ПОВЫШЕНИЕ УРОВНЯ ДОВЕРИЯ К АППАРАТНО-ПРОГРАММНЫМ ПЛАТФОРМАМ С ЦЕЛЬЮ ПРЕДУПРЕЖДЕНИЯ КОМПЬЮТЕРНЫХ АТАК ИЗ-ЗА УЯЗВИМОСТЕЙ В ПО BIOS

Боровиков А.Ю.[1], Маслов О.А.[2], Мордвинов С.А.[3], Есафьев А.А.[4]

Аннотация: *в статье изложен метод по повышению уровня доверия к аппаратно-программным платформам на базе системной логики иностранного и отечественного производства, предназначенным для построения специализированых изделий и средств вычислительной техники, обрабатывающих информацию ограниченного доступа, соответствующим требованиями по безопасности информации и неподверженным компьютерным атакам с использованием уязвимостей в ПО BIOS. Указаны проблемы, с которыми сталкивается разработчик, предложены способы их решения и сделаны соответствующие выводы.*

Цель исследования: *исследование возможности создания доверенной аппаратно-программной платформы на базе системной логики иностранного и отечественного производства, неподверженной компьютерным атакам с использованием уязвимостей в ПО BIOS.*

Методы исследования: *для достижения поставленной цели был проведен анализ отечественного рынка процессорных модулей с целью выбора модуля для создания доверенной аппаратно-программной платформы, проведен анализ существующих уязвимостей ПО BIOS, проведены работы по замещению проприетарного ПО BIOS процессорного модуля на программное обеспечение отечественной разработки ЗОС Горизонт, реализующего функции ПО BIOS и меры защиты от несанкционированного доступа, и рассмотрена возможность практического применения доверенной аппаратно-программной платформы с программным обеспечением ЗОС Горизонт.*

Полученный результат: *выбран процессорный модуль для создания доверенной аппаратно-программной платформы, проведено замещение проприетарного программного обеспечения BIOS процессорного модуля на программное обеспечение отечественной разработки «Загрузчик операционных систем Горизонт», реализующего функции программного обеспечения BIOS и меры защиты от несанкционированного доступа, сформирован метод по повышению уровня доверия к аппаратно-программным платформам на базе системной логики иностранного и отечественного производства, предназначенным для построения специализированых изделий и средств вычислительной техники, обрабатывающих информацию ограниченного доступа, соответствующим требованиями по безопасности информации и неподверженным компьютерным атакам с использованием уязвимостей в программном обеспечении BIOS, сформированы требования к доверенной аппаратно-программной платформе и условия их выполнения, обоснована необходимость исключения потенциально опасных функциональных возможностей микроконтроллера Intel Management Engine из ПО BIOS аппаратно-программной платформы на базе системной логики фирмы Intel и сформированы предложения по практическому применению доверенной аппаратно-программной платформы с программным обеспечением «Загрузчик операционных систем Горизонт».*

Ключевые слова: *кибербезопасность, импортозамещение, доверенная загрузка, доверенная аппаратно-программная платформа, программное обеспечение BIOS, Загрузчик операционных систем Горизонт, несанкционированный доступ к информации, компьютерные атаки, уязвимости.*

DOI:10.21681/2311-3456-2021-6-68-77

Введение

При создании специализированных изделий в частности и средств вычислительной техники (СВТ) в целом, предназначенных для обработки информации ограниченного доступа и ее защиты, помимо реализации целевых функций, перед Разработчиком стоит задача выполнения требований по обеспечению отсутствия

1 Боровиков Алексей Юрьевич, заместитель начальника специализированного отдела №6 Пензенского филиала АО «Научно-технический центр «Атлас», г. Пенза, Россия. E-mail: alexey_bau@mail.ru

2 Маслов Олег Алексеевич, начальник специализированного отдела №6 Пензенского филиала Акционерного общества «Научно-технический центр «Атлас», г. Пенза, Россия, oa_de_ao@mail.ru

3 Мордвинов Степан Алексеевич, инженер второй категории специализированного отдела №6 Пензенского филиала АО «Научно-технический центр «Атлас», г. Пенза, Россия. E-mail: zoi.kun@mail.ru

4 Есафьев Андрей Андреевич, научный сотрудник специализированного отдела №6 Пензенского филиала АО «Научно-технический центр «Атлас», г. Пенза, Россия. E-mail: peterpozinsky@ya.ru

недокументированных функциональных возможностей и уязвимостей программного обеспечения, способных нарушить штатный алгоритм работы изделий и заданные характеристики безопасности, такие как доступность, целостность, конфиденциальность. К рассматриваемым специализированным изделиям могут быть отнесены устройства управления техническими средствами (каналообразующими средствами, робототехникой, производственным оборудованием и иными системами), средства защиты информации от несанкционированного доступа (межсетевые экраны, средства обнаружения вторжений, автоматизированные рабочие места в защищенном исполнении и т.п.) и прочие вычислительные устройства, к которым предъявляются требования по обеспечению высокой надежности и доступности информации [1].

Также СВТ должны обеспечивать определенные гарантии по противодействию компьютерным атакам. При этом компьютерные атаки можно условно разделить на два класса: атаки, ориентированные на уязвимости в ПО (ОС, СУБД, прикладное ПО и т.д.), функционирующем на произвольной аппаратной платформе, и атаки, ориентированные на ПО, жестко установленное в аппаратные компоненты (firmware), используемые при создании аппаратных платформ.

