

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ СМАРТФОНА НА ОСНОВЕ ДАННЫХ, ПОЛУЧЕННЫХ С АКСЕЛЕРОМЕТРА

Статья поступила в редакцию 09.01.2023, в окончательном варианте – 20.01.2023.

Корякова Виктория Андреевна, Астраханский государственный университет им. В. Н. Татищева, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
магистрант, ORCID: 0000-0002-2472-9248, e-mail: koryakova-01@mail.ru

Марченков Александр Николаевич, Астраханский государственный университет им. В. Н. Татищева, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
кандидат технических наук, доцент, ORCID: 0000-0003-1378-3553, e-mail: marenkovan17@gmail.com

В связи с ростом числа пользователей смартфонов и последующим увеличением объемов личной информации, хранящихся на них, все чаще стали подниматься многочисленные вопросы в области безопасности и конфиденциальности данных на мобильных устройствах. Чтобы решить эти проблемы, исследователи внедрили множество методов, включая подходы непрерывной аутентификации, основанные на поведении пользователя. В ходе анализа существующих решений было выявлено, что использование алгоритмов машинного обучения обеспечивает лучшее решение проблем аутентификации на основе поведенческой биометрии, которая направлена на выявление поведенческих черт, которыми обладает пользователь, таких как движения рук и модели размахивания руками. Новые методы должны фокусироваться на нескольких характеристиках и защищать от различных атак, делая систему безопасности простой в использовании и адаптированной для каждого владельца. Анализ и оценка научных, методологических, технологических, алгоритмических, программных решений показали, что необходимо разработать методику мониторинга и анализа информации, поступающей от различных датчиков мобильных устройств, на основе которой можно было бы с достаточным успехом использовать данные для аутентификации пользователя мобильного устройства, его типичное и атипичное поведение, а также различные жесты, производимые пользователем с помощью мобильного устройства. Были спроектированы архитектуры одиннадцати полносвязных нейронных сетей, содержащих в себе разное количество слоев и нейронов. В результате экспериментов было выявлено, что наиболее оптимальной НС для распознавания жестов мобильным устройством является нейронная сеть, состоящая из двух скрытых слоев с 32 и 16 нейронами соответственно. Качество (Accuracay) разработанной модели в среднем составило 94 % верно предсказанных жестов. В результате было разработано, протестировано и описано клиент-серверное приложение, которое позволяет: собирать показания акселерометра смартфона и передавать их на сервер; распознавать жесты пользователя, совершаемые мобильным устройством; выводить на экран мобильного устройства информацию о характере движения.

Ключевые слова: аутентификация пользователя, поведенческая биометрия, распознавание жестов, трехосевые акселерометры, мобильные устройства, машинное обучение

SMAРТPHONE USER AUTHENTICATION BASED ON DATA RECEIVED FROM THE ACCELEROMETER

The article was received by the editorial board on 09.01.2023, in the final version – 20.01.2023.

Koryakova Victoria A., Astrakhan Tatishchev State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,

undergraduate student, ORCID: 0000-0002-2472-9248, e-mail: koryakova-01@mail.ru

Marenkov Alexander N., Astrakhan Tatishchev State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,

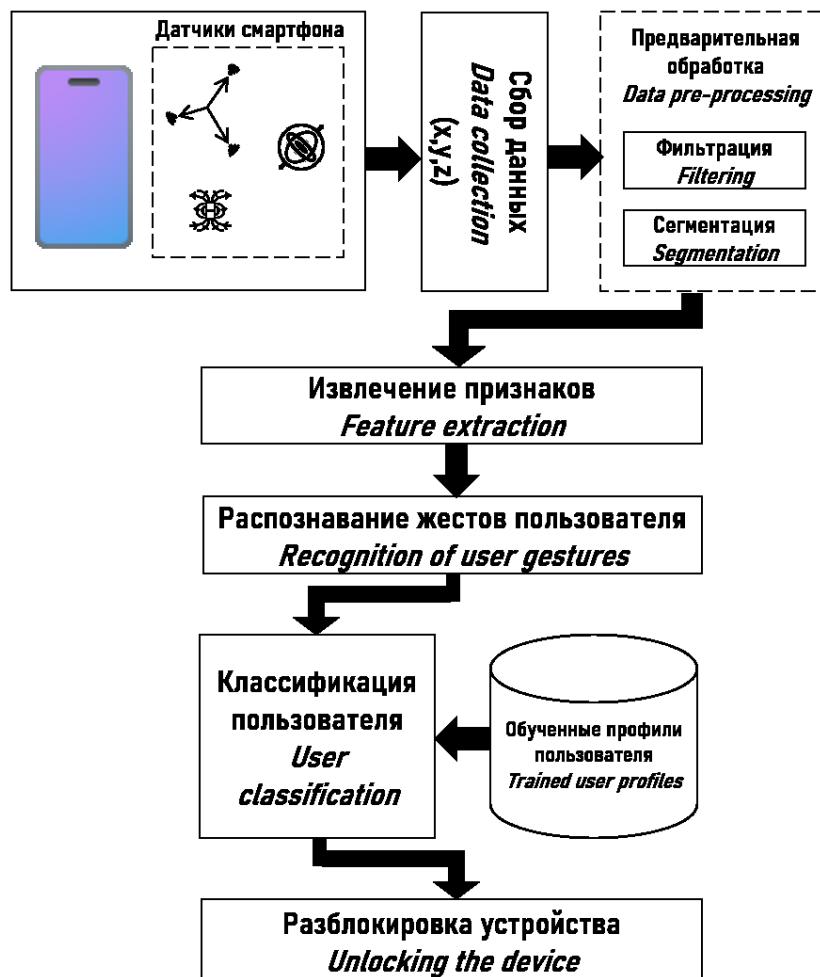
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0003-1378-3553, e-mail: marenkovan17@gmail.com

With the growing number of smartphone users and the subsequent increase in the amount of personal information stored on them, numerous questions have been raised regarding the security and privacy of data on mobile devices. To solve these problems, researchers have implemented a variety of methods, including continuous authentication approaches based on user behavior. In the course of the analysis of existing solutions, it was found that the use of machine learning algorithms provides a better solution to authentication problems based on behavioral biometrics, which aims to identify behavioral traits that the user possesses, such as hand movements and hand-waving patterns. New methods should focus on multiple characteristics and protect against various attacks, making the security system easy to use and tailored to each owner. Analysis and evaluation of scientific, methodological, technological, algorithmic, software solutions showed that it is necessary to develop a methodology for monitoring and analyzing information coming from various sensors of mobile devices, on the basis of which it would be possible to authenticate a user of a mobile device with a sufficiently high probability, his typical and atypical behavior, as well as various gestures made by the user using a mobile device. The architectures of eleven fully connected neural networks were designed, containing a different number of layers and neurons. As a result of the experiments, it was found that the most optimal neural network

for gesture recognition by a mobile device is a neural network consisting of two hidden layers with 32 and 16 neurons, respectively. The quality (Accuracy) of the developed model averaged 94 % of correctly predicted gestures. As a result, a client-server application was developed, tested and described, which allows you to: collect smartphone accelerometer readings and transfer them to the server; recognize user gestures made by the mobile device; display information about the nature of the movement on the screen of the mobile device.

