Review the secure operating system for smartphones
Kashin N.

Обзор защищённой операционной системы для смартфонов
Кашин Н. А.

Кашин Николай Александрович / Kashin Nikolay – студент,
кафедра информационной безопасности,
Институт кибернетики,
Федеральное государственное бюджетное образовательное учреждение высшего образования
Московский технологический университет, г. Москва

Аннотация: *в статье рассматривается вопрос безопасности мобильных операционных систем. Уровень защиты новой операционной системы Samsung Tizen 2.x., какие средства позволят его повысить.*
Abstract: *the article discusses the security of mobile operating systems. The level of protection of the new operating system Samsung Tizen 2.x., which means allow it to increase.*

Ключевые слова: *смартфон, операционная система, безопасность, сертификат соответствия.*
Keywords: *smart phone operating system, security, certificate of conformity.*

Мобильные устройства, такие как планшеты и смартфоны, стали неотъемлемым атрибутом нашей повседневной жизни. Мы стали их использовать не только как средства связи, но и доверили им хранение личных данных таких как: фото и видео, непредназначенные для широкой общественности, пароли от различных аккаунтов и личных кабинетов, паспортные и банковские данные, истории переписок и другую информацию, которой мы дорожим и боимся забыть или потерять. Но помимо утери важной для нас информации есть ещё и другая угроза – её кража. В прессе часто появляются статьи, в которых говорится о вредоносном программном обеспечении (ПО), похищающем банковские и личные данные со смартфонов, как злоумышленники могут проникнуть в ваше мобильное устройство, воспользовавшись уязвимостями его операционной системы (ОС), и, взяв под контроль управление гаджетом, совершать транзакции с вашей банковской карты (если телефон к ней привязан) без вашего ведома, а также атакующие могут воспользоваться вашими личными данными, полученными в результате атаки, для шантажа, вымогательства или других преступных действий. Чтобы уменьшить урон от подобного рода преступлений, вам поможет соблюдение следующих рекомендаций:

- не хранить пароли в смартфоне,
- шифровать данные, хранящиеся на устройстве,
- не посещать сайты, которые вызывают у вас подозрение,
- скачивать данные только из проверенных источников,
- пользоваться антивирусом,
- не пользоваться wi-fi соединением общего доступа.

Но даже соблюдение всех этих мер предосторожностей не даёт нам 100% защиты от киберпреступников. Остаются еще уязвимости самой ОС. И вопрос безопасности является очень важным для всех создателей мобильных операционных систем.

Недавно компания Samsung выпустила смартфон под управлением собственной операционной системы Tizen. Уровень защищенности своей новой ОС Tizen Южнокорейский производитель подтвердил, получив сертификат соответствия Федеральной службы по техническому и экспертному контролю (ФСТЭК России). Этот сертификат (№ 3441) выданный ОС Samsung Tizen 2.x удостоверят, что ОС Samsung Tizen 2.x соответствует требованиям по 4 уровню контроля отсутствия недекларированных возможностей (НДВ) и наличие встроенных средств защиты от несанкционированного доступа (НСД) к информации [1].

Руководящий документ, по которому был выдан сертификат соответствия (Приказ председателя Гостехкомиссии России от 4 июня 1999 г. № 114), устанавливает классификацию программного обеспечения (ПО) (как отечественного, так и импортного производства) средств защиты информации (СЗИ), в том числе и встроенных в общесистемное и прикладное ПО, по уровню контроля отсутствия в нем недекларированных возможностей. Также в этом документе сказано, что действие документа не распространяется на программное обеспечение средств криптографической защиты информации. В нём установлены четыре уровня контроля отсутствия НДВ. Самый высокий уровень контроля - первый, достаточен для ПО, используемого при защите информации с грифом «особой важности (ОВ)». Второй уровень контроля достаточен для ПО, используемого при защите информации с грифом « совершенно секретно (СС)». Третий уровень контроля достаточен для ПО, используемого при защите информации с

грифом «секретно (С)». Самый низкий уровень контроля - четвертый, достаточен для ПО, используемого при защите конфиденциальной информации [2, с. 1].

В таблице 1 наглядно представлены требования, предъявляемые к каждому из уровней контроля.

