УДК 681.3

А.Р. Биричевский

УНИВЕРСАЛЬНАЯ МОБИЛЬНАЯ ОПЕРАЦИОННАЯ СИСТЕМА С ПОДСИСТЕМАМИ АУТЕНТИФИКАЦИИ И ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ПСЕВДОВЕРОЯТНОСТНОГО ПРЕОБРАЗОВАНИЯ

Биричевский А.Р. **Универсальная мобильная операционная система с подсистемами аутентификации и защиты информации на основе псевдовероятностного преобразования.**

Аннотация. Данная статья посвящена архитектуре универсальной мобильной операционной системе. В работе описаны основные подсистемы разработанной операционной системы, структура системы защиты операционной системы. Отличительной особенностью разработанной операционной системы является интеграция псевдовероятностных преобразований в модули защиты информации.

Ключевые слова: псевдовероятностное преобразование, операционная система, аутентификация, криптовровайдер, виртуальная среда.

Birichevskij A.R. **Universal Mobile Operating System Including Subsystems of Authentication and Data Protection Based on the Pseudo-Probability Transformation.**

Abstract. This article focuses on the architecture of a universal mobile operating system. The paper describes the main subsystems of the developed operating system and the structure of the operating system protection. A distinctive feature of the developed operating system is the integration of pseudo-probability transformations into information protection modules.

Keywords: pseudo-probability transformation; the operating system; authentication; cryptographic; virtual environment.

1. Введение. На сегодняшний день разработано очень большое количество операционных систем. Операционная система представляет собой прекрасный механизм экономичного использования ресурсов. Операционные системы успешно применяются и в средствах защиты информации различных типов.

При разработке средств защиты информации производители нередко используют схожую элементную базу. Например, средство защиты программных продуктов Guardant Stealth II [1] и персональные идентификаторы Рутокен ЭЦП [2] реализованы на базе микроконтроллера общего назначения (Guardant Stealth II имеет процессор тактовой частотой 60 МГц, 32 разряда, архитектура ARM) с интерфейсом USB и энергонезависимой памяти. Чуть более сложную структуру имеют средства защиты от НСД производства ОКБ САПР [3]. Аккорд-5МХ реализован на базе микроконтроллера общего назначения (тактовая частота 16 МГц, архитектура RISC, 8 разрядов) и контроллера программируемой логики. Как можно видеть, все представленные средства защиты имеют в своем составе микроконтроллер общего назначе-

ния. Стоит отметить, что применяемые микроконтроллеры имеют сравнительно невысокие вычислительные возможности.

В данной работе под мобильными устройствами понимается устройство, реализованное на однокристальном микроконтроллере и имеющее низкие вычислительные мощности (тактовая частота до 200 МГц, оперативная и постоянная память до десятков мегабайт). В данный класс устройств попадает большое количество средств защиты информации:

– персональные идентификаторы (USB-токены);

– средства защиты программных продуктов (USB-ключи);

– смарт-карты;

– средства защиты информации от несанкционированного доступа.

Сравнительно невысокая производительность аппаратной платформы не позволяет применять достаточно сложные операционные системы. Существующие защищенные операционные системы для мобильных систем (например, операционная система MULTOS [4]) часто привязаны к конкретной аппаратной платформе (в данном случае аппаратная платформа — специализированный контроллер для смарт-карт). Данная особенность сильно ограничивает область применения операционной системы. Применение универсальной операционной системы в системах защиты информации позволит унифицировать подходы к обеспечению безопасности при разработке систем защиты информации, что может значительно снизить затраты при разработке средств защиты информации и, соответственно, сделает такие продукты более конкурентоспособными.

В данной работе будет рассмотрена структура универсальной операционной системы, которая может быть использована в мобильных системах различного назначения.

Отличительной особенностью разработанной операционной системы является интеграция псевдовероятностных преобразований в модули защиты информации. Под понятием псевдовероятностного преобразования понимается способ криптографического преобразования, в котором зашифровываются совместно два или более различных сообщений на двух или более различных ключах [5]. Псевдовероятностное преобразование позволяет обеспечить высокий уровень защищенности от атаки с принуждением.

