ИСПОЛЬЗОВАНИЕ СКАНЕРА ОТПЕЧАТКА ПАЛЬЦА ДЛЯ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ НА МОБИЛЬНОМ УСТРОЙСТВЕ

Новик А.М.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Пискун Г.А. – канд. техн. наук, доцент

С информатизацией общества всё больше внимания уделяется защите персональных данных и противостоянию киберпреступникам. Как правило, персональными данными являются сведения, прямо или косвенно относящиеся к физическому лицу [1].

Аутентификация пользователя применяется для того, чтобы никто другой не мог воспользоваться персональной информацией, а также получить доступ к финансовым операциям пользователя.

На сегодняшний день существует несколько способов защиты пользовательских данных на мобильных устройствах. Одним из наиболее популярным является сканер отпечатка пальца.

Сканер отпечатка пальца – это встроенный в приложение уровень защиты. Такой способ поможет спасти, не предоставив доступ к приложению, конфиденциальные данные от злоумышленника или посторонних лиц. Сканер отпечатков пальцев представляет собой тип электронной системы безопасности, которая использует отпечатки пальцев для биометрической аутентификации, чтобы предоставить пользователю доступ к информации или для одобрения транзакций.

Отпечатки пальцев каждого человека уникальны, поэтому они успешно идентифицируют людей. Усовершенствования технологий позволили включить считыватель отпечатков на задней крышке или на экране в качестве другой (необязательной) функции безопасности для мобильных устройств. Этот идентификатор можно вручную включить для безопасности (это делается в настройках безопасности), или отключить при необходимости.

Сканер отпечатка пальца появился самым последним из всех способов идентификации. Уже были пин-коды, коды шаблонов, пароли, распознавание лиц, определение местоположения, сканирование диафрагмы, распознавание голоса.

Достоинства сканеров отпечатков пальцев:

- простота блокировки и разблокировки одним пальцем;
- отличный способ идентифицировать уникальных людей;
- чрезвычайно сложно подделать/дублировать (по сравнению с карточками идентификации/доступа и т. д.);
- практически невозможно угадать/взломать (по сравнению с пин-кодами, паролями и т. д.), но можно обмануть;
- пользователь не сможет забыть свой отпечаток пальца (как это часто бывает с паролями, кодами, шаблонами, картами доступа и т. д.);

Несмотря на то, что считыватели считаются довольно точными, может быть несколько причин, по которым не происходит авторизация:

- влажные или жирные руки;
- электронный сбой;
- дефект на пальце;

Поэтому разработчикам стоит предусмотреть альтернативный вход в приложение, например, PIN-код, одноразовый SMS-код.

Данный способ удобен, придаёт пользователю уверенность в защищённости своих сведений, является интуитивно понятным и лаконично вписывается в дизайн как устройства, так и приложения. Такой способ защиты может привлечь пользователей, тем самым повысив спрос на продукт компании.

Список использованных источников:

1. Защита персональных данных [Электронный ресурс]. – Режим доступа: https://scam.zone/stati/zaschita-informatsii-v-internete/. – Дата доступа: 07.03.2020.