ПОДХОД К СЕРТИФИКАЦИИ МОБИЛЬНЫХ УСТРОЙСТВ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Горюнов М.Н.[1], Ершов А.Л.[2], Поляков С.А.[3]

Цель статьи: *разработка предложений по обеспечению доверия к безопасности функционирования мобильных устройств.*

Метод: *комплексный теоретико-прикладной анализ существующих нормативных документов в области обеспечения безопасности информации и результатов экспериментов по функционированию firmware мобильных устройств.*

Результаты: *проанализированы аппаратно-программные особенности мобильных устройств, выявлены важные аспекты их функционирования, существенно влияющие на безопасность обрабатываемой информации. Установлено, что программный код большинства модулей firmware является более привилегированным, чем код операционной системы, что обусловливает возможность его деструктивного воздействия на функционирование операционной системы в течение всего времени работы мобильного устройства. Приведены результаты оценки возможности сертификации мобильных устройств по требованиям безопасности информации, позволяющие сделать вывод об ограниченности существующей нормативной базы в данной области. Предложен подход, при котором в качестве объекта оценки рассматривается мобильное устройство как совокупность аппаратной платформы, операционной системы и firmware, а сертификация проводится на соответствие «Требованиям безопасности информации к операционным системам», дополненным функциональными требованиями безопасности к firmware мобильного устройства. Данные требования разработаны основе методологии ГОСТ ИСО/МЭК 15408 и направлены на обеспечение безопасного функционирования операционной системы устройства.*

Ключевые слова: *встроенное программное обеспечение (firmware), операционная система, доверенная загрузка, защита от отключения и обхода функций безопасности, общие критерии.*

DOI: *10.21681/2311-3456-2019-2-29-35*

Введение

Мобильные устройства являются неотъемлемой частью современного мира. Люди привыкли к высокому уровню коммуникаций и повсеместному и ежечасному доступу к необходимой информации. На сегодняшний день практически каждый человек владеет тем или иным личным мобильным устройством. Не являются исключением и сотрудники государственных структур, которым использование мобильных устройств позволяет значительно повысить оперативность принятия решений по различным служебным вопросам. Кроме того, данные устройства широко применяются и во множестве технологических процессов на производстве. Все это обусловливает повышенный интерес к ним и злоумышленников.

Проблемы безопасности, связанные с использованием мобильных устройств, были наглядно продемонстрированы имеющимися в открытых источниках данных о «прослушке» спецслужбами США телефонных переговоров первых лиц некоторых государств и международных организаций, об утечках конфиденциальных данных пользователей смартфонов, заражении их вирусами, об уязвимостях встроенного программного обеспечения мобильных устройств и т. д.

Таким образом, на сегодняшний день является актуальной проблема обеспечения безопасности информации при ее обработке в мобильных устройствах. Ее решение может заключаться в проведении сертификации таких устройств или отдельных их компонентов по требованиям безопасности информации.

Анализ мобильного устройства как объекта оценки

Мобильное устройство представляет собой сложное программно-техническое изделие. Условно его можно разделить на аппаратную и программную составляющие.

Аппаратная составляющая мобильного устройства обычно представляет собой совокупность специализированных однокристальных систем (SoC), микроконтроллеров, сигнальных (DSP) и др. процессоров, различного рода подсистем периферийных устройств (экрана, аудио, сенсоров и т. д.) и других модулей, необходимых для выполнения мобильным устройством своих функций (рис. 1).

Программное обеспечение мобильного устройства можно разделить на две основные составляющие: операционная система (ОС) и встроенное проприетарное программное обеспечение аппаратной платформы (далее – firmware).

В большинстве мобильных устройств выполнение кода программного обеспечения разделяется между двумя основными процессорами, реализованными в виде SoC: «application-процессор» и «baseband-

1 Горюнов Максим Николаевич, кандидат технических наук, сотрудник Академии ФСО России, г. Орёл, Россия. E-mail: max.gor@mail.ru.

2 Ершов Алексей Леонидович, кандидат технических наук, сотрудник Академии ФСО России, г. Орёл, Россия. E-mail: al.er@rambler.ru.

3 Поляков Сергей Александрович, кандидат технических наук, сотрудник Академии ФСО России, г. Орёл, Россия. E-mail: polyakovsergey@yandex.ru.

