Из рисунка 4 видим, что программа представляет пользователю исходные ранее введенные им данные и иллюстрирует их на графе переходов. Затем по этим данным рассчитывает нормирующую константу с помощью метода Бузена, возможные состояния сети, стационарные вероятности сети, среднее число заявок в каждой системе и среднее число заявок в очереди.

Разработанная программа может быть использована математиками для быстрого анализа замкнутых СеМО через расчет соответствующих характеристик сети и систем, входящих в данную сеть.

Литература

1 Вишневский, В. М. Теоретические основы проектирования компьютерных сетей / В. М. Вишневский. – М.: Техносфера, 2003. – 512 с.

2 Бусленко, Н. П. Моделирование сложных систем / Н. П. Бусленко. – М.: Наука, 1978. – 400 с.

3 Новиков, О. А. Прикладные вопросы теории массового обслуживания / О. А. Новиков, С. Н. Петухов. – М.: Сов. радио, 1969. – 315 с.

4 Самусевич, Г. А. Основы теории массового обслуживания: учебное пособие / Г. А. Самусевич. – Екатеринбург: УГТУ – УПИ, 2005. – 102 с.

УДК 004.492

Е. И. Ключинский, Н. Б. Осипенко

ИНСТРУМЕНТАРИЙ АНАЛИЗА ДАННЫХ БЕЗОПАСНОСТИ ANDROID-ПРИЛОЖЕНИЙ

Описывается разработанный веб-сервис, предназначенный для анализа приложений на платформе Android на предмет наличия вредоносного кода, агрессивной рекламы, фишинга данных пользователя и другого подозрительного функционала. В процессе создания веб-сервиса были разработаны необходимые алгоритмы детального анализа декомпилированного Android-кода; спроектировано, разработано и оттестировано веб-приложение с использованием алгоритмов поиска по базе сигнатур, методов эвристического анализа, декомпиляции и деобфускации Android-приложений.

С ростом числа пользователей смартфонов Android становится актуальной тема защиты пользовательских девайсов от различных вредоносных программ, способных как похищать данные, так и отправлять SMS-сообщения незаметно для пользователя. Буквально несколько лет назад даже среди достаточно осведомленных в IT-тематике пользователей бытовало мнение, что вирусов на смартфонах нет, ведь разработчики мобильных платформ с самого начала закладывали в свои продукты максимальную защищенность от вредоносного ПО. Мобильные операционные системы не позволяли вредоносным программам так просто захватывать управление и хозяйничать на устройстве. Со временем эта ситуация изменилась в корне, в первую очередь благодаря расширению возможностей мобильных устройств. Современный смартфон – это полноценный рабочий инструмент, центр развлечений и средство управления личными финансами. И чем больше он умеет, тем сильнее привлекает злоумышленников, которые не против поживиться за чужой счет, тем больше вредоносных приложений они выпускают, и тем больше способов распространения и заражения придумывают. Это подтверждает стремительный рост числа мобильных троянцев. Динамика впечатляет: с первого квартала 2012 года число «зловредов» выросло более чем в десять раз и в четвертом квартале 2014 года превысило 12 миллионов [1].

Вирус для сотового телефона представляет собой приложение, которое маскируется под какую-нибудь игру или завлекательный интернет-файл. После того как абонент скачивает его на свой телефон, начинается «подрывная деятельность». Мобильный вирус может либо заблокировать карту памяти, либо незаметно для пользователя рассылать SMS- или MMS-сообщения на платные номера, он может также воровать данные из адресной книжки и отправлять их хозяину зловредной программы.

Как известно, среди десктопных ОС наиболее подвержены всевозможным атакам представители Windows-семейства. Ситуация с мобильными платформами несколько иная. На выбор злоумышленниками мобильной платформы влияют два фактора – распространенность ОС и ее открытость. Лидером по обоим критериям эксперты считают ОС Android [1]. Данные о популярности у пользователей той или иной мобильной ОС для России и Европе в целом несколько разнятся. Так, аналитики российских антивирусных компаний отмечают высокую популярность Symbian и Java-платформ, хотя считается, что Symbian уже сдает свои позиции. А вот за рубежом среди лидеров числятся iOS и Blackberry, пока еще не очень распространенные в России [2]. Но по скорости роста популярности Android обгоняет всех. Именно потому интерес вирусописателей и направлен в большей степени на данную платформу. Способствует этому и ее открытость – написать вирус, замаскировать его под приложение и предложить пользователю не представляет особых сложностей.