В данной работе рассматривается подход по созданию доверенной аппаратно-программной платформы на базе системной логики фирмы Intel для создания СВТ, неподверженных компьютерным атакам на ПО BIOS.

Описание уязвимостей ПО BIOS

Актуальность вопроса по созданию доверенной аппаратно-программной платформы на базе системной логики фирмы Intel подтверждается неоднократными фактами обнаружения критичных с точки зрения информационной безопасности уязвимостей в ПО BIOS [2, 3].

Так, по результатам проведенного анализа базы данных уязвимостей CVE, было установлено наличие более 20 актуальных уязвимостей в ПО BIOS, в основном связанных с ошибками в программном обеспечении встроенных в BIOS технологий Intel ME (Intel TXE, Intel ATM) [4].

Технология Intel Management Engine (ME) представляет собой интегрированный в микросхему SoC процессора или контроллера периферийных устройств (PCH) микроконтроллер с функциями, позволяющий работать СВТ в выключенном состоянии и осуществлять доступ ко всем устройствам, находящимся внутри SoC или PCH. Контроллер IME работает под управлением ПО, которое расположено в составе ПО BIOS [5, с. 41–42], [6].

В таблице 1 приведен перечень характерных актуальных уязвимостей в ПО BIOS в формате описания CVE, эксплуатация которых может привести к нарушению безопасности защищаемой информации.

Эксплуатация уязвимостей IME в худшем случае может привести к замещению кода ПО IME и прямому выполнению кода злоумышленника внутри IME, имея прямой доступ ко всем устройствам SoC, даже, если само СВТ находится в выключенном состоянии, но при этом на него подается дежурное питание [8, 9, 10].

Указанные уязвимости в настоящее время устранены в новых версиях ПО IME, однако с учетом большого объема кода IME (4Мб бинарного кода) и невозможности провести соответствующие исследования в связи с отсутствием исходного кода на ПО IME в данный момент невозможно гарантировать полное устранение уязвимостей, которые могут быть со временем найдены злоумышленником и использованы для осуществления компьютерных атак на СВТ [11 с. 1035-1036], [12].

При этом также не стоит забывать о потенциально опасных функциональных возможностях, заложенных разработчиком и незадекларированных в документации, для возможности получения скрытого контроля и доступа к информации и ресурсам в дальнейшем при эксплуатации СВТ, построенного на базе выбранной аппаратной платформы.

Решение данного вопроса усложняется также тем, что подавляющее большинство российских средств вычислительной техники построены на аппаратно-программных платформах иностранного производства, для которых не обеспечиваются гарантии проектирования и архитектуры, а также зачастую отсутствует необходимый комплект конструкторской и программной документации, позволяющий обеспечить требуемый уровень доверия к указанным платформам.

Безусловно в ходе проведения государственной программы по импортозамещению на российском рынке появились аппаратные компоненты, такие как процессоры, СБИС, специализированные микроконтроллеры и т.д., отечественной разработки от ведущих производителей АО «МЦСТ» [13, с. 108-110], АО НПЦ «ЭЛВИС», АО «Байкал Электроникс». Однако их номенклатура, характеристики и объемы производства в настоящее время не позволяют в полной мере заместить аппаратные компоненты импортного производства – особенно в специализированых изделиях, которые используются в жестких условиях эксплуатации.

Таким образом, вопрос доверия к аппаратно-программным платформам иностранного производства в части предотвращения компьютерных атак на ПО BIOS является в настоящее время одним из приоритетных вопросов для обеспечения безопасности информации [14].

Выявление проблем при создании доверенной аппаратно-программной платформы

Под доверенной аппаратно-программной платформой (ДАПП) будем понимать совокупность аппаратно-программных средств и коммуникационных ресурсов, для которых однозначно определены состав, архитектура, алгоритмы функционирования, условия применения, правила обработки информации, проведены исследования на соответствие требованиям по безопасности информации в объеме, согласованном с регулятором, и получены соответствующие разрешительные документы на программные компоненты, в том числе на микропрограммное обеспечение.

В общем случае для обеспечения возможности соответствия необходимому уровню доверия и соответствия предъявляемым требованиям по безопасности

