УДК 316.776.22

# ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В МИРЕ МОБИЛЬНЫХ УСТРОЙСТВ

МФПУ "Синергия"(2)
**Игорь Александрович Нестеров,** к.т.н., доцент,
**Андрей Иванович Касьян,** к.т.н., доцент ,
**Александр Николаевич Медведь,** к.т.н., с.н.с.

**Современного человека нередко определяют как homo-mobilius, счастливого обладателя мобильного телефона, нередко планшета или других средств коммуникации. Бесполезно противиться ускоряющейся homo-mobilius'зации – этому веянию времени и двигателю прогресса. Однако у каждого блага, как водится, имеется и другая сторона. В частности, сегодня отчетливо наблюдается неуклонный рост числа угроз, связанный с внедрением мобильных телекоммуникационных средств, той же мобильностью и обусловленных. Конечно, можно жить, не обращая внимания на "всевидящее око Большого брата", зловредных вирусов и "червей" или на постоянные попытки всякого рода жуликов залезть в Ваш электронный, но совсем не виртуальный, карман. На извечный вопрос "что делать" когда-нибудь придется искать ответ, так как масштабы бедствия возрастают с каждым днем. Так, в прошлом году число атак на мобильные устройства впервые превысило число взломов компьютеров и POS-систем в торговых центрах. В связи с этим интересно попытаться разобраться – кто, когда и с какой целью может воспользоваться Вашей "мобильностью" в своих корыстных интересах.**

**Modern man is often defined as homo-mobilius, happy owner of a mobile phone often tablet or other means of communication. It is useless to resist accelerating homo-mobilius'of the organization – the spirit of the time and the engine of progress. However, each benefit, as usual, there is another side. In particular, today, clearly there has been a steady increase in the number of threats associated with the introduction of mobile telecommunications, the same mobility and due. Of course, you can live oblivious to the "all-seeing eye of Big brother", malicious viruses and worms or constant attempts all kinds of crooks to get into Your email, but not virtual pocket. The eternal question "what to do" ever have to search for the answer, as the scale of the disaster is growing by the day. So, last year the number of attacks on mobile devices for the first time exceeded the number of burglaries of computers and POS systems in shopping malls. In this connection it is interesting to try to understand – who, when and for what purpose may I use Your "mobility" in their own selfish interests.**

***Ключевые слова: средства коммуникации, вирусы, хакерские атаки, международный идентификационный номер, безопасность***

***Keywords: units of communication, viruses, hackers attacks, IMEI, security***

Как известно, источники угроз принято подразделять на антропогенные, техногенные и стихийные. Начнем с последних. Стихийные угрозы - это пожары, наводнения, различные непредвиденные обстоятельства, необъяснимые явления и др. Последствия воздействия стихийных угроз на мобильные устройства чаще всего связаны с практически полным уничтожением гаджетов и данных на них. С одной стороны, поскольку материалом, из которого изготовляют большинство конструктивных компонентов мобильных устройств, является пластик, то воздействие повышенных температур или затопление приводит к уничтожению аппаратов и полной потере информации.

С другой стороны, в случае стихийных угроз человек стремится сберечь свой гаджет, чтобы обеспечить себе связь с внешним миром, и это существенно повышает выживаемость мобильных устройств. Парирование воздействия стихийных угроз затруднено в связи с неопределенностью момента возникновения самой угрозы, степенью ее опасности и характера возможного воздействия. Наиболее надежным способом ограничения последствий такого рода угроз может служить страхование мобильного устройства, а также резервное копирование данных, причем лучше всего на облачных сервисах.

Перейдем к рассмотрению техногенных угроз, которые обычно разделяют на две подгруппы. К внешним техногенным угрозам можно отнести неблагоприятные воздействия со стороны средств связи, сетей инженерных коммуникаций, транспорта. К внутренним - неисправности технических средств обработки данных, ошибки программных продуктов, предназначенных для обработки информации, отказы или некорректная работа некачественных вспомогательных средств и др.

Последствия воздействий со стороны этой группы источников угроз прогнозировать затруднительно, так как они напрямую зависят от свойств сложных технических устройств (напомним читателю, к примеру, о внезапно воспламеняющихся высокотехнологичных аккумуляторах одного из смартфонов). Каким-то образом скомпенсировать ущерб от техногенного аварийного воздействия, как и в случае стихийных угроз, можно только путем страхования рисков наступления события.

Заметим, однако, что в вопросе страхования мобильных устройств есть свои нюансы. Например, в некоторых кампаниях страховыми случаями не являются хищение и кража гаджета. Тут мы переходим к так называемым антропогенным угрозам.

