Алексей Ю. Боровиков[1], Олег А. Маслов[2], Степан А. Мордвинов[3], Андрей А. Есафьев[4]
Пензенский филиал АО «Научно-технический центр «Атлас»,
пр-кт Победы, 69, Пенза, 440028, Россия
[1]e-mail: alexey_bau@mail.ru, https://orcid.org/0000-0002-3595-2533
[2]e-mail: oa_de_ao@mail.ru, https://orcid.org/0000-0003-2978-725X
[3]e-mail: zoi.kun@mail.ru, https://orcid.org/0000-0003-0253-8456
[4]e-mail: peterpozinsky@ya.ru, https://orcid.org/0000-0003-1256-9061

СПОСОБ СОЗДАНИЯ ДОВЕРЕННОЙ АППАРАТНО-ПРОГРАММНОЙ ПЛАТФОРМЫ ДЛЯ ПРИМЕНЕНИЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

DOI: http://dx.doi.org/10.26583/bit.2021.4.08

Аннотация. В статье представлен способ по созданию доверенной аппаратно-программной платформы на электронной компонентной базе иностранного производства, предназначенной для построения специализированных изделий и средств вычислительной техники, обрабатывающих информацию ограниченного доступа. Данная платформа соответствует требованиями по безопасности информации и не подвержена компьютерным атакам с использованием уязвимостей в программном обеспечении (ПО) BIOS. **Цель:** исследование возможности создания доверенной аппаратно-программной платформы на электронной компонентной базе иностранного 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 иностранного ПО BIOS процессорного модуля на ПО отечественной разработки «Загрузчик операционных систем Горизонт» (ЗОС Горизонт), реализующее функции ПО BIOS и меры защиты от несанкционированного доступа, и рассмотрена возможность практического применения доверенной аппаратно-программной платформы с ЗОС Горизонт. **Полученный результат:** выбран процессорный модуль для создания доверенной аппаратно-программной платформы, проведено замещение иностранного ПО BIOS процессорного модуля на ПО отечественной разработки ЗОС Горизонт, реализующее функции ПО BIOS и меры защиты от несанкционированного доступа, обеспечено повышение уровня доверия к аппаратно-программным платформам на электронной компонентной базе иностранного производства, предназначенным для построения специализированых изделий и средств вычислительной техники, обрабатывающих информацию ограниченного доступа, сформированы требования к доверенной аппаратно-программной платформе и условия их выполнения, обоснована необходимость исключения потенциально опасных функциональных возможностей ПО микроконтроллера Intel Management Engine аппаратно-программной платформы на электронной компонентой базе иностранного производства и сформированы предложения по практическому применению доверенной аппаратно-программной платформы с ЗОС Горизонт.

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

Для цитирования: БОРОВИКОВ, Алексей Ю. и др. СПОСОБ СОЗДАНИЯ ДОВЕРЕННОЙ АППАРАТНО-ПРОГРАММНОЙ ПЛАТФОРМЫ ДЛЯ ПРИМЕНЕНИЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ. Безопасность информационных технологий, [S.l.], т. 28, №. 4, с. 104–117, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1380. DOI: http://dx.doi.org/10.26583/bit.2021.4.08.

Alexey Y. Borovikov[1], Oleg A. Maslov[2], Stepan A. Mordvinov[3], Andrey A. Esafiev[4]
Penza Branch of Atlas Scientific and Technical Center JSC,
69 Pobedy Avenue, Penza, 440028, Russia.
[1]e-mail: alexey_bau@mail.ru, https://orcid.org/0000-0002-3595-2533
[2]e-mail: oa_de_ao@mail.ru, https://orcid.org/0000-0003-2978-725X
[3]e-mail: zoi.kun@mail.ru, https://orcid.org/0000-0003-0253-8456
[4]e-mail: peterpozinsky@ya.ru, https://orcid.org/0000-0003-1256-9061

The Method for creating a trusted hardware-software platform for its application in special purpose information systems

