Жернаков С.В., д-р техн. наук, проф.,
Гаврилов Г.Н., аспирант
Уфимский государственный авиационный технический университет

ОБЗОР СОВРЕМЕННОГО СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В МОБИЛЬНЫХ СИСТЕМАХ

grigorijgavrilov@mail.ru

В данной статье были рассмотрены мобильные системы с точки зрения защиты информации. Был выполнен анализ статистики угроз для мобильных систем. А также был проведем обзор современных уязвимостей и рассмотрена модель безопасности мобильной системы. Согласно анализу статистики, современных угроз и рассмотренной модели безопасности были сделаны соответствующие выводы об актуальности исследований в данном направлении.

Ключевые слова: *мобильная система, уязвимости, модель безопасности, Android.*

Введение. В настоящее время актуальность исследований в сфере мобильных систем находится на высоком уровне, так как современные мобильные системы имеют огромный функционал и возможности. Пользователи хранят множество личных данных на мобильных устройствах: фотографии, контакты, деловые переписки, документы, пароли, номер кредиток, мобильный банк и т.д. Следовательно мобильное устройство вызывает интерес со стороны злоумышленников, как объект для получения прибыли. Таким образом количество вредоносного программного обеспечения растет с большой скоростью. Методы сигнатурного анализа эффективно работают, однако идентифицировать и устранять новые вредоносные программы они не способны. Это дает повод рассмотреть применимость современных интеллектуальных методов для детектирования вредоносных программ на основе эвристического анализа.

Методология. Обзор, анализ и выявление необходимости исследований в направлении защиты информации в мобильных устройствах.

Основная часть. Мобильные системы являются неотъемлемой частью нашей повседневной жизни, количество персональных данных, которые хранятся на них, постоянно увеличивается. В отличие от персональных компьютеров, мобильные системы развиваются гораздо быстрее. По имеющимся данным Википедии (рис. 1), Android работает на 64 % устройства [1]. Учитывая, что доля Android устройств на рынке неуклонно растет, то и число пользователей смартфонов будет продолжать неуклонно расти.

Но при этом область защиты информации не всегда поддерживается разработчиком и успевает вслед за развитием самой системы. В современный век мобильные устройства используются для множества операции – это банк-клиент, почта, документы, облачные сервисы, фото, видео и т.д. Мобильный телефон своего рода банк персональной информации, при потере контроля над этим удобным для нас устройством, мы можем потерять все персональные данные, финансы, авторитет. Например, десятки тысяч пользователей «Сбербанка» стали жертвами мошенничества. Как заявил агентству FlashNord источник в МВД, пострадали 20–30 тысяч человек. Все пострадавшие использовали смартфоны различных марок на базе операционной системы Android. Вирус-троян, относящийся к семейству вредоносного ПО Backdoor.AndroidOS.Obad, похищал денежные средства с привязанных к телефонным номерам карт Сбербанка. Жертвы долго остаются в неведении, так как программа блокировала sms-сообщения о снятии средств со счета. Пострадали 20–30 тысяч человек и ущерб составил огромную сумму [3].

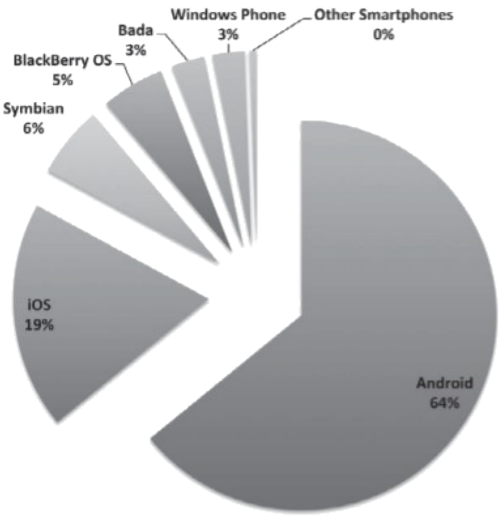

Рис. 1. Глобальная статистика роста операционных систем

За последние два года число мобильных вредоносных программ выросло более чем в 10 раз и превысило 12 миллионов в четвертом квартале 2014 [4].

