Принципы реализации программного модуля доверенной загрузки

Алексей Боровиков, Константин Новиков, Олег Маслов

На автоматизированных рабочих местах, обрабатывающих конфиденциальную информацию, должны применяться сертифицированные аппаратно-программные модули доверенной загрузки для обеспечения защиты от несанкционированного доступа к информации на этапе начального старта и загрузки операционной системы. Однако в изделиях, применяемых во встраиваемых системах, использование данных модулей не всегда представляется возможным в связи с жёсткими требованиями к габаритам изделия, энергопотреблению и тепловыделению. В рамках данной статьи рассмотрены принципы реализации программного модуля доверенной загрузки ОС, предназначенного для обеспечения защиты от НСД к информации.

Введение

Важнейшей задачей в области обеспечения информационной безопасности автоматизированных систем (АС) является сохранение свойств информации, таких как доступность, целостность и конфиденциальность.

На автоматизированных рабочих местах (АРМ), на которых обрабатывается конфиденциальная информация, для защиты от несанкционированного доступа к информации (НСД) внутреннего нарушителя с целью нарушения указанных свойств, как правило, применяется следующий комплекс мероприятий:

- в случае однопользовательской системы и отсутствия необходимости ввода/вывода информации на внешние носители применяются организационно-режимные (технические) меры защиты, такие как опечатывание корпуса и всех разъёмов для подключения внешних устройств, направленные на защиту от несанкционированной загрузки и считывания защищаемой информации;
- в случае многопользовательской системы и при необходимости ввода/вывода информации на внешние носители применяются сертифицированные аппаратно-программные средства защиты информации, такие как аппаратно-программные модули доверенной загрузки информации (АПМДЗ) и средства защиты информации от несанкционированного доступа (СЗИ от НСД), обеспечивающие защиту от НСД и замкнутость программной среды [1].

Однако ситуация осложняется в тех случаях, когда необходимо обеспечить защиту от НСД к информации на объектах, критичных к способу и месту размещения АРМ, или для специализированных устройств, реализующих критичные функции, с точки зрения требований нормативных документов по безопасности информации (межсетевые экраны, коммутационное оборудование и т.д.).

В данных случаях указанные мероприятия не могут быть реализованы в полной мере из-за отсутствия возможности установить АПМДЗ в изделия с малыми габаритами и критичными к увеличению тепловыделения и потребляемой мощности, а компенсировать отсутствие АПМДЗ за счёт организационно-режимных (технических) мероприятий не представляется возможным, так как данные изделия требуют обслуживания в процессе эксплуатации и использования внешних разъёмов для ввода/вывода информации.

Отсутствие АПМДЗ в данных изделиях приводит к тому, что до или в процессе загрузки операционной системы (ОС) появляется возможность осуществить преднамеренные попытки НСД к информации или среде её обработки (хранения), так как на данном этапе отсутствуют какие-либо меры её защиты. Наиболее простым способом атаки является загрузка ОС с внешнего носителя, позволяющая внутреннему нарушителю получить доступ к защищаемой информации.

Для защиты от указанных угроз для данных типов изделий может быть применён подход по реализации в них процедуры доверенной загрузки.

Процедура доверенной загрузки – это процесс загрузки системного программного обеспечения после выполнения успешной аутентификации оператора изделия и исключительно с выбранного учтённого носителя, реализованный в доверенной среде.

Доверенная среда – это совокупность программно-технических средств и коммуникационных ресурсов, для которых однозначно определены состав, архитектура, алгоритмы функционирования, правила обработки информации и в отношении которой верны следующие предположения:

- проведены исследования по требованиям нормативных документов по безопасности информации в объёме, согласованном с регулятором;
- гарантирована её целостность и неизменность в составе изделия на период эксплуатации за счёт реализации соответствующих программно-

технических и организационно-режимных мер.

Средства, обеспечивающие процедуру доверенной загрузки, должны иметь соответствующие разрешительные документы для их применения. Средства доверенной загрузки могут быть реализованы и на программном уровне.

Программные средства или модули доверенной загрузки (ПМДЗ) получают управление при выполнении ПО BIOS и не требуют наличия дополнительных аппаратных устройств для их функционирования [2].