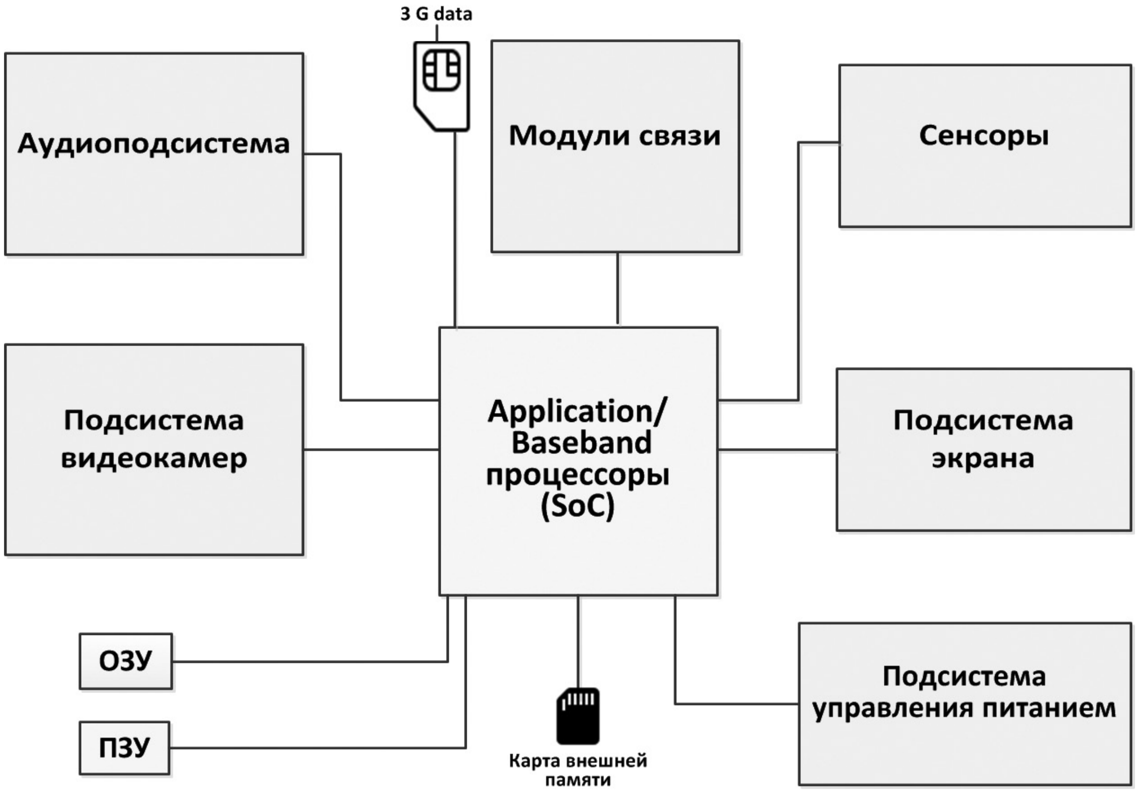

Рис. 1. Аппаратная составляющая мобильного устройства

процессор». При этом в SoC мобильных устройств возможна реализация дополнительных сопроцессоров.

Необходимо отметить, что программный код firmware в зависимости от назначения конкретного модуля может выполняться на разных процессорах и сопроцессорах. Вместе с тем в современных мобильных устройствах реализуются следующие принципы:

- программный код операционной системы и приложений пользователя выполняется на процессоре приложений («application-процессоре»), который обычно является составной частью SoC, интегрирующего в себе ядра графических процессоров и (или) ядра процессоров общего назначения, а также микроконтроллеры интерфейсов энергонезависимой памяти и т. д;

- программный код, отвечающий за обработку аудио-, фото- и видеоинформации, и ее передачу (прием) по различным беспроводным интерфейсам, выполняется на «baseband-процессоре», является составной частью SoC, интегрирующего в одном корпусе несколько вычислительных ядер процессоров общего назначения вместе с ядрами DSP-процессоров.

Анализ процесса инициализации мобильных устройств показывает, что программный код большинства модулей firmware загружается и исполняется до момента загрузки операционной системы. При этом часть из этих модулей остается в памяти и после ее загрузки [1-5]. Для примера на рис. 2 представлена последовательность загрузки модулей программного обеспечения мобильного устройства на базе SoC семейства Snapdragon компании Qualcomm до момента передачи управления операционной системе.

