УДК.519.681.3

Р.Н. Чекин

Современные угрозы безопасности обработки информации со стороны встроенного программного обеспечения BIOS

Рассматриваются возможные угрозы безопасности информации в средствах вычислительной техники, построенных на базе покупных компьютерных комплектующих со стороны встроенного программного обеспечения BIOS данных комплектующих.
Ключевые слова: информационная безопасность, угрозы безопасности обработки информации, встроенное программное обеспечение, BIOS, деструктивное программное обеспечение, недокументированные возможности, исследования программного обеспечения.

При разработке на базе покупных компьютерных комплектующих средств вычислительной техники, предназначенных для обработки конфиденциальной информации, возникает вопрос о доверенности встроенного программного обеспечения BIOS таких комплектующих.

Встроенное программное обеспечение BIOS подавляющего большинства компьютерных комплектующих не предназначено для построения защищенных систем. Оно может содержать встроенные функции для перепрошивки BIOS, недокументированные возможности управления загрузкой операционной системы, удаленного администрирования, средства изменения настроек, влияющие на надежность работы оборудования, пароли постоянного действия, средства для отладки кода и отладочные входы. Данные возможности позволяют, при получении злоумышленником доступа к оборудованию, внедрить в BIOS код, выполняющий деструктивные функции.

Широкое распространение при построении средств вычислительной техники на базе персональных компьютеров получили аппаратные модули доверенной загрузки (АМДЗ), которые представляют собой платы расширения с дополнительным BIOS. Производители, как правило, не уточняют материнские платы, на которых данные устройства работают корректно. Однако могут ли они выполнить заявленные функции на любой плате? Для получения управления в АМДЗ используются методы перехвата прерываний. Данные методы базируются на недокументированных особенностях работы популярных версий BIOS от Phoenix и AMI. В то же время интеллектуальное программное обеспечение BIOS способно восстанавливать перехваченные адреса векторов прерываний и предлагать пользователю возможность обхода АМДЗ.

Современные версии BIOS содержат утилиты перепрограммирования микросхемы BIOS файлами-образами, полученными как из сети, так и с внешних носителей: USB-накопителей, компакт-дисков, флоппи-дисков и т.п. Данная возможность позволяет злоумышленнику внедрить в BIOS закладки, выполняющие обход программно-аппаратных средств защиты.

Большинство версий встроенного программного обеспечения BIOS содержит утилиты настройки оборудования. Данные утилиты позволяют добиться неустойчивой работы оборудования, что может привести к обходу инициализации плат расширения (в том числе АМДЗ) или их некорректной работе.

Многие современные чипсеты для IA32/IA-64-платформ аппаратно поддерживают технологию Active Management Technology. Данная технология позволяет получить доступ к удаленной ПЭВМ даже в случае, если она выключена или «зависла». Среди критичных возможностей управления AMT можно выделить следующие: удаленное перенаправление источника загрузки операционной системы, перенаправление ввода-вывода системы во время процесса загрузки, удаленная смена установок BIOS, изменение содержимого жесткого диска, блокирование сетевого трафика, включение/выключения питания, сброс компьютера и т.п. Управление поддержкой технологии AMT чипсетом осуществляется из программного обеспечения BIOS.

Широкое распространение в современных процессорах получили технологии виртуализации. Аппаратная поддержка процессорами технологий виртуализации позволяет деструктивному программному обеспечению минимальными средствами реализовать скрытый контроль над выполнением специального программного обеспечения, обрабатывающего конфиденциальную информацию. В случае если деструктивное программное обеспе-

чение получает управление из BIOS, его выявление и устранение в отдельных случаях невозможно без исследования и модификации BIOS.

В таких условиях для разработки доверенных средств вычислительной техники на базе обычных компьютерных комплектующих необходимы сведения о возможностях используемых версий BIOS, которые могут быть получены только в ходе восстановления алгоритмов работы BIOS. Поэтому в рамках обеспечения безопасности обработки информации необходимо проведение мероприятий по анализу программного обеспечения BIOS и предотвращению его несанкционированной модификации.

ПФ ФГУП НТЦ «Атлас» проводит работы по дизассемблированию, восстановлению алгоритмов функционирования BIOS, определению недокументированных возможностей и доработке BIOS для удовлетворения требованиям по защите информации.

Чекин Роман Николаевич
Зам. начальника отдела Пензенского филиала ФГУП «НТЦ «Атлас», г. Пенза
Тел.: (+7-841-2) 54-80-73)
Эл. адрес: atlas@e-pen.ru

R.N. Chekin
The modern BIOS firmware threats of information security

It is considered possible information threats on the bought-in computer components with distrusted BIOS firmware.
Keywords: information security, firmware, BIOS, malware, malware detection.
