программном уровне, но и на уровне железа. Иными словами, нет гарантий, что ваш смартфон надежно защищен от прослушки и съёма информации. Именно поэтому, мы должны понимать, что даже российский смартфон не всегда является безопасным решением, так как его начинка произведена на заводах в Китае. Он может быть неуязвим на программном уровне, но это не даёт гарантий в его комплектующих. Из этого следует, что применять смартфоны в области науки, военной отрасли и иных важных отраслей не всегда целесообразно, ведь смартфон может нас подвести и мы можем потерять информацию.

Необходимо отметить, что смартфон всё чаще и чаще используется в различных структурах, как вспомогательное устройство, именно поэтому безопасности ваших данных на смартфоне нужно уделять внимание. Если организация занимается секретными разработками, то для неё не должно быть понятия корпоративный мобильный телефон или личный мобильный телефон, так как вся информация, циркулируемая в организации, должна передаваться только по защищенным от утечки каналам. Говоря об обычных пользователях мобильных телефонов стоит учитывать тот факт, что возможны хищения паролей, аккаунтов и карт, и сам пользователь лично обеспечивает безопасность своих данных.

Несмотря на ту пользу, которую нам приносят смартфоны, они в себе таят и угрозы, поэтому к выбору и использованию смартфонов стоит подходить тщательно и щепетильно. Некоторые рекомендации по выбору смартфона:

1) При выборе смартфона стоит покупать прежде всего новый, никем не используемый ранее;

2) Стоит ориентироваться на известные, зарекомендовавшие себя бренды, да стоимость телефона будет дороже, но и надежность выше, так как крупные компании, как правило, дорожат своей репутацией;

3) Внимание стоит обращать на модели под управлением ОС Android,Windowsили IOS, эти операционные системы показали весьма неплохую защиту, хотя и имеют уязвимости и подвержены вирусам;

4) Читайте и смотри обзоры телефона в интернете;

5) Внимательно относитесь к прошивке телефона, старайтесь чтобы это была официальная прошивка. Бывает, что для некоторых телефонов прошивку создают сами пользователи, такая прошивка может быть в чем-то удобнее и лучше, но как правило, она более уязвима.

Соблюдая данные рекомендации можно выбрать относительно безопасный смартфон для личного использования.

Список использованной литературы:

1. ВЕДОМОСТИ [Электронный ресурс] Режим доступа: http://www.vedomosti.ru/technology/articles/2017/01/13/672938-rossiiskii-rinok-smartfonov (Дата обращения: 13.03.2017)

2. К вопросу о защите персональных данных в сети интернет / Хлестова Д.Р., Попов К.Г. Символ науки. 2016. № 5-2 (17). С. 108-109.

УДК 004

Казыханов Артем Азаматович
Студент 3 курса ИУБП БашГУ, г. Уфа, РФ
E-mail: archi-uzumaki@mail.ru
Редников Дмитрий Валерьевич
ст.преп. кафедры Экономики и менеджмента БашГУ, г. Уфа, РФ
E-mail: dvr2005@mail.ru

УЯЗВИМОСТИ ANDROID - РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА СМАРТФОНЕ

Аннотация

Данная статья представляет собой исследование уязвимостей ОС ANDROID, а также анализ уровня

обеспечения безопасности информации на самой популярной платформе для сегодняшних смартфонов. В процессе написания статьи будут сформированы рекомендации для обеспечения надежной работы данной ОС, а также исключения возможности "поймать" вирус.

Ключевые слова

ОС, платформа, android, ИБ, рекомендации по использованию

Говоря о телефонах, мы уже подразумеваем смартфоны, и по большей части, эти девайсы находятся под управлением ОС Android. Данная ОС была выпущена в свет в 2008 году. Быстро и стремительно развиваясь, ОС Android смогла захватить лидирующие позиции на рынке операционных систем для телефонов, и даже мобильная версия всем известной Windows на сегодняшний день уступает ей. Однако, видя такую популярность, злоумышленники решили воспользоваться этим и появились первые вирусы для Android, чем популярнее становилась система, тем большее количество злоумышленников старалось создать вредоносные программы.

