УДК 621.3.049.77–048.24:537.2

АНАЛИЗ БЕЗОПАСНОСТИ 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. Проведён анализ безопасности идентификации пользователя в мобильном приложении при различных методах защиты персональных данных. Установлено, что наименее подверженным к воздействию злоумышленников является биометрический способ (сканирование отпечатка пальца). Уровень защищённости процесса идентификации посредством отпечатка пальца достигает 96,7 – 98%.

Ключевые слова: персональные данные, мобильное приложение, идентификация, биометрия

Введение. В настоящее время люди вынуждены задуматься о безопасности своих персональных данных из-за цифровизации повседневной жизни. Практически каждое приложение, установленное на смартфоне/планшете, хранит наши персональные данные. Это могут быть номера банковских карт, информация о различных финансовых транзакциях, документы, номера телефонов, адреса и т.д.

В данной статье проведён анализ безопасности идентификации пользователя в мобильном приложении посредством различных методов защиты персональных данных: сравнение основных методов защиты и анализ полученных результатов.

Основная часть. Объектами анализа являются стандартные и биометрические методы идентификации пользователей в мобильных приложениях: «Логин/пароль», *PIN*-код, одноразовый *SMS*-код, отпечаток пальца, распознавание по лицу, распознавание по голосу [1].

1. Стандартные методы *«Логин/Пароль»* и *PIN-код* не являются уникальными. Логин, пароль и *PIN*-код легко подделать, если знать некоторые индивидуальные данные пользователя. Часто в качестве логина используется адрес электронной почты, номер телефона или никнейм, в качестве пароля пользователи часто устанавливают дату рождения, пустой пароль, используют одну цифру или букву. Национальный центр кибербезопасности Великобритании представил список худших паролей на планете. Эти комбинации используют большинство пользователей. Основой для создания статистики стал сайт для проверки паролей *haveibeenpwned.com*. Статистика популярных паролей представлена на рисунке 1.

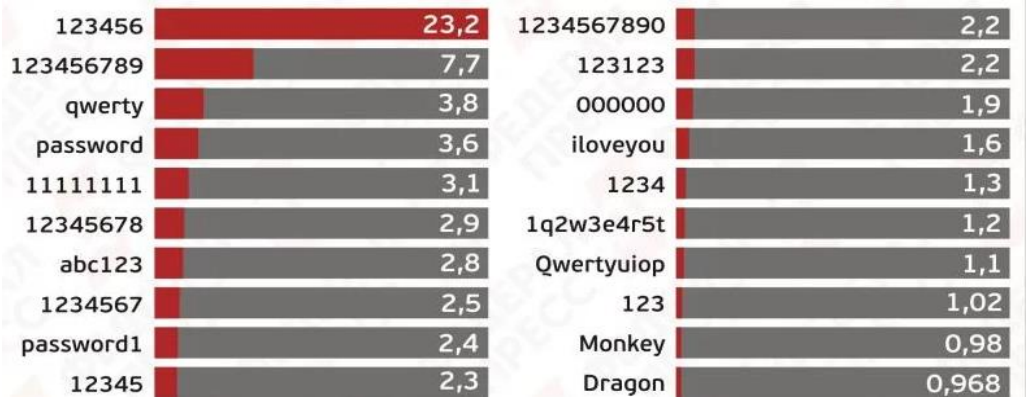

Рисунок 1 – Статистика наиболее популярных паролей [2]

Американская компания *Data Genetics* провела наиболее полный и масштабный статистический анализ *PIN*-кодов, использовав все доступные базы данных с паролями и отфильтровав их по цифровым комбинациям от 0000 до 9999. Общая база после применения фильтра составила 3,4 миллиона *PIN*-кодов. На рисунке 2 представлена статистика популярных *PIN*-кодов [3].

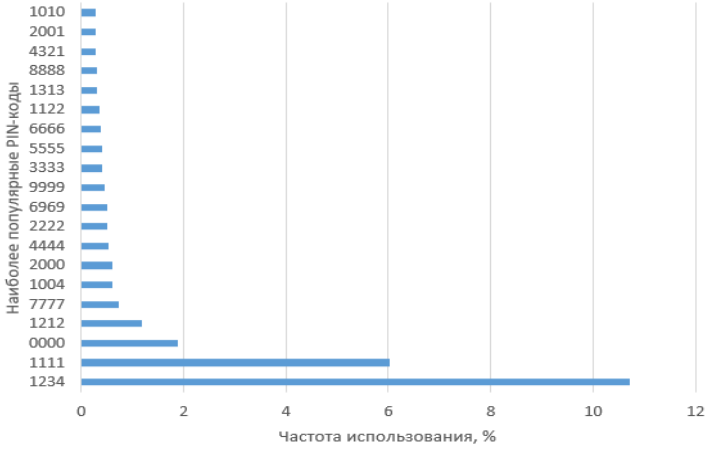

Рисунок 2 – График наиболее популярных *PIN*-кодов

Представленные комбинации покрывают около 26,83% всех кодов.