2. Архитектура операционной системы. На рисунке 1 представлена архитектура разработанной операционной системы. В качестве целевой аппаратной платформы была выбрана архитектура контроллеров

ARM. Данная архитектура широко распространена в современных мобильных устройствах и имеет большое количество модификаций.

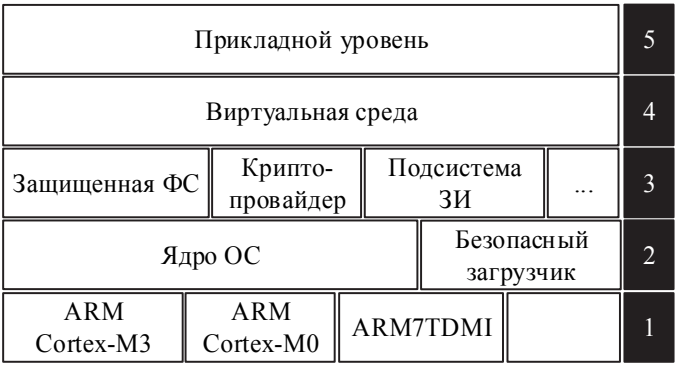

Рис. 1. Архитектура операционной системы

Операционная система организована по классической архитектуре типа «микроядро»[6]. Данная архитектура была выбрана по следующим причинам:

– необходимостью реализации в операционной системе режима «аварийного завершения» (так как система будет эксплуатироваться в неблагоприятных условиях мобильных устройств);

– достаточно низкой производительностью аппаратной платформы (мобильные системы имеют сравнительно небольшую производительность);

– многоцелевой характер применения операционной системы (различным видам устройств необходим различный набор сервисных приложений).

Так как основные функции системы разграничения доступа реализованы в ядре операционной системы, аутентичность программного кода ядра операционной системы имеет большое значение в системе защиты операционной системы в целом. Для обеспечения защиты программного кода ядра в состав разработанной операционной системы входит безопасный загрузчик, который производит проверку ядра перед загрузкой системы.

На третьем уровне архитектуры операционной системы располагаются различные служебные подсистемы (файловая система, криптопровайдер и т.д.). Набор служебных подсистем может варьироваться в зависимости от места эксплуатации операционной системы. Отключение служб осуществляется путем правки конфигурационного файла ядра операционной системы.

В операционной системе предусмотрена подсистема виртуализации. На рисунке 2 изображена схема виртуальной среды выполнения команд.

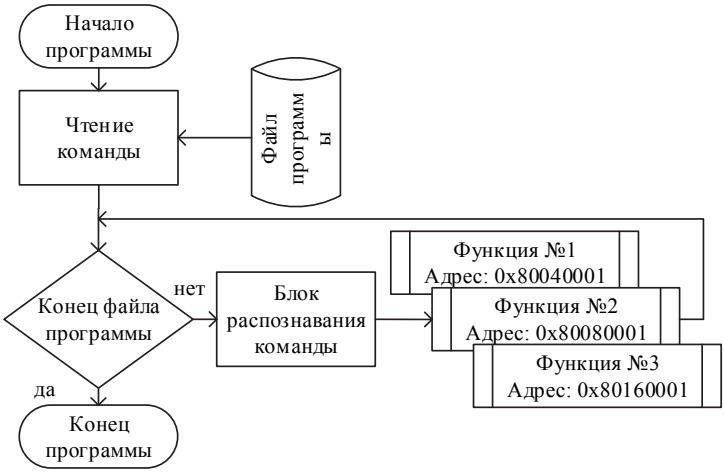

Рис. 2. Схема виртуальной среды выполнения команд

Для удобства разработчиков прикладного программного обеспечения операционной системы виртуальные команды имеют схожий синтаксис с языком программирования ASSEMBLER.

В операционной системе предусмотрены механизмы обнаружения вторжений. В частности, выполняется контроль использования оперативной памяти и доступа к файловым объектам. Виртуальная машина следит, чтобы приложение не выходило за пределы своего адресного пространства. При попытке получить доступ вне выделенного адресного пространства приложение будет завершено с ошибкой.

3. Подсистема аутентификации. Подсистема аутентификации в разработанной операционной системе играет одну из наиболее важных ролей. В подсистеме аутентификации ОС реализована аутентификация локальных и удаленных пользователей.

