DOI: 10.55648/1998-6920-2026-20-2-28-44 УДК 004.056.53

Анализ устойчивости модели адаптивной аутентификации к целевым оптимизационным атакам имитации гибридного цифрового отпечатка

А. А. Саломатин[1], А. С. Широков[1], А. К. Мельников[2]

[1] Институт проблем управления им. В. А. Трапезникова РАН
[2] АО «Вычислительные решения», Москва, Россия

Аннотация: В статье исследуется устойчивость модели адаптивной аутентификации к целевым оптимизационным атакам имитации гибридного цифрового отпечатка. Предложено адверсариальное расширение модели адаптивной аутентификации, основанной на цифровом отпечатке, объединяющем технические и поведенческие атрибуты. Атака формализована как задача условной оптимизации с раздельными величинами допустимых возмущений технических (ε_d) и поведенческих (ε_b) атрибутов в условиях ограниченной обратной связи. Для оценки устойчивости модели введена вероятностная мера устойчивости R, согласованная с классическими метриками FAR/FRR. Экспериментальная проверка проведена на датасете из 1280 сессий (32 пользователя, 30 признаков) с использованием алгоритма CMA-ES. Результаты экспериментов показали, что модели с адаптивным взвешиванием обеспечивают двукратное повышение устойчивости относительно модели с равными весами в зоне реалистичных атак $(\varepsilon_b \le 0.2)$: $R = 0.66 - 0.79$ против 0.39–0.53, и снижают вероятность успешной атаки до 0.36 при стратегии оптимизации технических и поведенческих признаков. Экспериментально установлено, что автоматическое снижение весов при росте дисперсии признаков затрудняет целевые оптимизационные атаки злоумышленников. Выявленная уязвимость защиты при $\varepsilon_d \ge 0.5$ $(R \le 0.07)$ определяет границы применимости модели и обосновывает необходимость многофакторной аутентификации при высокой доле возмущений.

Ключевые слова: гибридный цифровой отпечаток; адаптивная аутентификация; целевые оптимизационные атаки; устойчивость аутентификации; поведенческая биометрия, кибербезопасность.

Для цитирования: Саломатин А. А., Широков А. С., Мельников А. К. Анализ устойчивости модели адаптивной аутентификации к целевым оптимизационным атакам имитации гибридного цифрового отпечатка // Вестник СибГУТИ. 2026. Т. 20, № 2. С. 28–44. https://doi.org/10.55648/1998-6920-2026-20-2-28-44.

Статья поступила в редакцию 10.04.2026;
переработанный вариант – 17.04.2026;
принята к публикации 05.05.2026.

1. Введение

Современные информационные системы активно используют механизмы аутентификации, основанные на анализе цифровых отпечатков пользователей [1]. При этом *гибридный цифровой отпечаток* – уникальный идентификатор, формируемый путём совместной обработки технических параметров устройства и поведенческих характеристик взаимодействия

пользователя с интерфейсом. В отличие от однокомпонентных отпечатков, он позволяет реализовать аутентификацию с повышенной устойчивостью к подмене сессии.

Развитие технологий анонимизации и специализированных средств подмены атрибутов существенно усложняет задачу аутентификации. На практике злоумышленники применяют следующие меры противодействия отслеживанию атрибутов цифрового отпечатка: подмена строки-идентификатора User-Agent, искажение графических параметров Canvas и WebGL, изменение сетевых характеристик (IP-адрес, прокси, VPN), использование виртуальных машин и антифингерпринт-браузеров. Отмеченные меры, применяемые в целях защиты приватности, приводят к естественной вариативности признаков гибридного цифрового отпечатка. Однако в условиях активного противодействия те же технические приёмы могут быть использованы злоумышленником для целенаправленной имитации профиля легитимного пользователя.

В предыдущем исследовании [2] была предложена модель адаптивной аутентификации пользователя, основанная на взвешенном векторе атрибутов гибридного цифрового отпечатка и динамическом обновлении эталонного профиля. Данная модель устойчива к естественным вариациям параметров цифрового отпечатка, возникающим вследствие легитимной смены условий доступа или применения мер анонимизации пользователя. Вместе с тем она ограничивается пассивными изменениями признаков и не учитывает, что злоумышленник может целенаправленно формировать цифровой отпечаток, оптимизируя его под характеристики легитимного пользователя для обхода механизма аутентификации.

Таким образом, возникает задача анализа устойчивости предложенной модели в условиях целенаправленных атак имитации цифрового отпечатка, при которых изменение признаков носит не случайный, а оптимизационный характер. Целью данной работы является исследование устойчивости модели адаптивной аутентификации пользователя к адверсариальным (целевым оптимизационным) атакам имитации гибридного цифрового отпечатка в условиях ограниченной обратной связи, а также оценка эффективности системы аутентификации при рациональном поведении злоумышленника воспроизвести профиль легитимного пользователя в условиях ограничений на изменение признаков.

Для достижения поставленной цели решаются следующие задачи:

– формализация модели атаки имитации гибридного цифрового отпечатка как задачи условной оптимизации с раздельными величинами допустимого возмущения для технической и поведенческой компоненты;

– классификация и определение стратегий поведения злоумышленника в условиях ограниченной обратной связи;

– разработка вероятностной модели оценки устойчивости модели к целевым оптимизационным атакам;

– экспериментальное моделирование целевых оптимизационных атак при разных стратегиях поведения злоумышленника и анализ эффективности системы аутентификации;

– определение границ применимости предложенной модели адаптивной аутентификации в условиях целевых оптимизационных атак.

В следующем разделе приводится обзор существующих подходов к анализу цифровых отпечатков пользователя и устойчивости аутентификации к целевым оптимизационным атакам имитации.

2. Обзор литературы

Задачи аутентификации пользователей в условиях активного противодействия рассматриваются в рамках направлений адаптивной аутентификации и адверсариального машинного обучения [1–4]. В отличие от классических статических моделей, предполагающих стационарность распределений признаков, современные подходы учитывают возможность целенаправленной модификации характеристик с целью обхода системы аутентификации.

Методы адаптивной аутентификации предполагают динамическое обновление профиля пользователя и параметров решающего правила на основе накопленных наблюдений [5, 6]. В исследованиях по риск-ориентированной аутентификации показано, что учет контекста сессии и вариативности поведения пользователя позволяет повысить устойчивость к несанкционированному доступу.

Отдельное направление связано с использованием поведенческих биометрических признаков: динамики нажатий клавиш, кликов мыши, а также других особенностей взаимодействия с интерфейсом [7–9]. Данные параметры обладают высокой индивидуальностью и сложно воспроизводимы, что делает их перспективным дополнением к техническим параметрам устройства. Однако показано, что даже поведенческие биометрические системы уязвимы к целевым атакам имитации [10]. При этом в литературе преобладает раздельный анализ технических и поведенческих характеристик, тогда как задачи устойчивости аутентификации для гибридных цифровых отпечатков, объединяющих оба типа данных, остаются недостаточно изученными.