В 2014 году продукты «Лаборатории Касперского» заблокировали 6 167 233 068

вредоносных атак на компьютеры и мобильные устройства пользователей. Отражено 1 363 549 атак на Android-устрйства. Решения «Лаборатории Касперского» отразили 1 432 660 467 атак, проводившихся с Интернет-ресурсов, размещенных в разных странах мира.

За отчетный период было обнаружено:

- 4 643 582 вредоносных установочных пакета;
- 295 539 новых мобильных вредоносных программ;
- 12 100 мобильных банковских троянцев [1, 2].

Несколько лет назад вредоносного программного обеспечения практически не существовало. Разработчики мобильных операционных систем с самого начала закладывали в свои продукты максимальную защищенность от вредоносного программного обеспечения. Мобильные операционные системы не позволяли вредоносным программам захватывать управление устройством.

В настоящее время ситуация изменилась, в первую очередь благодаря расширению возможностей мобильных устройств. Современное мобильное устройство – полноценный рабочий инструмент, центр развлечений и средство управления личными финансами. Чем больше возможностей у мобильного устройства, тем сильнее он привлекает злоумышленников, тем больше вредоносных приложений появляются, и тем больше способов распространения и заражения появляется.

На рисунке 2 изображен рост числа мобильных троянских программ.

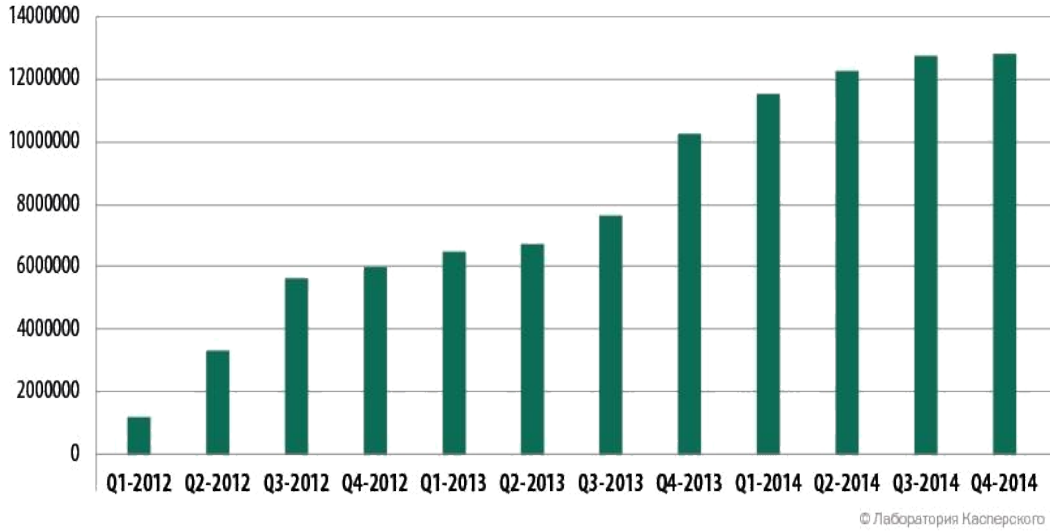

Рис. 2. Количество обнаруженных вредоносных установочных пакетов

С первого квартала 2012 года число мобильных вредоносных программ выросло более чем в десять раз и в четвертом квартале 2014 года превысило 12 миллионов.

Показательно меняется и распределение вредоносных программ по типам. Легко заметить, что традиционные SMS-трояны и многофункциональные бэкдоры уступают дорогу рекламным вредоносным программам и троянам-банкерам. При этом уменьшение доли вредоносных программ какого-либо типа вовсе не говорит о том, что они уходят со сцены – не забывайте про рост общего числа вредоносных программ для мобильных устройств [2, 4, 5].

Современные угрозы информационной безопасности мобильных систем

Угрозы с описанием представлены в таблице 1.

Также можно выделить следующие уязвимости:

- возможность установки программы как из официального каталога программ, так и из любого другого доступного источника;
- возможность любому желающему размещать в официальном каталоге программ свои программы;
- программы не подвергаются предварительной проверке или тестированию после загрузки в каталог программ;
- отсутствие системных обновлений со стороны разработчика.