Подсистема аутентификации представляет собой набор библиотек, которые используются для проведения процедур аутентификации. Прототипом структуры подсистемы аутентификации послужила применяемая в операционных системах семейства Linux архитектура PAM (Pluggable Authentication Modules — подключаемые модули аутентификации)[7].

Подсистема аутентификации локальных пользователей обеспечивает проверку пользователей с использование многоразовых паролей.

Для защиты пользователей от принуждающей атаки в операционной системе был разработан алгоритм аутентификации пользователей на базе многоразовых паролей с защитой от принуждающей атаки. При этом для защиты пользователей было выбрано достаточно простое и эффективное решение. На этапе создания пользователя в системе выбирается два имени пользователя с похожим написанием. Например, имена «user1» и «userl» визуально похожи, однако они отличаются одним последним символом (цифра «1» и латинская буква «l»). Один пользователь имеет необходимые права в системе. Второй пользователь имеет минимальные права. В случае ввода резервного пароля (при принуждающей атаке) будет выполнен вход ограниченным пользователем.

Для создания аутентификационных данных у пользователя запрашиваются две пары значений логина и пароля: основной бор ($login_1$, $pass_1$), дополнительный набор ($login_2$, $pass_2$). Далее вычисляется значение ключей K_1, K_2 по формуле:

$$K_n = h(login_n, pass_n). \quad (1)$$

Далее необходимо найти значение шифртекста C_{login} такое, что выполняется:

$$\begin{cases} E_{K_1}(M_1) = C_{login} \\ E_{K_2}(M_2) = C_{login}, \end{cases} \quad (2)$$

где $M_1 = \{login_1 \mid h(login_1)\}$, $M_2 = \{login_2 \mid h(login_2)\}$, $h()$ — хеш-функция, $E_K()$ — функция шифрования. Стоит заметить, что в сообщения M_1, M_2 дополнительно введено хеш-значение для возможности дальнейшей проверки. В операционной системе хранится файл хранилища шифртекстов пользователей. В данном файле хранится шифротекст C_{login}.

Процесс аутентификации начинается с запроса у пользователя логина и пароля. Далее необходимо вычислить ключ шифрования K по формуле (1).

Далее необходимо выполнить чтение шифротекста C_{login} из файла и расшифровать сообщение ключом, полученным на предыдущем шаге по формуле:

$$M = D_K(C_{login}) = \{login \| h(login)\}, \quad (3)$$

где M — расшифрованное сообщение, K — ключи шифрования, $D_K()$ — функция расшифрования, $h()$ — хеш-функция. Если сообще-

ние состоит из *login'*и хеш-значения $login$", то необходимо выполнить вход в систему пользователем *login*."

При вводе резервного пароля ($pass_2$) будет расшифровано значение резервного логина ($login_2$). А вход в систему будет выполнен пользователем с усеченными правами.

Для защиты удаленных пользователей в операционной системе реализован предложенный в [8] протокол аутентификации с использованием одноразовых паролей на основе алгебраического алгоритма псевдовероятностного защитного преобразования. Данный протокол обеспечивает дополнительную защиту удаленных пользователей от принуждающей атаки.

4. Защита от анализа приложений. Защита прикладных программных продуктов от анализа в операционной системе реализуется в виртуальной среде выполнения команд. При создании прикладного приложения разработчику предлагается использовать специальные библиотечные функции операционной системы.

В операционной системе классические методы защиты приложений от анализа дополнительно усилены посредством применения псевдовероятностных преобразований.

Наиболее часто используемой в приложениях структурой является «условие». «Условие» используется как самостоятельно, так и в более сложных структурах, таких как «цикл».

Для защиты от статического анализа (дизассемблирования) целесообразно в ключевых блоках программы вместо структуры «условие» использовать псевдовероятностные преобразование. Вместо ключа использовать входные данные «условия». На выходе необходимо реализовать ложные ветви кода (например, в зашифрованном сообщении может содержаться адрес следующего блока программы).

На рисунке 3 изображена блок-схема функции, которая в качестве конструкции типа «условие» использует блок шифрования.

