ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ УСТРОЙСТВ

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

На сегодняшний день информационные технологии включают в себя процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Информационные технологии призваны, основываясь и рационально используя современные достижения в области компьютерной техники и иных высоких технологий, новейших средств коммуникации, программного обеспечения и практического опыта, решать задачи по эффективной организации информационного процесса для снижения затрат времени, труда, энергии и материальных ресурсов во всех сферах человеческой жизни и современного общества. Информационные технологии взаимодействуют и часто составляющей частью входят в сферы услуг, области управления, промышленного производства, социальных процессов [1].

Научное направление в области информационных технологий, а именно, обеспечение безопасности персональных данных, является актуальным, так как в настоящее время существует огромное количество различных технических устройств, которые упрощают и усовершенствуют деятельность человека в разных сферах жизни. На телефонах хранятся большие объёмы информации, в том числе и личная, которая должна быть защищена от посторонних пользователей.

Наиболее популярными способами потери конфиденциальной информации являются:

- кража/утеря;
- доступ к телефону третьих лиц;
- атака злонамеренного ПО;
- фишинговая атака.

Для обеспечения безопасности персональных данных можно воспользоваться встроенными программными модулями, разработанными для этих целей и имеющие соответствующий алгоритм.

Существует несколько методов защиты приложений при их запуске от нежелательных пользователей:

- по отпечатку пальца;
- по распознаванию лица;
- по распознаванию голоса;
- по подписи;
- по графическому рисунку;
- по PIN-коду;
- по паролю;
- по одноразовому SMS-паролю.

Каждый из методов имеет как положительные, так и отрицательные стороны. Сегодня наиболее надёжными являются сканер отпечатка пальца и использование одноразового SMS-пароля.

Как правило, крупные компании предоставляют пользователю возможность выбора того или иного способа защиты или одновременно использовать несколько. Это наиболее актуально в приложениях, имеющих доступ к финансовым операциям пользователя.

Список использованных источников:

1. Информационные технологии [Электронный ресурс]. – Режим доступа: https://www.yaklass.ru/materiali?mode=cht&chtid=456. – Дата доступа: 07.03.2020