12. Paniotto V. I., Maksimenko V. S. *Kolichestvennye metody v sotsiologicheskikh issledovaniyakh* [Quantitative methods in sociological research]. Kiev, Naukova Dumka Publ., 1982. 272 p.

13. Prioritetnyy proekt «Sovremennaya tsifrovaya obrazovatelnaya sreda v Rossiyskoy Federatsii», utverzhdennyy Prezidiumom Soveta pri Prezidente RF po strategicheskomu razvitiyu i prioritetnym proektam (protokol ot 25 oktyabrya 2016 g. № 9)], [Priority project "Modern digital educational environment in the Russian Federation"]. *Konsultant* [Consultant]. Available at: http://www.consultant.ru/ (accessed 20.01.2020)

14. *Prioritetnyy proekt «Tsifrovaya shkola»* [Priority project "Digital school"]. Available at: http://government.ru/projects/selection/693/30822/ (accessed 20.01.2020)

15. *Realizatsiya dostupa k onlayn-kursam po printsipu «odnogo okna»* [Realization of access to online courses on a one-stop basis]. Available at: http://neorusedu.ru/activity/realizatsiya-dostupa-k-onlayn-kursam-po-printsipu-odnogo-okna (accessed 10.04.2020).

DOI 10.21672/2074-1707.2020.51.1.083-093
УДК 004.056

ИССЛЕДОВАНИЕ СИСТЕМЫ ИДЕНТИФИКАЦИИ И ПОДТВЕРЖДЕНИЯ ЛЕГИТИМНОСТИ ДОСТУПА НА ОСНОВЕ ДИНАМИЧЕСКИХ МЕТОДОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ[1]

Статья поступила в редакцию 19.04.2020, в окончательном варианте – 10.09.2020.

Путято Михаил Михайлович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,

кандидат технических наук, доцент, ORCID: https://orcid.org/0000-0001-9974-7144, e-mail: putyato.m@gmail.com

***Макарян Александр Самвелович*,** Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,

кандидат технических наук, доцент, e-mail: msanya@yandex.ru

Чич Шамиль Муратович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,

студент, e-mail: shama_chich@icloud.com

Маркова Валентина Константиновна, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,

студентка, e-mail: markokovt@yandex.ru

Биометрические методы основаны на определении личности человека по присущим только ему признакам. В статье рассматриваются характеристики клавиатурного прочерка как динамической биометрической характеристики личности. Осуществляется анализ и выбор характеристик, необходимых для идентификации. Алгоритм процесса формирования эталонного образца клавиатурного почерка основан на основе фиксации временных параметров. Рассматриваются классические статистические подходы идентификации пользователей по клавиатурному почерку. Исследованиями установлено, что подходы для сбора и анализа параметров подходят и для формирования клавиатурного почерка на мобильных устройствах. Отмечено, что использование клавиатурного почерка в качестве единственного фактора аутентификации на мобильном устройстве пока не достигает достаточной точности, но вполне приемлемо в качестве дополнительного фактора аутентификации. Для решения задачи идентификации предложено использовать клиент-серверное приложение, дана его характеристика, проведены тестовые испытания и проведен анализ полученных результатов.

Ключевые слова: кибербезопасность, форензика, динамические биометрические характеристики, идентификация, биометрия, защита данных, клавиатурный почерк, защита информации, база данных

[1] Статья подготовлена в рамках исследований, проводимых при реализации гранта РФФИ (2.10.187 «Разработка теоретических основ и алгоритмов функционирования адаптивных систем управления ситуационных центров на основе методов искусственного интеллекта»).

Графическая аннотация (Graphical annotation)

SYSTEM DEVELOPMENT FOR IDENTIFICATION AND CONFIRMATION OF ACCESS LEGITIMACY BASED ON BIOMETRIC AUTHENTICATION DYNAMIC METHODS

The article has been received by editorial board 19.04.2020, in the final version 10.09.2020.

Putyato Michael M., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,

Cand. Sci (Engineering), Associate Professor, ORCID: https://orcid.org/0000-0001-9974-7144, e-mail: putyato.m@gmail.com

Makaryan Alexander S., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,

Cand. Sci (Engineering), Associate Professor, e-mail: msanya@yandex.ru

Chich Shamil M., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,

student, e-mail: shama_chich@icloud.com

Markova Valentina K., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,

student, e-mail: markokovt@yandex.ru

Biometric methods are based on determining a person's identity based on characteristics that are unique to them. The article considers the characteristics of the keyboard dash as a dynamic biometric characteristic of a person. The analysis and selection of characteristics necessary for identification is carried out. Algorithm for the process of forming a reference sample of keyboard handwriting based on fixing time parameters. Classical statistical approaches to identifying users by keyboard handwriting are considered. It was found that approaches for collecting and analyzing parameters are also suitable for forming keyboard handwriting on mobile devices. It is noted that the use of keyboard handwriting as the only authentication factor on a mobile device does not yet achieve sufficient accuracy, but it is quite acceptable as an additional authentication factor. To solve the identification problem, it is proposed to use a client-server application, its characteristics are given, test tests are carried out and the results of the results are analyzed.