Всем известно, что современное "брендовое" мобильное устройство - это дорогостоящая вещь, которая может быть у Вас украдена только по этой причине. Таких случаев абсолютное большинство. Вор рассчитывает получить выгоду от перепродажи самого "приватизированного" им устройства, пусть и по относительно невысокой цене. Ему, как правило, неинтересны Ваши данные, телефонные базы, фотографии. Однако кража современного смартфона - не такое уж распространенное преступление. Люди, делающие бизнес на воровстве мобильников, уже столкнулись с определенными сложностями при сбыте такой "продукции".

Дело в том, что сотовые операторы и производители телефонов предприняли ряд мероприятий, позволяющих достаточно быстро определить местонахождение включенного смартфона, даже если в нем сменили sim-карту. Поиск осуществляется благодаря знанию серийного номера изделия. Смартфоны и мобильные телефоны снабжены встроенным IMEI - международным идентификационным номером, уникальным для каждого аппарата и состоящий из 15 цифр. При включении мобильного устройства этот номер автоматически передается оператору, и именно по нему происходит поиск украденных телефонов.

Как только IMEI появляется у оператора, с ним сопоставляется и телефонный номер sim-карты. Собственно, после этих действий отыскание смартфона является делом достаточно тривиальным. Как правило, это устройство находится у "очень удачливого" молодого человека, купившего мобильник у неизвестного лица по случаю, без документов и "за копейки". После посещения молодого человека представителями правоохранительных органов или хозя-

ином гаджета он остается, в лучшем для него случае, без мобильного устройства и без истраченных денег. Поэтому никому не рекомендуем приобретать мобильники "с рук", пусть даже и за гроши.

Правда, в России реализация вышеуказанного алгоритма поиска мобильного устройства серьезно затруднена из-за проблемы "серых двойников". Дело в том, что в результате завоза телефонов в Россию по "серой" схеме IMEI нередко перестает быть уникальным. То есть появляются дубликаты мобильников, которые мешают поиску воришек. А можно ли проверить, что телефон не "серый"?

Вообще-то существует целый перечень признаков "серости" мобильного гаджета. Самый простой и надежный способ проверки мобильника на подлинность - сверить его IMEI с надписью на коробке, в гарантийном талоне или в "укромном месте" под батареей устройства. Достаточно набрать комбинацию *#06#, и на экране смартфона высветится набор из 15 цифр, которые должны в точности совпадать с указанными на коробке или гарантийном талоне.

Кстати, большая часть современных гаджетов содержит специальную программу, которая не позволяет "народным умельцам" изменять IMEI. Во многих европейских странах за выполнение подобной операции предусмотрена уголовная ответственность.

Еще одним способом противодействия воровству является применение специальных программ, позволяющих дистанционно выполнить действия по блокировке и определению местоположения украденного гаджета. Таких программ достаточно много, например: iTag, Avast! Mobile Security, Mobile Defense, Prey Anti-Theft, Plan B, SeekDroid Lite, AntiDroidTheft, McAfee Antivirus & Security, Cerberus, Lookout Security & Antivirus (Android/iOS), Android Lost Free, Kaspersky Mobile Security (Android/iOS) и др. Как правило, указанные программы обеспечивают выполнение ряда удаленных функций:

- блокировка функций устройства;
- деинсталляция приложений;
- отслеживание положения смартфона с использованием GPS-координат, Wi-Fi и GoogleMaps даже после замены sim-карты;
- блокировка нежелательных звонков, сообщений;
- скрытие нежелательной информации от людей, случайно получивших доступ к устройству.

Но стоит злоумышленнику просто выключить украденный гаджет - и программы, естественно, перестают работать. Но устанавливать какую-то разновидность такой программы всё-таки целесообразно, так как при ее наличии на устройстве шансы найти гаджет увеличиваются. Выбор же конкретной программы не играет большой роли.

Следующий способ отъёма денег у homo-mobilius - наглое вымогательство. Существуют основные три типа программ-вымогателей:

- шифрующие файлы;
- блокирующие работу системы;
- блокирующие работу в браузерах.

После "нечаянной" установки программы на гаджет жертвы программа-вымогатель обычно шифрует все файлы или блокирует работу устройства. Пока гаджет не заблокировался, пользователь ничего не замечает, так как все процессы проходят в фоновом режиме. Вслед за завершением зловредных действий на экране устройства появляется надпись с требованием заплатить деньги, как правило каким-нибудь анонимным способом (очень часто в качестве платы требуют BitCoin). Запись иногда сопровождается грозными словами с упоминанием статей уголовного кодекса, которые якобы нарушил владелец гаджета.

Полиция и специалисты по кибербезопасности (в том числе "Лаборатория Касперского") периодически ловят преступников и выкладывают инструменты для восстановления пораженных вирусами гаджетов в Сеть. Однако современный вымогатель весьма и весьма продвинут. Он все чаще использует новые, и при том весьма сложные алгоритмы шифрования. Поэтому перспектива лишиться своих файлов (в какой-то отнюдь не прекрасный день) достаточно реальна для большинства активных пользователей Сети.