Таблица 1. Предъявляемые требования к уровням контроля

№	Наименование требования	Уровень контроля			
		4	3	2	1
	Требования к документации				
1.	Контроль состава и содержания документации				
1.1.	Спецификация (ГОСТ 19.202-78)	+	=	=	=
1.2.	Описание программы (ГОСТ 19.402-78)	+	=	=	=
1.3.	Описание применения (ГОСТ 19.502-78)	+	=	=	=
1.4.	Пояснительная записка (ГОСТ 19.404-79)	-	+	=	=
1.5.	Тексты программ, входящих в состав ПО (ГОСТ 19.401-78)	+	=	=	=
	Требования к содержанию испытаний				
2.	Контроль исходного состояния ПО	+	=	=	=
3.	Статический анализ исходных текстов программ				
3.1.	Контроль полноты и отсутствия избыточности исходных текстов	+	+	+	=
3.2.	Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду	+	=	=	+
3.3.	Контроль связей функциональных объектов по управлению	-	+	=	=
3.4.	Контроль связей функциональных объектов по информации	-	+	=	=
3.5.	Контроль информационных объектов	-	+	=	=
3.6.	Контроль наличия заданных конструкций в исходных текстах	-	-	+	+
3.7.	Формирование перечня маршрутов выполнения функциональных объектов	-	+	+	=
3.8.	Анализ критических маршрутов выполнения функциональных объектов	-	-	+	=
3.9.	Анализ алгоритма работы функциональных объектов на основе блок-схем, диаграмм и т. п., построенных по исходным текстам контролируемого ПО	-	-	+	=
4.	Динамический анализ исходных текстов программ				
4.1.	Контроль выполнения функциональных объектов	-	+	+	=
4.2.	Сопоставление фактических маршрутов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа	-	+	+	=
5.	Отчетность	+	+	+	+

Обозначения: "-" - нет требований к данному уровню;"+" - новые или дополнительные требования;"=" - требования совпадают с требованиями предыдущего уровня [2, с. 2].

Более детально рассмотрим требования к четвертому уровню контроля.

Контроль состава и содержания документации. В состав документации, представляемой заявителем, должны входить:

- Спецификация (ГОСТ 19.202-78), содержащая сведения о составе ПО и документации на него;
- Описание программы (ГОСТ 19.402-78), содержащее основные сведения о составе (с указанием контрольных сумм файлов, входящих в состав ПО), логической структуре и среде функционирования ПО, а также описание методов, приемов и правил эксплуатации средств технологического оснащения при создании ПО;
- Описание применения (ГОСТ 19.502-78), содержащее сведения о назначении ПО, области применения, применяемых методах, классе решаемых задач, ограничениях при применении, минимальной конфигурации технических средств, среде функционирования и порядке работы.
- Исходные тексты программ (ГОСТ 19.401-78), входящих в состав ПО.

Для ПО импортного производства состав документации может отличаться от требуемого, однако содержание должно соответствовать требованиям указанных ГОСТ.

Контроль исходного состояния заключается в фиксации исходного состояния ПО и сравнении полученных результатов с приведенными в документации. Результатами контроля исходного состояния ПО должны быть рассчитанные уникальные значения контрольных сумм загрузочных модулей и исходных текстов программ, входящих в состав ПО. Контрольные суммы должны рассчитываться для каждого файла, входящего в состав ПО.

Статический анализ исходных текстов программ должен включать следующие технологические операции:

- контроль полноты и отсутствия избыточности исходных текстов ПО на уровне файлов;
- контроль соответствия исходных текстов ПО его объектному (загрузочному) коду.

По окончании испытаний оформляется отчет (протокол), содержащий результаты:

- контроля исходного состояния ПО;
- контроля полноты и отсутствия избыточности исходных текстов контролируемого ПО на уровне файлов;
- контроля соответствия исходных текстов ПО его объектному (загрузочному) коду.

Таким образом, можно сделать вывод, что ОС Samsung Tizen 2.x соответствует минимальным требованиям безопасности, предъявляемым в данном руководящем документе ФСТЭК России. Однако отсутствие закладок и НДВ не гарантирует отсутствие уязвимостей ОС.

Для повышения уровня безопасности встраивание в систему криптографических средств защиты информации (СКЗИ). И для подтверждения корректности и качества реализации встроенных СКЗИ, необходимо пройти сертификацию в Федеральной службе безопасности (ФСБ России), которая установила свою шкалу классов защиты. На данный момент есть 6 классов СКЗИ: КС1, КС2, КС3, КВ1, КВ2, КА1.

Литература

1. ООО «НИИ СОКБ». [Электронный ресурс]: официальный сайт компании. Компания «НИИ СОКБ» сообщает об успешном завершении сертификации во ФСТЭК России операционной системы Samsung Tizen 2.x. URL: http://safe-phone.ru/kompaniya-nii-sokb-soobshhaet-ob-uspeshnom-zavershenii-sertifikatsii-vo-fstek-rossii-operatsionnoj-sistemy-samsung-tizen-2-x (дата обращения: 20.08.2016).
2. Приказ председателя Гостехкомиссии России от 4 июня 1999 г. № 114. 9 с.