различием в характере кликов между источниками и объясняет, почему признаки действий, несмотря на низкое собственное качество классификации, вносят непропорционально большой вклад при объединении с траекторией.

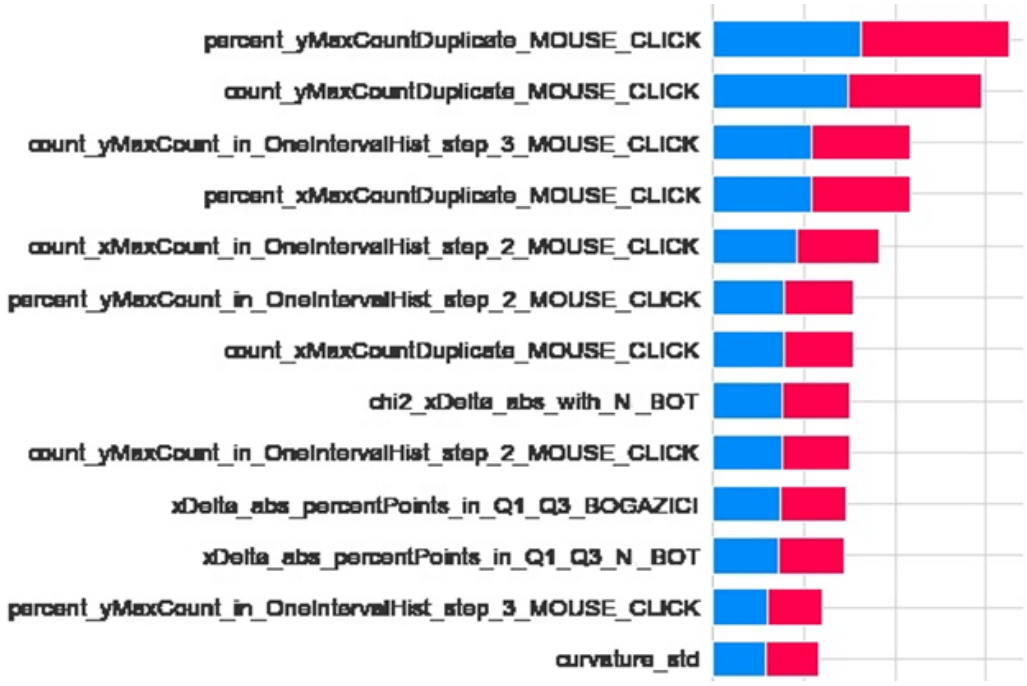


Рис. 3. Верхние позиции ранжирования важности признаков методом SHAP в объединенном пространстве «action + trajectory»

Обсуждение результатов эксперимента

Полученные результаты показывают, что низкое собственное качество классификации у пространства «action» не означает отсутствия у него содержательной информации. В объединении с траекторией именно признаки на основе кликов оказываются наиболее значимыми, по независимой оценке,

SHAP, а параметры марковской цепи дают понятное, интерпретируемое объяснение этому эффекту. Распространенные инструменты автоматизации (Selenium-скрипты) кликают заметно чаще подряд, чем это делает человек или более сложно имитирующий его бот. Это позволяет сделать методологически важный вывод – оценка ценности признакового пространства только по его собственным метрикам (precision, recall, F1-мера) в изоляции может недооценивать потенциальный вклад, вносимый этими признаками в составе более широкого пространства.

Практический вывод состоит в целесообразности включения статистик по типам действий (в частности, показателей повторяемости кликов) в состав признакового пространства детектора, дополнительно к траекторным признакам, поскольку такие статистики отражают логику работы скрипта автоматизации, которую сложно замаскировать без явного усложнения самого скрипта. Одновременно наблюдаемый неоднородный эффект на ложноположительную долю по разным источникам легитимных пользователей указывает на необходимость проверки такого расширения на представительной для конкретной эксплуатационной среды выборке пользователей.

Верхние пять позиций ранжирования SHAP в объединенном пространстве заняли исключительно признаки на основе повторяемости кликов (доля и число дублирующихся по координатам кликов, число точек клика в интервалах гистограммы), опередив ранее ключевые для чисто траекторного пространства признаки (критерий хи-квадрат при сравнении с эталонными датасетами и угловые характеристики). Это означает, что практическая ценность объединения пространств обеспечивается не суммарным, распределенным вкладом множества новых признаков, а вкладом узкой группы из нескольких конкретных, интерпретируемых индикаторов. Этот результат отличается от ранее полученного для чисто траекторного пространства, в [13] наиболее значимой по SHAP группой признаков были порядковые статистики рывка и ускорения, тогда как в настоящей работе, при добавлении признаков действий, верхние позиции занимают признаки совершенно другой природы – статистики повторяемости кликов. Это говорит о том, что ранжирование важности признаков существенно зависит от состава признакового пространства, в котором оно рассчитывается.