DOI:10.21681/2311-3456-2021-6-68-77

Таблица 1

Актуальные уязвимости в ПО BIOS

Наименование уязвимости	Описание уязвимости	Идентификатор уязвимости
Множественные уязвимости подсистемы Intel Management Engine (ME) микропрограммного обеспечения семейства микросхем Platform Controller Hub, позволяющие выполнить неподписанный код	Множественные уязвимости подсистемы Intel Management Engine (ME) микропрограммного обеспечения семейства микросхем Platform Controller Hub (PCH), выполняющих роль южного моста, вызваны переполнением буфера. Эксплуатация уязвимостей может позволить нарушителю выполнить неподписанный код	CVE-2017-5705
Множественные уязвимости подсистемы Intel Management Engine (ME) микропрограммного обеспечения семейства микросхем Platform Controller Hub, позволяющие нарушителю повысить свои привилегии	Множественные уязвимости подсистемы Intel Management Engine (ME) микропрограммного обеспечения семейства микросхем Platform Controller Hub (PCH), выполняющих роль южного моста, вызваны переполнением буфера, связана с недостатками разграничения доступа. Эксплуатация уязвимостей позволит нарушителю повысить свои привилегии	CVE-2017-5708
Множественные уязвимости подсистем Active Management Technology (AMT) и Intel Management Engine (ME) микропрограммного обеспечения семейства микросхем Platform Controller Hub, позволяющие выполнить произвольный код	Множественные уязвимости подсистем Active Management Technology (AMT) и Intel Management Engine (ME) микропрограммного обеспечения семейства микросхем Platform Controller Hub (PCH), выполняющих роль южного моста, вызваны переполнением буфера. Эксплуатация уязвимостей может позволить нарушителю, действующему удаленно с привилегиями администратора, выполнить произвольный код с привилегиями AMT	CVE-2017-5712
Уязвимость реализации технологии Intel Active Management Technology микропрограммного обеспечения Intel Converged Security and Manageability Engine и Intel Management Engine, позволяющая нарушителю вызвать отказ в обслуживании	Уязвимость реализации технологии Intel Active Management Technology (AMT) микропрограммного обеспечения Intel Converged Security and Manageability Engine (CSME) и Intel Management Engine (ME) вызвана ошибками при обработке объектов памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании	CVE-2018-3658, INTEL-SA-00141
Уязвимость реализации протокола TLS подсистемы Intel Active Management Technology (AMT) микропрограммного обеспечения Intel Converged Security and Manageability Engine и Intel Management Engine, позволяющая нарушителю получить ключ сеанса TLS	Уязвимость реализации протокола TLS подсистемы Intel Active Management Technology (AMT) микропрограммного обеспечения Intel Converged Security and Manageability Engine и Intel Management Engine вызвана несоблюдением мер безопасности стандарта TLS. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить ключ сеанса TLS	CVE-2018-3616, INTEL-SA-00141

Наименование уязвимости	Описание уязвимости	Идентификатор уязвимости
Уязвимость микропрограммного обеспечения Intel Converged Security and Manageability Engine (CSME), Intel Server Platform Services (SPS) и Intel Trusted Execution Engine (TXE), вызванная ошибками управления привилегиями, позволяющая нарушителю раскрыть или модифицировать защищаемую информацию	Уязвимость микропрограммного обеспечения Intel CSME, Intel SPS и Intel TXE вызвана ошибками управления привилегиями. Эксплуатация уязвимости может позволить нарушителю раскрыть или модифицировать защищаемую информацию	CVE-2018-3655, INTEL-SA-00125
Уязвимость микропрограммного обеспечения Intel Converged Security and Manageability Engine и Intel Trusted Execution Engine, связанная с недостаточной проверкой вводимых данных, позволяющая нарушителю получить доступ к защищаемой информации	Уязвимость микропрограммного обеспечения Intel Converged Security and Manageability Engine (CSME) и Intel Trusted Execution Engine (TXE) связана с недостаточной проверкой вводимых данных. Эксплуатация уязвимости может позволить нарушителю получить доступ к защищаемой информации	CVE-2018-12189
Уязвимость web-сервера модуля, реализующего технологию удалённого управления компьютером Intel Active Management Technology, позволяющая нарушителю получить доступ к устройству	Уязвимость web-сервера модуля, реализующего технологию удалённого управления компьютером Intel Active Management Technology, связана с недостатками процедуры аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к устройству путём отправки специально сформированных HTTP-запросов	BID ID:98269, CVE-2017-5689, INTEL-SA-00075, LEN-14963, Siemens Security ID:874235
Уязвимость установщика микропрограммного обеспечения Intel Converged Security and Manageability Engine и Intel Trusted Execution Engine, связанная с неверным управлением генерацией кода, позволяющая нарушителю повысить свои привилегии	Уязвимость установщика микропрограммного обеспечения Intel Converged Security and Manageability Engine и Intel Trusted Execution Engine связана с неверным управлением генерацией кода. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии	CVE-2019-0091
Уязвимость микропрограммного обеспечения Intel Converged Security and Manageability Engine и Intel Trusted Execution Engine, связанная с недостатками разграничения доступа, позволяющая нарушителю повысить свои привилегии	Уязвимость микропрограммного обеспечения Intel Converged Security and Manageability Engine и Intel Trusted Execution Engine связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии	CVE-2019-0098
Уязвимость микропрограммного обеспечения Intel Converged Security and Manageability Engine (CSME) и Intel Trusted Execution Engine (TXE), связанная с недостаточной проверкой входных данных, позволяющая нарушителю раскрыть защищаемую информацию	Уязвимость микропрограммного обеспечения Intel Converged Security and Manageability Engine (CSME) и Intel Trusted Execution Engine (TXE) связана с недостаточной проверкой входных данных. Эксплуатация уязвимости может позволить нарушителю раскрыть защищаемую информацию	CVE-2019-0168