DOI: http://dx.doi.org/10.26583/bit.2021.4.08

Abstract. The paper presents a method to increase trust levels of foreign and domestic-made hardware-software platforms, designed to build specialised devices and computing facilities, which are meeting safety requirements and protected from BIOS vulnerabilities, to work with classified information. **The purpose of the study is** to investigate the ability of designing trusted foreign and domestic-made hardware-software platforms, protected from exploiting BIOS vulnerabilities. **Research methods:** in order to choose PC module that will be used for designing trusted hardware-software platform an analysis of Russian industrial-grade PC modules was made. In addition 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 as well as a possibility 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; an increase in the level of trust levels of foreign and domestic-made hardware-software platforms, which are used to create specialized devices and computing facilities while meeting safety requirements and protected from BIOS vulnerabilities to work with classified information has been ensured; an approach to create trusted hardware-software platform design requirements and conditions was proposed; 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 justified.

Keywords: cybersecurity, import substitution, trusted boot, trusted hardware and software platform, BIOS software, Horizon operating system loader, Intel Management Engine, unauthorized access, computer attacks, vulnerabilities.
For citation: BOROVIKOV, Alexey Y. et al. The Method for creating a trusted hardware-software platform for its application in special purpose information systems. IT Security (Russia), [S.l.], v. 28, n. 4, p. 104–117, 2021. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1380. DOI: http://dx.doi.org/10.26583/bit.2021.4.08.

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 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 способ создания доверенной аппаратно-программной платформы на электронной компонентной базе иностранного производства фирмы Intel для создания специализированных изделий и СВТ, неподверженных компьютерным атакам на ПО BIOS.

1. Описание уязвимостей ПО BIOS

Актуальность вопроса по созданию доверенной аппаратно-программной платформы на электронной компонентной базе 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 электронную компонентную базу технологий Intel ME, Intel TXE, Intel ATM, BMC, Intel GE [4].

Технология Intel Management Engine (IME) представляет собой интегрированный в процессор или контроллер периферийных устройств (PCH) специализированный микроконтроллер с функциями, позволяющими работать СВТ в выключенном состоянии и обеспечивающими возможность доступа 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 табл. 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 [7–10].

Указанные уязвимости в настоящее время устранены в новых версиях ПО IME, однако с учетом большого объема бинарного кода IME (4 Мб и более) и невозможности провести полноценные соответствующие исследования в связи с отсутствием исходного кода на ПО IME, 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 при эксплуатации СВТ, построенных 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, требуемый для проведения соответствующих исследований с целью обеспечения заданного уровня доверия к указанным платформам.

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	Уязвимости 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	Уязвимости 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	Уязвимости 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 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 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 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 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 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 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 связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии	CVE-2019-0098

Наименование уязвимости	**Описание уязвимости**	**Идентификатор уязвимости**
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 связана с недостаточной проверкой входных данных. Эксплуатация уязвимости может позволить нарушителю раскрыть защищаемую информацию	CVE-2019-0168
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 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

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», АО «ПКК Миландр». Однако их номенклатура, характеристики и объемы производства в настоящее время не позволяют в полной мере заместить аппаратные компоненты иностранного производства особенно в специализированных изделиях, которые используются в жестких условиях эксплуатации.

Таким образом, вопрос повышения уровня 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].

2. Выявление проблем при создании доверенной аппаратно-программной платформы

Под термином «Доверенная аппаратно-программная платформа» (ДАПП) в данной работе понимается совокупность аппаратно-программных компонент и коммуникационных ресурсов, для которых однозначно определены состав, архитектура, алгоритмы функционирования, условия применения, ограничения на использование, проведены исследования на соответствие требованиям по безопасности информации государственных регуляторов и получены соответствующие разрешительные документы на аппаратно-программное обеспечение, в том числе на встроенное программное обеспечение (ПО BIOS).

В общем случае для ДАПП должны выполняться следующие условия доверия (УД):

1. Наличие проектной, конструкторской и эксплуатационной документации на аппаратную платформу (УД1).