Полученные результаты имеют значение для проектирования признаковых пространств детекторов автоматизированного трафика за пределами конкретной рассмотренной задачи. Во-первых, они демонстрируют, что оценка признакового пространства только по его собственному, изолированному качеству классификации может вводить в заблуждение относительно

его практической ценности. Во-вторых, интерпретируемость найденного различия – конкретная, понятная эксплуатирующему специалисту причина (повышенная частота повторных кликов у типовых скриптов автоматизации) – позволяет использовать этот признак не только в составе модели машинного обучения, но и как самостоятельный, объяснимый индикатор при ручном разборе подозрительных сессий. В-третьих, поскольку признаки на основе действий строятся на статистике типов событий, а не на геометрии координат, они потенциально более устойчивы к простым методам маскировки, ориентированным на имитацию правдоподобной формы траектории, но не корректирующим статистику типов действий.

Заключение

В работе продемонстрировано, что моделирование последовательности типов действий (перемещение, клик, прокрутка) марковской цепью первого порядка дает признаковое пространство, самостоятельно уступающее по качеству классификации траекторному, но при объединении этих пространств наблюдается прирост полноты (recall) с 0,937 до 0,947 и F1-меры с 0,837 до 0,844 по классу «бот». Независимое ранжирование важности признаков методом SHAP показывает, что признаки на основе кликов занимают верхние позиции в объединенном пространстве, а анализ параметров марковской цепи объясняет эту находку конкретным поведенческим различием – скрипты на основе Selenium кликают подряд значительно чаще, чем реальные пользователи и ранее изученные боты. Практическая рекомендация состоит во включении статистик повторяемости и последовательности действий в состав признакового пространства детектора как источника информации, дополняющей, а не дублирующей траекторные признаки. Возможным продолжением работы является проверка марковских цепей более высокого порядка (второго и выше), при которых вероятность следующего действия зависит не от одного, а от нескольких предшествующих.

Работа выполнена в рамках государственного задания на оказание государственных услуг (выполнение работ) № 109-03-2026-004 от 16.01.2026 г. по теме «Разработка технологии выявление автоматизированных средств подмены пользователя в информационной среде с помощью алгоритмов моторной идентификации поведенческих паттернов».

Литература

1. 2025 Imperva Bad Bot Report [Электронный ресурс]. URL: https://www.imperva.com/resources/resource-library/reports/2025-imperva-bad-bot-report (дата обращения: 22.08.2026).

2. Афанасьева Н.С. Формирование пространства признаков, позволяющих осуществлять детектирование автоматизированных средств подмены пользователя в информационной среде // Безопасность информационных технологий. – 2026 (в печати).

3. Norris J. R. Markov chains. – Cambridge: Cambridge university press, 1998. – № 2.

4. Alahmadi B. A., Mariconti E., Spolaor R., Stringhini G., Martinovic I. BOTection: Bot detection by building Markov Chain models of bots network behavior // Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS '20). – New York: ACM, 2020. – P. 652–664.

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. – New York: ACM, 2011. – P. 139–150.

6. Feher C., Elovici Y., Moskovitch R., Rokach L., Schclar A. User identity verification via mouse dynamics // Information Sciences. – 2012. – Vol. 201. – P. 19–36.

7. Gamboa H., Fred A. A behavioral biometric system based on human-computer interaction // Proceedings of SPIE, Vol. 5404, Biometric Technology for Human Identification. – Bellingham: SPIE, 2004. – P. 381–392.

8. Chuda D., Kratky P. Usage of computer mouse characteristics for identification in web browsing // Proceedings of the 15th International Conference on Computer Systems and Technologies (CompSysTech '14). – New York: ACM, 2014. – P. 218–225.

9. Antal M., Fejer N. Mouse dynamics based user recognition using deep learning // Acta Universitatis Sapientiae, Informatica. – 2020. – Vol. 12, № 1. – P. 39–50.

10. Wei A., Zhao Y., Cai Z. A deep learning approach to web bot detection using mouse behavioral biometrics // Biometric Recognition (CCBR 2019), Lecture Notes in Computer Science, Vol. 11818. – Cham: Springer, 2019. – P. 388–395.