Да и легкость, с которой преступники получают деньги от владельцев пострадавших мобильных устройств, приводит к тому, что программы-вымогатели используют все чаще. По данным "Лаборатории Касперского", всего за год - с апреля 2015 г. по апрель 2016 г., разработанные "Лабораторией" программные продукты заблокировали 2 315 931 атак вымогателей, что на 17,7% больше, чем годом ранее.


Что же делать? Рекомендации вполне традиционны: достаточно часто производить резервное копирование, не открывать подозрительные письма и sms, устанавливать на мобильное устройство антивирус и регулярно вносить свежие обновления в программное обеспечение. При этом следует отчетливо понимать, что единственное, что наверняка поможет - это свежий "бэкап".

Если же вымогатели добрались до Вас, а "бэкапа" нет, то рекомендуется испробовать свежий антивирус, заимствованный из надежного источника. Если и его нет, или результаты применения неудовлетворительны - все равно не платите вымогателям. Да, они будут Вам обещать, что после получения соответствующей мзды важную для Вас информацию восстановят. Но где гарантия, что они это сделают после получения денег?

Те сотни долларов, которые требуют вымогатели за разблокировку мобильного устройства, - всего лишь детские шалости по сравнению с последствиями действий мобильных банковских "зловредов", которые могут полностью подчистить Ваши счета. Для жителей крупных городов времена толстых кошельков канули в небытие. Появление мобильного онлайн-банкинга значительно облегчило оплату счетов, но принесло и новые угрозы. Хотя система мобильного онлайн-банкинга защищена более серьезно по сравнению с традиционным онлайн-банкингом, попытки вскрыть мобильные виртуальные кошельки не прекращаются. В десятке наиболее часто атакуемых стран мира Россия по доле пострадавших пользователей (2,92 %) во втором квартале текущего года выдвинулась на второе место.

Фантазии преступников на этом поприще очень разнообразны. В ход идут поддельные сайты с просьбой ввести данные, письма и sms с "троянами", а также телефонные звонки с применением социальных технологий. Особой любовью у хакеров пользуются открытые сети Wi-Fi. С целью добывания информации преступники даже стали формировать собственные открытые сети Wi-Fi.

Чтобы уменьшить вероятность кражи из электронного кошелька, пользователю необходимо соблюдать ряд правил:

1. Регулярно повышать безопасность мобильного устройства. Чем больше антивирусов, тем лучше.

2. Избегать случаев пользования мобильным устройством в общественных местах и бесплатным Wi-Fi для проведения банковских операций.

3. Обращать внимание на подозрительные e-mail и sms-сообщения.

4. Немедленно сообщать банку о любых подозрительных действиях.

5. Регулярно загружать обновления операцион-

ных систем, программ и приложения, причем только из официальных источников.

К числу самых мощных и опасных инструментов электронного "зловредства" в отношении ничего не подозревающих пользователей мобильных устройств можно отнести так называемые государственные "трояны", разрабатываемые частными компаниями и продаваемые властям (точнее - соответствующим службам). На сленге это называется "законный перехват". Государственными органами обычно декларируется направленность перехвата информации только против террористов, педофилов и т.д. Однако кто мешает использовать эти "трояны" и для других целей? Специальные службы с помощью указанного программного обеспечения могут запросто "отследить" и оценить действия практически любого человека, используя данные GPS, сигналы базовых станций сотовых операторов, данные в соцсетях и телефонные звонки. Причем государственные границы "трояны" преодолевают с легкостью. Вот как выглядят, к примеру, основные возможности специального программного обеспечения FinSpyMobile, первоначально предназначавшегося для налоговиков:

1. Переадресация вызовов, SMS и электронных писем.

2. Незаметное для пользователя включение микрофона устройства.

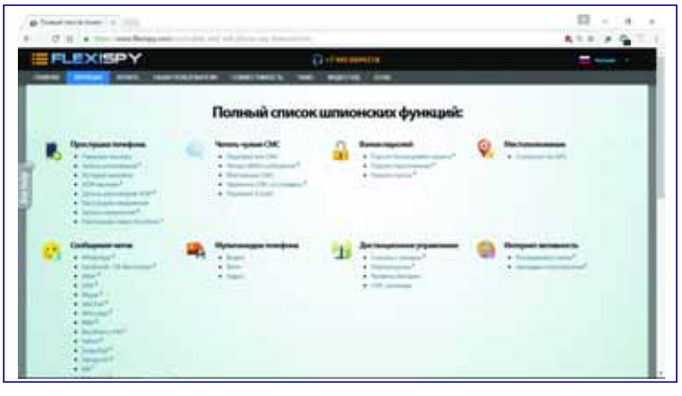
3. Доступ к контактам, записям, файлам.

