УДК 004.2

Гарантированное отключение периферии: общая постановка задачи

[1,2] *В. М. Елькин;* [2] *Д. Ю. Счастный*
[1] АО "Электроавтоматика", Ставрополь, Россия
[2] ЗАО "ОКБ САПР", Москва, Россия

Рассматривается постановка задачи гарантированного отключения периферии в условиях обработки защищаемой информации на недоверенных процессорах. Задача рассматривается в парадигме концепции разделения сеансов, требующих большей и меньшей защищенности. Проанализированы различные подходы к решению данной задачи, выявлен наиболее приемлемый. На основе проведенного анализа намечены предполагаемые направления дальнейшего исследования.

Ключевые слова: гарантированное отключение периферии, резидентный компонент безопасности, доверенный сеанс связи, недоверенный процессор.

В профессиональной среде активно обсуждается вопрос правомерности выбора между удобством использования средства вычислительной техники (СВТ) и его защищенностью. С тех пор как у подхода "защищенное и не должно быть удобно" появились оппоненты (причины их появления хорошо известны, и на них нет смысла останавливаться), вопрос перешел в плоскость обсуждения *приемлемого соотношения* защищенности и удобства. В рамках борьбы за удобство как разрабатываются новые технологии (технология доверенного сеанса связи — ДСС [1—7]) и архитектуры устройств (новая гарвардская архитектура компьютеров [8—16], архитектура защищенных служебных носителей информации [7, 8, 17—23]), так и обосновывается допустимость применения решений, имитирующих защиту, а пользователи, действия которых не подотчетны регуляторам (например, частные лица—клиенты банков), просто осознанно или неосознанно склоняются к принятию риска, связанного с использованием откровенно небезопасных технологий [1, 2, 24].

Другая крайность, в которую зачастую впадают те, кто не хочет мириться с имитацией защиты, — так называемое закручивание гаек. Не вызывает сомнений, что при обработке информации ограниченного распространения желательно максимально сократить число возможных каналов утечки информации всеми доступными мерами. В результате появляются требования отключить Интернет при использовании интернет-банкинга. В отличие от таких откровенно странных рекомендаций более здраво звучащие требования, в частности отключить беспроводные и проводные сети, устройства ввода и вывода информации, не задействованные в процессе обработки информации (далее будем обобщенно называть их периферией), воспринимаются с пониманием.

Приемлемый баланс защищенности и удобства возможен, и принципиальный подход к достижению этого баланса обозначен упомянутой концепцией ДСС: необходимо разделить сеансы работы на требующие большей и меньшей защищенности и, соответственно, больших или меньших ограничений [25].

Схема, предполагающая разделение сеансов работы, реализованная впервые в средстве обеспечения доверенного сеанса связи (СОДС) МАРШ! [1, 2], предназначенном для решения довольно далеких от гарантированного отключения периферии задач, представляется, однако, крайне продуктивной и для тех сценариев работы с СВТ, когда искомая разница условий сводится к тому, что пользователю одного и того же устройства надо работать то в условиях доступности широкого спектра каналов передачи данных, то в условиях гарантированного отключения этих каналов.

Рассмотрим подробнее, каким именно способом можно блокировать угрозы утечки защищаемой информации через периферию в концепции разделения сеансов большей и меньшей защищенности.

Отключать периферию можно на разных уровнях. Здесь можно выделить следующие основные подходы.

- Отключение периферии посредством функционала операционной системы (ОС), установленной на устройстве (при помощи встроенных служб

Елькин Василий Михайлович, инженер-конструктор, программист.
E-mail: elkin@okbsapr.ru
Счастный Дмитрий Юрьевич, заместитель генерального директора.
E-mail: DimaS@okbsapr.ru

Статья поступила в редакцию 13 ноября 2017 г.

и компонент). Подобные функции встроены в подавляющее большинство современных операционных систем. Этот способ едва ли можно считать правильным, так как в общем случае (если мы не берем в рассмотрение доверенные ОС с набором необходимых средств защиты информации — СЗИ) нельзя исключить наличие вредоносного кода в программном обеспечении (в том числе и в ОС). В частном же случае (с использованием доверенных ОС с необходимыми СЗИ) нельзя гарантировать отсутствие влияния аппаратных закладок (например, ориентированных на хищение обрабатываемой информации и сведений об операциях над ней) в процессоре и чипсете.