С развитием методов адверсариального машинного обучения активно исследуются атаки, при которых злоумышленник модифицирует входной вектор признаков с целью минимизации функции потерь [11–13]. Исследования показывают, что высокоточные модели могут быть уязвимы к малым, но целенаправленным изменениям входного вектора. Как отмечается в работе [14], применение методов машинного обучения в задачах кибербезопасности осложняется несоответствием между доступностью обучающей выборки и информации о реальных атаках. Особое внимание уделяется моделированию атак как задач условной оптимизации [15]. Такой подход позволяет формализовать рациональное поведение злоумышленника и оценить устойчивость модели в зависимости от доступных ресурсов и технологических ограничений на модификацию признаков.

Одновременно с этим рассматриваются вероятностные модели оценки угроз, позволяющие рассчитывать вероятность успешного обхода аутентификации с учетом распределения ошибок имитации и структуры признакового пространства [16–20]. Подобные модели особенно востребованы в условиях неполной информации и стохастической природы поведенческих данных.

Несмотря на значительный прогресс, большинство существующих подходов либо рассматривают адаптивную аутентификацию без учёта целевых оптимизационных атак, либо анализируют эти атаки в отрыве от механизмов динамического обновления эталонных профилей. Критическим пробелом остаётся отсутствие формализованных моделей устойчивости гибридных цифровых отпечатков к целевым оптимизационным атакам в условиях адаптивного взвешивания признаков. В данной работе предлагается преодолеть это ограничение, объединив указанные направления в рамках единой вероятностно-оптимизационной модели и исследовав поведение системы аутентификации при целенаправленной имитации легитимного профиля.

3. Базовая модель адаптивной аутентификации

В базовой модели [2] система аутентификации оперирует множеством из n идентификационных атрибутов. Значение каждого i приводится к целочисленной шкале и принимает значения из множества $\{0,1,\ldots,Q_i-1\}$ (Q_i – количество разных уникальных значений i атрибута).

Гибридный цифровой отпечаток пользователя на каждой сессии представляется вектором $u=(u_1,\ u_2,\ \ldots,\ u_n)\ \epsilon\ R^n$. Эталонный вектор, хранящийся на сервере, обозначается как $v=(v_1,\ v_2,\ \ldots,\ v_n)\epsilon\ R^n$. Вектор весовых коэффициентов признаков представляется как $w=(w_1,w_2,\ \ldots,\ w_n)\epsilon\ R^n\ (\sum_{i=1}^{n} w_i=1, w_i\geq 0)$ и отражает относительную информативность каждого атрибута.

С учетом доступности атрибутов их веса вычисляются следующим образом:

$$w_i = \frac{I_i c_i L_i}{\sum_{j=1}^{n} I_j c_j L_j},$$

где

$I_i = \frac{S_i}{\sigma_i^2}$ – информативность i признака, рассчитываемая через разделительную способность S_i и дисперсию σ_i^2;

c_i – понижающий коэффициент, учитывающий корреляцию i признака с другими и рассчитываемый через коэффициенты r_{ij} корреляции Пирсона между i и j атрибутами и заданное пороговое значение высокой корреляции r_{max} как:

$$c_i = \begin{cases} 1, \ \textit{если} \ \max_{j \neq i} |r_{ij}| \leq r_{max}, \\ 1 - \frac{1}{n-1} \sum_{j \neq i} |r_{ij}|, \ \textit{иначе;} \end{cases}$$

$L_i \in \{0,1\}$ – индикатор доступности атрибута ($L_i = 1$, если атрибут измерен; $L_i = 0$, если атрибут заблокирован или рандомизирован).

При $w_i \to 0$ атрибут исключается из модели как избыточно шумовой. В условиях рандомизации (например, частой смены разрешения экрана) рост σ_i^2 снижает w_i, автоматически перераспределяя веса в сторону более стабильных признаков.

Для оценки близости вектора u к эталонному v используется взвешенное расстояние:

$$d(u, v) = \sum_{i=1}^{n} w_i \gamma_i(u_i, v_i),$$

где $\gamma_i(u_i, v_i)$ – отклонение по i атрибуту, вычисляемое с учетом индикаторной функции I_0:

$$\gamma_i(u_i, v_i) = \begin{cases} \frac{|u_i - v_i|}{Q_i - 1}, \ \textit{где } i \textit{ признак - количественный или порядковый}, \\ I_0(u_i \neq v_i), \ \textit{где } i \textit{ признак - категориальный или бинарный}. \end{cases}$$

Решение о подлинности пользователя (принятии нулевой гипотезы H_0) принимается по правилу:

$$\textit{Принять } H_0 \Leftrightarrow d(u, v) \leq t,$$

где t – порог допустимого отклонения.

Поскольку отклонения по отдельным атрибутам γ_i являются случайными величинами, при достаточно большом n распределение суммарного отклонения $D = d(U, v)$ аппроксимируется нормальным:

$$D / H_k \sim N(\mu_k, \sigma_k^2), k \in \{0,1\}$$

где H_1 – гипотеза о предъявлении вектора признаков злоумышленником;

Вероятность ошибок первого рода (*FRR*) и второго рода (*FAR*) рассчитываются через функцию стандартного нормального распределения $\Phi(\cdot)$:

$$\alpha(t) = P(D > t / H_0) = 1 - \Phi\left(\frac{t - \mu_0}{\sigma_0}\right),$$

$$\beta(t) = P(D \leq t / H_1) = \Phi\left(\frac{t - \mu_1}{\sigma_1}\right).$$

Выбор порога t^*, как правило, производится на основе точки равных ошибок (*EER*) из условия $\alpha(t) = \beta(t)$. Минимальное значение *EER* характеризует максимальную эффективность выбранного набора атрибутов.

Для адаптации к медленным изменениям поведения эталонный вектор обновляется при каждой успешной аутентификации по правилу экспоненциального сглаживания:

$$v_{new} = (1 - \lambda) v_{old} + \lambda u, \lambda \in [0,1],$$

где λ – коэффициент скорости обучения.

Пересчёт весов w производится накопительно (каждые 10–50 сессий), порога t – редко или при существенном изменении структуры весов w.

Инициализация модели проходит в четыре этапа:

1. Накопление первичной выборки: сбор m измерений $\{u^1, \ldots, u^m\}$.
2. Формирование первичного эталона: $v_0 = \frac{1}{m} \sum_{k=1}^{m} u^k$.
3. Определение начальных весов и порога: $w_i = \frac{1}{n}$, порог t устанавливается завышенным для снижения *FRR* на этапе обучения.
4. Переход в рабочий режим: после стабилизации дисперсий σ_i^2 активируется стандартный режим аутентификации.