Keywords: cybersecurity, forensics, dynamic biometric characteristics, identification, biometrics, data protection, keyboard handwriting, information security, database

Введение. В эпоху цифровых технологий задачинепрерывного обеспечения защиты информации являются наиболее актуальными. Современные классические программно-аппаратные средства идентификации и аутентификации функционируют непосредственно во время авторизации пользователя в системе. Однако данные методы не обеспечивают достоверность того, что после авторизации в системе продолжает работать легитимный пользователь. С точки зрения оценки безопасности и механизмов защиты данных пользователей, например, на мобильных платформах, локальные критичные данные вызывают наибольший интерес [3]. В том случае, когда доступ к устройству получает злоумышленник, на весь период взаимодействия остается угроза утечки важной информации.

Для решения проблемы утечки конфиденциальной информации возможно использовать клавиатурный мониторинг пользователей.

В настоящее время одним из перспективных методов является распознавание клавиатурного почерка на основе анализа динамических биометрических характеристик человека. Данный метод основан на анализе следующих характеристик пользователя [8]:

- скорость ввода текста;
- время удержания клавиш [2];
- интервал между нажатиями на клавиши;
- частота образования ошибок при вводе (частота нажатия на клавишу delete);

- частота использования функциональных клавиш и комбинаций, применительно к одному и тому же классу устройств ввода;
- уровень аритмичности при наборе и др.

Общая характеристика методов биометрической аутентификации. Биометрические методы основаны на определении личности человека по присущим только ему признакам. Основное достоинство биометрических методов состоит в том, что такие признаки невозможно украсть или передать другому человеку.

Биометрические методы делятся на физиологические, поведенческие и комбинированные. Подробная классификация представлена на рисунке 1.

Поведенческие характеристики сложнее распознать с высокой точностью, но вместе с тем сложнее и подделать.

Современная биометрическая аутентификация основывается на двух методах [15]:

- статический метод. Этот метод аутентификации основан на распознании физических параметров человека, которыми он обладает на протяжении всей жизни: отпечатки пальцев, отличительные характеристики радужной оболочки глаза, рисунок глазной сетчатки, термограмма, геометрия лица, геометрия кисти руки и даже фрагмент генетического кода);
- динамический метод. Основан на анализе особенностей поведения пользователя, которые проявляются в процессе выполнения повседневных действий (подпись, клавиатурный почерк, голос и др.).

Биометрическая аутентификация не определяет пользователя с абсолютной точностью. В связи с тем, что некоторые реализации стойких криптосистем, например, систем аутентификации, основанных на постквантовых преобразованиях, находятся на этапе теоретического обоснования и прототипной проработки [5], биометрические характеристики пользователей будут занимать основную роль в процессе подтверждения личности. При этом существует вероятность допуска ошибок первого (отказ в доступе) и второго рода (ложный доступ) [7].

Рисунок 1 – Классификация биометрических методов

Эффективность систем биометрической аутентификации принято оценивать по двум характеристикам:

- *отказ в доступе* (ошибка первого рода – FRR, false. rejectionrate) – с какой вероятностью система не узнает зарегистрированного пользователя;

- *ложный доступ* (ошибка второго рода – FAR, falseaccessrate) – вероятность ошибочного допуска нелегального пользователя.

Процесс получения оценочных данных для конкретного человека подразумевает однократное, периодическое или непрерывное получение данных о его действиях при вводе контрольной фразы или набора данных, характерных для его постоянной деятельности.

Основное место на рынке биометрической защиты всегда занимал статический метод, динамическая аутентификация и комбинированные системы защиты информации занимали всего лишь 20 % рынка [17].

Следует отметить, что классическая биометрия, использующая *статические* методы, имеет ряд проблем [13]:

- идентификация пользователя только на определенном этапе взаимодействия: вход, подтверждение транзакции и т.п.;
- механизмы основаны на анализе персональных данных пользователя;
- требуют внедрения дополнительных технических устройств;
- каждый дополнительный фактор идентификации уменьшает успешность транзакции на 15–20 %;
- основаны на внешних (видимых) физиологических характеристиках.

Преимущества *динамических* методов биометрической аутентификации над статическими очевидны:

- непрерывная проверка подлинности для обнаружения несанкционированного доступа во время всего сеанса;
- не требует изменения пользовательского поведения (скрытый метод идентификации);
- работает на всех платформах и устройствах без дополнительного оборудования.

Следует отметить, что в последние годы, наблюдается резкая тенденция развития динамических методов защиты [12]. Сравнение существующих методов представлено в таблице 1.

Таблица 1 – Сравнение результативности использования методов биометрической аутентификации

Метод биометрической аутентификации	**FAR (коэффициент ложного допуска)**	**FRR (коэффициент ложного отказа)**	**Фальсификация**	**Комфорт пользователя**	**Стоимость**
Отпечаток пальца	0,001%	0,6 %	Возможна	Средний	Низкая
Распознавание лица 2D	0,1%	2,5 %	Возможна	Средний	Средняя
Распознавание лица 3D	0,0005%	0,1 %	Проблематична	Средний, ниже среднего	Высокая
Радужная оболочка глаза	0,00001%	0,016 %	Невозможна	Высокий	Высокая
Сетчатка глаза	0,0001%	0,4 %	Невозможна	Низкий	Высокая
Рисунок вен ладони	0,0008%	0,01 %	Невозможна	Средний	Средняя
Голос	0,75%	0,75 %	Возможна	Средний	Низкая
Клавиатурный почерк	0.01%	0,01 %	Возможна	Высокий	Низкая

Основываясь на приведённых данных, можно сделать вывод о том, что применение динамических методов биометрической аутентификации, а именно клавиатурного почерка, является востребованным. Однако при существующем уровне интегрированности программного обеспечения такое применение возможно только в качестве вспомогательного фактора аутентификации для мобильных устройств. Обратим внимание, что выполняются три основных требования к аутентификации [14]:

- знания какой-то информации, известной только пользователю, например, пароль или контрольная фраза;
- владения какого-то устройства, которое имеется только у пользователя, – телефон;
- уникальности, присущей пользователю и однозначно идентифицирующей личность, – биометрические данные.