Наименование уязвимости	Описание уязвимости	Идентификатор уязвимости
Уязвимость микропрограммного обеспечения Intel Converged Security and Manageability Engine (CSME) и Intel Trusted Execution Engine (TXE), связанная с переполнением буфера в динамической памяти, позволяющая нарушителю раскрыть защищаемую информацию, вызвать отказ в обслуживании или повысить свои привилегии	Уязвимость микропрограммного обеспечения Intel Converged Security and Manageability Engine (CSME) и Intel Trusted Execution Engine (TXE) связана с переполнением буфера в динамической памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, раскрыть защищаемую информацию, вызвать отказ в обслуживании или повысить свои привилегии	CVE-2019-0169

информации для средств вычислительной техники, применяемых в специальных автоматизированных системах, необходимо обеспечить выполнение следующих обязательных условий:

1. Обеспечить гарантию проектирования и наличие конструкторской документации на аппаратную платформу.
2. Обеспечить наличие исходного кода, программной документации и отсутствие опасных функциональных возможностей в микропрограммном обеспечении аппаратной платформы.
3. Обеспечить применение сертифицированных по требованиям безопасности информации общесистемного, прикладного и специального программного обеспечения по соответствующему уровню контроля отсутствия недекларированных возможностей.
4. Обеспечить применение сертифицированных аппаратно-программных или программных средств защиты информации и средств антивирусной защиты для обеспечения невозможности работы несанкционированных пользователей и замкнутости программной среды.

При этом на объекте применения средств вычислительной техники необходимо обеспечить наличие конструктивных средств защиты от несанкционированного доступа к внутренним цепям, аппаратному обеспечению и внешним разъемам, реализовать организационно-режимные и технические меры защиты, а также сформировать и применить регламент настройки и тестирования работоспособности и корректности работы используемых механизмов и средств защиты.

Выполнение указанных условий позволит создавать средства вычислительной техники (далее – изделия), отвечающие требованиям нормативно-правовых актов и руководящих документов по защите информации, и обеспечивающие необходимый уровень доверия к ним.

Так как в данной работе рассматривается вопрос противодействия компьютерным атакам на ПО BIOS аппаратно-программных платформ, то далее рассматривается возможность выполнения первых двух обязательных условий, а именно: гарантия проектирования, наличие конструкторской документации на аппаратную платформу и наличие исходного кода на микропрограммное обеспечение аппаратной платформы, в котором должны отсутствовать опасные функциональные возможности.

Учитывая распространенность, доступность, оптимальные технические характеристики и себестоимость аппаратных платформ на базе системной логики фирмы Intel, в большинстве случаев для создания средств вычислительной техники выбираются аппаратные платформы на базе системной логики именно этой фирмы.

Ниже описан подход, позволяющий повысить уровень доверия к аппаратно-программной платформе на базе системной логики фирмы Intel, применяемой для построения средств вычислительной техники, обрабатывающих информацию ограниченного доступа, а также выполняющих функции защиты информации.

Для ДАПП однозначно должны выполняться следующие условия:

А) Гарантия проектирования и наличие конструкторской документациина аппаратную платформу

Для выполнения данного условия необходимо подтвердить, что аппаратная платформа выпускается на территории РФ, и на нее имеется необходимая конструкторская и эксплуатационная документация, содержащая сведения о ее составе, условиях эксплуатации, ограничениях по применению.

Учитывая тот факт, что на российском рынке присутствуют аппаратные платформы отечественного производителя ЗАО «НПФ «Доломант», АО «Миландр», АО «НПК «Атроник» и др., которые могут быть применены в ДАПП, то обеспечить выполнение данного условия возможно в полном объеме.

В) Наличие исходного кода, программной документации и гарантированное отсутствие опасных функциональных возможностей в микропрограммном обеспечении аппаратной платформы

Для выполнения данного условия необходимо представить исходный код и программную документацию на микропрограммное обеспечение аппаратной платформы в объеме, достаточном для проведения соответствующих исследований, и при необходимости обеспечить доработку микропрограммного обеспечения, позволяющую гарантировать отсутствие опасных функциональных возможностей и уязвимостей в указанном программном обеспечении.

Учитывая тот факт, что для аппаратных платформ фирмы Intel микропрограммное обеспечение

Рис. 1. Компьютерный модуль CPC1311

(ПО BIOS) разрабатывается зарубежными компаниями и отечественные аналоги на российском рынке отсутствуют, получить исходный код и программную документацию на микропрограммное обеспечение, а при необходимости его доработать на настоящее время является крайне трудоемкой задачей и в большинстве случаев невыполнимой.

Исходя из изложенного сделан вывод, что основной проблемой при создании ДАПП на базе системной логики фирмы Intel является получение ПО BIOS в исходных кодах и программной документации на него, достаточной для обеспечения возможности проведения соответствующих испытаний по требованиям безопасности информации, и оперативного исключения из ПО BIOS опасных функциональных возможностей и уязвимостей для предупреждения возможных компьютерных атак, направленных на эксплуатацию данных уязвимостей.

Описание решения проблем

С целью определения возможности решения данной проблемы ведущими специалистами ПФ АО «НТЦ «Атлас» был проведены исследования, включающие:

- выбор аппаратной платформы для ДАПП;
- замещение ПО BIOS на программное обеспечение загрузчика операционной системы собственной разработки (ПО ЗОС), включающее программу начальной инициализации и конфигурации аппаратного обеспечения, для выбранной аппаратной платформы;
- проведение функционального тестирования выбранной аппаратной платформы с ПО ЗОС;
- определение возможности серийного производства и поставок выбранной аппаратной платформы с ПО ЗОС.

