

УДК 004.056.5

Литвинов Алексей Сергеевич

Аспирант

Litvinov A.S.

E-mail: litvinlex1@gmail.com

Астахова Татьяна Николаевна

Заведующая кафедрой «Информационные
системы и технологии»

Astakhova T.N.

E-mail: ctn_af@mail.ru

Нижегородский государственный инженерно-
экономический университет

Nizhny Novgorod State University of
Engineering and Economics

Нижегородская обл., г. Княгинино,
ул. Октябрьская, д. 22А, Россия, 606340

Тел: +7 (83166) 4-15-50

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ НЕПРЕРЫВНОЙ ВЕРОЯТНОСТНОЙ ОЦЕНКИ ДОСТОВЕРНОСТИ ЦИФРОВОЙ ИДЕНТИЧНОСТИ ПОЛЬЗОВАТЕЛЯ

CONCEPTUAL MODEL FOR CONTINUOUS PROBABILISTIC ASSESSMENT OF THE AUTHENTICITY OF A USER'S DIGITAL IDENTITY

Аннотация

Объектом исследования выступает процесс непрерывной аутентификации пользователей в современных информационных системах. Предметом является вероятностная оценка достоверности цифровой идентичности в рамках отдельной пользовательской сессии. Цель работы заключается в обосновании и строгой формализации концептуальной модели непрерывной вероятностной оценки достоверности цифровой идентичности. Методология включает системный анализ существующих подходов к управлению доверием, детальную классификацию наблюдаемых признаков и вероятностное моделирование на основе байесовского обновления. В результате исследования сформировано комплексное признаковое пространство, объединяющее поведенческие, технические, сетевые и контекстно-временные характеристики взаимодействия. Предложен математический механизм последовательного обновления апостериорной вероятности с учетом логарифмического затухания влияния устаревших

наблюдений во времени. Разработана многоуровневая система интерпретации оценок доверия, позволяющая четко разделять состояния высокой уверенности, неопределенности и повышенного риска. Область применения полученных результатов охватывает проектирование систем адаптивной аутентификации для корпоративных сетей, финансовых сервисов и облачных платформ. Теоретическая значимость состоит в существенной конкретизации концепции динамического доверия применительно к изолированной пользовательской сессии. Практическая значимость определяется возможностью использования разработанной модели в качестве надежной архитектурной основы для создания программных прототипов непрерывного контроля сессий, обеспечивающих оптимальный баланс между информационной безопасностью и удобством пользователей.

Ключевые слова: вероятностная модель; динамическое доверие; непрерывная аутентификация; поведенческие признаки; цифровая идентичность.

Annotation

The object of the study is the process of continuous user authentication in modern information systems. The subject is the probabilistic assessment of the authenticity of digital identity within a single user session. The purpose of the work is to substantiate and rigorously formalize a conceptual model for continuous probabilistic assessment of the authenticity of digital identity. The methodology includes a systematic analysis of existing approaches to trust management, a detailed classification of observable features, and probabilistic modeling based on Bayesian updating. As a result of the study, a comprehensive feature space has been formed that combines behavioral, technical, network, and contextual-temporal characteristics of interaction. A mathematical mechanism is proposed for sequentially updating the posterior probability taking into account the logarithmic decay of the influence of outdated observations over time. A multi-level system for interpreting trust estimates has been developed, allowing a clear distinction between states of high confidence, uncertainty, and increased risk. The scope of application of the obtained results covers the design of adaptive authentication systems for corporate networks, financial services, and cloud platforms. The theoretical significance lies in a substantial concretization of the concept of dynamic trust as applied to an isolated user session. The practical significance is determined by the possibility of using the developed model as a reliable architectural basis for creating software prototypes for continuous session monitoring that ensure an optimal balance between information security and user convenience.

Keywords: probabilistic model; dynamic trust; continuous authentication; behavioral features; digital identity.

Введение

Современная информационная система после успешной аутентификации продолжает получать сведения о действиях пользователя, состоянии устройства, параметрах соединения и условиях выполнения операций. При этом исходное подтверждение личности относится только к

моменту установления доверия и не гарантирует, что на протяжении всей последующей сессии с учётной записью взаимодействует тот же субъект. Изменение устройства, сетевого окружения, характера выполняемых операций или поведенческого сценария, может быть, как следствием обычных условий работы, так и признаком изменения субъекта взаимодействия [1, 4]. Поэтому задача контроля идентичности не ограничивается первоначальной аутентификацией и требует оценки текущего состояния сессии по мере поступления новых наблюдений.

