Разработанная программа может быть использована математиками для быстрого анализа замкнутых сетей массового обслуживания с двумя типами заявок через расчет соответствующих характеристик сети и систем, входящих в данную сеть.

Литература

1 Boyarovich Yu. S. // Automation and Remote Control. 2012. Vol. 73. P. 1616–1623.

Е. И. Ключинский
Науч. рук. ***Н. Б. Осипенко****,*
канд. физ.-мат. наук, доцент

ОЦЕНКА БЕЗОПАСНОСТИ ANDROID-ПРИЛОЖЕНИЙ

Среди десктопных ОС наиболее подвержены всевозможным вирусным атакам представители Windows–семейства. Лидером атак злоумышленников на приложения мобильной платформы по критериям распространенности и открытости ОС эксперты считают ОС Android [1].

С целью оперативной экспресс-оценки степени вредоносности Android-приложений и наличия различных рекламных библиотек для организации ООО «ДжастМоби», занимающейся разработкой мобильных приложений, их продвижением и маркетингом, анализом различные Android-программ был разработан веб-сервис. Он позволяет получить полную объективную картину возможного функционала и рисков Android-приложений.

В процессе разработки веб-сервиса была продумана система баллов потенциальной зловредности поведения приложения для 20 выявленных различных вариантов поведений приложений. Разработанная шкала опасности поведения Android-приложений базируется на следующих вариантах поведения (в скобках указана их оценка в баллах): подключение к Интернету (2), шифрование и дешифрование данных (8), выполнение запросов в сети Интернет (2), запуск Shell-команд (9), существуют неиспользуемые права (3), получение списка установленных приложений (7), получение точного местоположения (3), отправка SMS-сообщений (9), прием SMS-сообщений (9), получение MCC-кода оператора (3), получение имени оператора сети (3), получение номера телефона (4), получение серийного номера сим-карты (4), получение IMEI телефона (6), динамическая загрузка кода (8), использование камеры (4), использование рефлексии (9), использование JNI (7).

Разработанное приложение было апробировано и в настоящий момент активно используется при анализе скачиваемых с интернета apk-файлов. Вручную были введены наиболее встречаемые при работе сигнатуры и модели поведения. Если при загрузке apk-файла выясняется, что для Android-приложения сигнатура имеется в базе данных, то выводится ее название и оценка опасности на основании разработанной шкалы эвристики, с ее помощью можно узнать, какой набор нежелательных действий может выполнять приложение. В организации ООО «ДжастМоби», использующей разработанный и описываемый в статье веб-сервис, осуществляется непрерывное расширение базы сигнатур для отображения полного состава приложения на уровне дополнительных библиотек.

Литература

1 AndroidInsider [Electronic resource] – Mode of access: http://www.androidinsider.ru/. – Data of access: 4.10.2015.