По итогам проведения указанных инициативных работ были получены следующие результаты:

1. Выбран компьютерный модуль CPC1311. В связи с тем, что процесс разработки ПО ЗОС и организация производства аппаратной платформы занимает достаточно длительное время – от одного до двух лет, одним из основных критериев при выборе аппаратной платформы для ДАПП является срок жизни аппаратных компонент (EOL). С учетом данного критерия в качестве базового модуля для аппаратной платформы выбран компьютерный модуль CPC1311 с EOL до 2030 г.

Компьютерный 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 жестких условиях окружающей среды.

Модуль CPC1311 построен на базе индустриального исполнения многоядерного процессора Intel Atom семейства BayTrail с 64-разрядной архитектурой. Отличительными особенностями 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 ГБ оперативной памяти DDR3L с поддержкой ECC и твердотельного диска 8 ГБ позволяет использовать изделие в качестве самодостаточного встраиваемого компьютера, способного решать большинство прикладных задач[5].

5 CPC1311 – Компьютерный модуль стандарта COM Express mini, Type 10, на базе процессоров Intel Atom E38xx. [Электронный ресурс] // URL: https://www.fastwel.ru/products/vstraivaemye-sistemy/kompiuternye-moduli/kompyuternyy-modul-standarta-som-express-mini-type-10-na-baze-pretsessorov-intel-atom-e38xx_506710_287/ (дата обращения: 20.06.2021).

DOI:10.21681/2311-3456-2021-6-68-77

Мультимедийные возможности СРС1311 включают в себя видеоконтроллер с интерфейсом LVDS (разрешение до 2560×1600 пикселей) и современный аудио кодек класса HD. Встроенные в процессор функции декодирования видео позволяют применять модуль в системах, связанных с обработкой мультимедийных потоков.

Через разъемы высокой плотности разработчикам доступен большой арсенал высокоскоростных интерфейсов: 1xGbEthernet, 5xUSB 2.0, 1xUSB 3.0, 2xSATA II, 3xPCIex1 (дополнительно одна линия PCIe может быть получена вместо GbEthernet). Из дополнительных возможностей следует отметить встроенную поддержку шины CAN 2.0, востребованную в системах реального времени, прежде всего на транспорте.

Все компоненты СРС1311 напаяны на плату, что обеспечивает высокую стойкость изделия к ударным и вибрационным нагрузкам. По заказу модуль поставляется с влагозащитным покрытием. Диапазон рабочих температур СРС1311 от -40 °С до +85 °С.

Компьютерный модуль СРС1311 по надежности, производительности и возможности его применения в жестких условиях эксплуатации в полной мере подходит для построения на его базе изделий, реализующих функции доверенного управления СКЗИ и межсетевого экранирования.

2. Для компьютерного модуля СРС1311 выполнено замещение ПО BIOS, разработанного иностранной компанией American Megatrends, на отечественное программное обеспечение загрузчика операционных систем Горизонт ЦИАТ.00169-01 (ПО ЗОС) [15], разработанное ПФ АО НТЦ «Атлас», включающее программу начальной инициализации и конфигурации и тестирования аппаратного обеспечения модуля.

Для защиты от несанкционированного доступа и выявления неисправностей аппаратного обеспечения в ПО ЗОС были реализованы следующие функциональные возможности:

