АНАЛИЗ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ БЕСПИЛОТНЫХ АВТОМОБИЛЕЙ ОТ ВНЕШНЕГО ВОЗДЕЙСТВИЯ

Д.В. Куприянова, Ю.И. Некревич, Д.Н. Одинец

На сегодняшний день наиболее распространены в качестве биометрической системы идентификации для мобильных устройств (например, ноутбукам, смартфонам и т.д.) следующие подходы: распознавание лица и анализ отпечатков пальцев. При это сканеры отпечатков нашли особую популярность, т. к. данный подход является относительно быстродействующим из-за того. Существует 3 основных типа сканеров: оптические, емкостные и ультразвуковые, отличающиеся между собой по принципу действия (размещены в порядке появления на рынке). Результаты, представленные в [1, 2], указывают, что каждый из указанных типов может быть «обманут», кроме того, можно предположить, что большинство разработчиков анализируют основные признаки, но не обращают внимание на локальные (это связано с необходимостью максимально быстро отсканировать, обработать и принять решение о соответствии эталону), имеются проблемы с высокой чувствительностью используемых сенсоров и некорректной интерпретацией результатов.

Решениями по устранению выявленных недостатков является применение дополнительных аппаратных и/или программных средств: дополнительная фиксация пульса, фиксация теплового излучения от кожи, программный поиск слишком «идеальных» снимков. В то же время, анализ ситуации показывает, что несмотря на выявленные недостатки, применение отпечатков пальца в качестве биометрической системы идентификации для систем, не связанных с хранением критически важной и/или ограниченной к распространению информации, является вполне приемлемым.

Литература

1. Подделка отпечатков пальцев – можно, но сложно [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/sas2020-fingerprint-cloning/28101. – Дата доступа: 21.04.2022.

2. Подделка отпечатков пальцев [Электронный ресурс]. – Режим доступа: http://www.techportal.ru/glossary/poddelka-otpechatkov-palcev.html. – Дата доступа: 21.04.2022.