- Отключение периферии посредством специально разработанного низкоуровневого ПО, использующего инструкции самого процессора (особенно актуально для процессоров с ARM-архитектурой, так как в абсолютном большинстве случаев они проектируются как система на чипе (SoC), а значит, содержат в себе модули взаимодействия с периферией). Данный способ также нельзя считать вполне безопасным из-за уже упомянутых аппаратных "закладок" в архитектуре процессора и чипсете, которые могут сымитировать отключение периферии, не выполнив этого действия фактически. Решением этой проблемы мог бы стать выбор изначально доверенных процессора и чипсета, однако это невозможно фактически, так как не существует доверенных отечественных процессоров и чипсетов достаточной производительности и разумной стоимости, а импортные невозможно проверить на соответствие заявленной документации.

По итогам рассмотрения первых двух способов задача сводится к решению вопроса о том, каким образом отключить периферию гарантированно с применением недоверенного процессора.

- Очевидно, можно спроектировать схемотехнику устройства таким образом, чтобы на корпус был выведен набор выключателей, которые будут физически разрывать линии питания (в идеале еще и информационные и сигнальные линии) периферии и тем самым гарантированно отключать ее от процессора. Однако и такой подход нельзя считать ни безопасным, ни удобным, так как рассчитывать на то, что пользователь будет для обеспечения защиты информации вручную отключать периферию перед началом работы с защищаемой информацией и включать по окончании, можно, но для минимальной работоспособности этого решения необходима серьезная поддержка организационными мерами.

Также нельзя не принимать в расчет то, что такое завершение работы с периферией (обрыв питания) с точки зрения ОС и процессора будет некорректным и может привести к накоплению ошибок и отказам.

Из приведенных выкладок логичным образом вытекают требования к правильному решению: правильным решением будет *физический* разрыв линий питания (а возможно, еще и информационных и сигнальных линий) с предварительным *корректным* с точки зрения ОС и процессора *завершением* работы периферии, но не в ручном режиме, а *в автоматизированном*.

Для этого в схемотехнику устройства понадобится ввести доверенный компонент (резидентный компонент безопасности — РКБ) [26, 27], через который процессор будет осуществлять работу с периферией и который будет осуществлять корректное доверенное и гарантированное подключение и отключение периферии.

Ключевым моментом для реализации этого способа будет выработка решений по следующим направлениям:

- принцип взаимодействия процессора с периферией через РКБ;
- перечень периферии, использование которой необходимо контролировать;
- схема смены сеансов большей и меньшей защищенности.

Литература

1. *Конявский В. А.* Серебряная пуля для хакера // Защита информации. INSIDE. 2013, № 4. С. 54—56.
2. *Конявский В. А.* Серебряная пуля для хакера (окончание) // Защита информации. INSIDE. 2013, № 5. С. 69—73.
3. Съемный носитель информации. Патент на полезную модель № 102139. 10.02.2011. Бюл. № 4.
4. Съемный носитель информации с безопасным управлением доступом. Патент на полезную модель № 123571. 27.12.2012. Бюл. № 36.
5. Съемный носитель информации на основе энергонезависимой памяти с расширенным набором функций информационной безопасности. Патент на полезную модель № 130441. 20.07.2013. Бюл. № 20.
6. Модем для безопасных коммуникаций в компьютерных сетях. Патент на полезную модель № 128055. 10.05.2013. Бюл. № 13.
7. Мобильное устройство защищенного хранения и обработки информации. Патент на полезную модель № 158714. 20.01.2016. Бюл. № 2.
8. *Конявский В. А.* Иммунитет как результат эволюции ЭВМ // Защита информации. INSIDE. 2017, № 4. С. 46—52.
9. *Конявская С. В.* О происхождении видов, или как лечить болезнь, а не симптомы // Защита информации. INSIDE. 2017, № 5. С. 64—74.
10. Компьютер типа "тонкий клиент" с аппаратной защитой данных. Патент на полезную модель № 118773. 27.07.12. Бюл. № 21.
11. Компьютер с аппаратной защитой данных от несанкционированного изменения. Патент на полезную модель № 137626. 20.02.2014. Бюл. № 5.