На рис. 2 использованы следующие сокращения и условные обозначения:

– PBL – первичный загрузчик;
– RPM SBL – вторичный загрузчик процессора RPM;
– RPM FW – модуль управления ресурсами устройства;
– APPS PBL – первичный загрузчик процессора APPS;
– APPS SBL – вторичный загрузчик процессора APPS;
– TrustZone – модуль доверенной среды выполнения;
– ABOOT – загрузчик операционной системы;
– HLOS – операционная система.

Порядок загрузки программных модулей соответствует цифрам на рис. 2. Штриховой линией показаны направления передачи сигналов уведомлений между модулями (например, об окончании его работы, готовности следующего модуля для запуска и т. д.). После загрузки операционной системой она загружает оставшиеся модули firmware (модули подсистем модема, сенсоров и т. д.).

Таким образом, можно сделать вывод о том, что программный код большинства модулей firmware является более привилегированным, чем код операционной системы, так как он выполняется до ее старта и может оставаться в оперативной памяти, что обусловливает возможность его влияния на функционирование ОС в течение всего времени работы мобильного устройства. Кроме того, не исключается возможность того, что выполняемый код модулей firmware может напрямую получить доступ к защищаемым ресурсам мобильного устройства и скомпрометировать механизмы защиты операционной системы мобильного устройства, а также организовать канал утечки информации с использованием беспроводных модулей связи.

Оценка возможности сертификации по требованиям безопасности

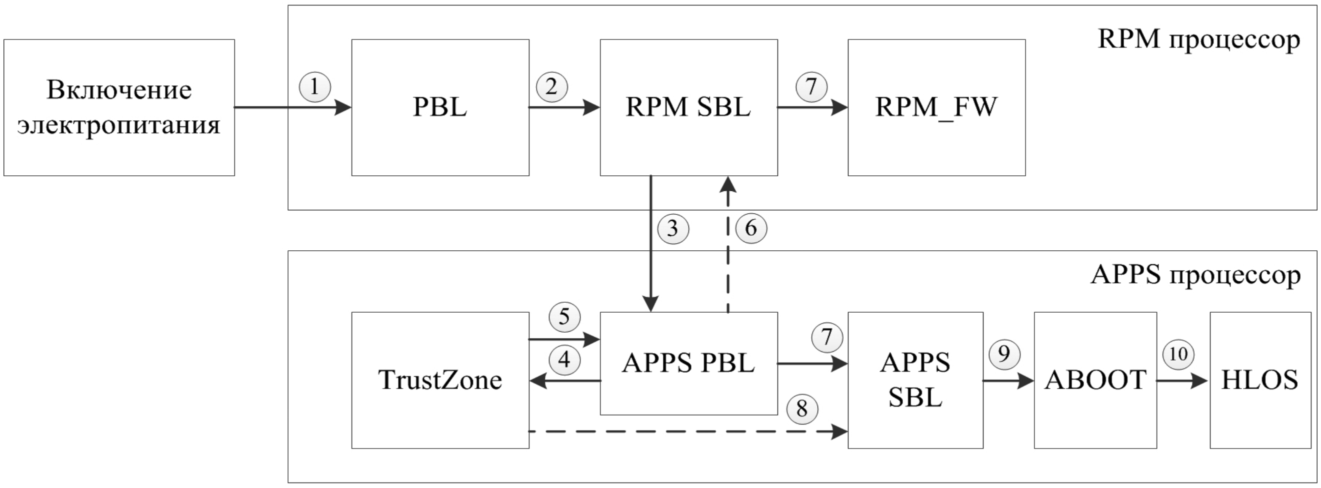

Рис. 2. Схема загрузки программного обеспечения мобильного устройства на базе SoC семейства Snapdragon компании Qualcomm до момента передачи управления операционной системе

Анализ современного опыта показал, что многие иностранные компании производят оценку соответствия своих мобильных устройств на основе методологии «Общих критериев» [6-8]. В настоящее время консорциум производителей разработал соответствующий профиль защиты (Protection Profile for Mobile Device Fundamentals), который является основой для разработки частных заданий по безопасности на мобильные устройства. Однако в нашей стране подобный опыт отсутствует.

Имеющаяся в настоящее время нормативно-методическая база может быть использована только в части проверки соответствия операционной системы мобильного устройства «Требованиям безопасности информации к операционным системам», утвержденным приказом ФСТЭК России № 119 от 19.08.2016 г.

