

ИССЛЕДОВАНИЕ СКОРОСТИ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ В МОБИЛЬНОМ ПРИЛОЖЕНИИ ПРИ РАЗЛИЧНЫХ МЕТОДАХ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Новик А.М.

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Научный руководитель: Пискун Г.А. – канд. техн. наук, доцент

Аннотация. Экспериментально исследовано время идентификации пользователя в мобильном приложении посредством различных методов защиты персональных данных. Установлено, что наименьшее время идентификации потребуется для отпечатка пальца (~1,6 секунды). Предложен комбинированный способ защиты персональных данных, состоящий из методов: отпечаток пальца и пара «Логин/Пароль», общее время идентификации которых составляет 30,4 секунды при последовательном использовании.

Ключевые слова: персональные данные, идентификация, мобильное приложение

Введение. На сегодняшний день существует несколько способов защиты персональных данных при идентификации пользователя в мобильном приложении. Однако для разработчиков стоит вопрос, как сделать процесс идентификации надёжнее, проще, быстрее и какой метод наиболее эффективный.

Таким образом, изучение скорости идентификации пользователя в мобильном приложении, а именно сравнение методов защиты персональных данных и анализ полученных результатов, является актуальным на сегодняшний день.

Основная часть. Объектами анализа являются наиболее популярные методы идентификации пользователей в мобильных приложениях [1]:

1. *Комбинированные методы* идентификации пользователей: отпечаток пальца и «Логин/Пароль»; «Логин/Пароль» и *PIN*-код; распознавание по лицу и «Логин/Пароль»; распознавание по голосу и «Логин/Пароль».

Под комбинированным методом стоит понимать наличие минимум двух стандартных/биометрических способов идентификации, используемых последовательно либо дающих возможность пользователю выбрать, какой способ использовать в данный момент.

В работе анализируются комбинированные способы идентификации, которые состоят только из двух отдельных способов, так как большее количество усложняет интуитивное понимание функционала для пользователя и требует дополнительных ресурсов при разработке программного представления.

2. *Отдельные (стандартные и биометрические) методы* идентификации пользователей: «Логин/пароль», *PIN*-код, одноразовый *SMS*-код, отпечаток пальца, распознавание по лицу, распознавание по голосу.

В таблице 1 представлены данные о среднем количестве входных данных для успешной идентификации посредством отдельных (стандартных и биометрических) методов [2]. На рисунке 1 представлены значения скорости идентификации с помощью отдельных методов. Данные из графика на рисунке 1 получены в ходе испытаний и измерений средней длительности идентификации пользователя для каждого способа. Скорость в данном случае понимается как время, затраченное на ввод полных идентификаторов, необходимых для успешной идентификации.

Таблица 1 – Среднестатистическое количество символов для успешной идентификации пользователя

Название метода	Среднее количество входных данных, шт
Логин и пароль	9
<i>PIN</i> -код	4
Одноразовый <i>SMS</i> -код	4
Отпечаток пальца	1
Распознавание по лицу	1
Распознавание по голосу	1

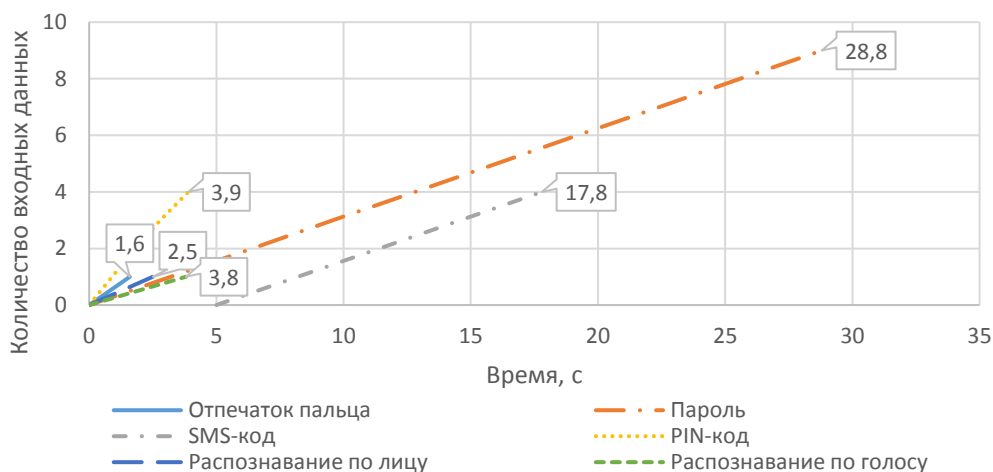


Рисунок 1 – Диаграмма времени ввода входных данных пользователем

По результатам данных из таблицы 1 наименьшее количество входных данных для успешной идентификации требуется для биометрических методов защиты персональных данных.