2. Наличие исходного кода, программной документации и обеспечение отсутствия опасных функциональных возможностей во встроенном программном обеспечении аппаратной платформы, реализующем функции базовой системы ввода/вывода (УД2).

3. Применение сертифицированных по требованиям безопасности информации общесистемного, прикладного и специального программного обеспечения по соответствующему уровню контроля отсутствия недекларированных возможностей или уровню доверия (УД3).

4. Применение сертифицированных средств защиты от несанкционированного доступа к информации (аппаратно-программных или программных) и средств антивирусной защиты для обеспечения защищенности и замкнутости программной среды (УД4).

5. Наличие на объекте применения организационно-режимных и технических мер защиты информации и регламента их проверки (УД5).

Способ создания ДАПП на электронной компонентной базе иностранного производства заключается в выполнении всех указанных условий доверия и дальнейшей оценки их качественной и количественной характеристик при проведении испытаний по требованиям информационной безопасности государственных регуляторов с выдачей соответствующих разрешительных документов.

Качественную и количественную характеристики дает специализированная организация (испытательная лаборатория) и подтверждает экспертная организация (орган по сертификации) при проведении экспертизы отчетных материалов для определения соответствия ДАПП требованиям государственных регуляторов по информационной безопасности.

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

Учитывая распространенность, доступность, оптимальные технические характеристики и себестоимость аппаратных платформ на электронной компонентной базе иностранного производства фирмы Intel, в большинстве случаев для создания изделий выбираются аппаратные платформы на базе системной логики именно этой фирмы.

Так как в данной работе основной целью исследований является обеспечение возможности противодействия компьютерным атакам на ПО BIOS аппаратно-программных платформ, то далее рассматривается возможность выполнения УД1 и УД2.

Наличие проектной, конструкторской и эксплуатационной документации на аппаратную платформу. Для выполнения данного условия необходимо обеспечить применение аппаратной платформы, отечественного производства, и наличие проектной, конструкторской и эксплуатационной документации, содержащей сведения о перечне электронной компонентной базы, описание технико-экономических показателей, условий эксплуатации, ограничений по применению и т.д. Для данной аппаратной платформы должны быть проведены специальные проверки электронной компонентной базы и ее сертификационные испытания.

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

Наличие исходного кода, программной документации и обеспечение отсутствия опасных функциональных возможностей во встроенном программном обеспечении аппаратной платформы, реализующем функции базовой системы ввода/вывода. Для выполнения данного условия необходимо обеспечить наличие исходного кода и документации на встроенное программное обеспечение аппаратной платформы в объеме, достаточном для проведения соответствующих исследований по требованиям информационной безопасности государственных регуляторов, и выполнить доработку встроенного программного обеспечения в части реализации мер защиты информации и функций выявления неисправностей, а также исключения опасных функциональных возможностей и уязвимостей.

Учитывая тот факт, что для аппаратных платформ на электронной компонентой базе иностранного производства фирмы Intel встроенное программное обеспечение (ПО BIOS) разрабатывается зарубежными компаниями и отечественные аналоги на российском рынке отсутствуют, получить исходный код и программную документацию на ПО BIOS, а при необходимости его доработать в настоящее время является крайне трудоемкой задачей и в большинстве случаев невыполнимой.

Исходя из изложенного сделан вывод, что основной проблемой при создании ДАПП на электронной компонентной базе 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 исключения из ПО BIOS опасных функциональных возможностей и уязвимостей для предупреждения возможных компьютерных атак, направленных на эксплуатацию данных уязвимостей.

3. Описание решения проблем

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

– выбор аппаратной платформы для ДАПП;

– замещение ПО BIOS на программное обеспечение загрузчика операционной системы собственной разработки (ПО ЗОС Горизонт), включающее программу начальной инициализации и конфигурации аппаратного обеспечения, для выбранной аппаратной платформы;

– проведение функционального тестирования выбранной аппаратной платформы с ЗОС Горизонт;

– определение возможности серийного производства и поставок выбранной аппаратной платформы с ЗОС Горизонт.