Обязательным условием программной реализации МДЗ является необходимость его встраивания в ПО BIOS. Данный процесс с учётом сложности современного ПО BIOS, его объёма и многофункциональности (наличие ядра ОС, продвинутый графический интерфейс, возможность подключения к Интернету и т.д.) является крайне трудоёмким. При этом данный вариант реализации может повлечь за собой нестабильность работы процессорной платы, выявить которую на этапе отладки и тестирования проблематично, в связи с отсутствием исходного кода на ПО BIOS и детального понимания его принципов функционирования. Также большой объём бинарного кода, на который отсутствует исходный код и программная документация, не позволяет гарантировать отсутствие программных ошибок или опасных функциональных возможностей, которые могут повлиять на правильное функционирование ПМДЗ.

Описание принципов программной реализации модуля доверенной загрузки

В настоящее время был проведён ряд научно-технических работ и по их результатам разработан подход, который лишён указанных недостатков. Для реализации данного подхода необходимо обеспечить полное замещение проприетарного ПО BIOS с получением на него исходного кода для возможности встраивания функций МДЗ. При этом ПО BIOS будет реализовывать исключительно базовые (минимально необходимые) функции проприетарного ПО BIOS, достаточные для корректного функционирования процессорной платы, с установленной операционной системы, а передачу управления на загрузчик операционной системы будет осуществлять ПМДЗ, что позволит обеспечить доверенную и максимально быструю загрузку процессорной платы и системы в целом.

Общий алгоритм работы ПО BIOS с функциями ПМДЗ представлен на рис. 1.

По сравнению с алгоритмом работы ПО BIOS процессорной платы, на которой установлен АПМДЗ в виде платы расширения, в описанном случае не требуется осуществлять поиск дополнительного встроенного программного обеспечения (*Option ROM*) внешней платы АПМДЗ и передавать на него управление, что позволяет исключить угрозы, связанные с перехватом управления и исполнения потенциально опасного ПО с других плат расширения до передачи управления на АПМДЗ.

В рамках указанных работ был проведён анализ существующих свободно распространяемых проектов для замещения ПО BIOS на ПО в исходных кодах с минимальным объёмом бинарных вставок, и по результатам анализа было определено, что наиболее подходящей основой для разработки ПМДЗ является ПО проекта “Coreboot”.

“Coreboot” – это проект по созданию свободной прошивки ПО BIOS. Основной целью проекта является получение минимальной прошивки, достаточной для быстрой и полной инициализации аппаратного обеспечения, необходимой для правильного его функционирования, по возможности свободной от бинарных вставок.

Анализ функциональных возможностей ПО проекта “Coreboot” показал, что оптимальным местом для встраивания ПМДЗ является полезная нагрузка (payload), так как её программная реализация не привязана к аппаратному обеспечению процессорной платы и собирается отдельно от ПО “Coreboot”. В настоящее время существуют различные типы полезной нагрузки, в которые возможно встроить функции защиты МДЗ:

- отечественная ЗОСРВ «Нейтрино» (разработчик – ООО «СВД Встраиваемые системы») или ядро Linux может использоваться в качестве полезной нагрузки и может быть встроена в микросхему ПЗУ вместе с бинарным кодом проекта “Coreboot”. При этом ЗОСРВ «Нейтрино» удовлетворяет требованиям к средствам вычислительной техники (СВТ) по 3-му классу защиты информации от несанкционированного доступа и может быть использована при создании автоматизированных систем, имеющих класс защищённости до 1Б включительно;
- SeaBIOS или GRUB2 может использоваться для загрузки ОС Astra Linux, МСВС и семейства Windows [3].

По результатам изучения ПО проекта “Coreboot” и его апробирования в процессе замещения проприетарного ПО BIOS на нескольких процессорных платах отечественного производителя ЗАО «НПФ «ДОЛОМАНТ» была разработана технология замещения проприетарного ПО BIOS, которая позволяет получить исходный код на ряд современных аппаратных платформ фирмы Intel и обеспечить возможность встраивания в его ПО ПМДЗ.