В предыдущей работе авторов рассматривалась общая концепция управления доверием к цифровой идентичности в многомерной интеллектуальной среде, включающей различные источники данных, устройства, сервисы и аналитические механизмы. В настоящем исследовании рассматривается более узкий уровень этой задачи – отдельная пользовательская сессия в информационной системе. Такой переход позволяет конкретизировать общий вероятностный подход применительно к последовательности событий, возникающих непосредственно в процессе взаимодействия пользователя с системой, и определить механизм изменения оценки достоверности идентичности во времени.

Основная проблема заключается в том, что отдельные наблюдаемые признаки обладают различной информативностью и не являются безусловными свидетельствами принадлежности сессии конкретному пользователю. Например, изменение IP-адреса может быть вызвано сменой сети, использование нового устройства – легитимными условиями работы, а отклонение скорости или последовательности действий – характером текущей задачи. Одновременно совокупность нескольких согласующихся отклонений может свидетельствовать о повышении вероятности компрометации сессии. Это требует перехода от независимой интерпретации отдельных признаков к их последовательному вероятностному учёту в рамках единого состояния пользовательской сессии [2, 5].

В связи с этим в статье рассматривается пользовательская сессия как последовательность наблюдений $(E_1, E_2, \dots, E_t)$, каждое из которых представляет новое свидетельство о текущем состоянии цифровой идентичности. Основу подхода составляет байесовская интерпретация свидетельств с использованием отношения правдоподобия, позволяющая учитывать направленность и силу влияния очередного наблюдения на текущую оценку [6, 7]. В развитие общей постановки предлагается рассматривать изменение доверия не только как накопление новых свидетельств, но и как динамический процесс, в котором влияние ранее полученной информации со временем может уменьшаться. Конкретные параметры такого механизма, включая характер временного затухания и пороги принятия решений, относятся к этапу последующей реализации и экспериментальной проверки.

Научная проблема исследования состоит в необходимости формализации последовательной оценки достоверности цифровой

идентичности в пределах пользовательской сессии при неоднородности, изменчивости и возможной взаимозависимости наблюдаемых признаков. Цель статьи – обосновать и формализовать применение вероятностного подхода для непрерывной оценки текущего состояния цифровой идентичности пользователя и определить принципы его последующей программной реализации.

Научная новизна исследования заключается в конкретизации общей концепции динамического доверия применительно к отдельной пользовательской сессии. В статье предлагается представлять состояние сессии как последовательно изменяющуюся вероятностную оценку, обновляемую при поступлении новых событий и учитывающую совокупность поведенческих, технических, сетевых, временных и контекстных признаков. В качестве элемента развития модели рассматривается механизм временного уменьшения влияния накопленной оценки, позволяющий учитывать ограниченную актуальность ранее полученных свидетельств. Дополнительно разделяются уровень вероятностной оценки состояния сессии и уровень принимаемого защитного решения, что позволяет учитывать критичность выполняемой операции независимо от самого значения доверия. При этом предлагаемые положения являются концептуальными: их программная реализация, калибровка параметров и экспериментальная проверка предполагаются на следующем этапе исследования.

Практическая значимость работы состоит в формировании основы для последующего создания программного прототипа непрерывной оценки цифровой идентичности. Предполагается, что реализация модели будет осуществлена с использованием Python, FastAPI и средств машинного обучения, включая Scikit-Learn. Указанные технологии рассматриваются как инструменты будущей реализации и экспериментального исследования предложенной модели, а не как самостоятельный научный результат.