Обзор существующих методов и алгоритмов обнаружения вредоносных программ в мобильных системах

Для открытой мобильной системы необходима надежная архитектура безопасности и программное обеспечение. В мобильной системе была реализована многоуровневая безопасность, которая обеспечивает гибкость, необходимую для открытой платформы и обеспечивает защиту для всех пользователей. В

системе был реализован контроль безопасности с точки зрения разработчиков и пользователей.

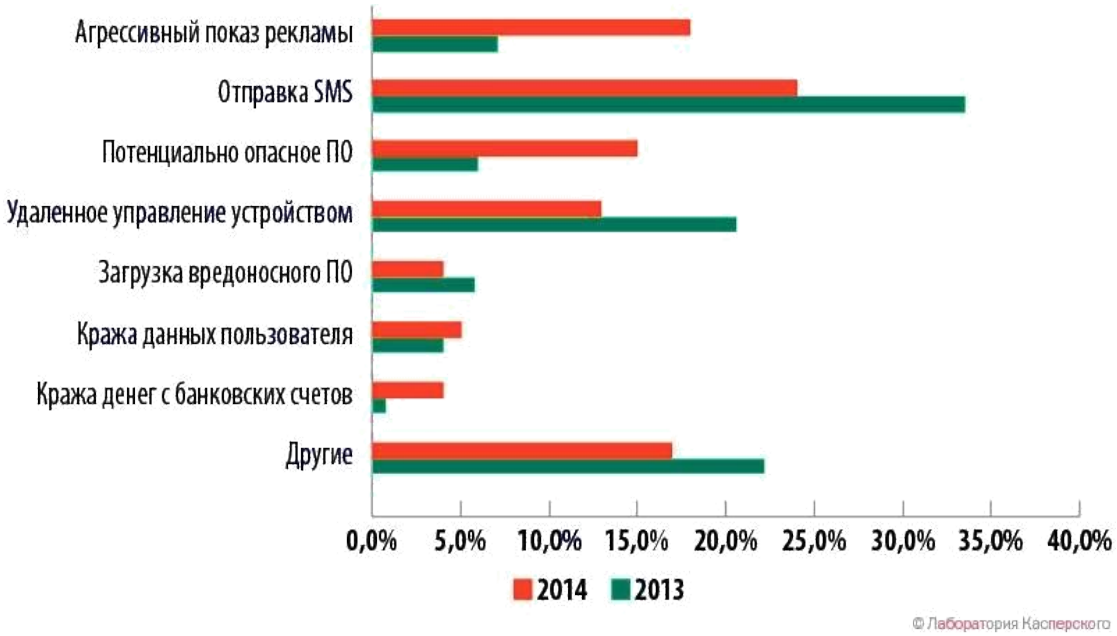

Рис. 3. Распределение мобильных вредоносных программ по функциям (файлы из коллекции «Лаборатории Касперского»)

Таблица 1

Угрозы существующие на сегодняшний день

Угроза	Описание
Эксплойты	Сложный тип вредоносного программного обеспечения, способный дать злоумышленнику всю информацию о пользователе, устройстве, местоположении и позволить управлять смартфоном удаленно [4]. Злоумышленники используют эту угрозу, а также уязвимости [8, 9] для реализации атак и получения прав чтобы беспрепятственно устанавливать программы без разрешения пользователя.
Система разрешений	При установке программы на мобильное устройство пользователю предоставляется список всех разрешений для функций, которые будут доступны программе. После установки программа получает возможность выполнять свои действия с предоставленными функциями без участия пользователя.
Модифицированные операционные системы	В такие мобильные операционные системы могут быть встроены вредоносные программы. Также, когда цифровой подписью образа системы подписывается программа, она получает те же права, что и сама система, в которой она работает.
Открытость мобильной системы	Так как код доступен, он может использоваться злоумышленниками чтобы находить уязвимости и ошибки.
Системная инженерия	Использование вредоносной программой человеческого фактора для получения прав на управление устройством.
СМС-троян	Отправляют смс с повышенной тарификацией на короткие номера.
Трояны	Сбор конфиденциальной информации пользователя, добавление закладок в браузер, выполнение команд, поступающих от злоумышленников, отправка СМС-сообщений, установка других приложений и т. п. Чтобы реализовать возможность установки приложений, не вызывая подозрений со стороны пользователя. Необходимы права root (права, с которыми работает ядро системы).
Коммерческие программы-шпионы	Эти приложения используются для слежки за пользователями.
Рекламные модули	Представляют собой приложения и игры, снабженные сервисным модулем, который остается работать даже после закрытия самого приложения и время от времени размещает рекламу в области уведомлений
Прочие	Вредоносные программы, которые сочетают в себе различные функции, описанные выше.