За блоком шифрования может быть реализовано любое количество истинных или ложных ветвей кода. При этом для злоумышленника последующее выполнение каждой из ветвей кода будет равновероятным (так как для шифрования адреса следующей команды применяется псевдовероятностное защитное преобразование).

Применение псевдовероятностного преобразования в качестве конструкции типа «условие» позволит значительно усложнить (особенно при многократном применении) статический анализ приложения (дизассемблирование).

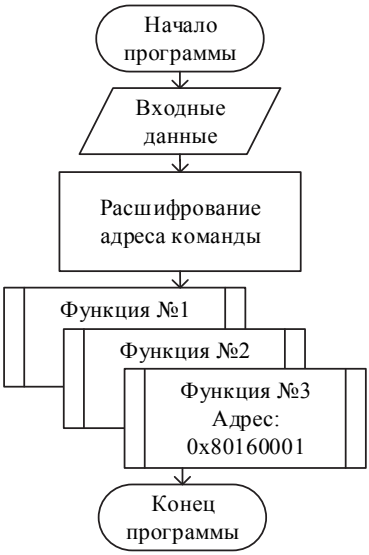

Рис. 3. Применение псевдовероятностных преобразований в качестве конструкции типа «если»

Для защиты программы от активного анализа средствами отладки также может применяться псевдовероятностное преобразование.

Один из способов применения псевдовероятностных преобразований для защиты программы от активного анализа — контроль времени выполнения. В данном случае ключом шифрования выступает разница во времени (например, количество тактов процессора, которое прошло за период времени). На выходе блока шифрования получается адрес следующего блока основной программы (либо ложной ветви алгоритма).

В докладе [9] был предложен и ряд других способов применения псевдовероятностных преобразований для обеспечения защиты приложений от анализа.

В ходе анализа работы приложения злоумышленником на вход блока шифрования подается определенное значение. Далее производится анализ реакции программы. В данном случае применение программ отладчиков может рассматриваться как «принуждение» программы к выполнению неких действий. Применение псевдовероятностных преобразований для противодействия атаке с принуждением позволяет более эффективно применять методы защиты приложений от анализа.

5. Криптографическая подсистема. В разработанной операционной системе предлагается применять псевдовероятностные преобразования также в рамках криптографической подсистемы для сокрытия

наличия резервных серий хранимой ключевой информации (данный способ был предложен в работе [10]). На рисунке 4 представлен алгоритм хранения набора резервных серий ключевой информации.

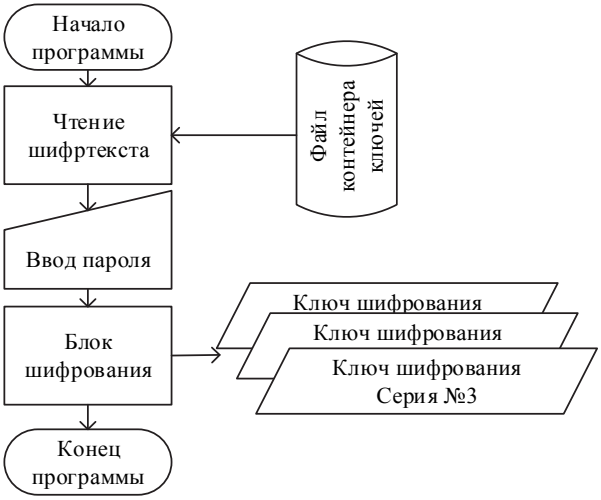

Рис. 4. Применение псевдовероятностных преобразований для хранения резервных серий ключевой информации

Контейнер ключей представляет собой файл, который содержит в себе значение шифртекста C. Для вычисления данного значения для n серий ключей необходимо найти решение системы уравнений:

$$\begin{cases} E_{K_1}(C) mod\ 2^r = M_1 \\ \dots \\ E_{K_n}(C) mod\ 2^r = M_n \end{cases}, \quad (4)$$

где $K_1 \dots K_n$ — ключи шифрования ключей (пароль фиксированной длины); $M_1 \dots M_n$ — защищаемые серии ключей; $E(\ )$ — функция шифрования; C — криптограмма; r — разрядность криптограммы. Информация о наличии резервных серий ключевой информации может иметь значительную ценность для злоумышленника. В качестве алгоритма шифрования применяется ГОСТ 28147-89. Так как длина файла шифртекста не зависит от количества зашифрованных серий ключевой информации, у злоумышленника отсутствует возможность доказать, что существуют несколько серий ключей.