Таким образом, базовая модель предполагает, что отклонения под гипотезой H_1 формируются пассивно (естественные различия между разными пользователями) или стохастически (рандомизация путем применения пользователем мер анонимизации). В следующем разделе данная модель расширяется на случай целевых оптимизационных атак, при которых злоумышленник целенаправленно минимизирует расстояние между входным вектором и эталонным в условиях ограничений на модификацию атрибутов.

4. Адверсариальное расширение модели адаптивной аутентификации

Гибридный цифровой отпечаток структурно разделяется на техническую и поведенческую компоненты: $u = (u^{(d)}, u^{(b)})$, $v = (v^{(d)}, v^{(b)})$, $w = (w^{(d)}, w^{(b)})$ (индексы (d) и (b) – множества индексов технических (T) и поведенческих (B) атрибутов соответственно. Взвешенная мера отклонения принимает вид:

$$d(u, v) = \sum_{i \in T} w_i \gamma_i(u_i, v_i) + \sum_{j \in B} w_j \gamma_j(u_j, v_j).$$

Атакующий формирует поддельный вектор $\bar{u}$, решая задачу минимизации дистанции до эталона:

$$\bar{u}^* = argmin_{\bar{u}} \; d(\bar{u}, v),$$

при соблюдении ограничений на модификацию атрибутов:

$$\begin{cases} \left\| \bar{u}^{(d)} - u_0^{(d)} \right\|_p \le \varepsilon_d, \\ \left\| \bar{u}^{(b)} - u_0^{(b)} \right\|_q \le \varepsilon_b, \\ \bar{u}^{(d)} \in C_d, \; \bar{u}^{(b)} \in C_b, \end{cases}$$

где

u_0 – исходный вектор атрибутов злоумышленника;

ε_d, ε_b – величины допустимых возмущений для модификации технических и поведенческих атрибутов (доли атрибутов, которые злоумышленник может изменить относительно своего исходного вектора);

p, q – нормы изменения технических и поведенческих атрибутов;

C_d, C_b – множества технически реализуемых и поведенчески правдоподобных значений наборов признаков.

В реальных системах аутентификации детальная обратная связь о причинах отказа не предоставляется в целях безопасности. В данной работе рассматривается постановка с чёрным ящиком, при которой атакующий имеет доступ только к решениям системы о том, разрешён ли доступ или запрещён. Для минимизации $d(\bar{u}, v)$ в таких условиях применяются градиент-независимые методы оптимизации (эволюционные стратегии, байесовская оптимиза-

ция и др.), что увеличивает требуемое количество запросов злоумышленника к системе без изменения сути задачи условной оптимизации.

При успешном решении задачи оптимизации параметры распределения отклонения под гипотезой H_1 смещаются:

$$\mu_1 \to \mu_1^* = E\left(d\left(\bar{u}^*, v\right) | H_1\right),$$
$$\sigma_1^2 \to \sigma_1^{*2} = D\left(d\left(\bar{u}^*, v\right) | H_1\right).$$

Вероятность ошибки второго рода становится функцией допустимых возмущений атаки и текущего вектора весов:

$$\beta^*\left(t,\ \varepsilon_d, \varepsilon_b; w\right) = \Phi\left(\frac{t - \mu_1^*}{\sigma_1^*}\right).$$

Чем меньше μ_1^* при фиксированном t, тем выше вероятность успешного обхода аутентификации.

Стандартные метрики качества аутентификации (*FAR*, *FRR*, *EER*) рассчитываются при фиксированных распределениях признаков и не учитывают целенаправленное смещение этих распределений злоумышленником. В имеющейся постановке эффективность системы явно зависит от величин допустимых возмущений (ε_d, ε_b), что делает статические показатели недостаточными. Для преодоления ограничений вводится вероятностная мера устойчивости R, которая учитывает допустимые возмущения атаки и текущий вектором весов, а в предельном случае отсутствия возмущений ($\varepsilon_d = \varepsilon_b = 0$) согласуется с классическим показателем $1 - \beta$:

$$R\left(\varepsilon_d, \varepsilon_b; w\right) = 1 - \beta^*\left(t,\ \varepsilon_d, \varepsilon_b; w\right) = P\left(d\left(\bar{u}^*, v\right) > t\right).$$

R отражает вероятность того, что даже оптимально сконструированный атакующим вектор будет отклонён системой. Порог t фиксируется на основе *EER*, вычисленного по пассивному распределению признаков. Это позволяет оценивать устойчивость модели к целевым возмущениям при сохранении стандартного баланса ошибок $\alpha = \beta$ в обычном режиме. Механизм адаптации весов, предложенный в базовой модели, обеспечивает защиту от целевых оптимизационных атак. При попытках активной подмены технических атрибутов ($\varepsilon_d \to max$) их дисперсия σ_i^2 возрастает, что автоматически снижает соответствующие веса $w_i^{(d)}$. Одновременно веса поведенческих атрибутов $w_j^{(b)}$ увеличиваются. Поскольку на практике $\varepsilon_b \ll \varepsilon_d$, задача минимизации $d\left(\bar{u}^*, v\right)$ становится существенно сложнее, а значение R возрастает.

Таким образом, оценка устойчивости модели аутентификации сводится к анализу зависимости $R\left(\varepsilon_d, \varepsilon_b; w(\tau)\right)$ при различных стратегиях оптимизационных атак (τ – момент начала атаки, например, номер сессии, определяющий текущее состояние весов признаков).

5. Экспериментальное моделирование атак

Проведём количественную оценку устойчивости модели адаптивной аутентификации к целевым оптимизационным атакам имитации гибридного цифрового отпечатка в условиях ограниченной обратной связи, что предполагает выполнение следующих действий:

1. Сравнение вероятностной меры устойчивости R для статической и адаптивной стратегий взвешивания признаков.
2. Анализ влияния величин допустимых возмущений (ε_d, ε_b) на эффективность обхода системы злоумышленником.
3. Исследование динамики перераспределения весов в условиях итерационных целевых оптимизационных атак.
4. Оценка компромисса между устойчивостью к атакам β^* и удобством для легитимного пользователя α.

Эксперимент проводился на собственном датасете, сформированном с участием 32 пользователей. Для каждого участника зафиксировано по 40 сессий взаимодействия с тестовым веб-интерфейсом, что даёт общую выборку из 1 280 сессий.

Гибридный цифровой отпечаток формируется на основе 30 идентификационных атрибутов, сгруппированных по пяти источникам данных для базовой модели, в соответствии с Таблицей 1. Признаки разделены на технические (20 атрибутов) и поведенческие (10 атрибутов) в соответствии с рассмотренной постановкой задачи.