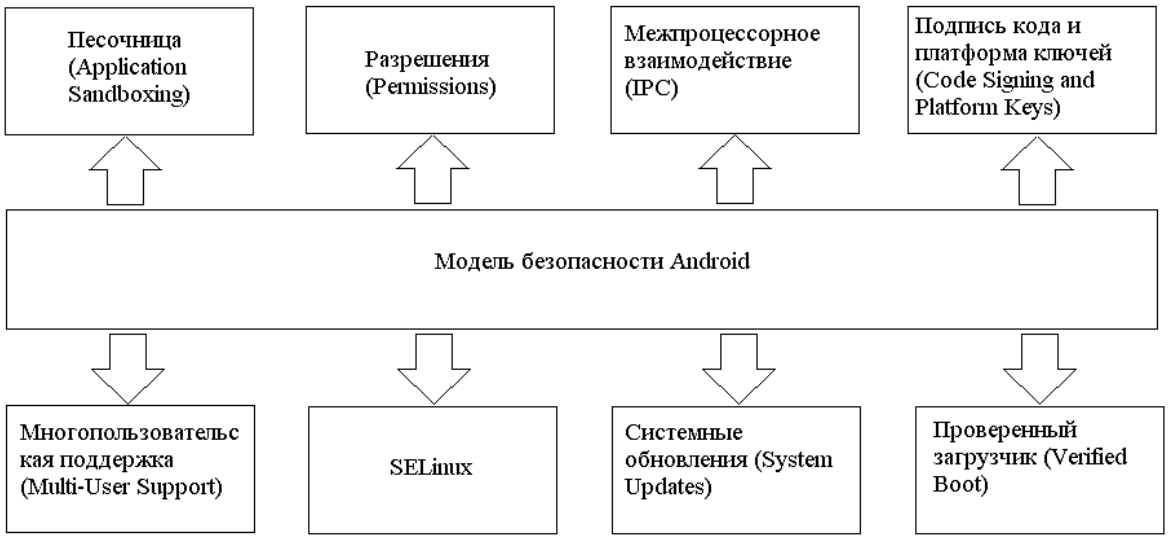

Рис. 4. Модель безопасности мобильной системы

- Песочница;

Программы изолируются, как на уровне процесса (выделяется отдельных процесс), так и на уровне файлов (выделяется отдельный каталог).

- Разрешения;

Мобильная система может присвоить дополнительные права - разрешения, чтобы программа могла расширить свой функционал. Они могут контролировать доступ к драйверам, Интернет соединению, данным или сервисам операционной системы.

- IPC;

В мобильной системе обмен сигналами и данными между процессами организован с помощью фреймворка межпроцессного взаимодействия (Inter-Process Communication) Binder.

- Подпись кода и платформа ключей;

Все программы мобильной системы должны быть подписаны их разработчиком, в том числе системных программы.

- Многопользовательский режим;

Этот режим дает возможность использовать устройство нескольким пользователями и при этом у каждого будет свое отведенное пространство, ресурсы, которые недоступны остальным.

- SELinux;

Система SELinux построена на этой основе (а также на основе 15 лет исследований NSA в области безопасности ОС), но добавляет еще один уровень безопасности, называемый «мандатное управление доступом» (Mandatory Access Control, MAC).

- Системные обновления;

- Проверенный загрузчик.

В настоящее время существует большое количество антивирусного программного обеспечения. Оно работает на основе сигнатурного анализа, следовательно, вредоносное программное обеспечение которого нет в базе сигнатур или они не обновлялись по какой-либо причине не будет обнаружено. Сам процесс обнаружения, выявления и добавления сигнатуры в базы антивирусов довольно кропотлив и занимает большое количество времени.