Keywords: user authentication, behavioral biometrics, gesture recognition, triaxial accelerometers, mobile devices, machine learning

Graphical annotation (Графическая аннотация)



Введение. Высокая производительность, мобильность, удобство в использовании позволили смартфонам и планшетам стать неотъемлемой частью повседневной жизни людей. С помощью мобильных устройств люди ежедневно выполняют множество задач, расширяют возможности общения, творчества и развлечений. Зачастую мобильные устройства становятся удобной и гибкой площадкой для реализации рабочих процессов. С развитием сектора разработки мобильных приложений современный гаджет получает все больше функциональных возможностей. С ростом установленных приложений увеличивается и объем информации, которые они хранят о пользователе. На смартфоне могут храниться персональные данные пользователя, рабочие документы, данные банковских карт, личная информация. Утечка такой информации может привести к нарушению конфиденциальности, финансовым и репутационным последствиям. В 2022 году доля утечки данных через мобильные устройства возросла на 5 % по сравнению с предыдущим периодом. При этом 60 % подобных инцидентов признаны крупными, а остальные 40 % – крупными с долгосрочными последствиями [1]. Подобные утечки информации могут возникать вследствие нелегитимного использования мобильного устройства/кражи мобильного устройства. Кроме того, смартфоны оснащены модулями GPS, NFC и Bluetooth, а также цифровой камерой и почти всегда подключены к интернету, тем самым раскрывая много информации о физической активности их владельцев.

Смартфоны гораздо более подвержены краже за счет своих размеров. Конфискация мобильных устройств, у которых отсутствует система аутентификации, либо она слабая и подвержена быстрому взлому, может привести к краже личных данных пользователя и использованию их с целью шантажа, вымогательства. Поэтому важно обезопасить свое мобильное устройство от нелегитимного доступа. Существующие методы аутентификации на смартфоне имеют ряд недостатков: пароль или ПИН-код можно подсмотреть, либо подобрать с помощью специального программного обеспечения, графический ключ можно воспроизвести по наличию отпечатков пальцев на экране смартфона, биометрическая верификация подвержена атакам спуфинга. Разработка методики мониторинга и анализа информации, поступающей от различных датчиков мобильных устройств, позволит с достаточно высокой вероятностью аутентифицировать пользователя мобильного устройства, его типичное и атипичное поведение, а также различные жесты, производимые пользователем с помощью мобильного устройства.

Анализ существующих подходов для аутентификации пользователя мобильных устройств. Существующие средства аутентификации можно разделить на три группы: методы аутентификации по паролю; метод аутентификации с помощью магнитных карт, токенов и других устройств; метод аутентификации, использующий персональные свойства пользователя (отпечаток пальца, структуру сетчатки глаза и т.д.) (рис. 1).



Рисунок 1 – Методы аутентификации

1. Метод с использованием пароля основан на том, что человек знает уникальный код или последовательность цифр и букв: это может быть пароль, ответ на секретный вопрос или идентификационный номер, который должен знать пользователь.
2. Метод с использованием уникального объекта, чем человек обладает в физическом смысле. Распространенными примерами этого типа являются токен, идентификационная карта или другое доверенное устройство.
3. Биометрические методы, обозначающие физическую или поведенческую характеристику: могут быть представлены одним или несколькими физическими или поведенческими атрибутами. Типичными примерами являются отпечатки пальцев и динамические модели нажатия клавиш владельца устройства.

Благодаря достижениям в области технологий, позволяющим точно измерять характеристики человека, а также доступности большей вычислительной мощности для анализа полученных характеристик, которые можно сравнивать в режиме реального времени, появилась биометрическая идентификация как эффективный и удобный способ проверки личности человека для осуществления непрерывной аутентификации.

Биометрия характеризует уникальные физические или поведенческие особенности человека. Выделяют две категории биометрии: поведенческую и физиологическую [2]. Физиологическая биометрия использует такие характеристики человека, как сетчатка или радужная оболочка глаза, отпечатки пальцев и лицо человека. Поведенческая биометрия основана на поведении пользователя и включает в себя анализ такой информации, как форма и направление почерка, время нажатия клавиш, уникальные паттерны, присущие походке, речи и использованию стилуса, а также другие особенности общего поведения человека [3].

Непрерывная аутентификация (СА) предлагает преимущества в отношении удобства использования и безопасности. Данный подход пассивно повторно аутентифицирует пользователей, не уведомляя пользователя и не требуя его внимания, и автоматически блокирует систему, если

пользователь неактивен или когда он наблюдает нарушения или аномальное поведение. Непрерывная аутентификация использует распознавание физиологических и поведенческих биометрических образов и режимы контекстно-зависимой аутентификации, иногда в комбинации. Сочетание нескольких режимов называют мультимодальной аутентификацией. Методы аутентификации на основе поведенческой биометрии были разделены на две категории: методы одномодальной и мультимодальной аутентификации. Схематичное разделение методов аутентификации на основе поведенческой биометрии представлено на рисунке 2.



Одномодальная система аутентификации относится к системе аутентификации на основе одной биометрической характеристики, такой как походка, динамика нажатия клавиш и размахивание рукой. Мультимодальная поведенческая биометрия относится к объединению различных биометрических показателей для аутентификации пользователя.

По мере развития вычислительных и сенсорных возможностей смартфонов исследователи начали использовать больше типов сенсорных данных с устройств для самых разных целей. Данные мобильного зондирования использовались для краудсорсинга, понимания контекста и распознавания активности. Были опубликованы обзорные статьи о поведенческих биометрических системах аутентификации, однако некоторые обзоры сосредоточены только на определенных поведенческих чертах [4, 5].