4. Определение местонахождения мобильного телефона с помощью GPS и данных сотовой сети.

5. Поддержка платформ iOS, Android, BlackBerry, Windows Mobile и Symbian.

Возникает и смежный с обсуждаемым вопрос: а что может "обычный гражданин" в части сбора информации о другом "обычном гражданине"? Оказывается, достаточно много. К примеру, в результате осуществления кратковременного доступа к мобильному устройству "партнера" на гаджет можно установить не вполне безобидный "троян", например FLEXISPY. Скриншот его титульной страницы позволяет оценить функциональные возможности очередного "зловредства".

Здесь есть все - от перехвата звонков до взлома паролей. FLEXISPY позиционируется как "полезная программка" для родителей и работодателей. Стоит максимум $349 в год - дорого, но добытая ею информация нередко оценивается намного дороже. После установки на мобильник FLEXISPY скрывает ярлык и ведет себя "очень скромно". Обнаружить практически невозможно.




Как можно со всем этим бороться? Правила опять-таки не слишком сложные, но придерживаться их нужно постоянно:

- не оставлять свое мобильное устройство без присмотра, особенно в местах, где с ним "может поработать" постороннее лицо: поставить шпионскую программу, скопировать данные, ну или снять деньги со счета.

- не производить с гаджетом действий, не разрешенных изготовителем.

Кстати, после установки программы FLEXISPY ее маленький агент, отслеживающий запретную активность пользователя, способен работать на любом компьютере. Однако для полноценного развертывания FLEXISPY на устройствах с ОС Android необходимо получить права PYT (от англ. root - корень, или суперпользователь - специальный аккаунт в UNIX-подобных системах с идентификатором 0, владелец которого имеет право на выполнение всех без исключения операций), а на iPhone - выполнить так называемый "джейлбрейк" (англ. Jailbreak - "Побег из тюрьмы").

Подчеркнем, что "джейлбрейк" - официально не поддерживаемая корпорацией Apple операция, которая позволяет получить доступ к файловой системе ряда моделей устройств iPhone, iPod или iPad. В результате появляется возможность расширить возможности аппарата, например, сделать возможным поддержку тем оформления, твиков и установку приложений от сторонних источников (не App Store). Однако после джейлбрейка вы лишаетесь официальной гарантии на iPhone.

Точно так же, для получения PYT-прав в операционной системе Android необходимо в зависимости от устройства выполнить особый алгоритм. Для разных гаджетов - уникальный алгоритм, универсального способа нет. Как и в случае с устройствами Apple, выполнение недокументированной процедуры получения PYT-прав лишает пользователя гарантии на устройство.

Мобильные системы продолжают развиваться. Сегодня они представляют собой одно из магистральных направлений развития современной техники. Мобильные системы занимают в жизни человека все больше места. Но чем шире люди используют мобильные системы, тем больше преступников пытаются использовать мобильность человека в своих целях. Проявляйте разумную осторожность.

### Литература

1 В. Безмалый. Безопасность мобильных устройств. / Windows IT Pro/re, № 1 - 2014

2. Михайлов Д.М., Жуков И.Ю. Под редакцией Ивашко А.М. Защита мобильных телефонов от атак. - М.: Фойлис, 2011. -192 с.: ил.

3. Андрей Косариков, Владимир Лагутин, Алексей Петраков. Утечка и защита информации в телефонных каналах. - М.: РадиоСофт, 2011. - 352 с.: ил.

**Связь с авторами: bearam07@ya.ru**

## ИНФОРМАЦИЯ

Созданием первого смартфона компании Apple занимались две команды, у которых были совершенно разные подходы к тому, какой должна быть iOS. Одни предлагали взять за основу навигацию и управление посредством аналогичного имеющемуся в iPod сенсорного колеса. Вторая предлагала для управления использовать площадь сенсорного дисплея и у каждого пункта меню свои собственные иконки.

У команд не было никакой конкуренции, работали сообща и обменивались идеями. Но секретность была строжайшая. Был даже эпизод, который заставил всех здорово поволноваться, когда прототип iPhone забыли в самолете (секретный гаджет нашли через два часа).

Идея превратить iPod в iPhone была ответом на то, что все мировые производители в тот момент пытались вставить компьютер в телефон. Сенсорное колесо для управления системой должно было быть виртуальным и исчезать при просмотре роликов. Таким образом, шутка Джобса про iPhone в виде iPod с дисковым номеронабирателем была недалека от истины. Всего рассматривали 17 разных концептов. В одном из вариантов предлагалось сделать набор номера, как в Nokia 3650 (см. фото), то есть разместить цифры по всему диску. Существовало понимание того, что это пустая трата времени, однако было потрачено несколько месяцев на внедрение сенсорного круга в систему. Все предлагаемые решения никого не устраивали, и надежда на то, что удастся воплотить эту идею в жизнь, тихо умерла...