В частности используется способ защиты от вредоносного программного обеспечения на основе разрешений, которые устанавливаемая программа запрашивает на этапе установки, но далеко не каждый пользователь не анализирует выдаваемый список запроса.

Выводы. Следовательно, можно сделать вывод в том, что система не имеет эффективных средств защиты от вредоносного программного обеспечения.

Анализ статистики, существующих угроз, а также структуры модели безопасности мобильной системы можно сделать вывод, что актуальность исследований в сфере мобильной системы находится на высоком уровне, так как эти системы активно развиваются, наращиваются возможности и функции. Непрерывно увеличивается количество вредоносных программ. При этом методы сигнатурного анализа эффективно работают, однако идентифицировать и устранить новое вредоносное программное обеспечения не способны. На основании изложенного выше, необходимо сделать вывод о разработке новых интеллектуальных методов аппаратно-

программных средств защиты информации в устройствах мобильной связи.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Kaspersky Security Bulletin 2014. Основная статистика за 2014 год [Электронный ресурс]. Систем. требования: браузер. URL: http://securelist.ru/analysis/24580/kaspersky-security-bulletin-2014-osnovnaya-statistika-za-2014-god/ (дата обращения: 20.10.2015)

2. Kaspersky Security Bulletin 2014. Прогнозы на 2015 год [Электронный ресурс]. Систем. требования: браузер. URL: https://securelist.ru/analysis/24575/kaspersky-security-bulletin-2014-prognozy-na-2015-god/ (дата обращения: 21.10.2015)

3. Пострадали десятки тысяч клиентов «Сбербанка» по всей стране [Электронный ресурс]. Систем. требования: браузер. URL: https://hi-tech.mail.ru/news/sbarbank-android-users-hacked-and-robbed-by-trojan.html (дата обращения: 10.11.2015)

4. Мобильные угрозы [Электронный ресурс]. Систем. требования: браузер. URL: http://www.kaspersky.ru/internet-security-center/threats/mobile (дата обращения: 20.10.2015)

5. Безопасность мобильных устройств [Электронный ресурс]. Систем. требования: браузер. URL: http://www.osp.ru/win2000/2014/01/13039202/ (дата обращения: 30.10.2015)

6. AV-Comparatives: Антивирусы для Android: Март 2015 [Электронный ресурс]. Систем. требования: браузер. URL: http://www.comss.ru/page.php?id=2424 (дата обращения: 20.11.2015)

7. Враг в телефоне [Электронный ресурс]. Систем. требования: браузер. URL: https://securelist.ru/analysis/obzor/25150/vrag-v-telefone/ (дата обращения: 18.11.2015)

8. CVE-2011-1823 [Электронный ресурс]. Систем. требования: AdobeAcrobatReader. URL: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1823 (дата обращения: 20.11.2015)

9. CVE-2009-1185 [Электронный ресурс]. Систем. требования: AdobeAcrobatReader. URL: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1185 (дата обращения: 20.11.2015)

10. Уязвимости платформы Android. Настоящее и будущее [Электронный ресурс]. Систем. требования: браузер. URL: http://habrahabr.ru/company/drweb/blog/142993/ (дата обращения: 25.10.2015)

Zhernakov S.V, Gavrilov G.N

THE PRESENT STATE OF INFORMATION SECURITY IN MOBILE SYSTEM

This article examined mobile systems in terms of data protection. Statistical analysis was performed threats to mobile systems. Also, a review was undertaken of modern vulnerabilities, and the model of the mobile security system. According to the analysis of statistics, current threats and discussed the security model were made conclusions about the relevance of research in this area.

Key words: *mobile system vulnerabilities, security model, Android.*

Жернаков Сергей Владимирович, доктор технических наук, профессор, заведующий кафедрой электроники и биометрических технологий.
Уфимский государственный авиационный технический университет.
Адрес: Россия, Республика Башкортостан, 450000, Уфа, ул. Карла Маркса, 12.
E-mail: zhsviit@mail.ru

Гаврилов Григорий Николаевич, аспирант кафедры электроники и биометрических технологий
Уфимский государственный авиационный технический университет.
Адрес: Россия, Республика Башкортостан, 452170, поселок Чишмы, ул. Ленина, д. 15.
E-mail: grigorijgavrilov@mail.ru