В рамках разработанного веб-сервиса для получения полной объективной картины возможного функционала и рисков Android-приложения была продумана система баллов потенциальной зловредности поведения приложения, приведенная в таблице 1. Каждое из 20 выявленных различных вариантов поведений приложений имеет свой коэффициент опасности в баллах. В сумме приложение может набрать 100 баллов максимум.

Таблица 1 – Шкала опасности поведений

Наименование	Баллы
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 при анализе скачиваемых с интернета apk-файлов. Вручную были введены наиболее встречаемые при работе сигнатуры и модели поведения. Через окно загрузки apk-файла выбирается Android-приложение для анализа. На рисунке 1 представлена общая информация об одном из анализируемых

приложений, с помощью шкалы эвристики получена оценка его вредоносности. Если сигнатура имеется в базе данных, то выводится ее название.

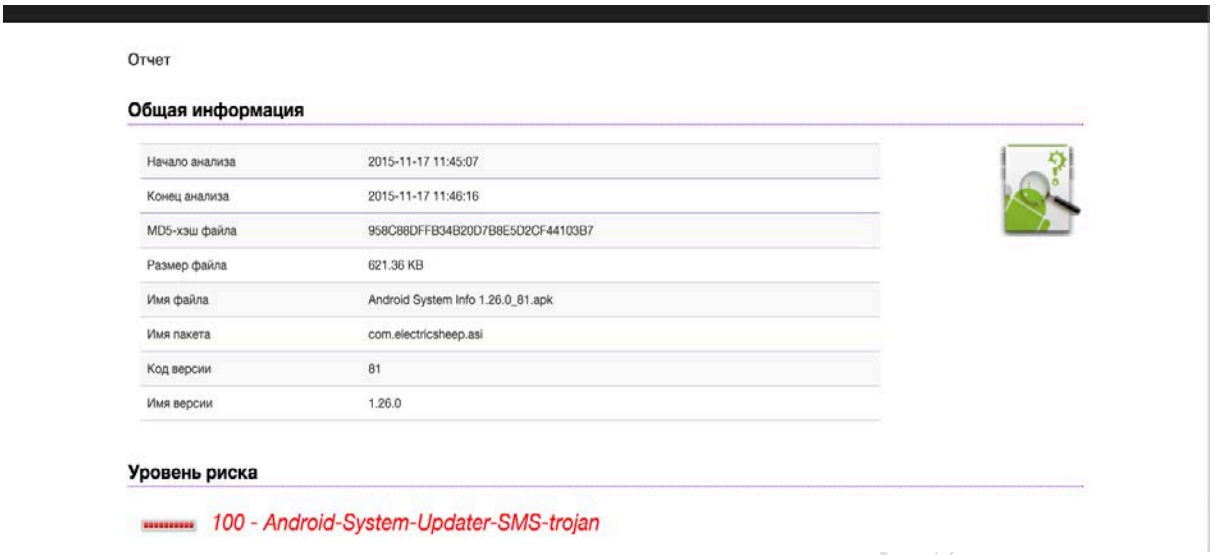


Рисунок 1 – Общая информация о приложении

На рисунке 2 представлена расшифровка шкалы эвристики, с ее помощью можно узнать, какой набор нежелательных действий может выполнять приложение.