Динамика нажатия клавиш широко используется для непрерывной идентификации пользователей смартфонов на основе их моделей набора текста. Так, авторы работы [6] предложили динамику нажатия клавиш, чтобы охарактеризовать поведение пользователей при наборе текста с помощью уникальных сенсорных функций. Благодаря использованию методов машинного обучения для аутентификации пользователей предложенный подход позволил достичь EER (одинаковую частоту ошибок) на уровне 0,08 %. В работе [7] исследовали эффективность функций нажатия клавиш для подмножества наиболее часто используемых английских слов, используя функции: длительность нажатия клавиш, время ожидания, общую продолжительность слова. Были проведены эксперименты для измерения производительности каждой функции в отдельности, а затем результатов различных комбинаций этих функций. Сенсорная динамическая биометрия предназначена для измерения и оценки сенсорного ритма пользователей на смартфонах. Данные получают, когда пользователь взаимодействует с сенсорным экраном, не требуя выполнения какой-либо конкретной задачи. Включив эту временную информацию в процесс аутентификации, предложенная модель смогла достичь средних равных коэффициентов ошибок ~4,0 % и ~2,5 % соответственно на двух наборах данных. Авторы [8] предложили динамическую аутентификацию пользователей смартфонов на основе их жестов на сенсорном экране. Были определены четыре типа жестов для аутентификации пользователя:

нажатие, прокрутка, перетаскивание и масштабирование. Для классификации признаков применялись различные классификаторы, в том числе MVP, k-NN и случайный лес (RF). Экспериментальные результаты показали, что классификатор MVP достиг наилучших результатов при использовании отдельных жестов, а k-NN сообщил о лучших результатах при объединении двух жестов. Классификатор k-NN достигает равного уровня ошибок 0 %, используя всего три жеста.

Голосовое поведение также используется для идентификации пользователей смартфонов по манере и характеру их речи. Каждый человек имеет различные голосовые подписи. В [9] представлены новые подходы к извлечению и использованию функций с помощью моделей глубокого обучения для проверки говорящего в зависимости от текста. Были исследованы четыре типа моделей глубокого обучения: ограниченная машина Больцмана, речевая дискриминантная глубокая нейронная сеть (DNN), дискриминантная глубокая нейронная сеть и многозадачная глубокая нейронная сеть с совместным обучением. Совместный линейный и вероятностный линейный дискриминантный анализ использовался в качестве классификаторов для признаков на основе вектора идентичности. Эксперименты с набором данных RSR2015 показали, что методы, основанные на глубоких функциях, могут обеспечить значительное повышение производительности по сравнению с традиционными базовыми показателями, достигающими EER 0,10 %. Авторы исследования [10] разработали эффективную систему на основе голосовых отпечатков (называемую DR-EiSV-IAS) для пользователей смартфонов на китайском языке. Авторы создали общедоступную базу данных мандаринского языка, записанную смартфонами, для исследования распознавания говорящего в зависимости от текста. Эксперименты подтвердили эффективность предложенного ими DR-EiSV-IAS, который обеспечивает наилучшее значение EER 1,17 %.

Поведенческое профилирование относится к проверке личности пользователя смартфона на основе приложений и служб, которые он использует. В работе [11] предложили подход к аутентификации для поведенческого профилирования пользователей на основе контекста использования мобильных устройств (использование приложения, местоположение, время, использование полосы пропускания и взаимодействие человека с устройством), где для аутентификации использовалась наивная байесовская модель. Авторы работы [12] изучали возможность использования метода поведенческого профилирования на основе истории использования приложений для постоянной проверки мобильных пользователей. Был достигнут EER 9,8 %. Кроме того, была предложена новая модульная структура профилирования поведения, которая не отклоняла бы доступ пользователя только после ряда последовательных нетипичных манипуляций с приложениями. В экспериментах с набором данных MIT Reality значения FRR и FAR составили 11,45 % и 4,17 %. В [13] представили метод аутентификации пользователя смартфона, основанный на статистике использования. Для оценки предложенного подхода использовались два общедоступных набора данных. При использовании двухклассовой SVM была достигнута точность более 85 %.

Авторы [14] использовали акселерометр, гироскоп и датчик сенсорного экрана для аутентификации пользователя смартфона путем анализа того, как пользователь касается телефона. Различные функции, такие как ускорение, давление, размер области касания и течение времени, были собраны с использованием экспериментальных данных как для четырехзначных, так и для восьмизначных PIN-кодов с использованием поведения касания для проверки кодов доступа разных участников. Авторы использовали одноклассовый классификатор, основанный на понятии расстояния до ближайшего соседа для распознавания пользователей. Авторы [15] предложили схему, сочетающую анализ нажатия клавиш и рукописного ввода на смартфонах с целью аутентификации пользователя. Во время записи данных авторы просили разных испытуемых ввести предложение или пароль определенное количество раз. Для оценки своего подхода авторы выбрали различные алгоритмы машинного обучения, включая дерево решений, байесовскую сеть и MLP.

Таким образом, поведенческая биометрия предлагает решения для пассивной и непрерывной аутентификации. Одномодальные системы поведенческой биометрии могут обеспечить приемлемую производительность, однако существует множество проблем, связанных с применением этого типа биометрии. Биометрические датчики очень чувствительны к внешним факторам, приводящим к плохому сбору данных, таким как шум в системах аутентификации на основе голосовых биометрических данных. Кроме того, эмоциональное или физическое состояние пользователя изменчиво с течением времени и может находиться в различных условиях окружающей среды. Также одномодальные биометрические данные уязвимы перед вредоносными атаками, такими как спуфинг и атаки ботов. Мультимодальные биометрические системы зачастую более надежны, чем одномодальные, поскольку они сочетают в себе различные биометрические данные, поэтому может быть достигнут высокий уровень безопасности. Кроме того, слияние нескольких модальностей преодолевает многочисленные проблемы одномодальных систем, включая неуниверсальность некоторых характеристик, внутриклассовые различия, зашумленные сигналы и высокий уровень ошибок. С ростом популярности новых инновационных смартфонов все вышеупомянутые биометрические

системы стали применимы на мобильных устройствах. Однако при выборе и реализации методов аутентификации необходимо учитывать многочисленные ограничения, такие как вычислительные затраты, аппаратные ограничения, скорость, время, необходимое для процесса аутентификации, и потребления энергии. Вопрос о балансе между безопасностью и удобством использования систем аутентификации на основе поведенческой биометрии требует детального анализа и проработки.

Анализ существующих программных решений и постановка задачи. В мобильных устройствах уже встроены различные способы аутентификации пользователя. Но часто используемые схемы аутентификации для защиты смартфонов (такие как пароли, PIN-коды и шаблоны блокировок) уязвимы для многих атак. Пароль или PIN-код можно подсмотреть, либо подобрать с помощью специального программного обеспечения. Пароль пользователя могут получить обманным путем. Не исключены ситуации, когда пароль может быть похищен или отнят у его владельца [16]. Графический ключ можно воспроизвести по наличию отпечатков пальцев на экране смартфона. Смарт-карты, карты с магнитной полоской, USB-ключи требуют специальное оборудование для работы. Не исключена возможность изготовления копии или эмулятора. Биометрическая верификация подвержена атакам спуфинга. Отдельные биометрические данные меняются как в результате старения, так и травм, ожогов, порезов, различных болезней [16].

Многие люди предпочитают использовать меньше барьеров конфиденциальности каждый раз, когда они решают получить доступ к своему устройству, что снижает эффективность таких схем аутентификации и в конечном итоге делает их уязвимыми для кражи данных. Кроме того, эти подходы бесполезны при идентификации пользователя в режиме реального времени из-за их неспособности обнаружить и распознать пользователя после того, как он прошел успешную аутентификацию. Поэтому крайне важно найти эффективные решения этих проблем для защиты конфиденциальных данных, доступных через эти устройства.