Вместе с тем, сертификация только операционной системы в отрыве от мобильного устройства не позволит в полной мере обеспечить доверие к ней, о чем свидетельствует рассмотренный выше процесс инициализации мобильного устройства (рис. 2). Кроме того, существующие профили защиты определяют ряд целей для среды функционирования, которые должны быть достигнуты для того, чтобы объект оценки (ОО) считался безопасным. По своей сути это ограничения на условия эксплуатации ОО. Среди них есть такие определяющие цели как:

– доверенная загрузка ОС;

– защита от отключения и обхода функций безопасности ОС.

В случае установки ОС на ПЭВМ достижение данных целей может быть обеспечено применением организационно-технических мер защиты и/или использованием аппаратно-программных модулей доверенной загрузки. Однако для мобильных устройств это на сегодняшний день практически нереализуемо, что ставит под сомнение возможность выполнения операционной системой заявленных функций безопасности после установки на мобильное устройство.

Результаты имеющихся в открытых источниках работ отечественных исследователей безопасности мобильных устройств в основном ограничиваются требованиями, предъявляемыми к операционной системе, без учета влияния на ее функционирование программного кода модулей firmware [9-11].

В этой связи при проведении сертификации является целесообразным рассматривать в качестве объекта оценки не операционную систему, а мобильное устройство в комплексе как совокупность аппаратной платформы, операционной системы и firmware. В данном случае, учитывая имеющуюся нормативную базу, сертификация мобильного устройства может быть проведена на соответствие «Требованиям безопасности информации к операционным системам», дополненным специальными требованиями, обусловленными спецификой функционирования мобильных устройств. При этом должны быть учтены такие особенности мобильных устройств, как работа в сетях связи общего пользования, использование беспроводных интерфейсов взаимодействия, ограничение доступа приложений к критичным системным службам, осуществляющим получение текущего местоположения мобильного устройства, получение доступа к микрофонам, видеокамерам, адресной книге, к функциям передачи данных и др.

Предложения по формированию задания по безопасности

Таким образом, при разработке задания по безопасности на мобильное устройство с оцениваемой операционной системой предлагается использовать существующие профили защиты, например, ИТ.ОС.А6.ПЗ «Профиль защиты ОС типа «А» шестого класса защиты». При этом должно быть обеспечено переложение части целей для среды функционирования ОС, изложенных в профиле защиты, на ОО, а конкретнее – на его firmware. В частности, это относится к таким целям как: «Доверенная загрузка ОС» и «Защита от отключения и обхода функций безопасности ОС». При необходимости в ЗБ могут быть включены функциональные требования из «Protection Profile for Mobile Device Fundamentals», а также другие дополнительные требования.

Практика задания требований безопасности к информационным технологиям [12-14] предполагает формулирование в начале функций безопасности ОО, для которых в дальнейшем с использованием ГОСТ ИСО/

Таблица 1.
Функции безопасности и функциональные возможности

Условное обозначение реализуемой функции безопасности	Условное обозначение семейства (функциональной возможности) (В соответствии с ГОСТ ИСО/МЭК 15408-2)	Наименование
ФБ 1	FPT_SDF_EXT	Контроль целостности модулей уровня firmware и предпринимаемые действия
	FPT_TUD_EXT	Безопасное обновление
ФБ 2	FPT_BBD_EXT	Изоляция критических ресурсов

МЭК 15408-2 определяются соответствующие функциональные требования.

Далее в статье рассмотрены только функции безопасности (ФБ) мобильного устройства, касающиеся двух уже упомянутых целей безопасности:

– ФБ 1 – Доверенная загрузка ОС;

– ФБ 2 – Защита от отключения и обхода функций безопасности ОС;

Анализ работ [9-14], а также существующей нормативной базы ФСТЭК России показал целесообразность использования для конкретизации обозначенных функций безопасности функциональных требований безопасности (ФТБ), задаваемых в явном виде. В табл. 1 представлены предлагаемые новые семейства функциональных требований, а их состав и содержание описано ниже.

Контроль целостности модулей уровня firmware и предпринимаемые действия (FPT_SDF_EXT)

FPT_SDF_EXT.1 Контроль целостности модулей уровня firmware и предпринимаемые действия

Иерархический для: Нет подчиненных компонентов.

FPT_SDF_EXT.1.1 Функциональные возможности безопасности firmware должны выполнять контроль целостности [выбор: хранимого, загруженного в оперативную память] исполняемого кода модулей firmware, загрузчика ОС и ядра ОС в следующих случаях [выбор: при загрузке в оперативную память, перед передачей управления загруженному исполняемому коду, [назначение: иные случаи]].