- предпусковой контроль аппаратного обеспечения. При предпусковом контроле проверяются флаги, условные переходы, арифметические операции процессора и работоспособность оперативной памяти (адресная шина, шина данных и ячейки памяти). При выявлении ошибок происходит блокировка работы и на дисплей выводится сообщение об ошибке. Ошибки предпускового контроля, обычно, означают неисправность компьютерного модуля;
- контроль целостности. По завершении предпускового контроля происходит автоматический подсчет контрольной суммы ПО ЗОС и автоматическая проверка рассчитанной контрольной суммы с эталонной контрольной суммой, хранящейся в прошивке ПО ЗОС. Рассчитанное значение контрольной суммы ПО ЗОС выводится на экран для проверки оператором. В случае возникновения ошибки при проведении контроля целостности происходит блокировка работы. Контроль целостности выполняется для всех регионов SPI Flash накопителя, в которых расположены исполняемый код и статичные данные;
- запрет на программную перезапись ПО ЗОС. Запрет выполнен при помощи конфигурации дескриптора Intel Firmware Descriptor, указывающей SPI контролеру, что чтение и запись, выполняемое с помощью какого-либо программного обеспечения, в регионе, где находится ПО ЗОС, запрещены, за исключением самого ПО ЗОС. Это позволяет ПО ЗОС использовать SPI Flash накопитель для хранения различной информации, например, параметров конфигурации. Дополнительно можно запретить перезапись ПО ЗОС на аппаратном уровне, согласно техническим требованиям изготовителя микросхемы (в случае, если данный режим поддерживается микросхемой);
- надежное хранение параметров конфигурации ПО ЗОС. Надежное хранение обеспечивается за счет расчета контрольной суммы на параметры конфигурации и запрета на чтение и запись региона SPI флеш-памяти, в котором хранятся параметры конфигурации, для всего программного обеспечения, кроме самого ПО ЗОС. После выполнения контроля целостности ПО ЗОС происходит расчет контрольной суммы на параметры конфигурации и последующее сравнение с последним сохраненным значением. В случае их несовпадения, на экран выводится соответствующее сообщение и требуется участие оператора для входа в меню конфигурации и их установки параметров конфигурации;
- ограничение доступа к меню конфигурации аппаратного обеспечения модуля. Ограничение накладывается посредством пароля, допустимая длина которого строго задана и составляет 8 знаков, поддерживаются буквы латинского алфавита (A-z), арабские цифры (0-9), специальные символы, строчные и заглавные буквы. Пароль сохраняется в виде свертки и записывается в регион параметров конфигурации. При необходимости, можно установить запрет доступа к меню настроек после их установки путем включения соответствующей опции в меню конфигурации;
- загрузка только с выбранного оператором носителя информации. В качестве загрузочного устройства допускается выбор USB Flash накопитель, жесткий диск или привод CD\DVD дисков. Выбор выполняется в меню конфигурации и в момент выбора происходит генерация контрольной суммы, используя уникальное ID устройства, которая записывается в регион SPI флеш-памяти, в котором хранятся параметры конфигурации. В процессе загрузки происходит расчет контрольной суммы для каждого устройства, присутствующего в системе, которые доступны для использования в качестве загрузочного устройства, с последующем сравнением с сохраненной контрольной суммой выбранного ранее устройства. При не обнаружении выбранного носителя происходит блокировка работы;
- монитор состояния аппаратных компонентов компьютерного модуля. Монитор реализован отдельным пунктом в меню конфигурации, в котором можно отслеживать доступные показатели напряжения питания и температуры компонентов, которые собирается с установленных на компьютерном модуле

датчиков. В случае превышения пороговых значений соответствующее сообщение выводится на экран.

3. В ПО ЗОС исключены потенциально опасные функциональные возможности встроенного в центральный процессор микроконтроллера Intel Managment Engine (Intel ME), эксплуатация которых может привести или создать условия для нарушения заданных характеристик безопасности обрабатываемой информации, путем полного исключения ПО IME из прошивки ЗОС.

4. Разработана программа функционального тестирования и проведено тестирование ПО ЗОС для компьютерного модуля СРС1311. Компьютерный модуль СРС1311 с ПО ЗОС реализует начальную инициализацию, конфигурацию и тестирование аппаратной платформы модуля, обеспечивает загрузку операционных систем российской разработки, таких как ЗОСРВ «Нейтрино», ДОС РВ «ТрастОС» и ОС «Astra Linux».

5. Разработана программная документация на ПО ЗОС, по составу и содержанию обеспечивающая возможность сопровождения проектов, в которых будет использоваться СРС1311 с ПО ЗОС, и проведения соответствующих испытаний по требованиям безопасности информации.

6. Определена возможность постановки серийного производства и поставок компьютерных модулей СРС1311 с ПО ЗОС с приемкой ОТК и с 5-ой приемкой.

7. Получен необходимый опыт, методическое и технологическое обеспечение при разработке и отладке ПО ЗОС для компьютерного модуля СРС1311, позволяющие существенно ускорить разработку ПО ЗОС для аппаратных платформ с меньшим EOL (5-7 лет).

8. На ПО ЗОС Горизонт ЦИАТ.00169-01 получен сертификат соответствия по требованиям безопасности информации МО РФ от 10.02.2021 г. №5196 по 2-му уровню контроля отсутствия недекларированных возможностей и по соответствию реальных и декларируемых в документации функциональных возможностей.

Выводы

В ходе проведения исследовательской работы был сформирован подход по созданию доверенной аппаратно-программной платформы на базе системной логики фирмы Intel, реализующей защиту от компьютерных атак на уровне ПО BIOS.

Данный подход был успешно применен ПФ АО «НТЦ «Атлас» при создании блока вычислительного БВ001 ЦИАТ.467444.251 на базе компьютерного модуля СРС1311 с загрузчиком операционных систем Горизонт ЦИАТ.00169-01, имеющим сертификат соответствия по требованиям безопасности информации МО РФ от 10.02.2021 г. №5196 по 2-му уровню контроля отсутствия недекларированных возможностей и по соответствию реальных и декларируемых в документации функциональных возможностей.

Также установлено, что данный подход может быть в полной мере применен и для аппаратно-программных платформ отечественного производства. На настоящее время ведущими специалистами ПФ АО «НТЦ «Атлас» ведутся работы по дальнейшему развитую ПО ЗОС Горизонт и созданию доверенных аппаратно-программных платформ на базе процессорных модулей с процессорами АО «МЦСТ» (Эльбрус 2С3) и АО НПЦ «ЭЛВИС» (1892ВА018).

Таким образом, полученные результаты в рамках работ позволяют сделать вывод о возможности создания доверенной аппаратно-программной платформы на базе аппаратных компонент иностранного и отечественного производства для её применения в специализированных изделиях и средствах вычислительной техники, соответствующей требованиями по безопасности информации и неподверженную компьютерным атакам с использованием уязвимостей в ПО BIOS.