Материалы и методы исследования

Исследование выполнено на основе системного, сравнительного и структурного анализа подходов к аутентификации пользователей и управлению доверием к цифровой идентичности, а также методов вероятностного моделирования и байесовского обновления оценки при поступлении последовательности новых свидетельств. В качестве методологической основы рассматривается представление аутентифицированной пользовательской сессии как динамического процесса, в котором состояние доверия к цифровой идентичности может изменяться под воздействием наблюдаемых характеристик поведения, устройства, сетевого взаимодействия и контекста. Такой подход соответствует современному представлению о session monitoring (continuous authentication), при котором в течение сессии могут анализироваться шаблоны использования, временные характеристики, поведенческие биометрические признаки, параметры устройства и браузера, а также характеристики IP-адреса и геолокации [7].

Объектом моделирования является состояние цифровой идентичности пользователя в рамках одной аутентифицированной сессии. После прохождения первоначальной процедуры аутентификации предполагается, что система получает последовательность наблюдений:

$$S_t = (E_1, E_2, \dots, E_t) \quad (1)$$

где E_t – очередное наблюдение, полученное в результате действия пользователя или изменения параметров сессии в момент t .

В рамках предлагаемого подхода рассматриваются две конкурирующие гипотезы: H_{legit} – текущую сессию продолжает легитимный пользователь, H_{comp} – сессию продолжает другой субъект либо она скомпрометирована.

Таким образом, задача последующей реализации заключается не в повторении первоначальной аутентификации после каждого действия, а в последовательной оценке того, насколько текущие наблюдения согласуются с гипотезой о продолжении сессии тем же пользователем. Такой принцип соответствует назначению мониторинга сессии, определяемому в NIST SP 800-63B-4 как непрерывной оценке характеристик сессии для выявления возможного мошенничества [1].

Для построения модели признаки предлагается разделять на несколько функциональных групп.

К поведенческим признакам относятся характеристики взаимодействия пользователя с системой: скорость и интервалы между нажатиями клавиш, последовательность действий, особенности навигации, длительность выполнения операций и другие параметры, отражающие индивидуальный поведенческий профиль. Возможность использования временных и поведенческих характеристик для непрерывной аутентификации рассматривается, в частности, в исследованиях поведенческой биометрии [8].

Технические признаки характеризуют используемое устройство и программную среду: тип устройства, характеристики браузера, набор доступных параметров среды и другие наблюдаемые характеристики конечной точки. Сетевые признаки включают характеристики сетевого подключения, в том числе IP-адрес и связанные с ним свойства. Контекстные и временные признаки описывают момент и условия выполнения действия: время, продолжительность интервала между событиями, последовательность операций и иные параметры текущей сессии.

При этом отдельный признак не рассматривается как безусловное доказательство принадлежности сессии конкретному пользователю. Например, IP-адрес может изменяться в течение сессии, устройство может использоваться несколькими лицами, а поведенческие характеристики могут изменяться в зависимости от условий взаимодействия. Поэтому в предлагаемой модели признаки рассматриваются как совокупность вероятностных свидетельств, имеющих различную информативность.

Для количественного представления состояния цифровой идентичности предлагается использовать апостериорную вероятность гипотезы H_{legit} , при

наличии совокупности наблюдений E . Базовое байесовское обновление имеет вид:

$$P(H_{legit} | E) = \frac{P(E|H_{legit})P(H_{legit})}{P(E|H_{legit})P(H_{legit}) + P(E|H_{comp})P(H_{comp})} \quad (2)$$

Здесь $P(H_{legit})$ и $P(H_{comp})$ являются априорными вероятностями соответствующих гипотез, а $P(E | H)$ характеризует вероятность наблюдаемого события при условии справедливости рассматриваемой гипотезы. Получаемое значение $P(H_{legit} | E)$ интерпретируется как текущая вероятностная оценка согласованности наблюдаемого поведения и контекста с ранее подтверждённой цифровой идентичностью.

Для последовательного обновления оценки целесообразно использовать отношение правдоподобия:

$$LR_t = \frac{P(E_t | H_{legit})}{P(E_t | H_{comp})} \quad (3)$$

Тогда отношение апостериорных шансов после поступления очередного наблюдения определяется как:

$$O_t = O_{t-1} \cdot LR_t \quad (4)$$

где

$$O_t = \frac{P(H_{legit} | E_1, \dots, E_t)}{P(H_{comp} | E_1, \dots, E_t)} \quad (5)$$

Такое представление позволяет не рассчитывать итоговую оценку независимо для каждого события, а последовательно учитывать историю наблюдений. В рамках статьи данная зависимость рассматривается как математическая основа будущего механизма обновления состояния доверия, а конкретные способы оценки вероятностей и параметры модели должны быть определены на последующем этапе экспериментальной реализации.