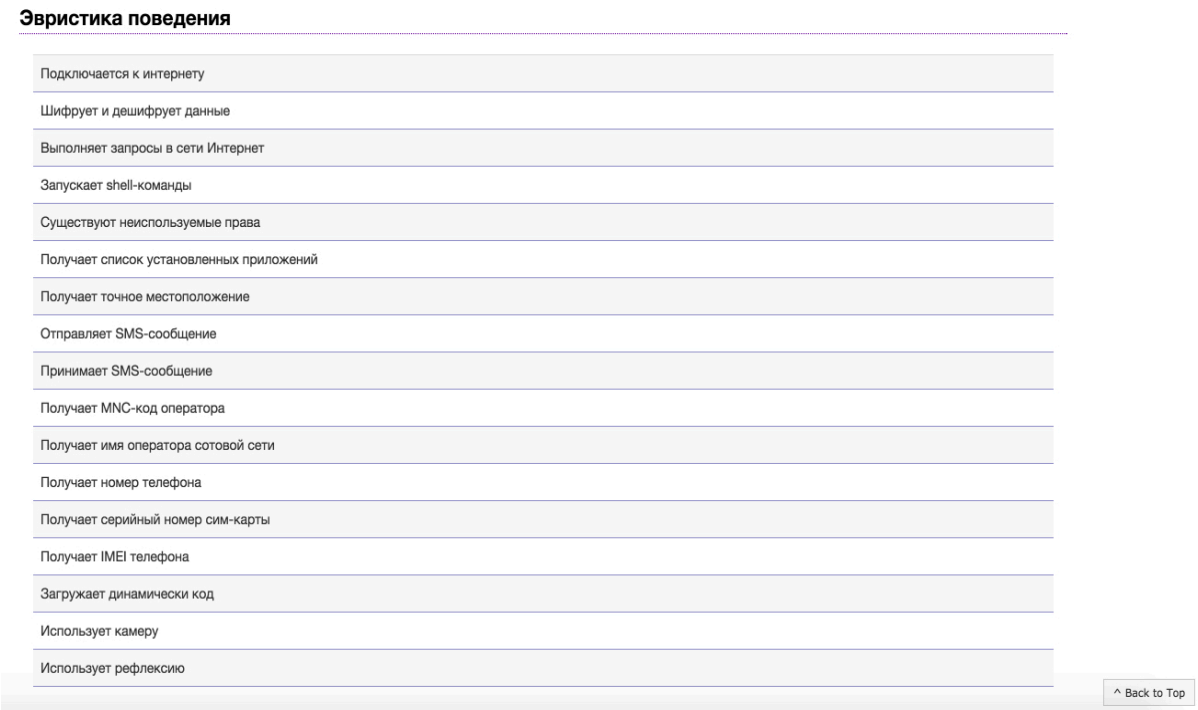
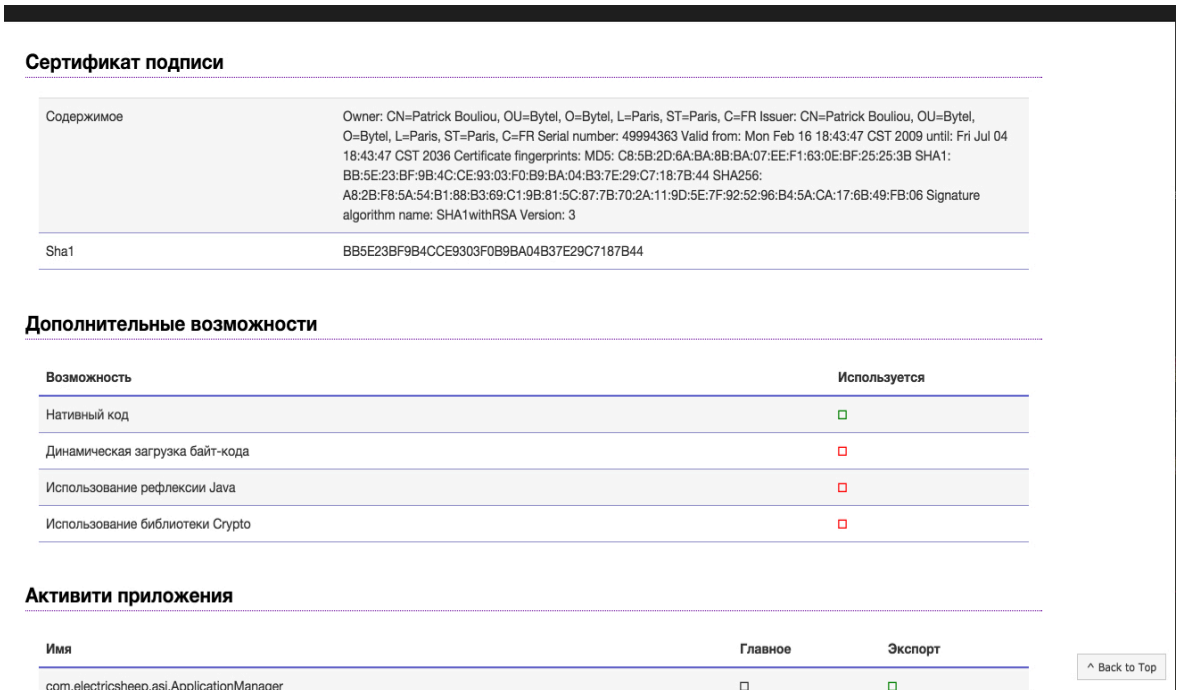