По данным из графика на рисунке 1 видно, чем меньше идентификаторов для ввода, тем быстрее выполняется операция идентификации. Таким образом, наибольшее время для идентификации потребуется для ввода логина и пароля (от 29 секунд и больше) и наименьшее время понадобится для ввода отпечатка пальца (~1,6 секунд).

На рисунке 2 представлены данные по скорости ввода идентификаторов для различных вариантов комбинированных методов.

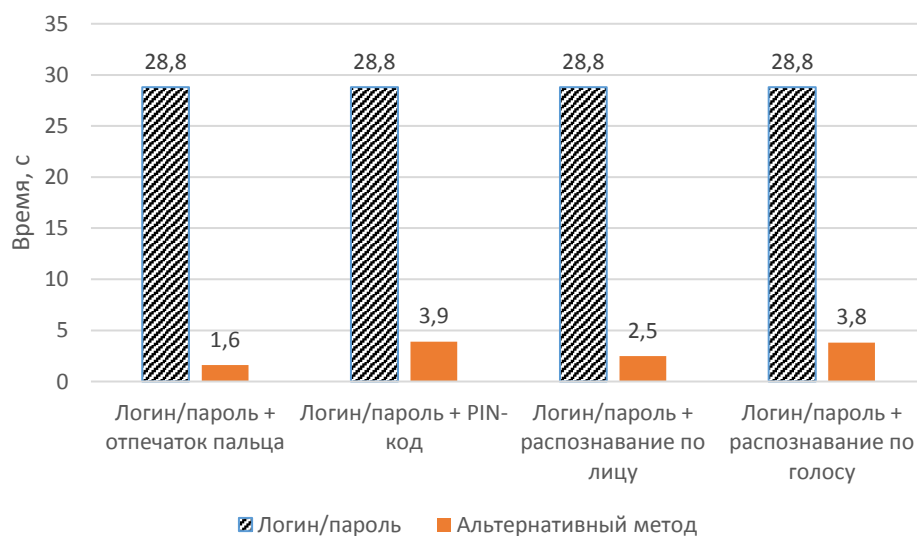


Рисунок 2 – Затраты времени на идентификацию при наличии комбинированных методов защиты

В таблице 2 представлено общее время идентификации пользователя для методов из графика на рисунке 2.

Таблица 2 – Общее время идентификации пользователя

Методы защиты	Общее время, с
«Логин/пароль» + распознавание по голосу	32,6
«Логин/пароль» + распознавание по лицу	31,3
«Логин/пароль» + PIN-код	32,7
«Логин/пароль» + отпечаток пальца	30,4

Общее время в данном случае – это время, которое надо будет потратить на идентификацию с помощью одного метода (неуспешный результат идентификации), переключение на альтернативный и идентификацию с помощью него. Наименьшее время понадобится для комбинированного метода защиты «Логин/пароль» + отпечаток пальца. Для остальных методов время увеличится на 7,2% («Логин/пароль» + распознавание по голосу), на 3% («Логин/пароль» + распознавание по лицу) и на 7,2% («Логин/пароль» + PIN-код).

В качестве одного из способа идентификации для комбинированного метода целесообразно рассматривать «Логин/Пароль». Такое решение принято в результате исследования различных параметров, одно из его преимуществ – возможность привязать пользователя к номеру телефона или электронной почте.

Заключение. Проведено исследование времени идентификации пользователя в мобильном приложении с помощью различных методов защиты персональных данных. Согласно полученным данным наименьшее время понадобится для ввода отпечатка пальца, а наибольшее – для ввода значений логина и пароля. При использовании пары «Логин/Пароль» в комбинированном методе время идентификации займёт от 29 секунд (в зависимости от количества и типа вводимых символов), при использовании отпечатка пальца – около 1,6 секунды. При последовательном использовании отпечатка пальца и пары «Логин/Пароль» минимальное затраченное время займёт 30,4 секунд.

Список литературы

1. Кухарев Г. А. Биометрические системы: методы и средства идентификации личности человека / Г. А. Кухарев – СПб.: Политехника, 2001. – 240 с.
2. Суомалайнен А., Биометрическая защита. Обзор технологии / А. Суомалайнен – М.: ДМК Пресс, 2019. – 106 с.

UDC 621.3.049.77–048.24:537.2

RESEARCHING THE USER IDENTIFICATION RATE IN A MOBILE APPLICATION WITH DIFFERENT METHODS OF PROTECTING PERSONAL DATA

Novik A.M.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Piskun G.A. – PhD, associate professor

Annotation. The time of user identification in a mobile application was experimentally investigated by means of various methods of protecting personal data. It has been found that the shortest identification time is required for a fingerprint (~ 1.6 seconds). A combined method of personal data protection is proposed, which consists of the following methods: a fingerprint and a “Login / Password” pair, the total identification time of which is 30.4 seconds in case of sequential use.

Keywords: personal data, identification, mobile application