Дополнительной положительной особенностью данного способа хранения ключевой информации является возможность совместить процесс генерации ключевой информации и выработки файла контей-

нера ключей. В данном случае вычисления сводится к генерации шифртекта C и нахождению n значений ключей шифрования ключей $K_1 ... K_n$ по формуле:

$$E_{K_n}(C) mod\ 2^r = M_n . \quad (5)$$

Стоит отметить, что данный метод может применяться только с учетом требований целевых алгоритмов шифрования для ключевой информации.

6. Заключение. В разработанной операционной системе подсистема информационной безопасности глубоко интегрирована в системные службы. ОС обеспечивает эшелонированную систему защиты от наиболее актуальных угроз безопасности. Отличительной особенностью операционной системы является применение псевдовероятностного шифрования в подсистемах защиты информации.

Применение универсальной операционной системы в мобильных устройствах телекоммуникационных и информационных систем, в том числе в системах защиты информации, позволит унифицировать подходы к обеспечению безопасности при разработке таких систем. Данный подход значительно сократит расходы на разработку и производство мобильных устройств на схожих аппаратных платформах. Область применения ОС: аутентифицирующие устройства (токены, идентификаторы), системы охраны, устройства защиты программного обеспечения, персональные устройства хранения данных (защищенные файловые хранилища), аппаратные средства шифрования (криптопровайдеры).

Литература

1. GuardantStealth II — электронный ключ с базовыми возможностями. URL: http://www.guardant.ru/products/guardant-stealth/ (дата обращения: 23.03.2016).
2. Рутокен ЭЦП. Электронный идентификатор с аппаратной реализацией российских стандартов электронной подписи, шифрования и хэширования. URL: http://www.rutoken.ru/products/all/rutoken-ecp/#features (дата обращения: 23.03.2016).
3. СЗИ НСД Аккорд-АМДЗ — это аппаратный модуль доверенной загрузки. URL: http://www.accord.ru/amdz.html (дата обращения: 23.03.2016).
4. Официальный сайт операционной системы MULTOS. URL: http://www.multos.com (дата обращения: 10.03.2016).
5. *Гордеев А.В.* Операционные системы: Учебник для вузов. 2-е изд // СПб.: Питер. 2007. 416 с.
6. *Колисниченко Д.Н.* Linux. От новичка к профессионалу // СПб.: БХВ-Петербург, 2010. 781 с.
7. *Березин А.Н., Биричевский А.Р., Молдовян Н.А., Рыжков А.В.* Способ отрицаемого шифрования // Вопросы защиты информации. 2013. № 2. С. 18–21.
8. *Биричевский А.Р.* Применение отрицаемого шифрования в протоколах одноразовых паролей // Вестник ИТАРК. 2015. № 1(1). С. 96–100.
9. *Биричевский А.Р.* Отрицаемое шифрование как механизм защиты приложений от отладки // Труды всеармейской научно-практической конференции «Инноваци-

онная деятельность в Вооруженных силах Российской Федерации». Спб: ВАС. 2013. С. 81–85.
10. *Биричевский А.Р.* Способ применения отрицаемого шифрования для хранения ключей // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России»: Материалы конференции. СПб. 2015. С. 98–99.