Роль статистических алгоритмов в динамических методах аутентификации и идентификации. Масштабное исследование биометрических методов, проведенное Национальным бюро стандартов, позволило сделать предельные оценки: вероятность правильного распознавания

пользователей с установившимися навыками работы с клавиатурой составила 98 %, что вполне достаточно для того, чтобы говорить об успешной практической применимости подобных систем [16].

Анализ клавиатурного почерка имеет свои достоинства и недостатки [6], ровно, как и любые биометрические методы [1].

К достоинствам можно отнести следующее:

- для биометрической идентификации достаточно физических параметров человека и не нужны никакие файлы (которые, например, можно скопировать) или пароли (которые, например, можно взломать)
- уникальные человеческие качества хороши тем, что их трудно подделать;
- в отличие от бумажных идентификаторов (паспорт, водительские права, страховое свидетельство, ИНН), или пароля, или персонального идентификационного номера (ПИН), биометрические характеристики не могут быть забыты или потеряны, их всегда легко «предъявить».

К недостаткам можно отнести:

- недоверие со стороны пользователей. (Широкие массы пользователей пока не готовы к переходу на такой вид идентификации);
- вопросы к точности и достоверности. (Ни один из биометрических подходов не дает 100%-й точности);
- высокая цена. (Издержки, связанные с реализацией и поддержкой биометрической системы выше, чем при использовании паролей);
- угроза конфиденциальности.

При анализе клавиатурного почерка существует ряд сложностей [9]:

- разброс параметров клавиатурного почерка в зависимости от психофизического состояния пользователя;
- разброс параметров клавиатурного почерка в зависимости от используемой клавиатуры. В работе [11] говорится, что исследование КП пользователя на разных клавиатурах дало разброс вероятности аутентификации на 0,5 %.
- необходимость сбора большого количества статистических данных для каждого исследования КП, отсутствие готовых баз данных с образцами КП.

Рассмотрим наиболее исследованный подход на основании вероятностно-статистических методов. Проведём сравнение статистических алгоритмов [16] по некоторым критериям оценки, характерным для функциональных характеристик человека (табл. 2).

Таблица 2 – Аутентификация и идентификация с использованием статистических алгоритмов

Параметры	**Тип тестирования**	**Метод распознавания**	**Количество пользователей**	**Количество образцов**	**FAR**	**FRR**	**ERR**
Время удержания	Статистический (Statistical)	Статичный	64	310	0,47	1,32	2,2
	Статистический (Statistical)	динамичный	25	1620	-	-	-
	Статисчические классификаторы (Statisticalclassifiers)	Статичный	100	5000	1,4	1,4	1,41
	Гипотезы (Hypothesis)	Статичный	16	3200	4,5	5,5	-
	Манхетоновское расстояние (Manhattan)	статичный	51	20400	-	-	9,6
	Угловыезадержки (Angle b/w latencies)	статичный	15	-	3,6	4,7	-
Интервалы между нажатиями	Статистический (Statistical)	Статичный	44	220	0	2,3	-
	Мера расстояния (Distancemeasure) (мера Хэмминга)	динамичный	31	-	8,33	2,6	-
	Относительный, абсолютная дистанция (Relative, Abs. distance)	Статичный, динамичный	205	765	0,005	5	0,5
	Степеньбеспорядка (Degree of disorder)	Статичный	18	810	0	0,55	-
Время удержания и интервалы между нажатиями	Статистический (Statistical)	Динамичный	21	-	9	5	-

Исходя из полученных результатов, аутентификацию на основе анализа клавиатурного почерка можно считать эффективной, также следует отметить, что в настоящее время нет приложения для анализа клавиатурного почерка для мобильных устройств, что подтверждает актуальность

дальнейшего исследования динамических методов биометрической аутентификации и дальнейшей реализации клиентского приложения для мобильных устройств.

Помимо анализа клавиатурного почерка был предложен способ идентификации и аутентификации, в основе которого лежит метод распознавания подписи субъекта доступа [11]. Этапы данного подхода:

1) получение геометрических данных подписи с дигитайзера;
2) оцифровка и передача данных в ПК с помощью стандартных интерфейсов;
3) дальнейший анализ с помощью различных программных средств.

В данном методе идентификации/аутентификации основными параметрами служат кривизна, скорость, время, нажим и топологические инварианты (связность, количество и последовательность точек самопересечения).

Входящий образ формируется путем ввода подписи в специальный планшет (дигитайзер). Далее производится цифровое преобразование таких величин, как: координаты конца пера, звуковое давление, положение рук). Далее параметры записываются в текстовый файл, структура которого состоит из трех столбцов x, y, t , где x, y – координаты пера, t – время.

Однако высокая чувствительность дигитайзера к условиям эксплуатации и внешним факторам, а также относительно низкая распространенность подобного рода устройств не позволяют считать данный подход перспективным для массового использования для идентификации/аутентификации пользователей [4]. Но данный подход можно адаптировать и использовать в мобильных устройствах, которые оснащены сенсорным экраном. Такой подход позволит полноценно производить аутентификацию и идентификацию пользователей.