По итогам проведения указанных инициативных работ были получены следующие результаты:

1. Выбран модуль процессора СРС1311 (рис. 1). В связи с тем, что процесс разработки ЗОС Горизонт и организация производства аппаратной платформы занимает достаточно длительное время – до 3-х 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 модуль процессора СРС1311 с EOL до 2028 г.

Модуль процессора СРС1311 выполнен в формате Com Express mini (Тип 10). Изделие ориентировано на российских ОЕМ-заказчиков нестандартных вычислителей для использования в системах повышенной ответственности, а также функционирующих в жестких условиях окружающей среды.

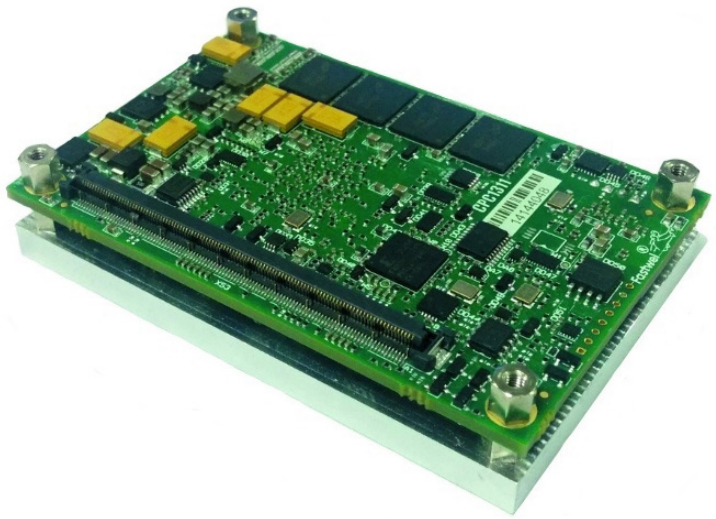

Рис. 1. Модуль процессора CPC1311
Fig. 1. Computer module CPC1311

Модуль процессора 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.

Мультимедийные возможности модуля процессора CPC1311 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 модуля процессора CPC1311 напаяны на плату, что обеспечивает высокую стойкость изделия к ударным и вибрационным нагрузкам. По заказу модуль поставляется с влагозащитным покрытием. Диапазон рабочих температур модуля процессора CPC1311 от -40°C до +85°C.

Модуль процессора CPC1311 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 модуля процессора СРС1311 выполнено замещение ПО BIOS, разработанного иностранной компанией American Megatrends, на отечественное программное обеспечение «Загрузчик операционных систем Горизонт» ЦИАТ.00169-01 [15], разработанное ПФ АО НТЦ «Атлас» и включающее программу начальной инициализации, конфигурации и тестирования аппаратного обеспечения модуля.

3. В ПО ЗОС Горизонт для защиты от несанкционированного доступа и выявления неисправностей аппаратного обеспечения реализованы следующие функциональные возможности:

– предпусковой контроль аппаратного обеспечения. В рамках предпускового контроля проверяются флаги, условные переходы, арифметические операции центрального процессора и работоспособность оперативной памяти (адресная шина, шина данных и ячейки памяти). В случае возникновения ошибки в процессе предпускового контроля происходит блокировка работы и требуется участие администратора безопасности (оператора) для устранения инцидента информационной безопасности;

– контроль целостности ПО ЗОС Горизонт. В рамках контроля целостности выполняется расчет контрольной суммы на исполняемый код и статические данные ПО ЗОС Горизонт и ее сравнение с эталонной контрольной суммой, хранящейся в энергонезависимой памяти. В случае возникновения ошибки при проведении контроля целостности происходит блокировка работы и требуется участие администратора безопасности (оператора) для устранения инцидента информационной безопасности;