11. Acien A., Morales A., Fierrez J., Vera-Rodriguez R. BeCAPTCHA-Mouse: Synthetic mouse trajectories and improved bot detection // Pattern Recognition. – 2022. – Vol. 127. – Art. 108643.

12. Niu H., Zhou Y., Chen J., Cai Z. Performance evaluation of lightweight network-based bot detection using mouse movements // Engineering Applications of Artificial Intelligence. – 2024. – Vol. 135. – Art. 108801.

13. Афанасьева Н.С. Экспериментальная оценка использования расширенного пространства признаков для детектирования автоматизированных

средств подмены пользователя // Информационные технологии. – 2026 (в печати).

14. Breiman L. Random Forests // Machine Learning. – 2001. – Vol. 45, № 1. – P. 5–32.

References

1. 2025 Imperva Bad Bot Report. Available at: https://www.imperva.com/resources/resource-library/reports/2025-imperva-bad-bot-report (accessed 12 August 2026).

2. Afanaseva N.S. Formirovanie prostranstva priznakov, pozvolyayushchikh osushchestvlyat' detektirovanie avtomatizirovannykh sredstv podmeny pol'zovatelya v informatsionnoy srede. Security of Information Technologies, 2026 (in press).

3. Norris J. R. Markov chains. Cambridge, Cambridge University Press, 1998, no. 2.

4. Alahmadi B. A., Mariconti E., Spolaor R., Stringhini G., Martinovic I. BOTection: Bot detection by building Markov Chain models of bots network behavior. Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS '20). New York, ACM, 2020, pp. 652–664.

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. New York, ACM, 2011, pp. 139–150.

6. Feher C., Elovici Y., Moskovitch R., Rokach L., Schclar A. User identity verification via mouse dynamics. Information Sciences, 2012, Vol. 201, pp. 19–36.

7. Gamboa H., Fred A. A behavioral biometric system based on human-computer interaction. Proceedings of SPIE, Vol. 5404, Biometric Technology for Human Identification. Bellingham, SPIE, 2004, pp. 381–392.

8. Chuda D., Kratky P. Usage of computer mouse characteristics for identification in web browsing. Proceedings of the 15th International Conference on Computer Systems and Technologies (CompSysTech '14). New York, ACM, 2014, pp. 218–225.

9. Antal M., Fejer N. Mouse dynamics based user recognition using deep learning. Acta Universitatis Sapientiae, Informatica, 2020, Vol. 12, no. 1, pp. 39–50.

10. Wei A., Zhao Y., Cai Z. A deep learning approach to web bot detection using mouse behavioral biometrics. Biometric Recognition (CCBR 2019), Lecture Notes in Computer Science, Vol. 11818. Cham, Springer, 2019, pp. 388–395.

11. Acien A., Morales A., Fierrez J., Vera-Rodriguez R. BeCAPTCHA-Mouse: Synthetic mouse trajectories and improved bot detection. Pattern Recognition, 2022, Vol. 127, art. 108643.

12. Niu H., Zhou Y., Chen J., Cai Z. Performance evaluation of lightweight network-based bot detection using mouse movements. Engineering Applications of Artificial Intelligence, 2024, Vol. 135, art. 108801.

13. Afanaseva N.S. Eksperimental'naya otsenka ispol'zovaniya rasshirennogo prostranstva priznakov dlya detektirovaniya avtomatizirovannykh sredstv podmeny pol'zovatelya. Information Technologies, 2026 (in press).

14. Breiman L. Random Forests. Machine Learning, 2001, Vol. 45, no. 1, pp. 5–32.

АФАНАСЬЕВА Наталья Сергеевна, старший преподаватель кафедры «Информационная безопасность», Омский государственный университет путей сообщения. 644046, г. Омск, пр-т К. Маркса, 35. E-mail: nati_dik@mail.ru

ЕЛИЗАРОВ Дмитрий Александрович, кандидат техн. наук, доцент, зав. кафедрой «Информационная безопасность», Омский государственный университет путей сообщения. 644046, г. Омск, пр-т К. Маркса, 35. E-mail: d.a.elizarov@yandex.ru

AFANASEVA Natalia Sergeevna, Senior Lecturer of Department «Information security», Omsk State Transport University. 644046, Omsk, Marx st.,35. E-mail: nati_dik@mail.ru

ELIZAROV Dmitriy Aleksandrovich, PhD in Technical Sciences, Associate Professor, Head of Department «Information security», Omsk State Transport University. 644046, Omsk, Marx st.,35. E-mail: d.a.elizarov@yandex.ru