Реализация применения динамических методов биометрической аутентификации для мобильных устройств на основе статистических алгоритмов. Разрабатываемое программное приложение (рис. 2) предназначено для непрерывного сбора информации о клавиатурных нажатиях на русском/английском языках и идентификации санкционированных или несанкционированных действий пользователя.

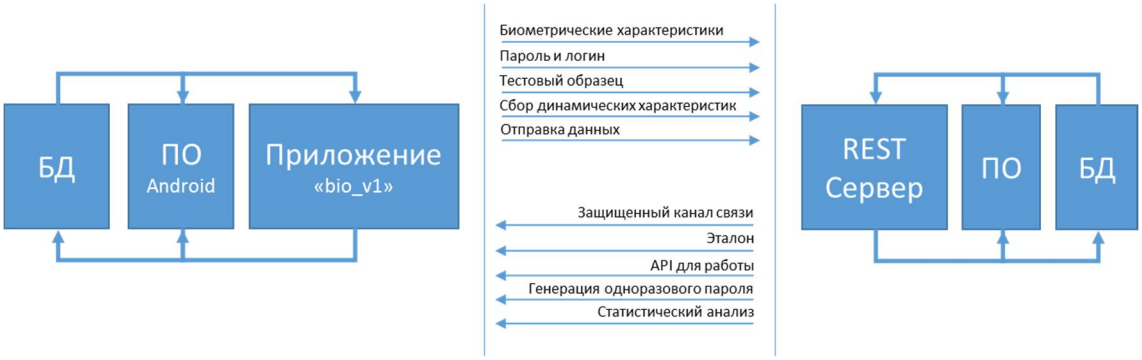

Рисунок 2 – Архитектура системы аутентификации и идентификации пользователей

Система реализуется на базе клиент-серверной архитектуры. На стороне клиента имеется приложение, позволяющее считывать биометрические данные – время удержания клавиш. Тестовый образец содержит введенный пароль и динамические характеристики, также имя профиля аутентификации. Иными словами, на первом этапе пользователь проходит регистрацию в приложении, тем самым формируя имя профиля. На втором этапе формируется тестовый образец путем ввода парольной фразы, в течение всего времени взаимодействия с клавиатурой устройства считывается время удержания клавиш. Данные отправляются на сервер и путем математических вычислений формируется эталонной образец клавиатурного почерка пользователя.

На стороне сервера находится БД с эталонами аутентификационных данных, также на сервере реализуются алгоритмы сравнения тестовых образцов и эталонов. Клиент от сервера получает ответ, являющийся результатом сравнения.

Для защиты от атаки «человек по середине» [10] между сервером и клиентом используется защищенный канал связи. Основные этапы работы приложения приведены на рисунке 3.

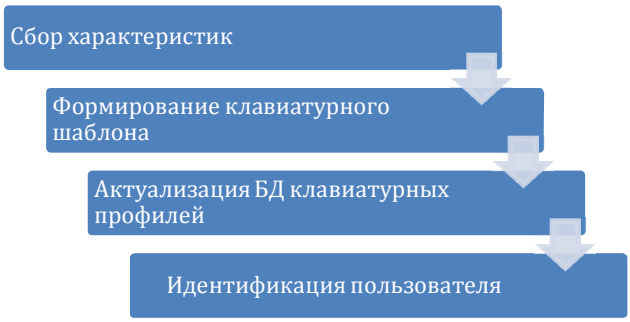

Рисунок 3 – Этапы работы программного приложения

Этап сбора характеристик включает в себя получение значений параметров, описанных выше.

Формирование клавиатурного шаблона включает в себя анализ полученных значений параметров (время удержания клавиш) и формирование эталонного шаблона, с которым в дальнейшем будут сравниваться значения, полученные при попытке авторизоваться в системе. Актуализация БД клавиатурных профилей заключается в обновлении эталонов, хранящихся в базе данных. Идентификация пользователя – подтверждение личности пользователя получение разрешения/отказа в доступе.

В настоящее время существует 2 метода реализации аутентификации пользователя по клавиатурному почерку [8]:

- по заранее известной парольной фразе;
- непрерывный мониторинг клавиатурной активности пользователя на протяжении всего времени взаимодействия с устройством.

При реализации аутентификации по парольной фразе выполняются следующие шаги:

- создание эталона по заранее предопределенному тексту – «паролю»;
- дальнейшее распознавание пользователя реализуется путем сравнения значений параметров, полученных при вводе парольной фразы во время аутентификации, с эталоном, полученным ранее.

Парольный метод может быть использован на этапе авторизации, но использование его далее затруднено, так как его реализация требует значительного уменьшения комфорта пользователя.

Суть непрерывного мониторинга заключается в том, что его можно использовать как во время аутентификации, так и после её прохождения:

- мониторинг всей клавиатурной активности пользователя. Достаточно ресурсоемко для решающего устройства, так как в базе эталонов требуется хранение временных меток всех символов, которые когда-то вводил пользователь;
- подход на основе частых биграмм. Менее ресурсоемко, так как используются лишь пары наиболее часто встречающихся букв [2].

В рамках статьи было разработано приложение на основе метода распознавания по парольной фразе для операционной системы Android (рис. 3).

