## ОЦЕНКА УЯЗВИМОСТИ МОБИЛЬНОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ SAILFISH OS

А.П. Жук, Е.С. Тран, Е.П. Жук

В настоящее время существует проблема импортозамещения в сфере информационных технологий, которая объясняется, в частности, потребностью в сертифицированных информационных технологиях, способных обрабатывать конфиденциальную информацию в соответствии с требованиями законодательства Российской Федерации.

Поскольку единственной отечественной мобильной операционной системой, которая имеет сертификат ФСТЭК по требованиям информационной безопасности, является Sailfish OS, разработанная ООО «Открытая мобильная платформа», то оценка ее безопасности и поиск уязвимых мест является актуальной задачей. С точки зрения возникновения уязвимостей, по мнению авторов, особый интерес представляет использование режима разработчика в Sailfish OS. Режим разработчика позволяет в разблокированном состоянии смартфона злоумышленнику получить root-доступ к нему, поэтому данное обстоятельство рассматривается авторами как уязвимость Sailfish OS. Данная схема атаки позволяет злоумышленнику загрузить на устройство вредоносное программное обеспечение, с помощью которого возможно удаленно контролировать все функции смартфона, а также скрытно использовать всю существующую периферию, что останется незамеченным для пользователя.

В качестве рекомендаций по локализации описанной уязвимости Sailfish OS, по мнению авторов, можно рекомендовать поддержание смартфона в состоянии физической безопасности, а также установку стойкого пароля на экран блокировки, что сделает невозможным реализацию атаки путем получения несанкционированного root-доступа к смартфону [1, 2].

**Литература**

1. Колисниченко Д.Н. Безопасный Android: защищаем свои деньги и данные от кражи. – СПб.: БХВ-Петербург, 2015. – 161 с.

2. Security – SailfishOS Documentation [Electronic resource]. – Access mode: https://sailfishos.org/wiki/Security. – Date of access: 03.04.2020.