Таблица 1. Группы признаков гибридного цифрового отпечатка

Группа	Признаки	Тип данных	Множество данных	Источник
Браузерные	userAgent, platform, language, languages, webdriver, acceptLanguage, screenWidth, screenHeight, devicePixelRatio	Строки, числа, булевы	T	fingerprint-generator [21]
Сетевые	ip, port, dns, traffic.sent, traffic.received, traffic.total	Строки, числа	T	Синтетическая генерация
Аппаратные	hardwareConcurrency, deviceMemory, gpu, gpuVendor, fontsCount	Числа, строки	T	Синтетическая генерация
Журналы событий	sessionDuration, requestsCount, pagesLoaded, errorsCount, sessionStartHour	Числа	B	Синтетическая генерация
Поведенческие	clicks, scrollDepth, pagesVisited, avgTimePerPage, bounce	Числа, булевы	B	Синтетическая генерация

Браузерные атрибуты собирались с помощью открытой библиотеки fingerprint-generator [20], которая эмулирует реальные браузерные окружения и генерирует согласованные наборы признаков (например, совместимые комбинации userAgent с platform и screenWidth).

Остальные признаки генерировались синтетически с помощью собственного Python-скрипта, обеспечивающего реалистичность распределений (параметры генерации (среднее, дисперсия, корреляции) калибровались с учётом результатов эмпирических исследований [22–25]), семантическую согласованность (например, deviceMemory коррелирует с hardwareConcurrency, sessionDuration влияет на pagesLoaded, scrollDepth ограничен диапазоном [0,1]), поведенческую правдоподобность.

Результирующий датасет сохранён в формате JSON, где каждая сессия представлена объектом с 30 атрибутами, как на рисунке 1.

Рис. 1. Структура сессии пользователя в формате JSON

Этап 1. Подготовка данных.

Все признаки обрабатываются дифференцированно в зависимости от типа для обеспечения семантически корректного вычисления отклонения. Непрерывные признаки (например, sessionDuration) дискретизируются по равномерным интервалам с $Q_i = 100$. Бинарные признаки (например, webdriver) отображаются в $\{0,1\}$. Категориальные атрибуты (например, userAgent) сохраняют свои номинальные значения. Таким образом, вклад каждого признака в метрику близости входного вектора к эталонному нормирован к отрезку $[0,1]$.

Для каждого пользователя эталонный вектор v формируется на основе первых 20 сессий, оставшиеся 20 сессий используются для тестирования и моделирования атак. Дисперсии σ_i^2 и разделительные способности S_i вычисляются на обучающей подвыборке и обновляются в процессе адаптации.

Этап 2. Моделирование атак.

Атаки генерировались путём решения задачи условной оптимизации. В соответствии с постановкой, что атакующий имеет доступ только к информации о доступе. Для минимизации $d(\bar{u}, v)$ использован алгоритм *Covariance Matrix Adaptation Evolution Strategy (CMA-ES)* [26], адаптированный для смешанного непрерывно-дискретного пространства признаков.

Максимальное число запросов ограничено $Q_{max} = 400$, что имитирует стандартные ограничения частоты запросов в реальных системах.

При генерации атакующих векторов $\vec{u}^*$ множества C_d и C_b формируются с учётом семантики признаков:

– для браузерных допустимы только значения из заранее собранного словаря реальных комбинаций операционных систем и браузеров;

– для сетевых атрибутов вводятся структурные и логические ограничения: валидные форматы IP-адресов, диапазон эфемерных портов для клиентских соединений, корреляция DNS с подсетью IP;

– для аппаратных признаков накладываются ограничения совместимости (например, определённая модель GPU не может сочетаться с низким deviceMemory);

– для поведенческих признаков вводятся ограничения на производные и временные корреляции, обеспечивающие правдоподобность поведения. При этом атрибуты журналов логов обладают меньшей «стоимостью» подмены, чем атрибуты поведенческих моделей, что отражено в дифференцированных ограничениях нормы возмущений для подгрупп B.

Целевые оптимизационные атаки проходят в рамках одной из четырёх стратегий, представленных в Таблице 2.

Таблица 2. Стратегии целевых оптимизационных атак в эксперименте

Стратегия	ε_d	ε_b	Описание
S_1	0.10–0.19	0.05–0.09	Пассивное изменение признаков путём рандомизации мерами анонимизации
S_2	0.50–0.90	0.05–0.09	Целевая подмена технических атрибутов при сохранении своего поведения
S_3	0.20–0.30	0.10–0.20	Гибридная оптимизация признаков обоих типов с учётом корреляций
S_4	Динамический рост от 0.10 к 0.90	Динамический рост от 0.05 к 0.30	Адаптивная итерационная атака: постепенное увеличение величин допустимых возмущений в ответ на пересчёт весов

Сравнивались три вида моделей аутентификации:

1. Модель C_1 аутентификации с фиксированными весами $w_i = \frac{1}{n}$ без адаптации эталона.
2. Модель C_2 аутентификации с адаптивными весами без учета понижающих коэффициентов и адаптацией эталона при $\lambda = 0.05$.
3. Предлагаемая модель C_3 аутентификации с адаптивными весами с понижающими коэффициентами, адаптацией эталона при $\lambda = 0.05$ и пересчёте весов.

6. Результаты эксперимента и обсуждение

По окончанию проведения экспериментов получены следующие результаты.

На Рисунке 2 представлена зависимость устойчивости R моделей аутентификации от величины допустимого возмущения технических признаков ε_d при фиксированном $\varepsilon_b = 0.15$ для 100 испытаний.

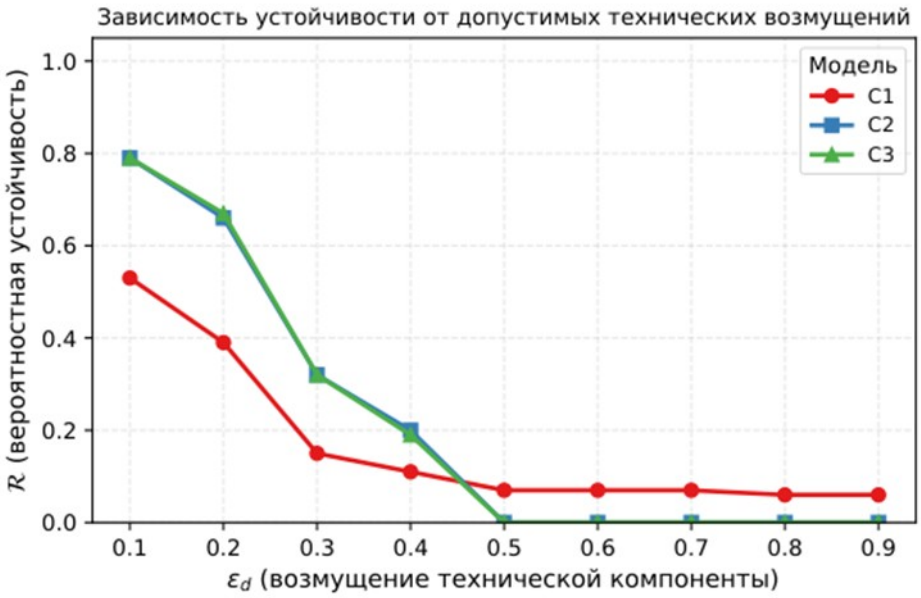

Рис. 2. Зависимость $R(\varepsilon_d)$ при $\varepsilon_b = 0.15$ для моделей C_1, C_2, C_3