Поскольку наблюдаемое поведение пользователя не является постоянным, при последующей реализации модели необходимо учитывать давность полученных свидетельств. Возврат к полной неопределенности ($P=0,5$) при отсутствии новых событий не является естественным для открытой сессии. Поэтому предлагается модифицированная формула затухания в логарифмической форме, возвращающая оценку к базовому априорному уровню доверия O_0 (состоянию сразу после успешной первичной аутентификации):

$$\log O_t = \log O_0 + \lambda_t (\log O_{t-1} - \log O_0) + \log LR_t \quad (6)$$

где $\lambda_t \in [0,1]$ – коэффициент сохранения влияния предыдущих наблюдений (затухания), O_0 – базовый уровень доверия после первоначальной аутентификации.

Такой механизм позволяет избежать предположения о том, что любое наблюдение, полученное в начале сессии, должно сохранять неизменный вес на всём её протяжении. Функция $\lambda_t = f(\Delta t)$ в настоящей работе не фиксируется численно, поскольку её конкретный вид и параметры должны определяться в ходе последующего экспериментального исследования на репрезентативных данных.

Результатом работы будущего алгоритма должна являться не только числовая вероятность, но и состояние текущей сессии, используемое для выбора дальнейшего действия системы. В общем виде предлагается выделять несколько состояний: доверенное состояние, неопределённое состояние и состояние повышенного риска.

Переход между состояниями должен определяться заранее заданными правилами интерпретации вероятностной оценки. При этом конкретные пороговые значения в настоящей статье не задаются, поскольку их выбор является предметом последующего экспериментального исследования и зависит от требований конкретной информационной системы, стоимости ошибок первого и второго рода и допустимого уровня пользовательских ограничений.

В зависимости от полученного состояния будущая система может продолжать текущую сессию, инициировать дополнительную проверку личности либо ограничить или завершить сессию. Такой механизм соответствует общему подходу *session monitoring*, при котором обнаружение потенциального мошенничества может приводить к повторной аутентификации, завершению сессии или другим защитным действиям.

Для последующей реализации концептуальной модели предполагается использовать программные средства Python и FastAPI, а также инструменты машинного обучения библиотеки Scikit-learn. Данные технологии рассматриваются исключительно как технологическая основа будущего прототипа и не являются самостоятельным научным результатом настоящей работы.

Предполагаемый процесс обработки данных включает последовательность: получение событий пользовательской сессии → формирование признаков → вероятностная оценка отдельного наблюдения → байесовское обновление текущего состояния → интерпретация полученной оценки → выбор дальнейшего действия системы. На данном этапе данная последовательность представляет архитектурно-методическую схему будущей реализации, тогда как её программная реализация и экспериментальная проверка относятся к следующим этапам исследования.

Результаты исследования

Результатом исследования является концептуальная модель непрерывной вероятностной оценки достоверности цифровой идентичности пользователя. В отличие от разовой аутентификации, модель предусматривает последующий контроль соответствия текущей активности ранее подтверждённой идентичности на протяжении пользовательской сессии. Такой подход соответствует направлению непрерывной аутентификации, основанной на анализе поведенческих и контекстных характеристик пользователя [8, 9].

Сформировано признаковое пространство, включающее четыре группы признаков:

- поведенческие – скорость ввода, интервалы между действиями, последовательность операций;
- технические – характеристики устройства и программной среды;
- сетевые – IP-адрес и параметры сетевого соединения;
- контекстно-временные – время выполнения действий и условия текущей сессии.

Подобное объединение разнородных характеристик используется в исследованиях поведенческой биометрии и цифровых отпечатков пользователя [8,9]. При этом отдельный признак не рассматривается как достаточное доказательство идентичности, поскольку его значение может изменяться без смены пользователя. Например, изменение IP-адреса или параметров поведения не обязательно свидетельствует о компрометации

Предложена последовательность обработки данных: аутентификация → получение события → формирование признаков → оценка свидетельства → обновление состояния → принятие решения.

