**Доклад на тему: “Биометрия в мобильных устройствах”**

**Глава 1. Введение.**

Широкое использование и возможности мобильных технологий сформировали потребность людей вести свою личную и деловую жизнь в движении, хотя раньше она была ограничена домашней и офисной средой. Для удовлетворения данной потребности мобильная связь, приложения, установленные на мобильные устройства, и транзакции должны быть защищены для обеспечения конфиденциальности пользователя и целостности транзакций. Это необходимо для создания доверенной среды мобильных платформ, в которой могут участвовать как отдельные лица, так и предприятия, некоммерческие организации и правительства. Аутентификация пользователя, удостоверяющая его личность, является важной частью создания этой среды. Её часто проводят с использованием имени пользователя и пароля, также биометрии вместо пароля. О биометрии мы сейчас и поговорим.

**Глава 2. Основные виды биометрии в мобильных устройствах.**

Популярные способы биометрической идентификации, по данным исследования:

* Сканер отпечатка пальца (fingerprint) – 57%
* Сканер геометрии лица (face ID) – 14%
* Прочие методы: сканеры радужной оболочки глаза (IRIS) и геометрии руки (3-5%).

Существуют и другие способы аутентификации, например, голосовая биометрия – однако, их надежность ниже, поэтому обращаются к ним реже.

Рассмотрим особенности нескольких из перечисленных наиболее распространенных способов.

1. **Сканер отпечатка пальца (fingerprint).**

Для того, чтобы «узнать» пользователя по отпечатку пальца и безопасно хранить его данные, каждый производитель мобильных устройств предлагает свои возможности. Так, на устройствах Apple образец отпечатка пальца проводится через хеш-функцию перед сохранением в защищенный вычислительном модуль. Все процессы, связанные с Touch ID, происходят именно в этом модуле, и извлечь такие данные невозможно.

На устройствах Android степень безопасности зависит от производителя, используемых им подходов и решений. Как правило, работа со сканерами отпечатка пальца регламентируется отдельными документами, в том числе спецификациями Google. Ведущие производители смартфонов, такие как Samsung, используют достаточно надежные и точные емкостные сенсорами и обеспечивают высокую степень безопасности данных.

Недостатки:

* Отдельные небольшие компании могут применять менее надежные сенсоры и хранить отпечатки на устройстве, иногда даже в свободном доступе.
* Высокий риск взлома. Злоумышник может заполучить различными способами ваш отпечаток пальцев и получить доступ к вашим данным.
* Когда пользователь сканирует отпечаток пальца, получившийся рисунок зависит от силы нажатия, смещения на долю миллиметра вправо или влево, наличия незначительных травм кожи. Поэтому возможны проблемы с аутентификацией.

1. **Сканер геометрии лица (face ID).**

Если приложение идентифицирует пользователя по лицу, сканирование осуществляют за счет емкостной камеры. По сравнению с предыдущим способом, здесь требуется еще более сложный алгоритм, требующий высокой точности захвата изображения и распределения более 30 тысяч контрольных точек по изображению лица пользователя. В свою очередь, это определяет более высокие требования к камере смартфона. По сути дела, емкостный сканер изучает лицо пользователя, выстраивая геометрическую модель и преобразуя её в результаты вычисления, которые можно хранить. Во время авторизации результат вычисления (с учетом погрешности) для конкретного пользователя сопоставляется с результатом, хранящимся в памяти.

Недостатки:

* Не все устройства предоставляют полноценные возможности для распознавания лиц.
* Бывают случаи, когда производители ограничиваются 2D-сканированием с помощью обычной камеры. В этом случае есть риск, что потенциальному злоумышленнику удастся разблокировать приложение, просто просканировав фотографию владельца.
* Так же на данный момент существует 3D- печать с помощью которой возможно создать не отличимый вид лица человека, что создает опасность конфиденциальности ваших данных.

1. **Сканер радужной оболочки глаза (IRIS).**

Важно помнить, что IRIS – это не сканер сетчатки глаза. Проще говоря, эта технология сканирует радужную оболочку, которая окружает зрачок, тогда как сетчатка располагается внутри глаза на задней стенке. Сканер определяет те или иные особенности внешности пользователя и геометрическую форму радужки, используя емкостные камеры.

Недостатки:

* С одной стороны, для снятия блокировки недостаточно найти и предъявить фотографию владельца, ведь камера определяет объем изображения. Однако, такой риск выше при одновременном использовании фотографии и контактных линз.

**Глава 3. Международные стандарты.**

Большинство терминов и определиний, а так же способов использования биометрии регламентируется:

* Российский стандарт: ПНСТ 379—2019 (ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ) Информационные технологии. Биометрия. Применение биометрии в мобильных устройствах
* Европейский стнадарт: ISO/IEC TR 30125:2016, Information technology — Biometrics used with mobile devices, MOD

**Глава 4. Выводы.**

В биометрической аутентификации используются различные «истинные» характеристики пользователя: отпечатки пальцев, сетчатки глаза, контуров лица или голоса. Биометрия позволяет снизить необходимость в запоминании и постоянном вводе сложного пароля, что будет по душе и пользователям и администраторам. Скопировать отпечатки пальцев намного сложнее, чем подсмотреть PIN-код, вводимый пользователем. Повышение уровня безопасности конфиденциальной информации, особенно по мере того, как мы находим новые сферы применения мобильным устройствам, и возрастает количество персональных данных, позволяет нам быть более уверенным относительного того, кто имеет доступ к этой информации. Но не стоит забывать, что идеальной защитной системы не существует. Поэтому советуем использовать несколько способов защиты информации, менять пароли хотя бы раз в пол года\ год и придумать все более сложные способы защиты.