FPT_SDF_EXT.1.2 Функциональные возможности безопасности firmware должны контролировать целостность хранимого исполняемого кода модулей firmware, загрузчика ОС и ядра ОС, основываясь на следующих атрибутах: [выбор: имена (идентификаторы), контрольные суммы, электронная подпись].

FPT_SDF_EXT.1.3 Функциональные возможности безопасности firmware при обнаружении нарушения целостности [выбор: хранимого, загруженного в оперативную память] исполняемого кода модулей firmware, загрузчика ОС и ядра ОС должны обеспечить [выбор: блокировку загрузки, блокировку передачи управления загруженному исполняемому коду, [назначение: иные действия]].

Зависимости: отсутствуют.

Безопасное обновление (FPT_TUD_EXT)

FPT_TUD_EXT.1 Запрос версии компонент ОО

Иерархический для: Нет подчиненных компонентов.

FPT_TUD_EXT.1.1 ФБО должны предоставлять авторизованным пользователям возможность [запрашивать текущую версию firmware и операционной системы].

FPT_TUD_EXT.1.2 ФБО должны предоставлять авторизованным пользователям возможность [запрашивать текущую версию (идентификатор) аппаратной модели устройства].

FPT_TUD_EXT.1.3 ФБО должны предоставлять авторизованным пользователям возможность [запрашивать текущую версию установленных приложений].

Зависимости: отсутствуют.

FPT_TUD_EXT.2 Проверка безопасности обновлений

Иерархический для: Нет подчиненных компонентов.

FPT_TUD_EXT.2.1 ФБО должны проверять [обновления программного обеспечения] с использованием [электронной подписи разработчика] до установки этих обновлений.

Зависимости: отсутствуют.

Изоляция критических ресурсов (FPT_ BBD_ EXT)

FPT_BBD_EXT.1 Защита ресурсов[4] процессора приложений

Иерархический для: Нет подчиненных компонентов.

FPT_BBD_EXT.1.1 Код, исполняемый на процессоре, отличном от процессора приложений, не должен иметь доступа к ресурсам процессора приложений, за исключением случаев, когда доступ к ресурсам инициирован непосредственно процессором приложений.

FPT_BBD_EXT.1.2 Код модулей firmware, исполняемый на процессоре приложений, не должен иметь доступа к его ресурсам после загрузки операционной системы, за исключением случаев, когда доступ к ним инициирован самой операционной системой.

FPT_BBD_EXT.2 Защита загруженного кода операционной системы

Иерархический для: Нет подчиненных компонентов.

FPT_BBD_EXT.2.1 Исполняемый код модулей firmware не должен осуществлять доступ к областям оперативной памяти, в которых размещается код ОС.

Зависимости: отсутствуют.

Представленные функциональные требования формулировались на основе результатов анализа [9-14] и существующей нормативной базы ФСТЭК России (в том числе требований к средствам доверенной загрузки).

В качестве основы функционального требования FPT_SDF_EXT.1 было использовано ФТБ FPT_SDI_EXT.1 из «Требований безопасности информации к операционным системам», как наиболее подходящее для использования с минимальными уточнениями.

За основу функциональных требований FPT_TUD_EXT.1 и FPT_TUD_EXT.2 были использованы одноименные требования из «Protection Profile for Mobile Device Fundamentals». Данные ФТБ направлены на обеспечение контроля идентичности программно-аппаратной среды.

За основу функционального требования FPT_BBD_EXT.1 было использовано одноименное требование из «Protection Profile for Mobile Device Fundamentals», адаптированное под разные аппаратные реализации процессоров мобильного устройства. Данное функциональное требование направлено на обеспечение защиты от обхода механизмов защиты операционной системы и возможных утечек защищаемой информации по беспроводным каналам связи.

Функциональное требование FPT_BBD_EXT.2 направлено на исключение возможности влияния firmware на функции безопасности операционной системы.

Проведенные исследования аппаратно-программной архитектуры и машинного кода мобильных устройств показали реализуемость данных функциональных требований. Вместе с тем, необходимо отметить, что при проведении сертификации мобильных устройств могут возникнуть сложности с предоставлением разработчиками исходных текстов firmware. В этих условиях проведение оценки соответствия может быть осуществлено только на основе использования методов реверс-инжиниринга машинного кода, что является решаемой, но трудоемкой задачей [15-20]. При этом существенно снизить затраты на сертификацию позволило бы внедрение сертификации в жизненный цикл программного обеспечения [21].