Анализ и оценка научных, методологических, технологических, алгоритмических, программных решений показали, что необходимо разработать методику мониторинга и анализа информации, поступающей от различных датчиков мобильных устройств, на основе которой можно было бы с достаточно высокой вероятностью аутентифицировать пользователя мобильного устройства, его типичное и атипичное поведение, а также различные жесты, производимые пользователем с помощью мобильного устройства.

В связи с этим цель работы – повышение безопасности данных пользователя смартфона путем разработки мобильного приложения для аутентификации на основе поведенческой биометрии с применением методов машинного обучения.

Схемы поведенческой биометрии позволяют выявить характеристики поведения пользователя, обладающие определенным паттерном в течение определенного периода времени, таких как движение рук и помахивание, взаимодействие с сенсорным экраном.

Методика аутентификации пользователя смартфона на основе его поведенческой биометрии. Предлагаемая методика состоит из пяти этапов: сбор данных, предварительная обработка данных, извлечение признаков, распознавание жестов пользователя и аутентификация пользователя. На рисунке 3 показаны этапы реализации разработанной методики.

На первом этапе происходит сбор данных, поступающих с датчиков мобильного устройства. Помимо указанных данных для обучения модели необходимо предусмотреть возможность размечать данные о типе выполненного движения. Размеченные данные будут использованы для обучения с учителем.

Данные, собранные с датчиков смартфона, содержат нежелательный шум, создаваемый участниками и генерируемые самими датчиками. Предварительная обработка данных необходима для уменьшения нежелательного шума от данных, поступающих с датчиков и разделения данных на небольшие сегменты для лучшего извлечения признаков. Предварительная обработка данных будет проводиться в два этапа (фильтрация и сегментация). Отфильтрованные данные можно в дальнейшем использовать для извлечения признаков.

Для идентификации пользователей на основе их взаимодействия со смартфоном предполагается использовать распространенные классификаторы: машина опорных векторов (SVM), случайные леса (RF) и байесовская сеть, а также нейронные сети. Классификаторы были выбраны из-за их частого использования и отличной эффективности в существующих исследованиях.

После того как паттерны поведения пользователя совпали с паттернами поведения легитимного пользователя, то есть на основе своих поведенческих черт пользователь подтвердил, что является владельцем мобильного устройства, телефон разблокируется. В случае если же поведенческие черты не совпадают с профилем владельца, занесенным в базу данных, ему будет отказано в доступе.

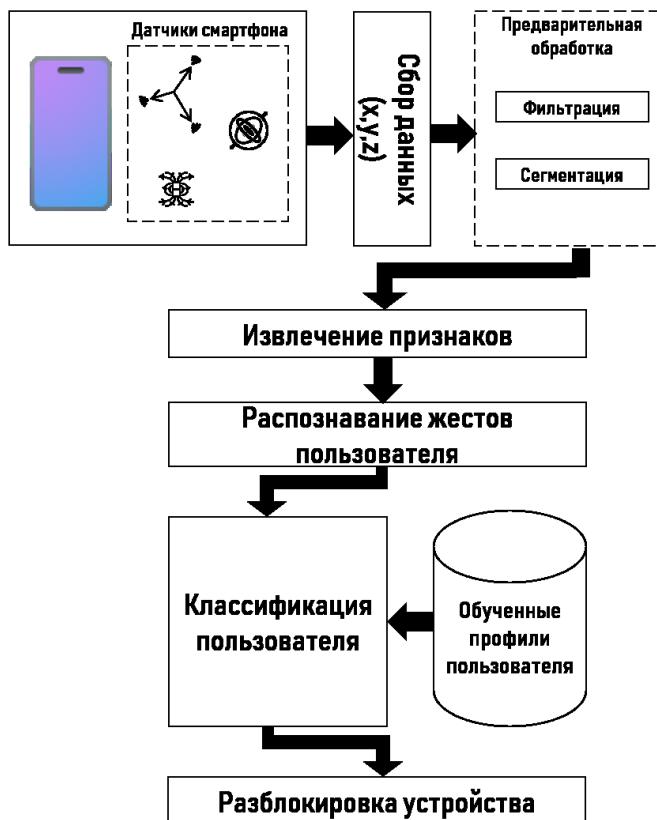


Рисунок 3 – Методика аутентификации пользователя смартфона

Во время эксплуатации модели будет производится непрерывная проверка данных, поступающих с датчиков смартфона. В состав получаемых данных, кроме информации с датчиков, поступают временные метки и информация для идентификации смартфона. В случае, если искомое движение было распознано, информация передается в блок реагирования. На данном этапе происходит обработка информации о выявленном движении пользователя с последующим принятием мер в соответствии с установленными правилами реагирования.

Описание разработанного программного продукта. На первом этапе авторами было принято решение реализовать методику распознавания жестов мобильным устройством. В основные этапы методики входили:

- 1) сбор, предварительная обработка и хранение данных с акселерометра мобильного устройства;
- 2) обучение модели распознавания жестов на основе собранных данных;
- 3) распознавание жеста пользователя смартфона;
- 4) реагирование на распознанные движения смартфоном пользователем.

На основании проведенного анализа исследований в области распознавания движений смартфоном было принято решение в работе в качестве данных использовать показания акселерометра.

Акселерометр – это специальный прибор, предназначенный для измерения кажущегося ускорения. Кажущееся ускорение – это разница между истинным ускорением объекта и гравитационным ускорением. Принципиально акселерометр состоит из пружины, подвижной массы и демпфера.

Необходимо предусмотреть три переменные для передачи информации с акселерометра. Кроме того, для распознавания жеста имеет значение последовательность данных, получаемых с датчика. Для этого необходимо ввести дополнительную переменную, передающую время получения показаний.

Чтобы обучить модель распознавания жестов с применением учителя, необходим большой набор размеченных данных, поэтому к уже перечисленным полям в приложение для сбора датасета необходимо добавить поле «тип жеста», в которое будет помещаться информация о том, какой жест описывает данные показания. Поскольку данные о различных экспериментах в базе будут храниться вместе, для удобства работы с ними также предлагается разметить каждый эксперимент, для этого ввести дополнительное поле для номера эксперимента.

Таким образом, приложение для сбора данных, а также база данных для сбора датасета должна позволять хранить следующие данные:

- измерения акселерометра по трем плоскостям;
- время получения данных с датчика;
- идентификатор мобильного устройства, с которого получены данные;
- тип выполняемого жеста (только в приложении для сбора данных);
- номер эксперимента (только в приложении для сбора данных).