При этом наличие исходного кода проекта “Coreboot” позволяет выполнить его анализ на предмет наличия программных ошибок и опасных функциональных возможностей и в случае обнаружения либо исключить их, либо встроить в состав функции доверенной

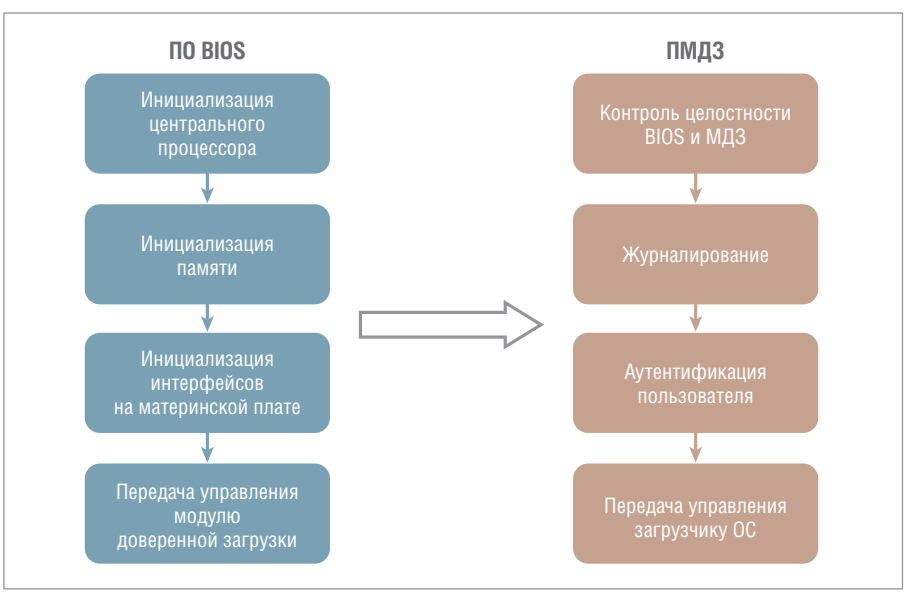

Рис. 1. Алгоритм работы ПО BIOS с функциями ПМДЗ

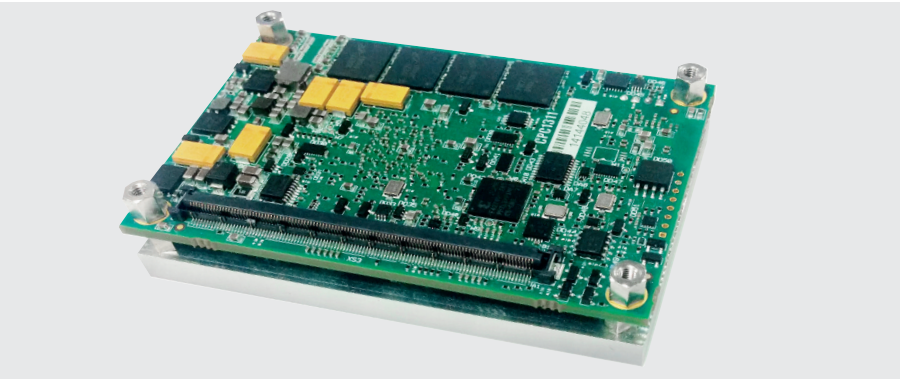

Рис. 2. Компьютерный модуль CPC1311

загрузки, такие как аутентификацию пользователей, в том числе с использованием внешних считывателей информации, контроль целостности ПО BIOS и системных файлов ОС, журналирование событий [4]. Наличие исходного кода и минимального объёма бинарных вставок позволяет повысить уровень доверия к ПО BIOS и существенно сократить объёмы и сроки проведения работ по обеспечению корректного встраивания ПМДЗ в ПО BIOS и получить соответствующие разрешительные документы.

Таким образом, по результатам рассмотрения возможности программной реализации функций доверенной загрузки сделан вывод, что в настоящее время возможно разработать ПО BIOS на базе свободно распространяемого ПО проекта “Coreboot”, реализующее функции доверенной загрузки ОС. Реализация программного модуля доверенной загрузки на основе ПО проекта “Coreboot” является оптимальным подходом, позволяющим в дальнейшем провести анализ ПО BIOS с функциями ПМДЗ на соответствие требованиям по информационной безопасности.