Ниже в таблице 1 на основе анализа можно увидеть развитие ОС и этапы становление уязвимостей у неё:

Версия Android	Название	Наличие уязвимостей
1.0	«Release 1»	Вредноносные программы отсутствуют, программные уязвимости существуют, оболочка достаточно кривая, но для того времени это выглядит "хорошим" решением
1.1	«Release 1.1»	Вирусы, как класс отсутствуют, существуют лишь программные уязвимости. Исправлено много ошибок по сравнению с 1.0
1.5	«Cupcake»	Аналогично 1.1, изменяются лишь возможности ОС
1.6	«Donut»	Аналогично 1.1, изменяются лишь возможности ОС
2.0	«Eclair»	В связи с появлением больших возможностей появляются программные баги, которые являются уязвимостью
2.2	«Froyo»	Появляются первые вредоносные программы, нацеленные на уничтожение данных
2.3	«Gingerbread»	Никаких изменений
3.0	«Honeycomb»	Присутствуют и вирусы и программные уязвимости
4.0	«Ice Cream Sandwich»	Присутствуют и вирусы и программные уязвимости
4.1	«Jelly Bean»	Присутствуют и вирусы и программные уязвимости
4.2	«Jelly Bean»	Присутствуют и вирусы и программные уязвимости
4.4	«KitKat	Присутствуют и вирусы и программные уязвимости
5.0	«Lollipop»	Количество багов значительно снижено, однако количество созданных вредоносных программ увеличивается очень быстро
-	Android M	Баги убраны, как таковые, вредоносное ПО почти отсутсвует
6.0	Marshmallow	Программные уязвимости есть, возможность их использовать у злоумышленников в основном при помощи социальной инженерии
-	Android N	Среда с повышенным уровнем безопасности
7.0	Nougat	Новинка рынка, сложно оценить уязвимости, но вирусы всё также существуют и в огромном количестве, однако заражать могут, только если пользователь сам "попался".

Анализируя данную таблицу, мы понимаем, что ОС Android по меркам информационной безопасности не является надежным, т.к. распространён массово и, соответственно, подвержен атакам многих злоумышленников.

Однако если выполнять основные рекомендации, то можно смело пользоваться смартфоном и не бояться за сохранность данных на смартфоне.

Итак, рекомендации:

- Не передавать свой смартфон третьим лицам;
- Устанавливать приложения только из доверенных лаунчеров (Play market);
- Использовать Антивирусное ПО;
- Соблюдать политику противодействия социальной инженерии

Список использованной литературы:

1. ВикипедиЯ [Электронный ресурс] Режим доступа: https://ru.wikipedia.org/wiki/Android (Дата обращения: 15.03.2017)

2. К вопросу о защите персональных данных в сети интернет / Хлестова Д.Р., Попов К.Г. Символ науки. 2016. № 5-2 (17). С. 108-109.

УДК 004

Казыханов Артем Азаматович
Студент 3 курса ИУБП БашГУ, г. Уфа, РФ
E-mail: archi-uzumaki@mail.ru
Редников Дмитрий Валерьевич
ст.преп. кафедры Экономики и менеджмента БашГУ, г. Уфа, РФ
E-mail: dvr2005@mail.ru

РАЗВИТИЕ РЫНКА ПРОГРАММНО-АППАРАТНЫХ РЕШЕНИЙ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация

В статье поднимается вопрос развития рынка программно-аппаратных решений для защиты информации, увеличение количества компаний-разработчиков ПО для защиты информации. Также, в процессе изучения вопроса будут указаны причины развития данного рынка и возможные позитивные факторы в результате развития. Рынок программно-аппаратных решений представляет собой конкуренцию между зарубежными и отечественными компаниями, занимающимися разработкой полезного ПО, которое позволит обеспечить безопасности информации. Прежде всего, данные решения направлены для защиты информации первой важности – государственная тайна, коммерческая тайна.

Ключевые слова

Информационная безопасность, программно-аппаратные решения, государственная тайна, коммерческая тайна

Для отраслей первой важности, таких как военная и научная самым главным является безопасность информации. Ведь сегодня, владея информацией, можно получать колоссальную выгоду, либо приносить колоссальный убыток. С 2000 годов принципиальный подход к обеспечению безопасности информации начал меняться, стали использоваться современные технологии, однако, в след за этим и злоумышленники стали использовать более изощренные способы похищения или уничтожения информации. Началась гонка «информационной безопасности» - со стороны защитников информации требовалось не только обеспечения сохранности данных, но и возможность доступа к ним у сотрудников в приемлемый промежуток времени.

Во время процесса компьютеризации сначала зачастую использовались либо программные решения, либо аппаратные решения для обеспечения должного уровня безопасности информации. Несколько позже стали использоваться комплексные решения, которые были нацелены на обеспечения более высокого уровня ИБ.

Поясним, программное решение обеспечения безопасности информации – это та или иная программа, которая представляет собой эффективное средство для защиты информации, осуществляя свою деятельность только на программном уровне, не требует установки дополнительной периферии к компьютеру. Аппаратное решение обеспечения безопасности информации – модуль или устройство, которое защищает информацию на физическом уровне, ограничивая возможности управления компьютером не программно, а аппаратно. Программно-аппаратное решение - это комбинация двух основных составляющих для обеспечения информационной безопасности, является наиболее эффективным так, как защищает информацию на физическом и программном уровне.