После первоначальной аутентификации каждое последующее событие рассматривается как дополнительное свидетельство относительно текущего состояния цифровой идентичности. Это позволяет перейти от однократного подтверждения личности к непрерывной оценке в ходе сессии.

Концепция оценки состояния через уровень доверия согласуется с терминологией ГОСТ Р 58833-2020, в котором уровень доверия к результатам аутентификации связывается с достигнутой уверенностью в том, что субъект является зарегистрированным пользователем [10].

Сформирован механизм последовательного обновления вероятностной оценки. Каждое новое событие изменяет текущее состояние с учётом ранее накопленных свидетельств.

В результате единичное отклонение не приводит автоматически к признанию пользователя посторонним. Устойчивое накопление нетипичных событий, напротив, постепенно изменяет оценку в сторону снижения доверия. Для учёта изменения поведения во времени предусмотрено уменьшение влияния устаревших наблюдений.

Оценка определяется не отдельным событием, а совокупностью последовательных наблюдений.

Для интерпретации полученной оценки предложены три состояния:

1. Высокое доверие – активность соответствует ожидаемому профилю;
2. Неопределённость – данных недостаточно для однозначного решения;
3. Низкое доверие – накопленная совокупность признаков существенно расходится с ожидаемым профилем.

Для каждого состояния определяется соответствующее действие: продолжение сессии, дополнительная аутентификация либо ограничение доступа.

Использование нескольких уровней вместо бинарного решения позволяет отделить недостаток информации от устойчивых признаков возможной смены пользователя. Сам принцип уровней доверия имеет соответствие российской нормативной базе: ГОСТ Р 70262.2-2025 устанавливает низкий, средний и высокий уровни доверия аутентификации [11].

На основе предложенной модели определена функциональная структура будущего прототипа: сбор событий → формирование признаков → вероятностная оценка → обновление состояния → принятие решения.

Для последующей реализации предполагается использовать Python и FastAPI, а Scikit-learn – для процедур обработки данных и машинного обучения. Указанные технологии рассматриваются как средства реализации модели, а не как самостоятельный научный результат.

Сформирована методическая основа будущего эксперимента. Проверке подлежат:

- способность выявлять изменение субъекта в ходе сессии;
- устойчивость к естественным изменениям поведения;
- вклад отдельных групп признаков;
- влияние изменения сетевых и технических условий;
- частота ложных срабатываний и пропусков.

Для оценки предполагается использовать FAR, FRR, EER и время обнаружения изменения субъекта. Конкретные пороговые значения и экспериментальные результаты в настоящей работе не приводятся, поскольку прототип и его испытание являются предметом последующего этапа исследования.

Результатом работы является концептуально-математическая основа будущей системы непрерывной оценки цифровой идентичности, объединяющая разнородные признаки, последовательное обновление оценки и многоуровневое принятие решений.

Обсуждение результатов

Предложенный подход является реалистичным с точки зрения используемых данных и методов, поскольку поведенческие, технические и контекстные признаки уже применяются в системах непрерывной аутентификации. Исследования показывают возможность использования динамики нажатий клавиш, сенсорного взаимодействия, характеристик устройства, сетевых параметров и других признаков для повторной оценки пользователя в течение сессии [4, 12]. При этом существующие работы также указывают, что эффективность таких систем существенно зависит от условий сбора данных, выбранных признаков и способа их объединения.

Основное ограничение связано с изменчивостью поведения пользователя. Скорость ввода, последовательность действий и другие поведенческие характеристики могут изменяться в зависимости от устройства, состояния среды и характера выполняемой задачи. Дополнительные сложности возникают при совместном использовании устройства

несколькими пользователями. Поэтому отклонение отдельного признака не может рассматриваться как достаточное основание для блокировки сессии. Сходная проблема отмечается в исследованиях поведенческой биометрии, где изменение поведенческого профиля во времени рассматривается как один из факторов снижения качества непрерывной аутентификации [12, 13].