Для хранения базы данных была использована система управления базами данных (СУБД) PostgreSQL версии 14. СУБД PostgreSQL является свободной объектно-реляционной системой управления базами данных. Хранение данных было организовано в таблице «stats» (рис. 4).

	public
	stats
	id integer
	field_x double precision
	field_y double precision
	field_z double precision
	timestamp double precision
	id_phone integer
	type_action integer
	num_ex integer

Рисунок 4 – Таблица «stats»

Для сбора датасета было написано клиент-серверное приложение. Для разработки сервера был использован Spring Framework – универсальный фреймворк с открытым исходным кодом для Java-платформы. В качестве метода для построения серверного API был использован REST (Representational state transfer). REST – это стиль архитектуры программного обеспечения для распределенных систем. Мобильное приложение было разработано для устройств с операционной системой Android. Язык программирования Java. Главная форма приложения представлена на рисунке 5.

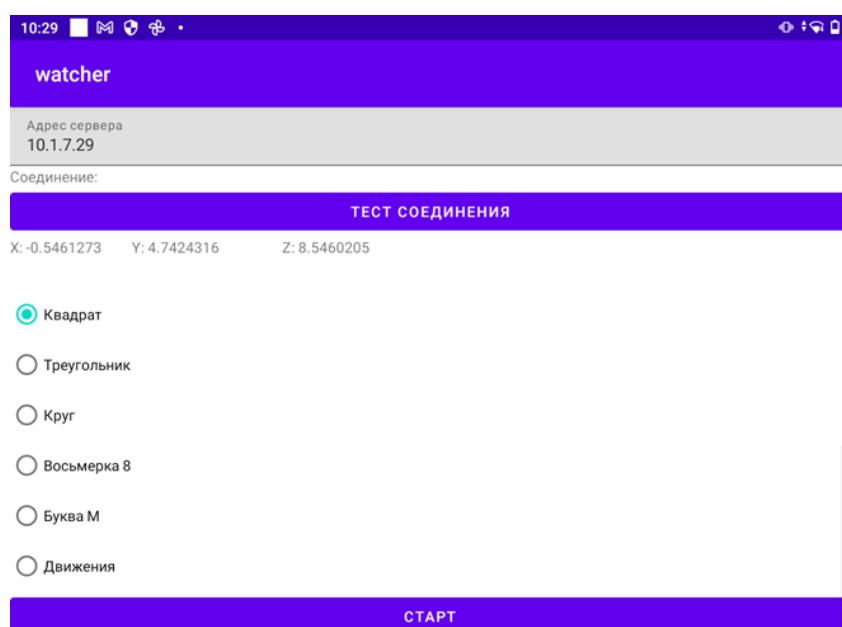


Рисунок 5 – Главная форма приложения для сбора статистики

Приложение состоит из поля для ввода адреса сервера и кнопки проверки соединения. Далее идет ряд переключателей, позволяющих разметить производимые пользователем движения (например, пользователь выбирает переключатель «квадрат» перед тем, как изобразить мобильным устройством квадрат и отправить данные на сервер).

Для сбора данных необходимо отметить переключателем необходимый жест, нажать кнопку «Старт» и воспроизвести жест мобильным устройством. После того как движение будет завершено, необходимо нажать кнопку «Стоп». Собранные данные в формате JSON будут отправлены на сервер и записаны в базу данных.

В результате было собрано 40415 строк данных с показаниями акселерометра при выполнении разных жестов. В ходе сбора данных выполнялись следующие жесты:

- квадрат (0);
- треугольник (1);
- круг (2);
- восьмерка (3);
- буква «M» (4);
- движения смартфоном при обычной эксплуатации (5).

Графическое представление выбранных жестов пользователя для распознавания показано на рисунке 6.

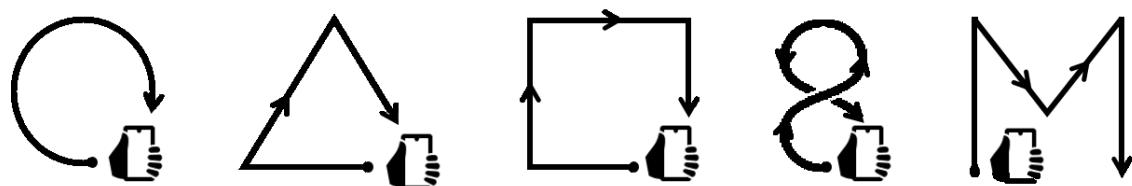


Рисунок 6 – Графическое представление выбранных жестов

Пример собранных данных представлен в таблице 1.

Таблица 1 – Пример данных для обучения модели

id	field_x	field_y	field_z	timestamp	id_phone	type_action	num_ex
53	0,61102062463760	-2,6297397613525	10,14796352386	2,53E+14	6,89E+08	4	7,31E+08
54	0,85807800292968	-1,9876708984375	9,588699340820	2,53E+14	6,89E+08	4	7,31E+08
55	0,85807800292968	-1,9876708984375	9,588699340820	2,53E+14	6,89E+08	4	7,31E+08
56	-0,352984607219696	-1,6766933202743	8,730855941772	2,53E+14	6,89E+08	4	7,31E+08
57	-0,37733459472656	-1,6704406738281	8,713607788085	2,53E+14	6,89E+08	4	7,31E+08

На рисунке 7 представлен график значений акселерометра по трем осям при воспроизведении фигуры «квадрат».

Далее полученные данные были использованы для обучения модели нейронной сети, которая лежит в основе распознавания жестов пользователя мобильного устройства.

Поскольку самым слабым местом в обработке параметров, поступающих с датчиков мобильных устройств, является этап выделения признаков, оптимальным решением будет применить метод машинного обучения, который меньше зависит от качества выделения этих признаков [17]. Кроме того, выделение признаков – довольно емкая операция с точки зрения временных затрат, и в большинстве случаев выбранные признаки могут не отражать всю сложность взаимосвязей и закономерностей, которые могут быть в анализируемых данных. При анализе методы глубокого обучения дают более высокие результаты по классификации и распознаванию объектов, чем подходы, которые основываются на признаках, выделенных вручную. Нейронные сети и глубокое обучение, в частности, все активнее захватывают первенство среди методов машинного обучения. При решении задачи распознавания жестов человека, совершаемых смартфоном, на основе показаний акселерометра данные с датчиков рассматриваются как одномерная сеть из выборочных совокупностей, полученных через равные интервалы времени. Как показывает анализ работ в этом области, нейронные сети можно использовать в обработке сигналов, что позволяет отказаться от этапа выделения признаков, поскольку обучение нейронной сети включает этот этап.