Рецензент: *Цирлов Валентин Леонидович, кандидат технических наук, доцент кафедры ИУ-8 «Информационная безопасность» МГТУ им.Н.Э.Баумана, г. Москва, Россия. E-mail: v.tsirlov@bmstu.ru*

Литература

1. Авезова Я.Э., Фадин А.А., Вопросы обеспечения доверенной загрузки в физических и виртуальных средах // Вопросы кибербезопасности. 2016. №1. С. 24-30. DOI:10.21681/2311-3456-2016-1-24-30
2. Лыдин С.С. О средствах доверенной загрузки для аппаратных платформ с UEFI BIOS // Вопросы защиты информации. 2016. №3. С. 45-50.
3. Чекин Р.Н. Современные угрозы безопасности обработки информации со стороны встроенного программного обеспечения // Доклады Томского государственного университета систем управления и радиоэлектроники. 2016. №1. С. 54-55.
4. Маркин Д.О., Умбетов Т.К., Архипов М.А., Миначев В.М. Современные технологии построения доверенных сред исполнения приложений на уровне базовой системы ввода-вывода // сборник статей по итогам Международной научно-практической конференции «Безопасные информационные технологии», 2019. С. 282-284.
5. Оголюк А.А., Шабалин А.В. Анализ безопасности удаленного доступа средствами Intel Management Engine // Известия высших учебных заведений. Приборостроение. 2018. Т. 61. №1. С. 41-46.
6. I.D. Pankov, A.S. Konoplev and A.Yu. Chernov Analysis of the Security of UEFI BIOS Embedded Software in Modern Intel-Based Computers // Automatic Control and Computer Sciences. 2019, Vol. 53. No 8. Pp. 865–869.
7. Чернов А.Ю., Коноплев А.С. Задача построения доверенной вычислительной среды на аппаратной платформе Intel // Проблемы информационной безопасности. Компьютерные системы. 2016. №4. С. 36-41.

8. M. Ermolov, M. Goryachy. How to Hack a Turned-off Computer, or Running Unsigned Code in Intel ME. [Электронный ресурс] // Positive Technologies - learn and secure. URL: http://blog.ptsecurity.com/2018/01/running-unsigned-code-in-intel-me.html. (дата обращения: 16.07.2021).
9. Rauchberger J., Luh. R., Schrittwieser S. Longkit – A Universal Framework for BIOS/UEFI Rootkits in System Management Mode // Proceedings of the 3rd International Conference on Information Systems Security and Privacy. 2017. Pp. 346-353.
10. Гефнер И.С., Марков А.С. Механизмы реализации атак на уровне базовой системы ввода/вывода // Защита информации. Инсайд. 2017. № 5. С. 80-83.
11. Kostromin K., Dokuchaev B., Kozlov D. Analysis of the Most Common Software and Hardware Vulnerabilities in Microprocessor Systems // 2020 International Russian Automation Conference (RusAutoCon). 2020. Pp 1031-1036.
12. A. Ogolyuk, A. Sheglov, K. Sheglov. UEFI BIOS and Intel Management Engine Attack Vectors and Vulnerabilities // Proceding of the 20th Conference of Fruct Association. 2017. Pp. 657-662.
13. Беззубов А.Ф., Синицын И.В., Применение вычислительных систем отечественного производства как средство повышения информационной безопасности ВУЗа // Вестник российской таможенной академии. 2017. №2. С. 106-110.
14. Алексеев Д.М., Иваненко К.Н., Убирайло В.Н. Доверенная загрузка как механизм информационной безопасности // Влияние науки на инновационное развитие. 2017. С. 19-20.
15. Боровиков А.Ю., Новиков К.Б., Маслов О.А. Описание подхода программной реализации модуля доверенной загрузки операционной системы // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 1. С. 43–48.

INCREASING HARDWARE-SOFTWARE PLATFORMS TRUST LEVELS TO PREVENT EXPLOITING BIOS VULNERABILITIES

Borovikov A.Y.[6], Maslov O.A.[7], Mordvinov S.A.[8], Esafiev A.A.[9]

Abstract: *in this publicaton, a technique to increase trust levels of foreign and domestic-made hardware-software platforms, which are used to create specialised devices and computing facilities, which are meeting safety requirements and protected from BIOS vulnerabilities, to work with classified information, was made. Problems, which developer might encounter, were listed; methods of troubleshooting were proposed, and conclusions were made.*

The purpose of research is *to investigate an ability of designing trusted foreign and domestic-made hardware-software platforms, protected from exploiting BIOS vulnerabilities.*

Research methods: *in order to achieve the purpose of research, an analysis of Russian's industrial-grade PC modules was made in order to choose PC module that will be used for designing trusted hardware-software platform, an analysis of known BIOS vulnerabilities was made; proprietary BIOS replacement in a form of domestic-made Horizon bootloader, which includes unauthorised access to information protection measures, was made and possibilty of practical use of trusted hardware-software platform with Horizon bootloader was overviewed.*