12. Мобильный компьютер с аппаратной защитой доверенной операционной системы. Патент на полезную модель № 138562. 20.03.2014. Бюл. № 8.

13. Мобильный компьютер с аппаратной защитой доверенной операционной системы от несанкционированных изменений. Патент на полезную модель № 139532. 20.04.2014. Бюл. № 11.

14. Мобильный компьютер с аппаратной защитой доверенной операционной системы. Патент на полезную модель № 147527. 10.11.2014. Бюл. № 31.

15. Мобильный компьютер с аппаратной защитой доверенной операционной системы от несанкционированных изменений. Патент на полезную модель № 151264. 27.03.2015. Бюл. № 9.

16. Рабочая станция с аппаратной защитой данных для компьютерных сетей с клиент-серверной или терминальной архитектурой. Патент на полезную модель № 153044. 27.06.2015. Бюл. № 18.

17. Съемный носитель ключевой и конфиденциальной информации. Патент на полезную модель № 147529. 10.11.2014. Бюл. 31.

18. *Кравец В. В.* Идеальный токен: мат. XX Научно-практической конф. "Комплексная защита информации". Минск, 19—21 мая 2015 г. — Минск: РИВШ, 2015. С. 114, 115.

19. *Ладынская Ю. П., Батраков А. Ю.* Хранение данных СКЗИ: выбор носителя: мат. XIII Международной конф. "Информационная безопасность". — Таганрог, 2013. Ч. 1. С. 129—134.

20. *Бирюков К. А.* Средства безопасного хранения ключей // Безопасность информационных технологий. 2013, № 3. С. 50—53.

21. Специальный съемный носитель информации. Патент на полезную модель № 94751. 27.05.2010. Бюл. № 15.

22. *Грунтович М. М.* Безопасное применение мобильных USB-носителей: мат. XVII Международной конф. "Комплексная защита информации. Безопасность информационных технологий". 15—18 мая 2012 г. — Суздаль. 2012. С. 72, 73.

23. *Лыдин С. С.* Психологические аспекты защищенного применения служебных носителей информации: мат. XVII Международной конф. "Комплексная защита информации. Безопасность информационных технологий". 15—18 мая 2012 г. — Суздаль. 2012. С. 167—169.

24. *Конявский В. А.* Минимизация рисков участников дистанционного банковского обслуживания // Вопросы защиты информации. 2014, № 4 (107). С. 3, 4.

25. *Конявский В. А.* Доверенный сеанс связи. Развитие парадигмы доверенных вычислительных систем — на старт, внимание, МАРШ!: мат. XV Межд. научно-практической конф. "Комплексная защита информации". Иркутск. 1—4 июня 2010 г.

26. *Конявский В. А.* Управление защитой информации на базе СЗИ НСД "Аккорд". — М., 1999. — 325 с.

27. *Конявский В. А., Гадасин В. А.* Основы понимания феномена электронного обмена информацией // Библиотека журнала "УЗИ". 2004. — 327 с.

Guaranteed disconnection of the periphery: general statement of the problem

[1, 2]V. M. Elkin, [2]D. Yu. Schastny

[1] Joint Stock Company "Electroavtomatika", Stavropol, Russia

[2] Closed Joint Stock Company "OKB SAPR", Moscow, Russia

This article is devoted to setting the task of peripherals guaranteed disconnection in conditions of protected information processing on untrusted processors. The task is considered in the paradigm of the sessions requiring greater and less security separation concept. Different approaches to the solution of this problem have been analyzed and the most acceptable one has been identified. Based on the analysis by the authors of the article the prospective directions for further research are outlined.

Keywords: guaranteed disconnection of the periphery, resident security component, trusted session, untrusted processor.

Bibliography — 27 references. *Received November 13, 2017*