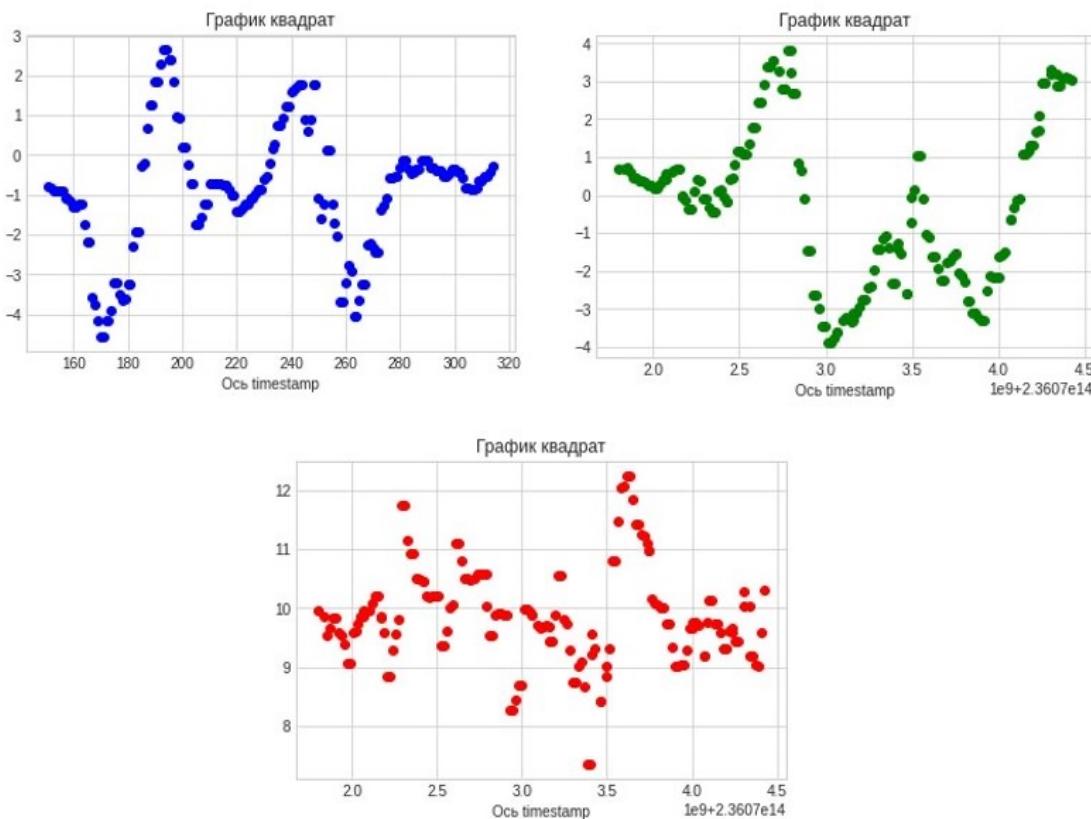


Рисунок 7 – График показаний трехосевого акселерометра для жеста «квадрат»

Для проектирования нейронной сети необходимо сначала определить количество нейронов во входном и выходном слоях. Поскольку в качестве примеров распознаваемых движений было выбрано 5 движений (круг, квадрат, треугольник, буква «М» и цифра «8»), а также обычные движения смартфоном, которые не должны быть определены как распознаваемое движение, то выходной слой нейронной сети должен составить 6 нейронов.

На вход нейронной сети подаются показания с трехосевого акселерометра. Проанализируем, сколько точек было получено для различных движений. Общее количество экспериментов составило 243. Из них:

- квадрат (40 штук);
- треугольник (36 штук);
- круг (40 штук);
- восьмерка (45 штук);
- буква «М» (43 штуки);
- движения смартфоном при обычной эксплуатации (39 штук).

Количество точек данных на эксперимент составило от 100 до 255. При этом поскольку показания снимались с трехосевого акселерометра, то каждая точка включала в себя значения по трем плоскостям. Таким образом, было принято решение – на вход сети подавать 100 точек данных, а количество нейронов во входном слое составило $100 * 3$ штук. Для работы были спроектированы несколько нейронных сетей с количеством скрытых слоев 2 и 3. Общие характеристики сетей представлены в таблице 2.

В качестве функции потери была использована «перекрестная энтропия классификации» и оптимизатор Adam. В оптимизаторе скорость обучения позволяет задать допустимую степень изменения весовых коэффициентов в нейронной сети в отношении градиента потери. В ходе обучения для данного параметра использовалось значение 0,001.

Далее имеющийся датасет был разделен на две части: для обучения и тестирования в отношении 70 % и 30 %. После этого нейронные сети были обучены. Количество эпох во всех экспериментах составило 50. Этого количества было достаточно, чтобы сеть обучилась и перестала улучшать свои показатели.

Таблица 2 – Параметры нейронных сетей

№	Количество скрытых слоев	Количество нейронов в первом слое	Количество нейронов во втором слое	Количество нейронов в третьем слое
HC 1	3	64	64	32
HC 2	3	256	128	64
HC 3	3	256	256	256
HC 4	3	64	64	64
HC 5	2	64	64	–
HC 6	2	32	32	–
HC 7	2	16	16	–
HC 8	2	32	16	–
HC 9	2	32	8	–
HC 10	2	64	32	–
HC 11	2	128	32	–

Лучше показатели обученных сетей представлены в таблице 3.

Таблица 3 – Результаты обучения нейронных сетей

	HC 1	HC 2	HC 3	HC 4	HC 5	HC 6	HC 7	HC 8	HC 9	HC 10	HC 11
Accuracy всей модели, %	91	91	91	93	93	93	93	94	93	94	93
Accuracy квадрат, %	82	88	82	88	88	88	82	88	82	88	88
Accuracy треугольник, %	80	60	100	100	100	100	100	100	100	100	100
Accuracy круг, %	100	100	91	100	91	91	100	100	100	100	91
Accuracy восьмерка, %	100	100	100	92	100	100	100	100	100	100	100
Accuracy буква «М», %	100	100	100	100	100	100	100	100	100	100	100
Accuracy обычные движения, %	85	85	85	85	85	85	85	85	85	85	85

Как видно из таблицы, лучшие показатели были у сетей с относительно небольшим количеством нейронов. Лучшие показатели были у сетей HC 8 и HC 10. В работу была выбрана сеть HC 8, так как у нее было наименьшее количество нейронов из рассмотренных двух сетей.

При разработке серверной части информационной системы были использованы следующие технологии:

- Spring Framework;
- Spring boot;
- Flask;
- СУБД PostgreSQL;
- языки программирования Java и Python.

При запуске сервер загружает переобученную модель полно связной нейронной сети и ожидает запросы, поступающие с основного сервера. После получения данных сначала происходит их обработка и сокращение количества элементов массива с показаниями акселерометра до 100 элементов. Далее все показатели «вытягиваются» в один массив, при этом показания по трем осям акселерометра записываются последовательно друг с другом. На выходе получается 300 точек данных, которые преобразовываются в тензор и передаются на вход модели. Выходные данные с информацией о распознанном жесте, а также информация об идентификаторе телефона в JSON-формате передаются на основной сервер.

