Operation Data // Electronics. – 2022. – Vol. 11. No. 8. – 1213. – DOI: 10.3390/electronics11081213.

9. *Zoppi T., Gharib M., Atif M., Bondavalli A.* Meta-Learning to Improve Unsupervised Intrusion Detection in Cyber-Physical Systems // ACM Transactions on Cyber-Physical Systems. – 2021. – Vol. 5. No. 4. – Article No. 42. – P. 1-27. – DOI: 10.1145/3467470.

10.*Zhong M., Zhou Y., Chen G.* A Security Log Analysis Scheme Using Deep Learning Algorithm for IDSs in Social Network // Security and Communication Networks. – 2021. – Vol. 2021. – Article ID 5542543. – P. 1-13. – DOI: 10.1155/2021/5542543.

Уймин А.Г.

Система непрерывно-дискретной биометрической идентификации на основе анализа потока данных компьютерной мыши

Аннотация: В данной работе рассматривается система непрерывно-дискретной биометрической идентификации, использующая данные движения компьютерной мыши для улучшения точности и надежности идентификации пользователей. Введение таких биометрических систем является актуальным в условиях глобализации цифровых технологий, поскольку обеспечивает защиту персональных данных и позволяет создать надежные механизмы аутентификации, учитывающие поведенческие особенности пользователя. Исследование направлено на разработку алгоритмов, способных эффективно анализировать пользовательские паттерны взаимодействия с мышью, что позволит повысить безопасность и адаптивность системы.

Ключевые слова: биометрическая идентификация, движения мыши, безопасность данных, поведенческие паттерны, алгоритмы анализа данных

В эпоху глобализации цифровых технологий и стремительного развития информационного общества, обеспечение личного

благополучия и защита персональных данных становятся приоритетными задачами. Особенно остро стоят вопросы защиты от несанкционированного доступа, утечек и неправомерного использования персональных данных. В связи с этим возникает необходимость всестороннего изучения современных методов аутентификации и идентификации в контексте обеспечения информационной безопасности [1].

В этом контексте ключевым аспектом защиты личных данных является применение эффективных механизмов аутентификации (действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации) и идентификации (действия по присвоению субъектам и объектам доступа идентификаторов и/или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов) [2].

Учитывая описанные выше вызовы в области защиты личных данных, а также сложности, связанные с безопасностью, удобством и эффективностью традиционных методов аутентификации и идентификации, таких как использование паролей и токенов, возникает потребность в разработке более надежных и передовых подходов. Одним из перспективных направлений в этой области является использование поведенческих биометрических данных, таких как движения мыши, которые могут предложить более удобное и безопасное средство идентификации пользователя.

В контексте работы под надёжностью биометрической системы на основе анализа движений мыши понимается способность точно и устойчиво распознавать пользователей на основании их уникальных паттернов поведения при взаимодействии с устройством. Эта надежность включает несколько ключевых аспектов: точность (accuracy), устойчивость (robustness), повторяемость (repeatability), скорость (speed), уровень ложных срабатываний (False Accept Rate, FAR и False Reject Rate, FRR), адаптивность (adaptability), удобство использования (usability).

Актуальность исследований в данной области определяется несколькими ключевыми факторами. Во-первых, стремительное развитие биометрических технологий, которые активно интегрируются в различные сферы жизнедеятельности человека,

требуют разработки и внедрения стандартов, касающихся сбора, обработки и защиты биометрической информации. Второй аспект актуальности связан с необходимостью адаптации механизмов идентификации и верификации к условиям постоянно развивающихся технологий, таких как Smart Home и IoT. Изменения в этих областях требуют новых подходов к обеспечению безопасности, в том числе защиты от угроз со стороны инсайдеров. Современные решения включают в себя использование специализированных алгоритмов и идентификаторов, однако постоянно развивающийся характер технологий требует постоянного совершенствования этих механизмов. Поэтому разработка усовершенствованных и адаптируемых моделей биометрической идентификации, способных работать в условиях новейших технологических реалий, представляет собой первоочередную задачу современной науки в области информационной безопасности [3].

Основной проблемой в данном вопросе является то, что современные методы биометрической аутентификации, хотя и предлагают повышенный уровень безопасности, зачастую сталкиваются с трудностями, связанными с защитой персональных данных и приватностью пользователей. Кроме того, затраты на специализированное оборудование, программное обеспечение и серверные мощности для хранения и обработки биометрических данных значительно увеличивают общую стоимость внедрения таких систем. Биометрические данные являются крайне чувствительной информацией, и их утечка или неправомерное использование могут привести к серьезным последствиям. К тому же, эффективность биометрических систем понижается в результате изменений физических характеристик пользователя, таких как старение, травмы или медицинские состояния. Также стоит учитывать потенциальные проблемы с точностью идентификации в разнообразных демографических группах. Все это требует разработки более совершенных, гибких и безопасных биометрических систем, способных реагировать на данные вызовы [4].

Методологию исследования составили методы математической статистики, теория вероятности, метод вычислительной комбинаторики, графический метод, описательный и

сопоставительный методы, а также основы системного подхода и диалектики.