Модели адаптивной аутентификации C_2 и C_3 обеспечивают двукратное повышение устойчивости относительно модели C_1 в зоне реалистичных атак при $\varepsilon_d \le 0.2$ ($R = 0.66 - 0.79$ для C_2, C_3; $R = 0.39 - 0.53$ для C_1. При $\varepsilon_d \ge 0.5$ наблюдается $R \le 0.07$, означающее, что при достаточном наборе средств злоумышленник может успешно имитировать легитимный профиль. Небольшое превышение R для модели C_1 в области $\varepsilon_d \ge 0.5$ объясняется следующим: равномерное распределение весов в C_1 приводит к тому, что даже при большой величине допустимых технических возмущений атакующий может случайно не затронуть критически важные для данной сессии признаки. В моделях C_2 и C_3 веса сконцентрированы на наиболее информативных признаках, поэтому при их успешной подмене атака гарантированно проходит $R = 0$. Различие между устойчивостью для моделей C_2 и C_3 находится в пределах статистической погрешности, подтверждая доминирующую роль механизма адаптивного взвешивания.

В Таблице 3 показана зависимость устойчивости R от величины допустимых поведенческих возмущений ε_b при фиксированной величине допустимых технических возмущений $\varepsilon_d = 0.2$.

Таблица 3. Значения устойчивости R для моделей C_1, C_2, C_3 при $\varepsilon_d = 0.2$ и варьируемом ε_b

ε_b	$R(C_1)$	$R(C_2)$	$R(C_3)$
0.05	0.32	0.62	0.65
0.10	0.40	0.66	0.68
0.15	0.22	0.66	0.68
0.20	0.22	0.66	0.66

Модель C_1 показывает низкую устойчивость ($0.22 \le R \le 0.40$), что указывает на высокую чувствительность к подмене поведенческих признаков. Модели адаптивной аутентификации C_2 и C_3 обеспечивают стабильно высокие значения устойчивости ($0.62 \le R \le 0.66$), что соответствует повышению вероятности отражения атаки в 1.5–1.7 раза относительно C_1. При этом различие между C_2 и C_3 находится в пределах статистической погрешности ±0.03, что свидетельствует о доминирующей роли механизма адаптивного взвешивания в обеспечении

устойчивости, тогда как использование понижающих коэффициентов для учета корреляций даёт дополнительный, но не критический вклад в данной стратегии

На Рисунке 3 показана динамика перераспределения суммарных весов технических W_d и поведенческих W_b признаков в условиях целевых оптимизационных атак по стратегии S_4.

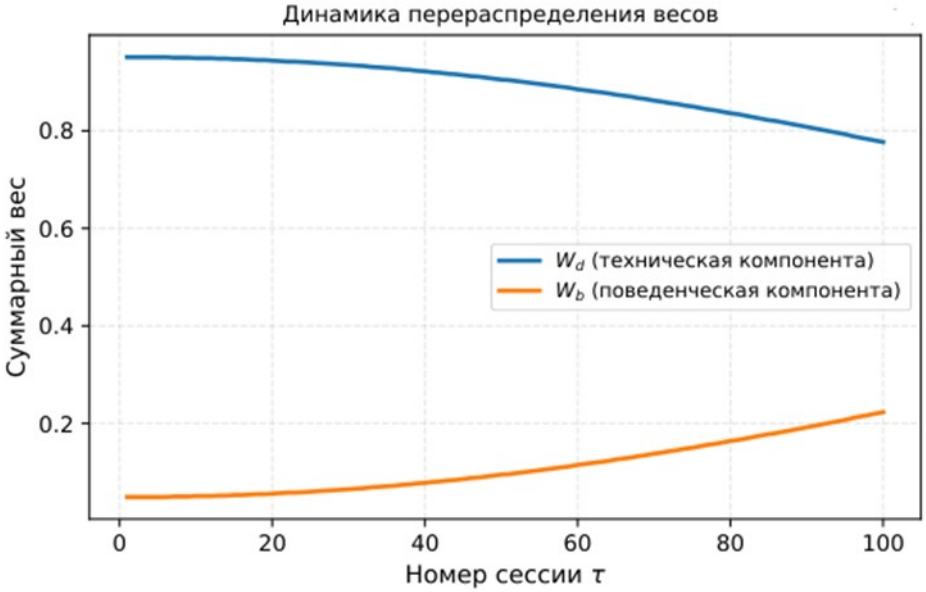

Рис. 3. Динамика суммарных весов W_d и W_b при атаках стратегии S_4

По мере роста величины допустимых технических возмущений ε_d система снижает доверие к технической компоненте, что подтверждается снижением W_d от 0.95 к 0.78, перераспределяя значимость на более устойчивые поведенческие признаки, повышая W_b от 0.05 до 0.22. Данный механизм затрудняет злоумышленнику целенаправленную оптимизацию признаков, уже утративших значимость для системы.

На Рисунке 4 представлены ROC-кривые для оценки компромисса между устойчивостью к атакам β^* и удобством для легитимного пользователя α в условиях стратегии S_3. Для обеспечения сопоставимости метрик β^* и R между моделями C_1, C_2, C_3 оценка устойчивости проводилась при фиксированном пороге принятия решения $t = 0.25$, что исключает погрешности автоматического сдвига EER в моделях адаптивной аутентификации.

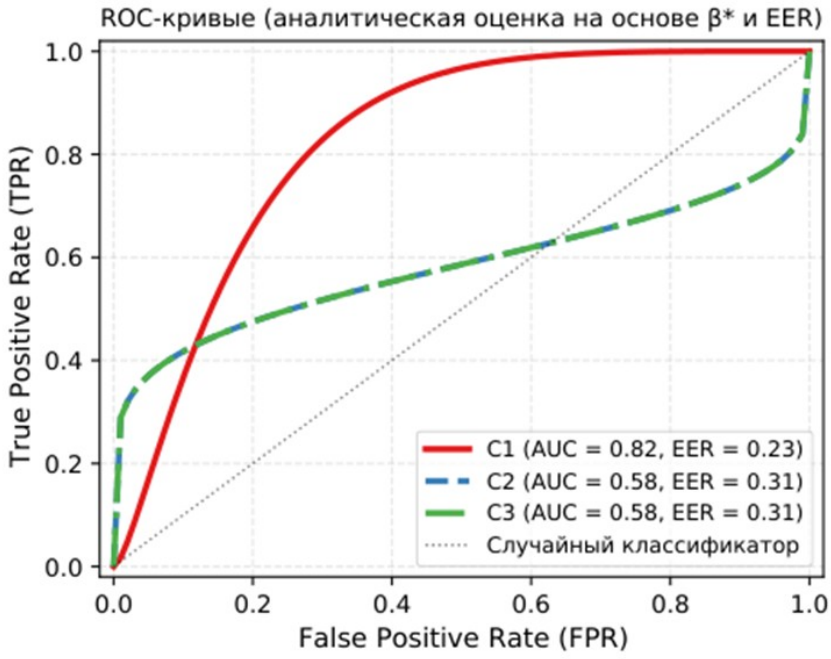

Рис. 4. ROC-кривые для моделей C_1, C_2, C_3 при атаках стратегии S_3

Оценки качества аутентификации моделей при пороге, установленном с учетом *EER*, приведены в Таблице 4.