Рисунок 2 – Эвристика поведения приложения

На рисунке 3 отображено содержимое ключа для подписи, которым подписано приложение. Благодаря подписи можно идентифицировать автора приложения, его страну, компанию, адрес. Из данного примера следует, что вирус довольно старый (был написан в 2009 году французским разработчиком).



Сертификат подписи

Содержимое	Owner: CN=Patrick Bouliou, OU=Bytel, O=Bytel, L=Paris, ST=Paris, C=FR Issuer: CN=Patrick Bouliou, OU=Bytel, O=Bytel, L=Paris, ST=Paris, C=FR Serial number: 49994363 Valid from: Mon Feb 16 18:43:47 CST 2009 until: Fri Jul 04 18:43:47 CST 2036 Certificate fingerprints: MD5: C8:5B:2D:6A:BA:8B:BA:07:EE:F1:63:0E:BF:25:25:3B SHA1: BB:5E:23:BF:9B:4C:CE:93:03:F0:B9:BA:04:B3:7E:29:C7:18:7B:44 SHA256: A8:2B:F8:5A:54:B1:88:B3:69:C1:9B:81:5C:87:7B:70:2A:11:9D:5E:7F:92:52:96:B4:5A:CA:17:6B:49:FB:06 Signature algorithm name: SHA1withRSA Version: 3
Sha1	BB5E23BF9B4CCE9303F0B9BA04B37E29C7187B44

Дополнительные возможности

Возможность	Используется
Нативный код	☐
Динамическая загрузка байт-кода	☐
Использование рефлексии Java	☐
Использование библиотеки Crypto	☐