Контекстные признаки также имеют ограниченную надёжность. IP-адрес может изменяться при переходе между сетями или использовании VPN, а характеристики устройства не гарантируют, что им управляет именно владелец учётной записи. Компрометация самого устройства создаёт отдельный сценарий угрозы: если злоумышленник получает доступ к уже аутентифицированной конечной точке, часть технических признаков продолжает соответствовать ожидаемому профилю. Поэтому использование нескольких групп признаков повышает информативность оценки, но не устраняет необходимость учитывать модель угроз. Обзоры непрерывной аутентификации указывают на уязвимость поведенческих механизмов к имитации, повторному воспроизведению и другим атакам.

Отдельной проблемой является зависимость результата от качества данных. Пропуски событий, изменение состава доступных признаков и корреляция между ними могут приводить к переоценке отдельных свидетельств. Для предлагаемой модели это означает необходимость проверки устойчивости вероятностной оценки при неполных и зависимых данных. На этапе последующей реализации потребуется определить правила обработки пропусков, способы оценки взаимозависимости признаков и методы предотвращения чрезмерного влияния одной группы характеристик. Поэтому выбранная математическая модель должна рассматриваться как основа, параметры которой требуют экспериментальной настройки, а не как готовый механизм с заранее гарантированной точностью.

Практическая эффективность системы будет определяться компромиссом между ошибками первого и второго рода. Ложное принятие может привести к сохранению доступа постороннего субъекта, тогда как ложное отклонение создаёт неудобства легитимному пользователю. В исследованиях непрерывной аутентификации для оценки этого компромисса используются FAR, FRR и EER; при этом повышение требований к безопасности может сопровождаться ухудшением удобства использования [4, 14]. Поэтому пороговые значения в предлагаемой модели нельзя выбирать только исходя из статистики признаков. Они должны определяться с учётом назначения информационной системы, стоимости ошибок и допустимой частоты дополнительных проверок.

Существенным ограничением является и возможность имитации поведения пользователя. Современные методы машинного обучения позволяют моделировать поведенческие характеристики, а исследования показывают уязвимость моделей поведенческой биометрии к специально сформированным атакам [12]. Это означает, что совпадение текущего поведения с ранее наблюдаемым профилем не является абсолютным

доказательством принадлежности сессии владельцу. Вероятностная оценка в предлагаемом подходе должна интерпретироваться именно как степень уверенности, а не как доказательство идентичности.

Обработка поведенческих и контекстных данных создаёт отдельные требования к конфиденциальности. Непрерывная аутентификация предполагает сбор значительного объёма информации о действиях пользователя, характеристиках устройства, сетевом взаимодействии и иногда местоположении. Такая информация может использоваться не только для проверки личности, но и для восстановления особенностей поведения пользователя. Поэтому будущая реализация должна предусматривать минимизацию собираемых данных, ограничение целей их использования и разграничение доступа к профилям. Проблемы приватности и необходимость специальных механизмов защиты данных отмечаются в исследованиях непрерывной аутентификации [4, 15].

Наконец, дополнительная проверка не должна выполняться при каждом небольшом отклонении. Частые запросы повторной аутентификации способны ухудшить пользовательский опыт и снизить практическую применимость системы. Поэтому промежуточное состояние неопределённости, предусмотренное моделью, может использоваться для накопления дополнительных свидетельств до принятия защитного решения. Конкретные правила перехода между состояниями, пороги и допустимая частота дополнительных проверок должны быть определены по результатам будущего эксперимента.

Предложенная модель не устраняет перечисленные ограничения, но позволяет формализовать их в рамках единого механизма оценки. Её практическая применимость должна быть подтверждена экспериментально на данных, отражающих различные устройства, условия сетевого взаимодействия, естественные изменения поведения и сценарии возможной смены субъекта. Именно такая проверка позволит определить информативность отдельных групп признаков, устойчивость модели и приемлемое соотношение безопасности и удобства использования.

Заключение

В работе предложена концептуальная модель непрерывной вероятностной оценки достоверности цифровой идентичности пользователя на основе совокупности поведенческих, технических, сетевых и контекстно-временных признаков. В отличие от разовой аутентификации, модель предусматривает последовательную оценку событий в ходе пользовательской сессии и динамическое обновление текущего уровня доверия.

Практическая применимость подхода определяется возможностью его адаптации к различным информационным системам и реализации в составе будущего прототипа. При этом модель не исключает ошибок распознавания, изменения поведения пользователя, нестабильности сетевых и технических признаков, а также угроз имитации поведения и компрометации устройства.