Таблица 4. Оценки качества аутентификации моделей

Модель	**EER**	$\beta^*(S_3)$	$R(S_3)$
C_1	0.23	0.66	0.34
C_2	0.31	0.36	0.64
C_3	0.31	0.36	0.64

Из Рисунка 4 и Таблицы 4 следует, что модель C_1 в спокойном (пассивном) режиме чётко отделяет легитимных пользователей от чужих с $AUC = 0.82$, $EER = 0.23$, однако модели адаптивной аутентификации C_2 и C_3 обеспечивают статистически значимое повышение устойчивости к целевым атакам, что подтверждается $\beta^* = 0.36$ против 0.66 при C_1. Данный компромисс согласуется с теоретическими ожиданиями: перераспределение весов на более устойчивые признаки затрудняет оптимизацию злоумышленнику, даже если это незначительно снижает чистоту разделения в спокойном режиме. Снижение показателя *AUC* для моделей C_2 и C_3 (0.58 против 0.82 у C_1) показывает, что перераспределение весов на признаки с высокой «стоимостью» имитации намеренно снижает чистоту разделения распределений в пассивном режиме, однако обеспечивает почти двукратное снижение вероятности успешной атаки ($\beta^* = 0.36$ против 0.66), что обосновано при стратегиях злоумышленника с целевыми оптимизационными атаками.

Проведённые эксперименты подтверждают высокую эффективность адаптивного взвешивания, реализуемого в модели C_3. Автоматическое снижение весов w_i атрибутов при росте их дисперсии σ_i^2 вынуждает злоумышленника оптимизировать признаки, уже утратившие значимость для системы. Пересчёт весов признаков и эталонного профиля требует $O(n^2)$ операций на сессию с 30 признаками и может выполняться в фоновом режиме без влияния на задержку процесса аутентификации. Установленные границы применимости модели показывают, что она сохраняет $R \geq 0.6$ при величинах допустимых возмущений

$\varepsilon_d, \varepsilon_b \le 0.2$. При возмущениях $\varepsilon_d \ge 0.5$ наблюдается неустойчивость для всех моделей аутентификации ($R \le 0.07$), что требует дополнительной многофакторной аутентификации.

Таким образом, экспериментально подтверждено, что предложенное адверсариальное расширение модели адаптивной аутентификации позволяет количественно оценивать устойчивость через метрику R и снизить вероятность успешной целевой оптимизационной атаки при сохранении высокой устойчивости.

Заключение

В работе решена задача анализа устойчивости модели адаптивной аутентификации к целевым оптимизационным атакам на гибридный цифровой отпечаток. Атака имитации формализована как задача условной оптимизации с раздельными величинами допустимых возмущений ε_d и ε_b, учитывающая технические и поведенческие ограничения на модификацию атрибутов, что обеспечивает реалистичность модели угрозы в постановке с чёрным ящиком. Для количественной оценки защищённости введена вероятностная мера устойчивости R, зависящая от допустимых возмущений и весового вектора. В предельном случае отсутствия атаки при $\varepsilon_d = \varepsilon_b = 0$ метрика согласуется с классическим показателем $1 - FAR$.

Экспериментальное подтверждение проведено на датасете из 1280 сессий (30 признаков, 5 семантических групп) путём моделирования четырёх стратегий поведения злоумышленника при атаках с использованием алгоритма *CMA-ES*. Результаты подтвердили высокую эффективность предлагаемой модели: она обеспечивает двукратное повышение устойчивости относительно модели C_1 со статическими весами признаков $0.66 \le R \le 0.79$ при величине допустимых возмущений технических атрибутов $\varepsilon_d \le 0.2$ и снижает вероятность успешной атаки до $\beta^* = 0.36$ в условиях целевых оптимизационных атак по стратегии S_3. Экспериментально подтверждено, что автоматическое снижение весов признаков при росте их дисперсии позволяет оперативно переносить значимость на поведенческие атрибуты с высокой стоимостью правдоподобной имитации, тем самым затрудняя целевую оптимизацию злоумышленником. Установленные границы применимости показывают, что модель сохраняет $R \ge 0.6$ при величинах допустимых возмущений ε_d, $\varepsilon_b \le 0.2$, а при высокой доле технических возмущений ($\varepsilon_d \ge 0.5$) система аутентификации требует обязательного дополнения многофакторной аутентификацией, поскольку становится неустойчивой ($R \le 0.07$).

Перспективы дальнейших исследований связаны с экспериментальным оцениванием модели на полностью реальных производственных датасетах и дальнейшим развитием модели путём интеграции элементов машинного обучения.

Литература

1. *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.
2. *Саломатин А. А.*, *Лукинова О. В.* Теоретические основы адаптации легитимизации пользователя на основе динамики вектора атрибутов цифрового отпечатка // Известия Юго-западного государственного университета. 2026.
3. *Bonneau J.*, *Herley C.*, *van Oorschot P. C.*, *Stajano F.* Passwords and the Evolution of Imperfect Authentication // Communications of the ACM. 2015. Vol. 58, no. 7. P. 78–87.
4. *Bonneau J.*, *Herley C.*, *van Oorschot P. C.*, *Stajano F.* The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes // IEEE Symposium on Security and Privacy. San Francisco, CA, USA. 2012. P. 553–567. DOI: 10.1109/SP.2012.44.