Логин, пароль и *PIN*-код доступны для посторонних лиц, так как их можно подсмотреть при вводе, прочитать, если они где-то записаны, восстановить по следам пальца на мобильном устройстве после ввода пользователем. Пользователь может забыть их, особенно если не часто использовать их, потерять, если они где-то записаны. Для восстановления потребуется дополнительное время. Это не очень благоприятно скажется на лояльности пользователя к программе.

В отличие от биометрических способов защиты персональных данных стандартные способы не подвержены влиянию внешних факторов.

2. *Одноразовый SMS-код* является уникальным, так как он генерируется каждый раз новый, его нельзя предугадать или подобрать, поэтому его невозможно подделать. Но его может подсмотреть постороннее лицо, однако в этом случае есть ограничения:

– после заполнения поля ввода кодом его нельзя использовать повторно;

– такой код имеет ограниченное время жизни;

– в некоторых приложениях реализована автоподстановка *SMS*-кода в соответствующее поле ввода.

Согласно этим ограничениям, возможность подсмотреть практически не способствует к получению доступа к персональным данным пользователя. Одноразовый *SMS*-код может подвергаться влиянию внешних факторов, например, наличие интернета. Важной особенностью одноразового *SMS*-кода как способа защиты персональных данных является использование его вкупе с каким-то дополнительным способом защиты, так как он не идентифицирует личность пользователя. По одиночке такой метод недостаточно эффективен и нецелесообразен.

3. *Отпечатки пальца* являются идентификатором личности, и, как правило, у каждого человека они разные. За счёт этого отпечаток пальца обладает уникальностью. Случаи, когда отпечатки пальцев намеренно портятся или изменяются, редкие и не учитываются в данном анализе. Отпечаток пальца возможно подделать, но для этого нужны специальные условия и оборудование. Современные технологии позволяют производить сенсоры для сканирования

пальца, которые могут распознавать признаки живучести организма. С усовершенствованием таких технологий подделка пальца станет практически невозможной. Фактически отпечаток пальца доступен для посторонних, то есть любой человек может видеть узор пальца, но практически это не имеет никакого значения, так как информация об узоре пальца пользователя не способствует идентификации в приложении.

В то же время отпечаток пальца больше подвержен влиянию внешних факторов, например, жирный или грязный палец затруднит идентификацию пользователя.

4. Метод *распознавания по лицу* считается уникальным, если человек не имеет близнеца или очень похожего на себя человека. Он идентифицирует личность. В данном случае не рассматриваются варианты пластических операций и наличие серьёзных повреждений на лице, так как это редкие случаи. Этот способ подвержен влиянию внешних факторов, например физические повреждения, наличие/отсутствие сильной растительности на лице, темнота или плохое освещение.

Подделать такой идентификатор возможно, но при определённых условиях. Как правило, это не просто, и развитие современных технологий усложняет возможность подделки.

5. *Идентификатор голоса* не относится к уникальным, так как голос относится к динамическим биометрическим методам идентификации, то есть может изменяться, и у некоторых людей могут быть похожи тональности, частоты и другие величины, по которым искусственный интеллект идентифицирует пользователя.

Голос легко подделать: его можно записать на диктофон или спародировать.

Голос подвержен влиянию внешних факторов, например простуда (в результате временное изменение голоса), внешние шумы и посторонние звуки. Но положительным для этого метода, как и для других биометрических, является то, что его нельзя забыть/потерять.

Заключение. Проведены сравнение и анализ методов защиты персональных данных пользователей мобильных приложений с точки зрения защищённости процесса идентификации. Согласно сравнению методов защиты самыми надёжными являются биометрические методы и наиболее надёжным из них на сегодняшний день – сканер отпечатка пальца. Уровень защищённости процесса идентификации пользователя с помощью отпечатка пальца достигает 96,7 – 98% [4].

Список литературы

1. *Кухарев Г. А. Биометрические системы: методы и средства идентификации личности человека / Г. А. Кухарев – СПб.: Политехника, 2001. – 240 с.*

2. *Пароли, которые легче всего взломать [Электронный ресурс]. – Режим доступа: https://front-test.fedpress.ru/news/western-europe/society/2225045*

3. *Популярные PIN-коды [Электронный ресурс]. – Режим доступа: https://xakep.ru/2012/09/19/59342/*

4. *Суомалайнен А., Биометрическая защита. Обзор технологии / А. Суомалайнен – М.: ДМК Пресс, 2019. – 106 с.*

UDC 621.3.049.77–048.24:537.2

ANALYSIS OF THE SECURITY OF USER IDENTIFICATION IN THE MOBILE APPLICATION WITH VARIOUS 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 analysis of the security of user identification in a mobile application with various methods of protecting personal data has been carried out. It was found that the least susceptible to attackers is the biometric method (fingerprint scanning). The level of security of the fingerprint identification process reaches 96.7 - 98%.

Keywords: personal data, mobile application, identification, biometrics