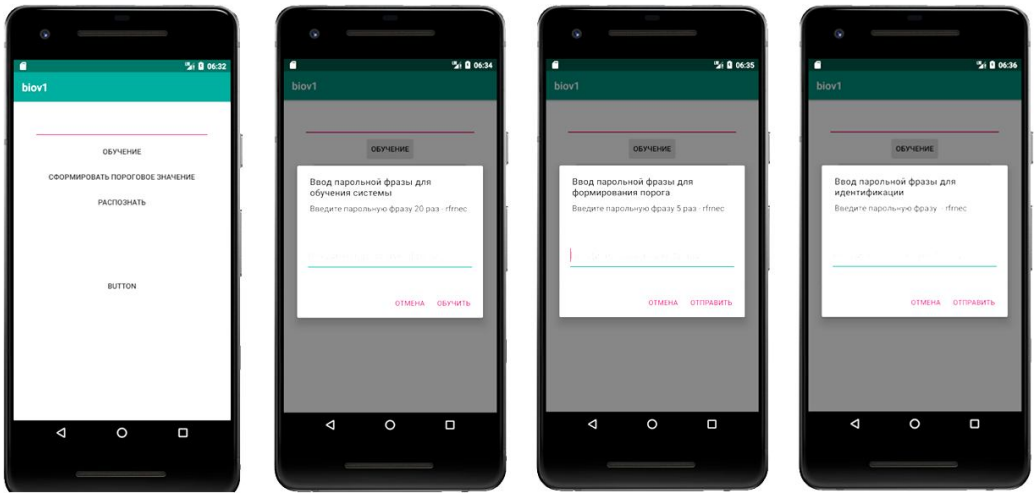

Рисунок 3 – Этапы работы приложения

В данном приложении реализованы 3 этапа распознавания клавиатурного почерка:

- обучение;
- формирование порогового значения;
- распознавание.

На этапе обучения пользователь вводит [12] парольную фразу 20 раз и отправляет данные на сервер. На сервере обрабатываются полученные значения, и формируется эталон клавиатурного почерка. Эталон формируется по принципу высчитывания среднего значения такого параметра, как время удержания клавиш.

На этапе формирования порогового значения пользователь вводит парольную фразу 5 раз и отправляет данные на сервер. На этом этапе на сервере формируется мера Хэмминга [10], иными словами, формируется значение допустимого количества несовпадений временных параметров a_1 с эталоном a_2:

$$H = a\_1 \oplus a\_2. \quad (1)$$

Для идентификации пользователя по клавиатурному почерку [12] отслеживаются значения двухмерного вектора:

$$P=(t\_r\ ,t\_i), \quad (2)$$

где t_r – время удержания; t_i – длительность паузы.

На этапе распознавания после ввода парольной фразы пользователь на экране увидит ответ от сервера либо с положительным результатом, либо с отрицательным, что означает «свой» или «чужой» пользователь вводил парольную фразу на этапе распознавания.

Было проведено тестирование приложения с участием нескольких пользователей. Пользователями являлись два студента разного пола в возрасте 18–23 лет.

В ходе тестирования каждый пользователь обучил систему и сформировал эталон клавиатурного почерка (табл. 3).

Таблица 3 – Тестирование приложения «bio_v1»

Количество итераций ввода парольной фразы на этапе обучения	**Количество символов, отправленных на сервер для обучения системы**	**Значение меры Хэмминга**	**Количество итераций распознавания**	**Количество ошибок первого рода (FRR), ложный отказ в доступе (свой принят за чужого)**	**Количество ошибок второго рода (FAR), коэффициент ложного доступа (чужой принят за своего)**
20	120	User1: 46,6	45	0,44	0
		User2: 46,6		0,53	0,04
40	240	User1: 50	45	0,73	0,044
		User2: 26,66		0,08	0,77
60	360	User1: 52,5	45	0,6	0,42
		User2: 46,6		0,28	0,64

В ходе анализа таблицы 2 выявлены следующие факты:

- большой процент ошибки первого рода для первого тестирования (44 % и 53 %) для первого и второго пользователя соответственно;
- большой процент ошибки первого рода для второго тестирования у первого пользователя (73 %), большой процент ошибки второго рода для второго пользователя (77 %);
- большой процент ошибки первого рода для третьего тестирования у первого пользователя (60 %), у второго пользователя – 28 %, большой процент ошибки второго рода у первого пользователя 42 %, у второго пользователя – 64 %.

Причинами получения данных результатов могут быть следующие факты:

- пользователи испытывали дискомфорт;
- индивидуальное психо-физиологическое состояние на момент проведения тестирования;
- монотонное повторение однотипных действий в течение небольшого промежутка времени.

На данном этапе разработки приложение строит эталонный шаблон по одному параметру – время удержания клавиш и по заданной парольной фразе, известной как легитимному пользователю, так и злоумышленнику. В таблице 4 представлены полученные результаты.

Таблица 4 – Тестирование приложения «bio_v1»

Количество итераций ввода парольной фразы на этапе обучения	**Пользователь**	**Значение временного параметра для символа «r», мс**	**Значение временного параметра для символа «f», мс**	**Значение временного параметра для символа «n», мс**	**Значение временного параметра для символа «e», мс**	**Значение временного параметра для символа «c», мс**
20	User1	80,5	75	97	79	60
	User2	89	94,5	96,4	87,5	86,5
40	User1	86	96	84	87,5	88,5
	User2	102	101	88,5	86	78
60	User1	85	83,5	91,5	92	69,5
	User2	95	80,5	81,5	90,5	103,5

По результатам, отображенным в таблице 4, сделаны следующие выводы:

- ни одно значение параметра эталонного шаблона клавиатурного почерка у пользователей не совпало, следовательно, можно сделать вывод о том, что каждый человек имеет свой уникальный клавиатурный почерк;
- для первого тестирования системы наименьшее различие наблюдается для удержания клавиши «n» (0,6мс), наибольшее – для клавиши «f» (19,5мс);
- для второго тестирования системы наименьшее различие наблюдается для удержания клавиши «e» (1,5мс), наибольшее – для клавиши «r» (16мс);
- для третьего тестирования системы наименьшее различие наблюдается для удержания клавиши «e» (1,5мс), наибольшее различие – для удержания клавиши «c» (34мс).