5. *Das A.*, *Bonneau J.*, *Caesar M.*, *Borisov N.*, *Wang X.* The Tangled Web of Password Reuse // Proceedings of the Network and Distributed System Security Symposium. 2014. DOI: 10.14722/ndss.2014.23357.
6. *Juels A.*, *Rivest R.* Honeywords: Making Password-Cracking Detectable // Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security. 2013. P. 145–160. DOI: 10.1145/2508859.2516671.
7. *Eberz S.*, *Rasmussen K. B.*, *Lenders V.*, *Martinovic I.* Evaluating Behavioral Biometrics for Continuous Authentication: Challenges and Metrics // Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. 2017. P. 386–399. DOI: 10.1145/3052973.3053032.
8. *Viswanath B.*, *Bashir M. A.*, *Crovella M., Guha S.*, *Gummadi K. P.*, *Krishnamurthy B.*, *Mislove A.* Towards Detecting Anomalous User Behavior in Online Social Networks // USENIX Security Symposium. 2014. P. 223–238.
9. *Monrose F.*, *Rubin A.* Authentication via Keystroke Dynamics // Proceedings of the 4th ACM Conference on Computer and Communications Security. 1997. P. 48–56. DOI: 10.1145/266420.266434.
10. *Killourhy K.*, *Maxion R.* Comparing Anomaly Detection Algorithms for Keystroke Dynamics // IEEE/IFIP International Conference on Dependable Systems and Networks. Lisbon, Portugal. 2009. P. 125–134. DOI: 10.1109/DSN.2009.5270346.
11. *Shen C.*, *Cai Z.*, *Guan X.*, *Maxion R.* Performance Evaluation of Anomaly-Detection Algorithms for Mouse Dynamics // Computers & Security. 2014. Vol. 45. P. 156–171. DOI: 10.1016/j.cose.2014.05.002.
12. *Serwadda A.*, *Phoha V.* When Kids' Toys Breach Mobile Phone Security // Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security. 2013. P. 599–610. DOI: 10.1145/2508859.2516659.
13. *Biggio B.*, *Roli F.* Wild Patterns: Ten Years after the Rise of Adversarial Machine Learning // Pattern Recognition. 2018. Vol. 84. P. 317–331. DOI: 10.1016/j.patcog.2018.07.023.
14. *Goodfellow I. J.*, *Shlens J.*, *Szegedy C.* Explaining and Harnessing Adversarial Examples // arXiv. 2015. DOI: 10.48550/arXiv.1412.6572.
15. *Papernot N. et al.* Practical Black-Box Attacks Against Machine Learning // Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. 2017. P. 506–519. DOI: 10.1145/3052973.3053009.
16. *Sommer R.*, *Paxson V.* Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // IEEE Symposium on Security and Privacy. Oakland, CA, USA. 2010. P. 305–316. DOI: 10.1109/SP.2010.25.
17. *Dalvi N. et al.* Adversarial Classification // Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2004. P. 99–108. DOI: 10.1145/1014052.1014066.
18. *Li B.*, *Vorobeychik Y.* Scalable Optimization of Randomized Operational Decisions in Adversarial Classification Settings // Proceedings of the Eighteenth International Conference on Artificial Intelligence and Statistics. 2015. Vol. 38. P. 599–607.
19. *Barreno M. et al.* The Security of Machine Learning // Machine Learning. 2010. Vol. 81. P. 121–148. DOI: 10.1007/s10994-010-5188-5.
20. *Chandola V. et al.* Anomaly Detection: A Survey // ACM Computing Surveys. 2009. Vol. 41, No. 3. Article 15. P. 1–58. DOI: 10.1145/1541880.1541882.
21. Apify. fingerprint-generator: Realistic browser fingerprint generator [Электронный ресурс]. 2024. URL: https://github.com/apify/fingerprint-generator (дата обращения: 06.04.2026).
22. *Andriamilanto N.*, *Allard T.*, *Le Guelvouit G.*, *Garel A.* A Large-scale Empirical Analysis of Browser Fingerprints Properties for Web Authentication // ACM Transactions on the Web. 2021. Vol. 16, No. 1. Art. 4. DOI: 10.1145/3478026.

23. *Barford P.*, *Crovella M.* Generating Representative Web Workloads for Network and Server Performance Evaluation // Proceedings of the 1998 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems. 1998. P. 151–160.
24. *Weinreich H.*, *Obendorf H.*, *Herder E.*, *Mayer H.* Not Quite the Average: An Empirical Study of Web Use // ACM Transactions on the Web. 2008. Vol. 2, No. 1. Art. 5. P. 1–31. DOI: 10.1145/1326561.1326566
25. *Zhang Y.*, *Chen W.*, *Wang D.*, *Yang Q.* User-click Modeling for Understanding and Predicting Search-Behavior // KDD '11: Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. San Diego, CA, USA, 2011. P. 1388–1396. DOI: 10.1145/2020408.2020613
26. *Hansen N.* The CMA Evolution Strategy: A Tutorial // arXiv preprint arXiv:1604.00772. 2016.

Саломатин Александр Александрович
к.т.н., старший научный сотрудник, Институт проблем управления им. В. А. Трапезникова РАН (ИПУ РАН, 117342, г. Москва, ул. Профсоюзная, д. 65, стр. 2), тел. +7 917 588-90-89, e-mail: sandr@ipu.ru, ORCID ID: 0000-0002-1143-5275.

Широков Александр Сергеевич
научный сотрудник, Институт проблем управления им. В. А. Трапезникова РАН (ИПУ РАН, 117342, г. Москва, ул. Профсоюзная, д. 65, стр. 2), тел. +7 495 198-17-20, e-mail: shiras@ipu.ru, ORCID ID: 0000-0002-8049-851X.

Мельников Андрей Кимович
к.т.н., доцент ВАК, главный научный сотрудник, АО «Вычислительные решения» (117587, город Москва, Варшавское ш, д. 125), тел. +7 495 287-00-35, e-mail: ak@comp-sol.ru.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Analysis of the resilience of the adaptive authentication model to adversarial attacks via hybrid digital fingerprint imitation

Aleksandr A. Salomatin[1], Aleksandr A. Shirokov[1], A. K. Melnikov[2]

[1] V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences (ICS RAS)
[2] SC «Computing solutions», Moscow, Russia

Abstract: The article investigates the resilience of the adaptive authentication model to adversarial attacks via hybrid digital fingerprint imitation. An adversarial extension of the adaptive authentication model based on a digital fingerprint combining technical and behavioral attributes is proposed. The attack is formalized as a conditional optimization problem with separate values of permissible perturbations of technical (ε_d) and behavioral (ε_b) attributes under conditions of limited feedback. To evaluate model resilence, a probabilistic resilience measure R is introduced, consistent with the classical FAR/FRR metrics. Experimental validation was performed on a dataset of 1280 sessions (32 users, 30 attributes) using the CMA-ES algorithm. The experimental results showed that models with adaptive weighting provide a twofold increase in resilience compared to the model with equal weights in the realistic attack regime

$(\varepsilon_d \le 0.2)$: $R = 0.66 - 0.79$ versus 0.39–0.53, and reduce the probability of a successful attack to 0.36 under a strategy for optimizing technical and behavioral features. It has been experimentally established that the automatic reduction of weights with an increase in the variance of features complicates adversarial attacks by attackers. The identified security vulnerability at $\varepsilon_d \ge 0.5$ $(R \le 0.07)$ defines the limits of the model's applicability and justifies the need for multifactor authentication with a high proportion of perturbations.

Keywords: hybrid digital fingerprint; adaptive authentication; adversarial attacks; authentication resilience; behavioral biometrics, cybersecurity.