Выводы

В работе предложен подход к сертификации мобильных устройств на основе существующей нормативной базы ФСТЭК России. Данный вариант предполагает рассмотрение в качестве объекта оценки мобильного устройства в комплексе как совокупности аппаратной платформы, операционной системы и firmware и проведение оценки на соответствие «Требованиям безопасности информации к операционным системам», дополненным специальными требованиями, обусловленными спецификой мобильных устройств. Предложены функциональные требования к firmware, позволяющие обеспечить доверенную загрузку операционной системы мобильного устройства и невозможность отключения ее функций безопасности. Реализация данных требований позволит повысить защищенность мобильного устройства в целом. Проведенные исследования аппаратно-программной архитектуры и машинного кода мобильных устройств показали практическую реализуемость предлагаемых решений.

Рецензент: *Мацкевич Андрей Георгиевич, кандидат технических наук, доцент, сотрудник Академии ФСО России, mag3d@rambler.ru.*

Литература:

1. Hua, Z., Gu, J., Xia, Y., Chen, H., Zang, B. and Guan, H. vTZ: Virtualizing ARM TrustZone. In USENIX Security Symposium. 2017. pp. 541-556.
2. Machiry, A., Gustafson, E., Spensky, C., Salls, C., Stephens, N., Wang, R., Bianchi, A., Choe, Y.R., Kruegel, C. and Vigna, G. BOOMERANG: Exploiting the Semantic Gap in Trusted Execution Environments. In Proceedings of the 24 Annual Network and Distributed System Security Symposium (NDSS). 2017
3. Pinto, S., Santos, N. Demystifying Arm TrustZone: A Comprehensive Survey. In ACM Computing Surveys. 2019. Vol. 51. No. 6. Article 130.
4. Chen, Y., Zhang, Y., Wang, Z., Wei, T. Downgrade Attack on TrustZone. In arXiv. 2017.
5. Zhang, Y., Chen, Z., Xue, H., Wei, T. Fingerprints On Mobile Devices: Abusing and Leaking. In Black Hat USA. 2015.
6. Барабанов А.В., Марков А.С., Цирлов В.Л. Международная сертификация в области информационной безопасности // Стандарты и качество. 2016. № 7. С. 30-33.
7. Барабанов А.В., Марков А.С., Цирлов В.Л. Оценка соответствия средств защиты информации «Общим Критериям» // Информационные технологии. 2015. Т. 21. № 4. С. 264-270.

4 К ресурсам процессора приложений относится:
– энергозависимая и энергонезависимая память;
– данные от интегрированных и неинтегрированных периферийных устройств (например, USB-контроллеров, контроллеров экрана, кодеков и др.);
– данные от интегрированных и неинтегрированных сенсоров (например, камер, подсветки, микрофона, навигации, акселерометров и др.).