В ходе выполнения исследования было разработано мобильное приложение для ОС Android. Приложение включает 8 форм и взаимодействует с сервером посредством сети с применением технологии REST. Снятие показаний с акселерометра осуществлялось стандартными средствами ОС Android. Для взаимодействия с сервером со стороны мобильного приложения был реализован ряд запросов, соответствующий API сервера. Для разработки запросов была использована библиотека Retrofit, применение которой позволило значительно ускорить и упростить разработку программного продукта. Каждый запрос выполняется в отдельном асинхронном потоке, что позволяет избавиться от «зависания» пользовательского интерфейса на время, пока ожидается ответ сервера. Поскольку приложение должно непрерывно отсыпать на сервер показания акселерометра (даже в случае, если пользователь его свернул или закрыл), было принято решение вынести код отправки данных на сервер в отдельный поток и оформить его в виде сервиса (Service) – специального компонента мобильного приложения, который может выполнять длительные операции в фоновом режиме.

Таким образом, разработанное мобильное приложение позволяет собирать показания акселерометра смартфона и передавать их на сервер для дальнейшего распознавания движения мобильным устройством с применением методов машинного обучения, выводить на экран информацию о характере движений, полученную с сервера.

Результаты распознанных жестов, отображаемые на главной форме, представлены на рисунках 8 и 9.

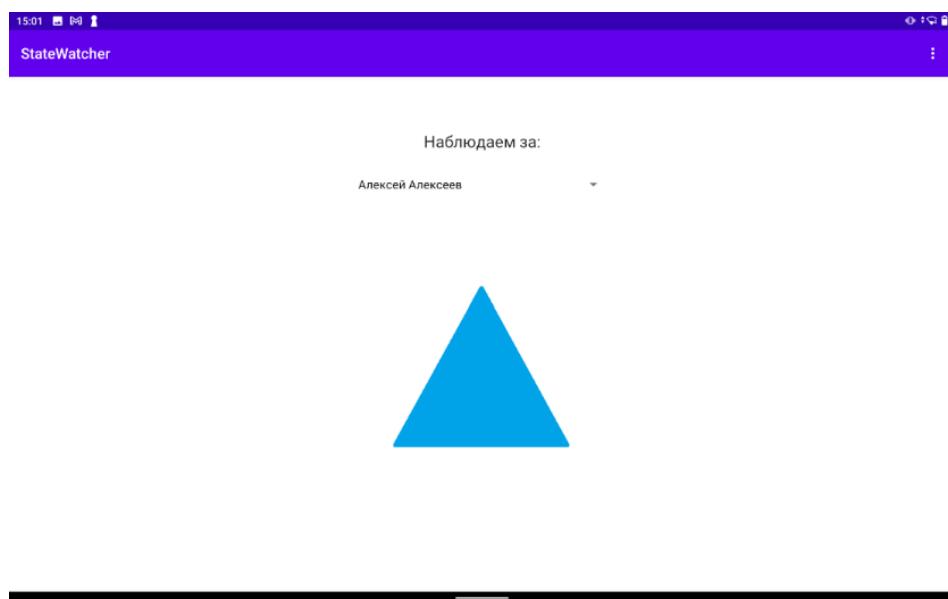


Рисунок 8 – Отображение распознанного жеста пользователя (треугольник)

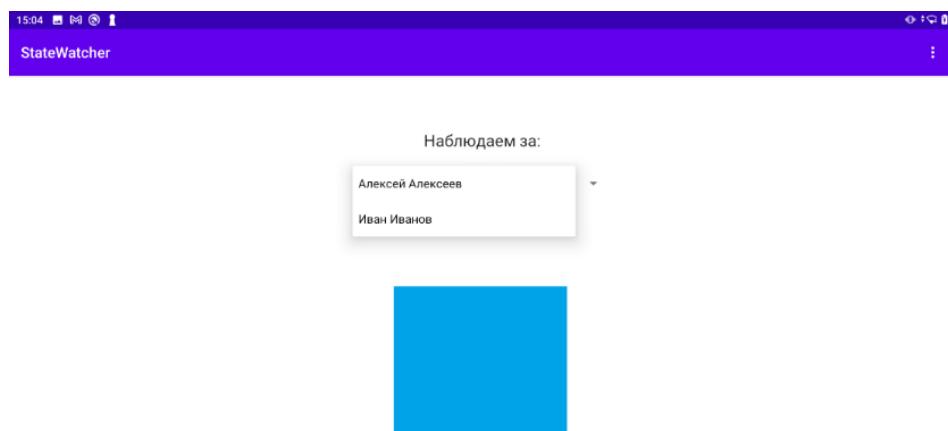


Рисунок 9 – Отображение распознанного жеста пользователя (квадрат)

Заключение. Таким образом, в ходе работы были предложены решения, направленные на сбор, обработку информации, получаемых от пользователя смартфона; была описана предложенная методика для распознавания поведенческих черт пользователя смартфона и методики формирования наборов данных для обучения модели. Было разработано и протестировано мобильное приложение, которое позволяет собирать показания акселерометра смартфона и передавать их на сервер для дальнейшего распознавания движения мобильным устройством с применением методов машинного обучения, выводить на экран информацию о характере движения, полученную с сервера. Результаты тестирования позволяют говорить о полноценности разработанного прототипа приложения.