For citation: Salomatin A. A., Shirokov A. S., Melnikov A. K. Analysis of the resilience of the adaptive authentication model to targeted optimization at-tacks of hybrid digital fingerprint simulation. *Vestnik SibGUTI*, 2026, vol. 20, no. 2, pp. 28-44. https://doi.org/10.55648/1998-6920-2026-20-2-28-44.

The article was submitted: 10.04.2026;
revised version: 17.04.2026;
accepted for publication 05.05.2026.

References

1. Vekhov V. B., Smushkin A. B. Kriminalisticheskoe issledovanie tsifrovykh otpechatkov komp'yuternykh ustroistv [Forensic Investigation of Digital Fingerprints of Computer Devices]. *Vserossiiskii kriminologicheskii zhurnal*, 2024, vol. 18, no. 4, pp. 390–397. DOI: 10.17150/2500-4255.2024.18(4).390-397.
2. Salomatin A. A., Lukinova O. V. Teoreticheskie osnovy adaptatsii legitimizatsii pol'zovatelya na osnove dinamiki vektora atributov tsifrovogo otpechatka [Theoretical Foundations of User Legitimization Adaptation Based on Digital Fingerprint Attribute Vector Dynamics]. *Izvestiya Yugo-zapadnogo gosudarstvennogo universiteta*, 2026, in press.
3. Bonneau J., Herley C., van Oorschot P. C., Stajano F. Passwords and the evolution of imperfect authentication. *Communications of the ACM*, 2015, vol. 58, no. 7, pp. 78–87.
4. Bonneau J., Herley C., van Oorschot P. C., Stajano F. The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. *IEEE Symposium on Security and Privacy*, San Francisco, CA, USA, 2012, pp. 553–567. DOI: 10.1109/SP.2012.44.
5. Das A., Bonneau J., Caesar M., Borisov N., Wang X. The tangled web of password reuse. *Proceedings of the Network and Distributed System Security Symposium*, 2014. DOI: 10.14722/ndss.2014.23357.
6. Juels A., Rivest R. Honeywords: making password-cracking detectable. *Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security*, 2013, pp. 145–160. DOI: 10.1145/2508859.2516671.
7. Eberz S., Rasmussen K. B., Lenders V., Martinovic I. Evaluating behavioral biometrics for continuous authentication: challenges and metrics. *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 2017, pp. 386–399. DOI: 10.1145/3052973.3053032.
8. Viswanath B., Bashir M. A., Crovella M., Guha S., Gummadi K. P., Krishnamurthy B., Mislove A. Towards detecting anomalous user behavior in online social networks. *USENIX Security Symposium*, 2014, pp. 223–238.
9. Monrose F., Rubin A. Authentication via keystroke dynamics. *Proceedings of the 4th ACM Conference on Computer and Communications Security*, 1997, pp. 48–56. DOI: 10.1145/266420.266434.
10. Killourhy K., Maxion R. Comparing anomaly detection algorithms for keystroke dynamics. *IEEE/IFIP International Conference on Dependable Systems and Networks*, Lisbon, Portugal, 2009, pp. 125–134. DOI: 10.1109/DSN.2009.5270346.
11. Shen C., Cai Z., Guan X., Maxion R. Performance evaluation of anomaly-detection algorithms for mouse dynamics. *Computers & Security*, 2014, vol. 45, pp. 156–171. DOI: 10.1016/j.cose.2014.05.002.

12. Serwadda A., Phoha V. When kids' toys breach mobile phone security. *Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security*, 2013, pp. 599–610. DOI: 10.1145/2508859.2516659.
13. Biggio B., Roli F. Wild patterns: ten years after the rise of adversarial machine learning. *Pattern Recognition*, 2018, vol. 84, pp. 317–331. DOI: 10.1016/j.patcog.2018.07.023.
14. Goodfellow I. J., Shlens J., Szegedy C. Explaining and harnessing adversarial examples. *arXiv*, 2015. DOI: 10.48550/arXiv.1412.6572.
15. Papernot N., et al. Practical black-box attacks against machine learning. *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 2017, pp. 506–519. DOI: 10.1145/3052973.3053009.
16. Sommer R., Paxson V. Outside the closed world: on using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 2010, pp. 305–316. DOI: 10.1109/SP.2010.25.
17. Dalvi N., et al. Adversarial classification. *Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2004, pp. 99–108. DOI: 10.1145/1014052.1014066.
18. Li B., Vorobeychik Y. Scalable optimization of randomized operational decisions in adversarial classification settings. *Proceedings of the Eighteenth International Conference on Artificial Intelligence and Statistics*, 2015, vol. 38, pp. 599–607.
19. Barreno M., et al. The security of machine learning. *Machine Learning*, 2010, vol. 81, pp. 121–148. DOI: 10.1007/s10994-010-5188-5.
20. Chandola V., et al. Anomaly detection: a survey. *ACM Computing Surveys*, 2009, vol. 41, no. 3, Article 15, pp. 1–58. DOI: 10.1145/1541880.1541882.
21. Apify. Fingerprint-generator: realistic browser fingerprint generator. Available at: `https://github.com/apify/fingerprint-generator` (accessed: 06.04.2026).
22. Andriamilanto N., Allard T., Le Guelvouit G., Garel A. A large-scale empirical analysis of browser fingerprints properties for web authentication. *ACM Transactions on the Web*, 2021, vol. 16, no. 1, Art. 4. DOI: 10.1145/3478026.
23. Barford P., Crovella M. Generating representative web workloads for network and server performance evaluation. *Proceedings of the 1998 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems*, 1998, pp. 151–160.
24. Weinreich H., Obendorf H., Herder E., Mayer H. Not quite the average: an empirical study of web use. *ACM Transactions on the Web*, 2008, vol. 2, no. 1, Art. 5, pp. 1–31. DOI: 10.1145/1326561.1326566.
25. Zhang Y., Chen W., Wang D., Yang Q. User-click modeling for understanding and predicting search-behavior. *KDD '11: Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Diego, CA, USA, 2011, pp. 1388–1396. DOI: 10.1145/2020408.2020613.
26. Hansen N. The CMA evolution strategy: a tutorial. *arXiv preprint* arXiv:1604.00772, 2016.

Aleksandr A. Salomatin

Cand. of Sci. (Engineering), senior researcher, V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences (ICS RAS, Russia, 117997, Moscow, Profsoyuznaya street, 65), phone: +7 817 588-90-89, e-mail: `sandr@ipu.ru`, ORCID ID: 0000-0002-1143-5275.

Aleksandr A. Shirokov

Researcher, V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences (ICS RAS, Russia, 117997, Moscow, Profsoyuznaya street, 65), phone: +7 495 198-17-20, e-mail: `shiras@ipu.ru`, ORCID ID: 0000-0002-8049-851X.

Andrey K. Melnikov

Cand. of Sci. (Engineering), Associate professor of SAC, chief research officer, SC “Computing solutions (Russia, 117587, Moscow, Varshavskoe sh, 125), phone: +7 495 287-00-35, e-mail: `ak@comp-sol.ru`.