8. Марков А.С., Рауткин Ю.В. Сертификация средств защиты информации по требованиям безопасности информации. Новая парадигма // Информационные и математические технологии в науке и управлении. 2016. № 1. С. 94-102.
9. Фроимсон М.И., Тараканов О.В., Кутепов С.В., Шереметов А.В. Основные принципы построения защищенной операционной системы для мобильных устройств // Спецтехника и связь. 2013. № 1. С. 43-46.
10. Бокова О.И., Михайлов Д.М., Фроимсон М.И. Выработка и анализ требований к защищенной мобильной операционной системе // Вестник ВИ МВД России. 2013. № 4. С. 242-247.
11. Зубков К. Н., Диасамидзе С. В. Проблемы защиты информации в приложениях для мобильных систем // Интеллектуальные технологии на транспорте. 2017. № 2. С. 40-46.
12. Горюнов М.Н., Юдичев Р.М. Оценка и ранжирование функциональных возможностей средств защиты среды виртуализации // Автоматизация и управление в технических системах. 2015. № 1 (13). С. 92-100.
13. Барабанов А.В., Гришин М.И., Марков А.С., Цирлов В.Л. Формирование требований по безопасности информации к DLP-системам // Вопросы радиоэлектроники. 2013. Т. 3. № 2. С. 67-76.
14. Веряев А.С., Фадин А.А. Формализация требований безопасности информации к средствам анализа защищенности // Вопросы кибербезопасности. 2015. № 4 (12). С. 23-27.
15. Поляков С.А., Карасев С.В. Особенности получения информации о ходе выполнения программы (трассы) с использованием аппаратного окружения // Вопросы кибербезопасности. 2016. № 3 (16). С. 40-44.
16. Ершов А.Л. Идентификация алгоритмов преобразования данных в исполняемых модулях программного обеспечения / А. Л. Ершов // Труды СПИИРАН. 2015. №. 41. С. 94-105.
17. Горюнов М.Н., Еременко С.В., Ершов А.Л., Мацкевич А.Г. Моделирование системы обнаружения функциональных объектов программного обеспечения в условиях отсутствия исходных текстов // Научно-технический журнал «Информационные системы и технологии». 2013. № 3 (77). С. 110-117.
18. Довгалюк П.М., Макаров В.А., Падарян В.А., Романеев М.С., Фурсова Н.И.. Применение программных эмуляторов в задачах анализа бинарного кода // Труды Института системного программирования. 2014. Том 26, вып. 1. С. 277-296.
19. Аветисян А.И., Белеванцев А.А., Чукляев И.И. Технологии статического и динамического анализа уязвимостей программного обеспечения // Вопросы кибербезопасности. 2014. № 3 (4). С. 20-28.
20. Мельников П.В., Горюнов М.Н., Анисимов Д.В. Подход к проведению динамического анализа исходных текстов программ // Вопросы кибербезопасности. 2016. № 3 (16). С. 33-39.
21. Горюнов М.Н., Юдичев Р.М., Фадин А.А. Внедрение сертификации в жизненный цикл программного обеспечения // Защита информации. Инсайд. 2016. № 3 (69). С. 28-35.

THE APPROACH TO MOBILE DEVICES SECURITY CERTIFICATION

Goryunov M.N.[5], Ershov A.L.[6], Polyakov C.A.[7]

Objective of the article: *developing proposals to ensure the security of the functioning of mobile devices.*

Method: complex theoretical and applied analysis of existing normative documents in the field of information protection and results of experiments on functioning of mobile device firmware.

Obtained result: *hardware and software features of mobile devices are analyzed, important features of their functioning are revealed, it significantly affects information security. It is established that the program code of most firmware modules is more privileged than the code of the operating system. This leads to the possibility of its destructive impact on the functioning of the operating system during the entire operation time of the mobile device. Results of evaluation of a possibility of mobile device certification on information security requirements are given. It allows to draw a conclusion on narrowness of the existing legal base in the field. An approach is proposed in which a mobile device is considered as a combination of a hardware, operating system and firmware. In this case, certification is carried out for compliance with the "Information Security Requirements for Operating Systems", supplemented by functional security requirements for the firmware of a mobile device. These requirements are based on the GOST ISO / IEC 15408 methodology and are aimed at ensuring the safe functioning of the device's operating system.*

Keywords: *embedded software (firmware), operating system, trusted boot, shutdown and safety function bypass protection, Common Criteria.*

References

1. Hua, Z., Gu, J., Xia, Y., Chen, H., Zang, B. and Guan, H. vTZ: Virtualizing ARM TrustZone. In USENIX Security Symposium. 2017. pp. 541-556.
2. Machiry, A., Gustafson, E., Spensky, C., Salls, C., Stephens, N., Wang, R., Bianchi, A., Choe, Y.R., Kruegel, C. and Vigna, G. BOOMERANG: Exploiting the Semantic Gap in Trusted Execution Environments. In Proceedings of the 24 Annual Network and Distributed System Security Symposium (NDSS). 2017
3. Pinto, S., Santos, N. Demystifying Arm TrustZone: A Comprehensive Survey. In ACM Computing Surveys. 2019. Vol. 51. No. 6. Article 130.

5 Maksim Goryunov, Ph.D, Employee at the Academy of the Federal Guard Service of the Russian Federation, Orel, Russia. E-mail: max.gor@mail.ru.

6 Aleksey Ershov, Ph.D, Employee at the Academy of the Federal Guard Service of the Russian Federation, Orel, Russia. E-mail: al.er@rambler.ru.

7 Sergey Polyakov, Ph.D, Employee at the Academy of the Federal Guard Service of the Russian Federation, Orel, Russia. E-mail: polyakovsergey@yandex.ru.