Практическое применение

В первую очередь замещение ПО BIOS и реализация функций ПМДЗ планируется на компьютерном модуле CPC1311 производства ЗАО «НПФ «ДОЛОМАНТ» (рис. 2).

Модуль CPC1311 выполнен в формате COM Express mini (тип 10). Изделие ориентировано на российских OEM-заказчиков нестандартных вычислителей для использования в системах повышенной ответственности, а также функционирующих в жёстких условиях окружающей среды.

Модуль CPC1311 построен на базе многоядерного процессора в индустриальном исполнении Intel Atom семейства Bay Trail с 64-разрядной архитектурой. Отличительными особенностями этих процессоров являются крайне низкое энергопотребление (до 10 Вт), поддержка памяти ECC и мощный графический контроллер. В CPC1311 используются два исполнения процессора: высокопроизводительное на базе 4-ядерного процессора E3845 с частотой 1,91 ГГц и малопотребляющее на базе 2-ядерного E3825 с частотой 1,33 ГГц. «Обвязка» процессора в виде 4 Гбайт оперативной памяти DDR3L с поддержкой EEC и твердотельного диска 8 Гбайт позволяет использовать изделие

в качестве самодостаточного встраиваемого компьютера, способного решать большинство прикладных задач.

Мультимедийные возможности CPC1311 включают в себя видеоконтроллер с интерфейсом LVDS (разрешение до 2560×1600 пикселей) и современный аудиокодек класса HD. Встроенные в процессор функции декодирования видео позволяют применять модуль в системах, связанных с обработкой мультимедийных потоков.

Через разъёмы высокой плотности разработчикам доступен большой арсенал высокоскоростных интерфейсов: 1×Gb Ethernet, 5×USB 2.0, 1×USB 3.0, 2×SATA II, 3×PCIe x1 (дополнительно одна линия PCIe может быть получена вместо Gb Ethernet). Из дополнительных возможностей следует отметить встроенную поддержку шины CAN 2.0, востребованную в системах реального времени, прежде всего, на транспорте.

Все компоненты CPC1311 напаяны на плату, что обеспечивает высокую стойкость изделия к ударным и вибрационным нагрузкам. По заказу модуль поставляется с влагозащитным покрытием. Диапазон рабочих температур CPC1311 –40...+85°C.

Применение процессоров из встраиваемой линейки Intel гарантирует российским потребителям длительную доступность CPC1311 – до 15 лет стандартно и более по отдельному договору.

CPC1311 поддерживает наиболее популярные операционные системы: Linux 3.8, Microsoft Windows Embedded Standard 7 и 8, QNX 6.x, а также Astra Linux и ЗОСРВ «Нейтрино».

Заключение

В данной статье были рассмотрены принципы реализации программного модуля доверенной загрузки операционных систем в ПО BIOS, реализованного на базе свободно распространяемого ПО проекта “Coreboot”, и описан компьютерный модуль CPC1311 производства ЗАО «НПФ «ДОЛОМАНТ», для которого планируется реализация функций ПМДЗ в ПО BIOS.

По результатам рассмотрения принципов реализации программного модуля доверенной загрузки можно заключить, что в настоящее время возможно разработать ПО BIOS на базе свободно распространяемого ПО проекта “Coreboot”, реализующее функции доверенной загрузки ОС. Реализация программного модуля доверенной загрузки на основе ПО проекта “Coreboot” является оптимальным подходом, позволяющим в дальнейшем провести анализ ПО BIOS с функциями ПМДЗ на соответствие требованиям информационной безопасности. ●

Литература

1. Лыдин С.С. О средствах доверенной загрузки для аппаратных платформ с UEFI BIOS // Вопросы защиты информации. – 2016. – № 3.
2. Счастный Д.Ю. Перспективы развития средств доверенной загрузки. Взгляд разработчика // Вопросы защиты информации. – 2017. – № 3.
3. Zimmer V., Sun J., Jones M., et al. Embedded Firmware Solutions: Development Best Practices for the Internet of Things. – NY : Apress Open, 2015.
4. Чепанова Е.Г. Формирование критериев сравнения модулей доверенной загрузки // Вопросы защиты информации. – 2014. – № 4.

E-mail: alexey_bau@mail.ru