Obtained result: *PC module for trusted hardware-software platform was selected, proprietary BIOS replacement in a form of domestic-made Horizon bootloader, which includes unauthorized access to information protection measures, was made; technique to increase trust levels of foreign and domestic-made hardware-software platforms, which are used to create specialized devices and computing facilities, which are meeting safety requirements and protected from BIOS vulnerabilities, to work with classified information, was made; an approach to create trusted hardware-software platform design requirements and conditions was made; needs to exclude potentially dangerous Intel Management Engine controller's functionality were justified and proposal to use trusted hardware-software platform with Horizon bootloader was made.*

Keywords: *cybersecurity, import substitution, trusted boot, trusted hardware-software platform, BIOS, Horizon bootloader, Intel Management Engine, specialised devices, computing facilities, unauthorised access to information, computer attacks, vulnerabilities.*

6 Aleksey Borovikov, deputy head of specialized department 6 of SSTS in Science and Technology Center "Atlas", Penza, Russia. E-mail: alexey_bau@mail.ru

7 Oleg Maslov, head of specialized department 6 of SSTS in Science and Technology Center "Atlas", Penza, Russia. E-mail: oa_de_ao@mail.ru

8 Stepan Mordvinov, engineer of specialized department 6 of SSTS in Science and Technology Center "Atlas", Penza, Russia. E-mail: zoi.kun@mail.ru

9 Andrei Esafiev, researcher of specialized department 6 of SSTS in Science and Technology Center "Atlas", Penza, Russia. E-mail: peterpozinsky@ya.ru

References

1. Avezova Ya.E., Fadin A.A., Voprosy obespecheniya doverennoi zagruzki v fizicheskih i virtualnyh sredah // Voprosy kiberbezopastnosti. 2016. №1. S. 24-30. DOI:10.21681/2311-3456-2016-1-24-30
2. Lydin S.S. O sredstvah doverennoi zagruzki dlya apparatnyh platform s UEFI BIOS // Voprosy zashity informacii. 2016. №3. S. 45-50.
3. Chekin R.N. Sovremennye ugrozy bezopastnosti obrabotki informacii so storony vstroennogo programnogo obespecheniya // Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki. 2016. №1. S. 54-55.
4. Markin D.O., Umbetov T.K., Arhipov M.A., Minachev V.M. Sovremennye tehnologii postroeniya doverennyh sred ispolneniya prilozhenii na urovne bazovoi sistemy vvoda-vyvoda // sbornik statei po itogam Mezhdunarodnoi nauchno-prakticheskoi konferencii «Bezopastnye informacionnye tehnologii», 2019. S. 282-284.
5. Ogoluk A.A., Shabalin A.V. Analiz bezopastnosti udalennogo dostupa sredstvami Intel Management Engine // Izvestiya vyshih uchebnyh zavedenii. Priborostroenie. 2018. T. 61. №1.
6. I. Pankova, A. Konopleva, and A.. Chernov. Analysis of the Security of UEFI BIOS Embedded Software in Modern Intel-Based Computers // Automatic Control and Computer Sciences, 2019, Vol. 53, No. 8, pp. 865–869.
7. Chernov A.Yu., Konoplev A.S. Zadacha postroeniya doverennoi vychislitelnoi sredy na apparatnoi platforme Intel // Problemy informacionnoi bezopastnosti. Kompyuternye sistemy. 2016. №4. S. 36-41.
8. M. Ermolov, M. Goryachy. How to Hack a Turned-off Computer, or Running Unsigned Code in Intel ME. // Positive Technologies - learn and secure. URL: http://blog.ptsecurity.com/2018/01/running-unsigned-code-in-intel-me.html.
9. (Accessed: 16.07.2021).
10. Rauchberger J., Luh. R., Schrittwieser S. Longkit – A Universal Framework for BIOS/UEFI Rootkits in System Management Mode // Proceedings of the 3rd International Conference on Information Systems Security and Privacy. 2017. pp. 346-353.
11. Gefner I.S., Markov A.S. Mehanizmy realizacii atak na urovne bazovoi sistemy vvoda/vyvoda // Zashita informacii. Insaid. 2017. № 5. S. 80-83.
12. Kostromin K., Dokuchaev B., Kozlov D. Analysis of the Most Common Software and Hardware Vulnerabilities in Microprocessor Systems. // 2020 International Russian Automation Conference (RusAutoCon). 2020. pp 1031-1036.
13. A. Ogolyuk, A. Sheglov, K. Sheglov. UEFI BIOS and Intel Management Engine Attack Vectors and Vulnerabilities // Proceding of the 20th Conference of Fruct Association. 2017. pp 657-662.
14. Bezzubov A.F., Sinitsiyn I.V., Primenenie vichislitelnikh sistem otechestvennogo proizvodstva kak sredstvo povisheniya informacionnoy bezopasnosty VUZa // Vestnik rossiyskoy tamojennoy akademii. 2017. №2. S. 106-110
15. Alekseev D.M., Ivanenko K.N., Ubirailo V.N. Doverennaya zagruzka kak mehanizm informacionnoi bezopastnosti // Vliyanie nauki na innovacionnoe razvitie. 2017. S. 19-20.
16. Borovikov A.Yu., Novikov K.B., Maslov O.A. Opisanie podhoda programnoi realizacii modulya doverennoi zagruzki operacionnoi sistemy // Naukoemkie tehnologii v kosmicheskih issledovaniyah Zemli. 2019. T. 11. No 1. S. 43–48.