4. Chen, Y., Zhang, Y., Wang, Z., Wei, T. Downgrade Attack on TrustZone. In arXiv. 2017.
5. Zhang, Y., Chen, Z., Xue, H., Wei, T. Fingerprints On Mobile Devices: Abusing and Leaking. In Black Hat USA. 2015.
6. Barabanov A.V., Markov A.S., Cirlov V.L. Mezhdunarodnaya sertifikaciya v oblasti informacionnoj bezopasnosti // Standarty i kachestvo. 2016. № 7. S. 30-33.
7. Barabanov A.V., Markov A.S., Cirlov V.L. Ocenka sootvetstviya sredstv zashchity informacii «Obshchim Kriteriyam» // Informacionnye tekhnologii. 2015. T. 21. № 4. S. 264-270.
8. Markov A.S., Rautkin YU.V. Sertifikaciya sredstv zashchity informacii po trebovaniyam bezopasnosti informacii. Novaya paradigma // Informacionnye i matematicheskie tekhnologii v nauke i upravlenii. 2016. № 1. S. 94-102.
9. Froimson M.I., Tarakanov O.V., Kutepov S.V., SHeremetov A.V. Osnovnye principy postroeniya zashchishchennoj operacionnoj sistemy dlya mobil'nyh ustrojstv // Spectekhnika i svyaz'. 2013. № 1. S. 43-46.
10. Bokova O.I., Mihajlov D.M., Froimson M.I. Vyrabotka i analiz trebovanij k zashchishchennoj mobil'noj operacionnoj sisteme // Vestnik VI MVD Rossii. 2013. № 4. S. 242-247.
11. Zubkov K. N., Diasamidze S. V. Problemy zashchity informacii v prilozheniyah dlya mobil'nyh sistem // Intellektual'nye tekhnologii na transporte. 2017. № 2. S. 40-46.
12. Goryunov M.N., YUdichev R.M. Ocenka i ranzhirovanie funkcional'nyh vozmozhnostej sredstv zashchity sredy virtualizacii // Avtomatizaciya i upravlenie v tekhnicheskih sistemah. 2015. № 1 (13). S. 92-100.
13. Barabanov A.V., Grishin M.I., Markov A.S., Cirlov V.L. Formirovanie trebovanij po bezopasnosti informacii k DLP-sistemam // Voprosy radioelektroniki. 2013. T. 3. № 2. S. 67-76.
14. Veryaev A.S., Fadin A.A. Formalizaciya trebovanij bezopasnosti informacii k sredstvam analiza zashchishchennosti // Voprosy kiberbezopasnosti. 2015. № 4 (12). S. 23-27.
15. Polyakov S.A., Karasev S.V. Osobennosti polucheniya informacii o hode vypolneniya programmy (trassy) s ispol'zovaniem apparatnogo okruzheniya // Voprosy kiberbezopasnosti. 2016. № 3 (16). S. 40-44.
16. Ershov A.L. Identifikaciya algoritmov preobrazovaniya dannyh v ispolnyaemyh modulyah programmnogo obespecheniya / A. L. Ershov // Trudy SPIIRAN. 2015. №. 41. C. 94-105.
17. Goryunov M.N., Eremenko S.V., Ershov A.L., Mackevich A.G. Modelirovanie sistemy obnaruzheniya funkcional'nyh ob»ektov programmnogo obespecheniya v usloviyah otsutstviya iskhodnyh tekstov // Nauchno-tekhnicheskij zhurnal «Informacionnye sistemy i tekhnologii». 2013. № 3 (77). S. 110-117.
18. Dovgalyuk P.M., Makarov V.A., Padaryan V.A., Romaneev M.S., Fursova N.I.. Primenenie programmnyh emulyatorov v zadachah analiza binarnogo koda // Trudy Instituta sistemnogo programmirovaniya. 2014. Tom 26, vyp. 1. C. 277-296.
19. Avetisyan A.I., Belevancev A.A., CHuklyaev I.I. Tekhnologii staticheskogo i dinamicheskogo analiza uyazvimostej programmnogo obespecheniya // Voprosy kiberbezopasnosti. 2014. № 3 (4). S. 20-28.
20. Mel'nikov P.V., Goryunov M.N., Anisimov D.V. Podhod k provedeniyu dinamicheskogo analiza iskhodnyh tekstov programm // Voprosy kiberbezopasnosti. 2016. № 3 (16). S. 33-39.
21. Goryunov M.N., Yudichev R.M., Fadin A.A. Vnedrenie sertifikacii v zhiznennyj cikl programmnogo obespecheniya // Zashchita informacii. Insajd. 2016. № 3 (69). S. 28-35.