

Греченева А.В., Бужинский В.С.

*Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
E-mail: GrechenevaAV@yandex.ru*

Определение требований к технологии аутентификации пользователей по данным носимых устройств и смартфонов на основе интеллектуальной обработки биометрических параметров походки

Процесс создания методов и алгоритмов аутентификации пользователей, которые будут положены в основу новой технологии усиленной аутентификации, сопряжен с необходимостью исследования требований выполнения определенных уровней доверия, а также требований к строгости аутентификации [1,2].

Согласно предлагаемой технологии, аутентификация пользователей будет осуществляться по данным носимых устройств и смартфонов на основе интеллектуальной обработки биометрических параметров походки. Носимые устройства (смартфоны, фитнес-трекеры, смарт-часы), оснащенные датчиками перемещения (акселерометры и гироскопы), позволяют получать данные об особенностях походки, которые регистрируются на протяжении повседневной деятельности отдельного пользователя, не ограничивая движений и не оказывая на человека дополнительного воздействия. Это позволяет за счет активного отслеживания аутентичности на протяжении всего времени доступа пользователя к устройству, на фоне основной работы системы, анализировать значительные объемы данных суточной активности и определять тренды в них, с целью повышения качества обучения нейросетей и процесса аутентификации в целом. В результате выполнения аутентификационного протокола будет совершаться автоматизированный процесс принятия решения о соответствии регистрируемых параметров походки индивидуальной норме движений пользователя по семи признакам: длина шага, база шага, скорость шага, частота шага, цикл шага, период опоры, период переноса, формирующим индивидуальные пространства движений.

При разработке технологии аутентификации следует выделить следующие системные требования:

- хранение не менее семи поведенческих и физиологических биометрических параметров (длина шага, база шага, скорость шага, частота шага, цикл шага, период опоры, период переноса);
- обеспечение целостности и непротиворечивости данных;
- защита данных от «растекания» (неотделимость образцов от базы данных);
- доступность сенсоров (акселерометры и гироскопы) носимых устройств (смартфоны, фитнес-трекеры, смарт-часы);

При решении задачи распознавания движений к каждому из формируемых пространств движений пользователя предъявляются особые требования:

- наличие различных стилей движений;
- наличие различных условий регистрации образцов движений (смена ландшафта, погодных условий, времени суток);
- наличие вариации пользователей (по полу, возрасту и т. п.);
- регистрация данных на носимые устройства, имеющие различные технические характеристики;
- необходимость разбиения двигательных актов на простейшие локомоции.

Критериями для оценки строгости аутентификации, характеризующими доверие к результатам процедуры аутентификации, являются показатели функциональной надёжности системы (уровень безошибочности выполнения заданных функций) и уровень безопасности информации пользователя, который система обрабатывает, передаёт и принимает. В результате анализа стандарта [3] были определены требования:

- Уровень достоверности результатов аутентификации.
- Функциональная надёжность выполнения основных процедур.
- Степень уверенности, что стороны взаимодействия являются теми, за кого себя выдают.
- Безопасность передачи и обработки персональных данных пользователей в процессе аутентификации.

Работа выполнена при финансовой поддержке гранта Президента Российской Федерации № МК-1558.2021.1.6.

Литература

1. ГОСТ Р 58833-2020 Национальный стандарт российской федерации. Защита информации. Идентификация и аутентификация. Общие положения/ Information protection. Identification and authentication. General (Дата введения 2020-05-01)

2. Единая система идентификации и аутентификации. Методические рекомендации по использованию Единой системы идентификации и аутентификации. Версия 2.25.

3. ГОСТ Р ИСО/МЭК 9594898. Информационная технология. Взаимосвязь открытых систем: Справочник. Ч. 8. Основы аутентификации. URL: <http://docs.cntd.ru/document/gostrisomek9594898>.