По результатам тестирования можно сделать вывод о том, что большой процент ошибок первого и второго рода обусловлен недостаточным количеством полученных данных на сервере для формирования эталона клавиатурного почерка, также сделан вывод о том, что одного параметра (время удержания клавиш) для формирования эталона клавиатурного почерка недостаточно. Следует отметить, что тестирование проводилось непрерывно для трех экспериментов. Пользователи монотонно вводили известную фразу в течение некоторого времени, что является некомфортным для пользователя. Из этого следует, что дальнейшие тестирования следует проводить с перерывами в течение длительного времени (минимально суток), чтобы проследить тенденцию изменения клавиатурного почерка разных людей в течение одного периода времени.

Также следует отметить, что монотонный ввод неменяющейся фразы приводит к искажению результатов, из чего следует вывод о том, что актуальнее проводить тестирования по вводу свободного текста.

Выводы. Таким образом, сочетание клавиатурного почерка с иными методами аутентификации повышает надежность системы защиты мобильных устройств. Реализация такого сочетания через разработку приложения, которое можно встроить в системные приложения смартфонов или которое может скачать любой желающий, не требует колоссальных ресурсов или производительных мощностей, а лишь только увеличивает количество манипуляций для пользователя. Конечно же, встает вопрос о дополнительных трудозатратах, но в погоне за конфиденциальностью и предотвращением несанкционированного доступа каждый пользователь выберет вариант с дополнительными временными затратами в угоду своей безопасности.

Остается проблема оценки устойчивости и индивидуальности биометрических характеристик. Тем не менее предложенный подход к распознаванию биометрического портрета пользователя позволяет выявить лица, чей клавиатурный почерк надежно их идентифицирует. Также необходимы дальнейшие исследования в данной области, направленные на повышение достоверности и точности результатов, модернизации графического интерфейса, оптимизации скорости работы и т.д.

Результаты исследования выявили следующие преимущества использования динамических методов биометрической аутентификации пользователей:

- не требуется приобретение никакого дополнительного оборудования [2];
- от пользователя не требуется никаких дополнительных навыков и действий;

- предусмотрена возможность скрытой аутентификации, пользователь даже может быть не в курсе, что включена дополнительная проверка, а значит, не сможет об этом сообщить злоумышленнику [15] (в случае применения подхода непрерывного мониторинга).

Эффективность распознавания пользователя на основе динамических методов биометрической аутентификации достигает 92,14 %, что позволяет говорить о высоком потенциале применения данного метода в рамках разработки систем доступа к мобильным устройствам.

Библиографический список

1. Абдалла Али А. А. Биометрическая идентификация личности / А. А. Абдалла Али // Физика и радиоэлектроника в медицине и экологии : сборник трудов 8-й Международной научно-технической конференции с научной молодежной школой имени И.Н. Спиридонова. – 2008. – Кн. 2. – С. 145–147. – Режим доступа : http://freme.vlsu.ru/trudy_pdf/freme_2008_book_2.pdf, свободный. – Заглавие с экрана. – Яз. рус.

2. Аверин А. И. Аутентификация пользователей по клавиатурному почерку / А. И. Аверин, Д. П. Сидоров // Огарев-онлайн. – 2015. – № 20 (61). – Режим доступа: http://journal.mrsu.ru/wp-content/uploads/2015/10/averin-sidorov.pdf, свободный. – Заглавие с экрана. – Яз. рус.

3. Васильев В. И., Калямов М. Ф., Калямова Л. Ф. Идентификация пользователей по клавиатурному почерку с применением алгоритма регистрации частых биграмм / В. И. Васильев, М. Ф. Калямов, Л. Ф. Калямова // Моделирование, оптимизация и информационные технологии. 2018. – Т. 6, № 1. – С. 399–407. – Режим доступа: https://www.elibrary.ru/item.asp?id=34971186, свободный. – Заглавие с экрана. – Яз. рус.

4. Брумштейн Ю. М. Анализ эффективности использования различных программно-аппаратных решений для исследования динамики выполнения подписи человеком / Ю. М. Брумштейн, Д. В. Харитонов, М. В. Иванова // Физика и радиоэлектроника в медицине и экологии : сборник трудов XI Международной научно-технической конференции с научной молодежной школой имени И.Н. Спиридонова. – 2014. – Кн. 2. – С. 56–60. – Режим доступа: http://freme.vlsu.ru/trudy_pdf/freme_2014_book_2.pdf, свободный. – Заглавие с экрана. – Яз. рус.

5. Горелик А. Л. Методы распознавания /А. Л. Горелик, В. А. Скрипкин. – Москва : Высшая школа, 1984. – 80 с.