References

1. Berezin A.N., Birichevskij A.R., Moldovjan N.A., Ryzhkov A.V. [Deniable encryption method]. *Voprosy zashhity informacii – Issues of protection of information.* 2013. no. 2. pp. 18–21. (In Russ.).
2. Birichevskij A.R. Application of deniable encryption protocols, in one-time passwords. *Vestnik ITARK – Bulletin ITARK*. 2015. no. 1(1). pp. 96–100. (In Russ.).
3. Birichevskij A.R. [Deniable encryption as a defense mechanism of the application debugging]. *Otricaemoe shifrovanie kak mehanizm zashhity prilozhenij ototladki. Trudy vsearmejskoj nauchnoprakticheskoj konferencii «Innovacionnaja dejatel'nost' v Vooruzhennyh silah Rossijskoj Federacii»*. [Proceedings of the All-Army scientific and practical conference «Innovative activity in the Armed Forces of the Russian Federation»]. SPb.: VAS. 2013. pp. 81–85. (In Russ.).
4. Birichevskij A.R. [Method of use deniable encryption for storage of keys]. *Sposob primenenija otricaemogo shifrovanija dlja hranenija kljuchej. IX Sankt-Peterburgskaja mezhregional'naja konferencija «Informacionnaja bezopasnost' regionov Rossii»: Materialy konferencii.* [IX St.Petersburg Interregional Conference «Information Security of Russian Regions»: Proceedings of the conference]. SPb. 2015. pp. 98–99. (In Russ.).
5. Oficial'nyj sajt operacionnoj sistemy MULTOS [The official website of MULTOS operating system]. Available at: http://www.multos.com (accessed 10.03.2016).
6. GuardantStealth II — jelektronnyj kljuch s bazovymi vozmozhnostjami [GuardantStealth II — electronic key with basic features]. Available at: http://www.guardant.ru/products/guardant-stealth/ (accessed: 23.03.2016) (In Russ.).
7. Rutoken JeCP. Jelektronnyj identifikator s apparatnoj realizaciej rossijskih standartov jelektronnoj podpisi, shifrovanija i hjeshirovanija [Rutoken EDS. Electronic ID with the hardware implementation of the Russian standards for electronic signatures, encryption and hashing]. Available at: http://www.rutoken.ru/products/all/rutoken-ecp/# features (accessed: 23.03.2016) (In Russ.).
8. SZI NSD Akkord-AMDZ — jeto apparatnyj modul' doverennoj zagruzki [SZI NSD Accord- AMDZ — a trusted hardware module loading]. Available at: http://www.accord.ru/amdz.html (accessed: 23.03.2016) (In Russ.).
9. Gordeev A.V. *Operacionnye sistemy: Uchebnik dlja vuzov* [Operating Systems: A Textbook for high schools]. 2-e izd. SPb.: Piter. 2007. 416 p.
10. Kolisnichenko D. N. *Linux. Ot novichka k professional* [Linux. From beginner to professional]. SPb.: BHV-Peterburg. 2010. 781 p.

Биричевский Алексей Романович — аспирант лаборатории криптологии, Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН), старший преподаватель, ФГБОУ ВО Сыктывкарский государственный университет им. Питирима Сорокина. Область научных интересов: методы защиты информации, теория вероятности, криптография. Число научных публикаций — 14. lehabirich@mail.ru; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: 89505675437.

Birichevskij Aleksej Romanovich — Ph.D. student of cryptology laboratory, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), senior lecturer, Syktyvkar State University named after Pitirim Sorokin. Research interests: methods of information protection, probability theory, cryptography. The number of publications — 14. lehabirich@mail.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: 89505675437.

РЕФЕРАТ

Биричевский А.Р. **Универсальная мобильная операционная система с подсистемами аутентификации и защиты информации на основе псевдовероятностного преобразования.**

Работа посвящена универсальной мобильной операционной системе. Данная операционная система может быть применена в средствах защиты информации. Применение универсальной операционной системы, позволит унифицировать подходы к разработке систем защиты информации. Это значительно снизит затраты при разработке.

Отличительной особенностью разработанной операционной системы является интеграция псевдовероятностных преобразований в модули защиты информации. В работе описаны методы применения псевдовероятностных преобразований в подсистемах аутентификации, защиты приложений от анализа и криптографической подсистеме.

SUMMARY

Birichevskij A.R. **Universal Mobile Operating System Including Subsystems of Authentication and Data Protection Based on the Pseudo-Probability Transformation.**

The work is dedicated to a universal mobile operating system. This operating system can be used in the protection of information systems. The use of a universal operating system in the information protection systems will lead to a unified approach to the development of the latter. This will significantly reduce costs in the development of information security facilities.

A distinctive feature of the developed operating system is the integration of pseudo-probability transformations into information protection modules. This paper describes methods for applying pseudo-probability transformations in subsystems of authentication and protection of applications from analysis as well as in a cryptographic subsystem.