Рабочей гипотезой в данном случае выступило предположение о том, что интеграция передовых методов цифровой обработки сигналов в процесс биометрической идентификации существенно улучшает эффективность и надежность биометрических систем.

Цель работы заключалась в разработке системы идентификации пользователей при дистанционном доступе к информационным системам с использованием данных, полученных от компьютерной мыши.

Научная новизна исследования:

– разработана система непрерывно-дискретной биометрической идентификации, которая не требует использования общих секретов или физических устройств [5];

– усовершенствованы алгоритмы обработки сигналов компьютерной мыши, способные эффективно извлекать и анализировать пользовательские паттерны, что улучшает точность и надежность идентификации [6];

– сформулированы особенности обучения свёрточных нейронных сетей (CNN) для классификации и распознавания индивидуальных признаков пользователей, использующих компьютерную мышь [7].

Проведена апробация и эмпирически обоснована эффективность биометрической идентификации в рамках предложенной модели.

Практическая значимость работы проявляется через потенциал применения ее результатов в профессиональной и учебной деятельности. Система может быть адаптирована для создания инновационных интеллектуальных систем в сфере биометрической идентификации, особенно в области телекоммуникационных систем образовательной сферы.

Результатами реализации проекта стали:

1) Система непрерывно-дискретной биометрической идентификации, разработанный в рамках данного исследования, обеспечивает улучшенную точность и надежность идентификации пользователей за счет сочетания непрерывного мониторинга и дискретного анализа, что представляет значительный шаг вперед в области биометрических технологий.

2) Алгоритмы обработки сигналов от компьютерной мыши, усовершенствованные в ходе исследования, способны эффективно извлекать и анализировать пользовательские паттерны, что повышает точность и надежность идентификации.

3) Особенности обучения свёрточных нейронных сетей (CNN), предложенные в работе, позволяют эффективно классифицировать и распознавать индивидуальные признаки пользователей, взаимодействующих с компьютерной мышью, что обеспечивает повышенный уровень точности в биометрической аутентификации.

4) Методика идентификации и аутентификации пользователя информационной системы, основанная на анализе данных компьютерной мыши, повышает точность идентификации, учитывая как технические, так и экономические показатели, и обеспечивает оптимизацию процесса безопасности.

Литература:

1. *Hub M., Příhodová K.* Impact of Globalization on Data Security–Authentication Issues // SHS Web of Conferences. – 2021. – Volume 92. – 05009. – DOI: 10.1051/shsconf/20219205009.

2. ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения. – М.: Стандартинформ, 2020. – 32 с.

3. *Savukynas R.* Internet of Things information system security for smart devices identification and authentication / 2020 9th Mediterranean Conference on Embedded Computing (MECO). – IEEE, 2020. – P. 1-5.

4. *Деркач Е.А., Шелупанов А.А.* Методологические подходы к обеспечению безопасности программных продуктов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2024. – Т. 27, № 1. – С. 37-43. – DOI: 10.21293/1818-0442-2024-27-1-37-43.

5. *Уймин А.Г., Греков В.С.* Применение алгоритма Дугласа-Пеккера в вопросах онлайн-аутентификации инструментов удалённой работы при подготовке специалистов укрупнённой группы специальностей 10.00.00 «Информационная безопасность» // Электронные библиотеки. – 2024. – Т. 27, № 4. – С. 679-694. – DOI: 10.26907/1562-5419-2024-27-4-679-694.

6. *Уймин А.Г., Морозов И.М.* Сравнительный анализ инструментов непрерывной онлайн-аутентификации и систем

обнаружения аномалий для постоянного подтверждения личности пользователя // T-Comm: Телекоммуникации и транспорт. – 2022. – Т. 16, № 5. – С. 48-55. – DOI: 10.36724/2072-8735-2022-16-5-48-55.

7. *Уймин А.Г.* Интеллектуальный анализ динамики трехпозиционного графического манипулятора типа «мышь» как элемента поведенческой биометрии // Системы управления и информационные технологии. – 2022. – № 2(88). – С. 92-96. – DOI: 10.36622/VSTU.2022.88.2.018.

Саломатин А.А.

Алгоритм аутентификации пользователей на основе статических характеристик аппаратного обеспечения компьютеров

Аннотация: Работа посвящена разработанному алгоритму аутентификации пользователей на основе статических характеристик аппаратного обеспечения компьютеров. Подробно изложены основные шаги алгоритма, описывающие используемые данные и их обработку для генерации характеристических профилей пользователей. Предложено программное обеспечение, реализующее алгоритм. Результаты работы могут быть использованы для дальнейшего усовершенствования алгоритма и его апробации.

Ключевые слова: информационная безопасность, аутентификация, цифровой след, аппаратное обеспечение, статические характеристики

Введение

В эпоху информационных технологий особую важность приобретает вопрос информационной безопасности (ИБ) пользователей сетей. Данные пользователей различных устройств должны обладать высокой степенью защиты от кибератак, направленных на потерю пользовательских данных, их сбор злоумышленниками и/или др.