6. Одинец Д. Н. Способы построения систем идентификации личности по биометрическим параметрам / Д. Н. Одинец // Электронное содружество. Парк высоких технологий. Безопасные телематические приложения : доклады V Международного конгресса. Минск, 10–11 ноября 2005 г. / под ред. М. М. Маханька, В. Е. Кратенка. – Минск : ГУ «БелИСА», 2005. – С. 152.

7. Путято М. М. Классификация мессенджеров на основе анализа уровня безопасности хранимых данных / М. М. Путято, А. С. Макарян // Прикаспийский журнал: управление и высокие технологии. – 2019. – С. 135–143. – Режим доступа: https://elibrary.ru/item.asp?id=41869982, свободный. – Заглавие с экрана. – Яз. рус.

8. Савинов А. Н. Решение проблем возникновения ошибок первого и второго рода в системах распознавания клавиатурного почерка / А. Н. Савинов, И. Г. Сидоркина // 81 – ИКТ: образование, наука, инновации : труды III Междунар. науч.-практ. конф. – Алматы : МУИТ, 2012. – Режим доступа: https://cyberleninka.ru/article/n/analiz-resheniya-problem-vozniknoveniya-oshibok-pervogo-i-vtorogo-roda-v-sistemah-raspoznavaniya-klaviaturnogo-pocherka, свободный. – Заглавие с экрана. – Яз. рус.

9. Сидоркина И. Г. Три алгоритма управления доступом к КСИИ на основе распознавания клавиатурного почерка оператора / И. Г.Сидоркина, А. Н. Савинов // Вестник Чувашского университета. – 2013. – № 3. – Режим доступа: https://www.elibrary.ru/download/elibrary_21115327_21253793.pdf, свободный. – Заглавие с экрана. – Яз. рус.

10. Скуратов С. В. Использование клавиатурного почерка для аутентификации вкомпьютерных информационных системах / С. В. Скуратов // Безопасность информационных технологий. – 2010. – Режим доступа: https://bit.mephi.ru/index.php/bit/article/view/724, свободный. – Заглавие с экрана. – Яз. рус.

11. Троцкий Д. П. Биометрическая система распознавания подписи / Д. П. Троцкий, К. В. Чирков, Л. Т. Сушкова // Физика и радиоэлектроника в медицине и экологии : сборник трудов 8-й Международной научно-технической конференции с научной молодежной школой имени И.Н. Спиридонова. – 2008. – Кн. 2. – С. 162–165. – Режим доступа: http://freme.vlsu.ru/trudy_pdf/freme_2008_book_2.pdf, свободный. – Заглавие с экрана. – Яз. рус.

12. Ходашинский И. А. Технология усиленной аутентификации пользователей информационных процессов / И. А. Ходашинский, М. В. Савчук, И. В. Горбунов, Р. В. Мещеряков // Управление, вычислительная техника и информатика. – 2011. – С. 236–248. – Режим доступа: https://www.elibrary.ru/item.asp?id=17873015, свободный. – Заглавие с экрана. – Яз. рус.

13. Биометрическая идентификация и аутентификация. – Режим доступа: http://www.techportal.ru /glossary/biometricheskaya_identifikaciya.html, свободный. – Заглавие с экрана. – Яз. рус.

14. Какова стратегия безопасного доступа для банковских продуктов. – Режим доступа: http://www.smartsecurity.tech/wp-content/uploads/2017/03/Smart-Security.pdf, свободный. – Заглавие с экрана. – Яз. рус.

15. Методы биометрической идентификации: сравнительный анализ. – Режим доступа: http://www.biometrics.ru/news/metodi_biometricheskoi_identifikacii_sravnitelnii_analiz/, свободный. – Заглавие с экрана. – Яз. рус.

16. El-Hadidi Kamal M. Biometrics. What and How. – Режим доступа: http://www.net-security.org/dl/articles/Biometrics.pdf, свободный. – Заглавие с экрана. – Яз. англ.

17. Современные методы биометрической идентификации. – Режим доступа: https://www.azone-it.ru/sovremennye-metody-biometricheskoy-identifikacii, свободный. – Заглавие с экрана. – Яз. рус.

References

1. Abdalla Ali A.A. Biometricheskaya identifikatsiya lichnosti [Biometric person identification]. *Fizika i radioelektronika v meditsine i ekologii : Sbornik trudov 8 Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii «s nauchnoy molodezhnoy shkoloy imeni I.N. Spiridonova* [Physics and radioelectronics in medicine and ecology : proceedings of the 8th International Scientific Conference «with the scientific youth school named after I.N. Spiridonov], 2008, Book 2, pp. 145–147. Available at: http://freme.vlsu.ru/trudy_pdf/freme_2008_book_2.pdf

2. Averin A. I., Sidorov D. P. Autentifikatsiya polzovateley po klaviaturnomu pocherku [User authentication base on keystroke dynamics]. *Ogarev-onlayn* [Ogarev-online], 2015, no. 20 (61). Available at: http://journal.mrsu.ru/wp-content/uploads/2015/10/averin-sidorov.pdf

3. Vasilev V. I., Kalyamov M. F., Kalyamova L. F. Identifikatsiya polzovateley po klaviaturnomu pocherku s primeneniem algoritma registratsii chastykh bigramm [Identification of users by keyboard handwriting using the algorithm of frequent bigrams registration.]. *Modelirovanie, optimizatsiya i informatsionnye tekhnologii* [Modeling, Optimization and Information Technologies], 2018, vol. 6, no. 1, pp. 399–407. Available at: https://www.elibrary.ru/item.asp?id=34971186