Дальнейшие исследования должны быть направлены на экспериментальную проверку модели, определение параметров и порогов принятия решений, оценку показателей ложного принятия и ложного отклонения, а также исследование устойчивости метода при изменении условий использования. Отдельное внимание необходимо уделить снижению объема собираемых данных и сохранению приемлемого уровня пользовательского взаимодействия.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Temoshok D., Fenton J. L., Choong Y.-Y. et al. Digital Identity Guidelines: Authentication and Authenticator Management. NIST SP 800-63B-4. Gaithersburg: National Institute of Standards and Technology, 2025. – <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.pdf>
2. Stylios I., Kokolakis S., Thanou O., Chatzis S. Behavioral biometrics & continuous user authentication on mobile devices: A survey // *Information Fusion*. 2021. Vol. 66. P. 76–99. DOI: 10.1016/j.inffus.2020.08.021.
3. Liang Y., Samtani S., Guo B., Yu Z. Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective // *IEEE Internet of Things Journal*. 2020. Vol. 7, No. 9. P. 9128–9143. DOI: 10.1109/JIOT.2020.3004077.
4. Baig A. F., Eskeland S. Security, Privacy, and Usability in Continuous Authentication: A Survey // *Sensors*. 2021. Vol. 21, No. 17. Article 5967.
5. Arias-Cabarcos P., Krupitzer C., Becker C. A Survey on Adaptive Authentication // *ACM Computing Surveys*. 2019. Vol. 52, No. 4. P. 1–30. DOI: 10.1145/3336117.
6. Якупов Д. Р., Намиот Д. Е. Рекомендательные системы на основе сессий-модели и задачи // *International Journal of Open Information Technologies*. – 2022. – Т. 10. – №. 7. – С. 128-155.
7. Grassi P. A., Garcia M. E., Fenton J. L. Digital Identity Guidelines (翻訳版) // NIST special publication. – 2017. – Т. 800. – С. 63-3.
8. Muratyan A. et al. Opportunistic multi-modal user authentication for health-tracking IoT wearables // *The Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021*. Cham : Springer International Publishing, 2022. С. 1–18.
9. Осин А. В., Мурашко Ю. В. Обзор методов идентификации пользователя на основе цифровых отпечатков // *Труды учебных заведений связи*. 2023. Т. 9. №. 5. С. 91–111.
10. ГОСТ Р 58833-2020. Защита информации. Идентификация и аутентификация. Общие положения. – М.: Стандартинформ, 2020.
11. ГОСТ Р 70262.2-2025. Защита информации. Идентификация и аутентификация. Уровни доверия аутентификации. – М.: Российский институт стандартизации, 2025.

12. Rayani P. K., Changder S. Continuous user authentication on smartphone via behavioral biometrics: a survey // *Multimedia Tools and Applications*. 2023. Vol. 82. No. 2. P. 1633–1667.
13. Mahfouz A., Mahmoud T. M., Eldin A. S. A survey on behavioral biometric authentication on smartphones // *Journal of information security and applications*. 2017. Vol. 37. P. 28–37. DOI: 10.1016/j.jisa.2017.10.002.
14. Ryu R. et al. Continuous multimodal biometric authentication schemes: a systematic review // *IEEe Access*. 2021. Vol. 9. P. 34541–34557.
15. Baig A. F., Eskeland S., Yang B. Privacy-preserving continuous authentication using behavioral biometrics // *International Journal of Information Security*. 2023. Vol. 22 (6). P. 1833–1847. DOI: 10.1007/s10207-023-00721-y.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Литвинов Алексей Сергеевич – аспирант, ГБОУ ВО «Нижегородский государственный инженерно-экономический университет», г. Княгинино, Россия, E-mail: litvinlex1@gmail.ru, ORCID: 0000-0002-7398-1052.

Астахова Татьяна Николаевна – кандидат физико-математических наук, доцент, заведующая кафедрой «Информационные системы и технологии», ГБОУ ВО «Нижегородский государственный инженерно-экономический университет», г. Княгинино, Россия, E-mail: ctn_af@mail.ru, ORCID: 0000-0002-7032-0697, SPIN-код: 2158-3392.