Библиографический список

1. Отчет об утечках данных за 1 полугодие 2022 года // INFOWATCH. – Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 21.12.2022).
2. Committee on technology, committee on homeland and national security, subcommittee on biometrics // Vascular Pattern Recognition. – 2006. – P. 1–33.
3. Banerjee, S. P. Biometric authentication and identification using keystroke dynamics: A survey / S. P. Banerjee and D. L. Woodard // Journal of Pattern Recognition Research. – 2012. – Vol. 7, no. 1. – P. 116–139.
4. Teh, Pin Shen. A survey on touch dynamics authentication in mobile devices / Teh, Pin Shen, Zhang, Ning, Teoh, Andrew Beng Jin et al. // Computers and Security. – 2016. – Vol. 59. – P. 210–235.
5. Wan, Changsheng. A survey on gait recognition / Wan, Changsheng, Wang, Li, Phoha, Vir V. // ACM Computing Surveys. 2018. – Vol. 51, № 5.
6. Giuffrida, C. I Sensed It Was You: Authenticating Mobile Users with Sensor-enhanced Keystroke Dynamics / C. Giuffrida, K. Majdanik, M. Conti et al. // Proceedings of the 11th Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA). – Springer, 2014. – P. 92–111 (Lecture Notes in Computer Science).
7. Darabseh, A. Keystroke Active Authentications Based on Most Frequently Used Words / A. Darabseh & A. S. Namin // Proceedings of the 2015 ACM International Workshop on International Workshop on Security and Privacy Analytics. – 2015.
8. Alghamdi, S. J. Dynamic authentication of smartphone users based on touchscreen gestures / S. J. Alghamdi, and L. A. Elrefaei // Arabian Journal for Science and Engineering. – 2018. – № 43 (2). – P. 789–810.
9. Larcher, A. Text-dependent speaker verification: Classifiers, databases and RSR2015 / A. Larcher, K. Lee, B. Ma, & H. Li // Speech Commun. – 2014. – Vol. 60. – P. 56–77.
10. Liu, X. Multi-source interactive behavior analysis for continuous user authentication on smartphones / X. Liu, C. Shen, Y. Chen // CCBR 2018. LNCS. – 2018. – Vol. 10996. – P. 669–677.
11. Bassu, D., Cochinwala, M. & Jain, A. // 2013 IEEE International Conference on Technologies for Homeland Security. – HST, 2013. – P. 441–446.
12. Li, Fudong. Active authentication for mobile devices utilising behaviour profiling / Li, Fudong, Clarke, Nathan, Papadaki, Maria et al. // International Journal of Information Security. – 2014. – Vol. 13, № 3. – P. 229–244.
13. Datta, Trisha. Using SVM for user profiling for autonomous smartphone authentication / Datta, Trisha and Kyriakos Manousakis // 2015 IEEE MIT Undergraduate Research Technology Conference (URTC). – 2015. – P. 1–5.
14. Zheng, N. You are how you touch: User verification on smartphones via tapping behaviors / N. Zheng, K. Bai, H. Huang, H. Wang // International Conference on Network Protocols, ICNP. – 2014. – P. 221–232.
15. Trojahn, M. Toward mobile authentication with keystroke dynamics on mobile phones and tablets / M. Trojahn, F. Ortmeier // Proceedings of the 27th International Conference on Advanced Information Networking and Applications Workshops, Barcelona, Spain, 25–28 March 2013. – P. 697–702.
16. Десятов, Сергей Васильевич. Сравнительный анализ достоинств и недостатков наиболее распространенных методов идентификации и аутентификации пользователей и других участников идентификационных процессов / Сергей Васильевич Десятов // Интерэкско Гео-Сибирь. – 2021. – Режим доступа: <https://cyberleninka.ru/article/n/sravnitelnyy-analiz-dostoinstv-i-nedostatkov-naiboleerasprostranennyh-metodov-identifikatsii-i-autentifikatsii-polzovatelye-i>, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 22.12.2022).
17. Panagiotis, Kasnesis. Changing Mobile Data Analysis through Deep Learning / Panagiotis Kasnesis, Charalampos Z. Patrikakis, Iakovos S. Venieris // IT Pro, May/June 2017. IEEE Computer Society. – Режим доступа: <https://www.osp.ru/os/2017/03/13052701>, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 04.01.2023).

References

1. Otchet ob utechkakh dannykh za 1 polugodiye 2022 goda [Data Breach Report for 1H 2022]. INFOWATCH. Available at: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf (accessed 12.21.2022).
2. Committee on technology, committee on homeland and national security, subcommittee on biometrics. Vascular Pattern Recognition, 2006, pp. 1–33.
3. Banerjee, S. P. and Woodard, D. L. Biometric authentication and identification using keystroke dynamics: A survey. *Journal of Pattern Recognition Research*, vol. 7, no. 1, 2012, pp. 116–139.
4. Teh, Pin Shen, Zhang, Ning, Teoh, Andrew Beng Jin et al. A survey on touch dynamics authentication in mobile devices. *Computers and Security*, 2016, vol. 59. pp. 210–235.
5. Wan, Changsheng, Wang, Li, Phoha, Vir V. A survey on gait recognition. *ACM Computing Surveys*, 2018, vol. 51, no. 5.

6. Giuffrida, C., Majdanik, K., Conti, M. et al. I Sensed It Was You: Authenticating Mobile Users with Sensor-enhanced Keystroke Dynamics. *Proceedings of the 11th Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*. Springer, 2014, pp. 92–111 (Lecture Notes in Computer Science).
7. Darabseh, A., & Namin, A. S. Keystroke Active Authentications Based on Most Frequently Used Words. *Proceedings of the 2015 ACM International Workshop on International Workshop on Security and Privacy Analytics*, 2015.
8. Alghamdi, S. J. and Elrefaei, L. A. Dynamic authentication of smartphone users based on touchscreen gestures. *Arabian Journal for Science and Engineering*, 2018, no. 43 (2), pp.789–810.
9. Larcher, A., Lee, K., Ma, B., & Li, H. Text-dependent speaker verification: Classifiers, databases and RSR2015. *Speech Commun.*, 2014, vol. 60, pp. 56–77.
10. Liu, X., Shen, C., Chen, Y. Multi-source interactive behavior analysis for continuous user authentication on smartphones. *CCBR 2018. LNCS*, 2018, vol. 10996, pp. 669–677.
11. Bassu, D., Cochiniwala, M. & Jain, A. *2013 IEEE International Conference on Technologies for Homeland Security. HST 2013*. pp. 441–446.
12. Li, Fudong, Clarke, Nathan, Papadaki, Maria et al. Active authentication for mobile devices utilising behaviour profiling. *International Journal of Information Security*, 2014, vol. 13, no. 3. pp. 229–244.
13. Datta, Trisha and Kyriakos Manousakis. Using SVM for user profiling for autonomous smartphone authentication. *2015 IEEE MIT Undergraduate Research Technology Conference (URTC)*, 2015, pp. 1–5.
14. Zheng, N., Bai, K., Huang, H., Wang, H. You are how you touch: User verification on smartphones via tapping behaviors. *International Conference on Network Protocols, ICNP*, 2014, pp. 221–232.
15. Trojahn, M., Ortmeier, F. Toward mobile authentication with keystroke dynamics on mobile phones and tablets. *Proceedings of the 27th International Conference on Advanced Information Networking and Applications Workshops, Barcelona, Spain, 25–28 March 2013*, pp. 697–702.
16. Desyatov, Sergey Vasilievich. Sravnitelnyy analiz dostoinstv i nedostatkov naiboleye rasprostranennykh metodov identifikatsii i autentifikatsii polzovateley i drugikh uchastnikov identifikatsionnykh protsessov [Comparative analysis of the advantages and disadvantages of the most common methods of identification and authentication of users and other participants in identification processes]. *Interexpo Geo-Siberia*, 2021. Available at: <https://cyberleninka.ru/article/n/sravnitelnyy-analiz-dostoinstv-i-nedostatkov-naiboleerasprostranennyh-metodov-identifikatsii-i-autentifikatsii-polzovateley-i> (accessed 12.22.2022).
17. Panagiotis, Kasnesis, Charalampos, Z. Patrikakis, Iakovos, S. Venieris, Changing Mobile Data Analysis through Deep Learning. *IT Pro, May/June 2017, IEEE Computer Society*. Available at: <https://www.osp.ru/os/2017/03/13052701> (accessed 04.01.2023).