4. Brumshteyn Yu. M., Kharitonov D. V., Ivanova M. V. Analiz effektivnosti ispolzovaniya razlichnykh programmno-apparatnykh reshcheniy dlya issledovaniya dinamiki vypolneniya podpisi chelovekom. *Fizika i radioelektronika v meditsine i ekologii : sbornik trudov XI Mezhdunarodnoy nauchno-tehnicheskoy konferentsii «s nauchnoy molodezhnoy shkoloy imeni I.N. Spiridonova* [Physics and radioelectronics in medicine and ecology : proceedings of the XI International Scientific Conference with the scientific youth school named after I.N. Spiridonov]. 2014, Book 2, pp. 56–60. Available at: http://freme.vlsu.ru/trudy_pdf/freme_2014_book_2.pdf4

5. Gorelik A. L., Skripkin V. A. *Metody raspoznavaniya* [Recognition methods]. Moscow, Vysshaya shkola Publ., 1984. 80 p.

6. Odinets D. N. Sposoby postroeniya sistem identifikatsii lichnosti po biometricheskim parametram [Methods of constructing personal identification systems based on biometric parameters]. *Elektronnoe sodruzhestvo. Park vysokikh tekhnologiy. Bezopasnye telematicheskie prilozheniya : doklady V Mezhdunarodnogo kongressa* [Electronic community. Hi-tech park. Secure telematics applications : proceedings of the V International Congress]. Minsk, November 10–11, 2005. Minsk, 2005, p. 152.

7. Putyato M. M., Makaryan A. S. Klassifikatsiya messendzherov na osnove analiza urovnya bezopasnosti khranimykh dannykh [Classification of messengers based on analysis of the security level of stored data]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2019, pp. 135–143. Available at: https://elibrary.ru/item.asp?id=41869982

8. Savinov A. N., Sidorkina I. G. Reshenie problem vozniknoveniya oshibok pervogo i vtorogo roda v sistemakh raspoznavaniya klaviaturnogo pocherka [Analysis of the solution problems the origin of type i errors and type ii errors in system of recognition of keystroke dinamics]. *IKT: obrazovanie, nauka, innovatsii : trudy III Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [ICT: education, science, innovation : proceedings of the Third International Scientific-Practical Conference]. Almaty, MUIT Publ., 2012. Available at: https://cyberleninka.ru/article/n/analiz-resheniya-problem-vozniknoveniya-oshibok-pervogo-i-vtorogo-roda-v-sistemah-raspoznavaniya-klaviaturnogo-pocherka

9. Sidorkina I. G., Savinov A. N. Tri algoritma upravleniya dostupom k KSII na osnove raspoznavaniya klaviaturnogo pocherka operatora [Three algorithms of control access to the KSII on the basis of recognition of keystroke dynamics]. *Vestnik Chuvashskogo universiteta* [Bulletin of Chuvashia University], 2013, no. 3. Available at: https://www.elibrary.ru/download/elibrary_21115327_21253793.pdf

10. Skuratov S.V. Ispolzovanie klaviaturnogo pocherka dlya autentifikatsii v kompyuternykh informatsionnykh sistemakh [Using keyboard handwriting for authentification in computer information systems]. *Bezopasnost informatsionnykh tekhnologiy* [IT Security], 2010, pp. 38–35 Available at: https://bit.mephi.ru/index.php /bit/article/view/724

11. Trotskiy D. P., Chirkov K. V., Sushkova L. T. Biometricheskaya sistema raspoznavaniya podpisi [Biometrical system for dynamic signature recognition]. *Fizika i radioelektronika v meditsine i ekologii : sbornik trudov 8-y Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii s nauchnoy molodezhnoy shkoloy imeni I.N. Spiridonova* [Physics and radioelectronics in medicine and ecology : proceedings of the 8th International Scientific and Technical Conference with the scientific youth school named after I.N. Spiridonov], 2008, book, 2, pp. 162–165. Available at: http://freme.vlsu.ru/trudy_pdf/freme_2008_book_2.pdf

12. Khodashinskiy I. A., Savchuk M. V., Gorbunov I. V., Mesheryakov R. V. Tekhnologiya usilennoy autentifikatsii polzovateley informatsionnykh protsessov [Strong authentication technology of the users of information processes]. *Upravlenie, vychislitelnaya tekhnika i informatika* [Management, computer engineering and informatics], 2011, pp. 236–248. Available at: https://www.elibrary.ru/item.asp?id=17873015

13. *Biometricheskaya identifikatsiya i autentifikatsiya* [Biometric identification and authentication]. Available at: http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html

14. *Kakova strategiya bezopasnogo dostupa dlya bankovskikh produktov* [What is a secure access strategy for banking products]. Available at: http://www.smartsecurity.tech/wp-content/uploads/2017/03/Smart-Security.pdf

15. *Metody biometricheskoy identifikatsii: sravnitelnyy analiz* [Biometric authentication methods: a comparative analysis]. Available at: http://www.biometrics.ru/news/metodi_biometricheskoi_identifikacii_sravnitelnii_analiz/

16. El-Hadidi Kamal M. *Biometrics. What and How.* Available at: http://www.net-security.org/dl/articles/Biometrics.pdf

17. *Sovremennye metody biometricheskoy identifikatsii* [Modern methods of biometric identification]. Available at: https://www.azone-it.ru/sovremennye-metody-biometricheskoy-identifikacii