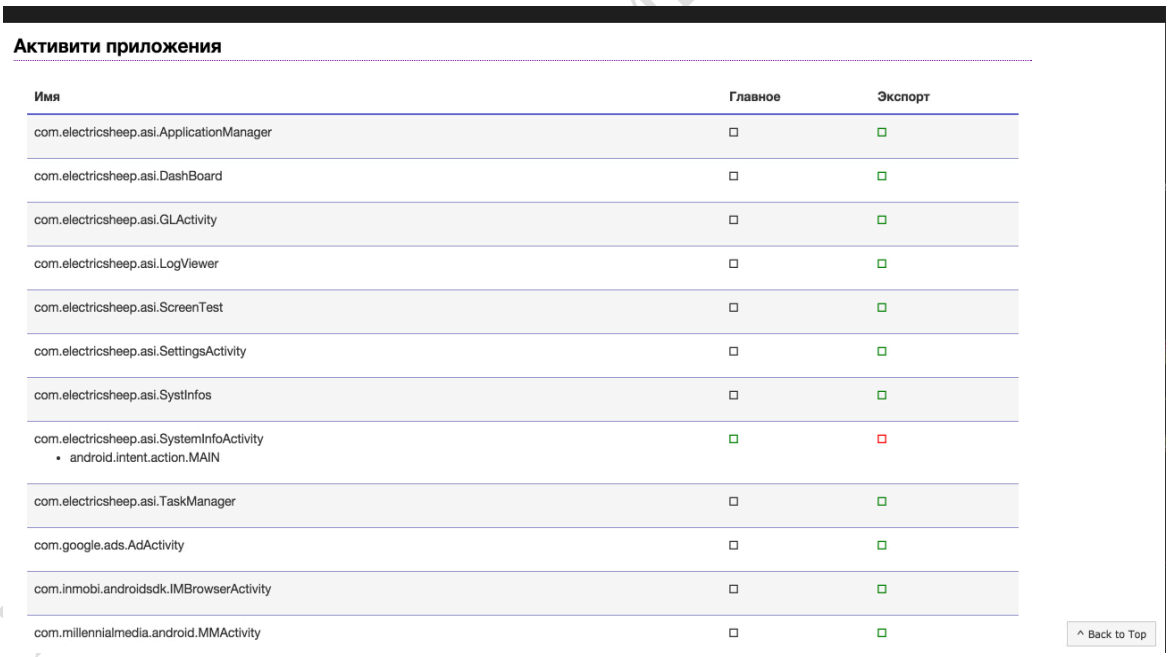
Активити приложения

Имя	Главное	Экспорт
com.electricsheep.asi.ApplicationManager	☐	☐

^ Back to Top

Рисунок 3 – Сертификат подписи приложения

На рисунке 4 изображены все активности приложения.



Активити приложения

Имя	Главное	Экспорт
com.electricsheep.asi.ApplicationManager	☐	☐
com.electricsheep.asi.DashBoard	☐	☐
com.electricsheep.asi.GLActivity	☐	☐
com.electricsheep.asi.LogViewer	☐	☐
com.electricsheep.asi.ScreenTest	☐	☐
com.electricsheep.asi.SettingsActivity	☐	☐
com.electricsheep.asi.SystInfos	☐	☐
com.electricsheep.asi.SystemInfoActivity • android.intent.action.MAIN	☐	☐
com.electricsheep.asi.TaskManager	☐	☐
com.google.ads.AdActivity	☐	☐
com.inmobi.androidsdk.IMBrowserActivity	☐	☐
com.millennialmedia.android.MMActivity	☐	☐

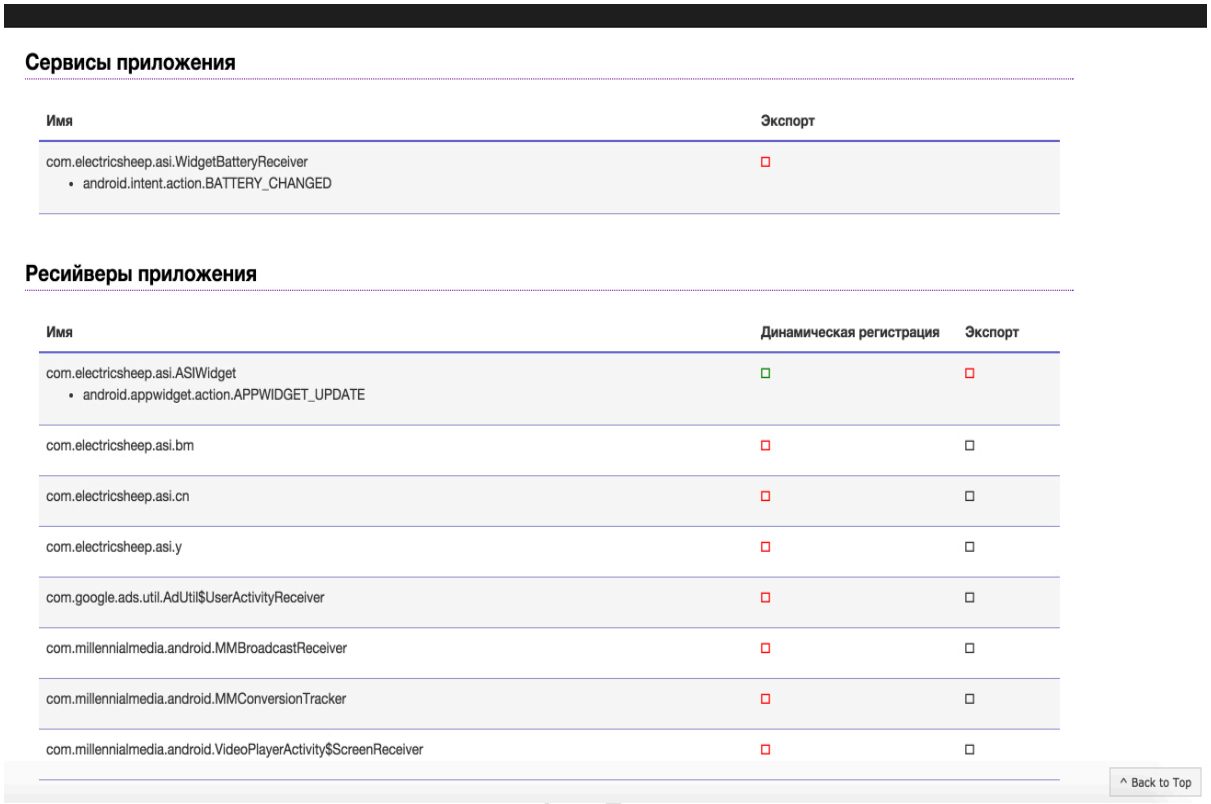
^ Back to Top

Рисунок 4 – Активности приложения

На рисунке 5 изображены все сервисы и широковещательные слушатели.

В настоящий момент разработанное приложение используется в организации ООО «ДжастМоби». Так как организация занимается разработкой мобильных приложений, их продвижением и маркетингом, при работе зачастую приходилось анализировать различные программы вручную на предмет используемых технологий, устанавливать их и декомпилировать. Благодаря описанному выше веб-приложению достаточно быстро

можно определить степень вредоносности Android-приложений и наличие различных рекламных библиотек, что уже экономит достаточно много времени. Также планируется добавление сигнатур всех популярных android-фреймворков для отображения полного состава приложения на уровне дополнительных библиотек.



Сервисы приложения

Имя	Экспорт
com.electricsheep.asi.WidgetBatteryReceiver • android.intent.action.BATTERY_CHANGED	☐

Ресийверы приложения

Имя	Динамическая регистрация	Экспорт
com.electricsheep.asi.ASIWidget • android.appwidget.action.APPWIDGET_UPDATE	☐	☐
com.electricsheep.asi.bm	☐	☐
com.electricsheep.asi.cn	☐	☐
com.electricsheep.asi.y	☐	☐
com.google.ads.util.AdUtil$UserActivityReceiver	☐	☐
com.millennialmedia.android.MMBroadcastReceiver	☐	☐
com.millennialmedia.android.MMConversionTracker	☐	☐
com.millennialmedia.android.VideoPlayerActivity$ScreenReceiver	☐	☐

^ Back to Top

Рисунок 5 – Широковещательные слушатели и сервисы приложения

Литература

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

2 4pda.ru [Electronic resource]. – Mode of access: http://www.4pda.ru/. – Data of access: 1.09.2015.

УДК 517.444

И. С. Ковалева

ОПЕРАТОР МАРКОВА–СТИЛТЬЕСА В ПРОСТРАНСТВЕ $L^2(0,1)$

Общее определение абстрактного преобразования Стилтьеса над полугруппой S было дано А. Р. Миротиным в монографии [1]. В случае аддитивной полугруппы целых неотрицательных чисел Z_+ получаем сингулярный интегральный оператор, который называется оператором Маркова–Стилтьеса. В данной статье доказана унитарная эквивалентность оператора Маркова–Стилтьеса в пространствах $H^2(D)$ и $L^2(0,1)$. Как следствие, получены спектр и норма данного оператора в пространстве $L^2(0,1)$.