– запрет на программную перезапись ПО ЗОС Горизонт. Запрет выполнен при помощи конфигурации дескриптора Intel Firmware Descriptor, указывающей SPI контролеру, что чтение и запись, выполняемое с помощью любого программного обеспечения, в регион SPI флеш-памяти, где находится ПО ЗОС Горизонт, запрещены, за исключением, если к этому региону обращается само ПО ЗОС Горизонт. 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. Надежное хранение параметров конфигурации 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 стороннего программного обеспечения, кроме самого ПО ЗОС Горизонт. После выполнения контроля целостности ПО ЗОС Горизонт происходит расчет контрольной суммы на параметры конфигурации и последующее сравнение с эталонным значением. В случае несовпадения контрольных сумм происходит блокировка работы и требуется участие администратора безопасности (оператора) для устранения инцидента информационной безопасности;

– ограничение доступа к меню конфигурации аппаратного обеспечения. Ограничение реализуется посредством пароля, допустимая длина которого строго задана и составляет 8 знаков, поддерживаются буквы латинского алфавита (A–Z, a-z), арабские цифры (0-9) и специальные символы. Пароль сохраняется в виде свертки и записывается в регион SPI флеш-памяти параметров конфигурации. При необходимости, можно установить программный запрет доступа к меню конфигурации путем установки соответствующей опции в меню;

– загрузка с единственного загрузочного устройства, выбранного администратором безопасности (оператором). В качестве загрузочного устройства допускается выбор USB Flash накопителей, жестких дисков (SATA, EMMC) или приводов CD\DVD дисков. Выбор выполняется в меню конфигурации. При выборе загрузочного

устройства происходит расчет контрольной свертки, используя уникальный идентификатор устройства, которая записывается в регион SPI флеш-памяти с параметрами конфигурации. В процессе загрузки происходит расчет контрольной свертки для каждого устройства, подключенного к аппаратной платформе, которые доступны для использования в качестве загрузочного устройства, с последующим сравнением с сохраненной контрольной сверткой выбранного устройства. При совпадении контрольной свертки происходит загрузка с выбранного устройства. В случае несовпадения контрольной свертки происходит блокировка работы и требуется участие администратора безопасности (оператора) для устранения инцидента информационной безопасности;

– восстановление начальной конфигурации. Восстановление начальной конфигурации реализуется по внешнему сигналу. В процессе загрузки определяется наличие внешнего сигнала и осуществляется сброс конфигурации в начальное состояние;

– диагностика параметров текущего состояния аппаратного обеспечения. В меню конфигурации выводятся значения показателей напряжения питания и температуры аппаратного обеспечения, которые собираются с установленных на аппаратной платформе датчиков. В случае нестабильной работы аппаратной платформы возможно провести диагностику параметров аппаратного обеспечения и определить причину сбоев (неисправностей).

4. В ПО ЗОС Горизонт отсутствуют следующие опасные функциональные возможности, эксплуатация которых может привести или создать условия для нарушения заданных характеристик безопасности обрабатываемой информации:

– возможность использования встроенных в аппаратное обеспечение специализированных микроконтроллеров Intel ME, Intel BMC, которые могут получать неконтролируемый центральным процессором доступ к аппаратным ресурсам платформы и функционировать параллельно с ним путем полного исключения их программного обеспечения из состава ПО ЗОС Горизонт;

– возможность загрузки операционной системы по сети;

– возможность загрузки операционной системы с других имеющихся носителей информации в случае, если основное устройство загрузки не найдено;

– возможность программной перезаписи ПО ЗОС Горизонт локально и дистанционно;

– возможность удаленного включения, настройки и управления;

– возможность перехода в спящий режим или в режим гибернации;

– возможность установки настроек аппаратного обеспечения, приводящих к ухудшению стабильности работы платформы. Например, параметры для «разгона» центрального процессора, памяти и графического процессора.

5. Разработана программа функционального тестирования и проведено тестирование ПО ЗОС Горизонт для модуля процессора СРС1311. Модуль процессора СРС1311 с ПО ЗОС Горизонт обеспечивает загрузку сертифицированных по требованиям безопасности информации операционных систем российской разработки, таких как ОС «Astra Linux», ЗОСРВ «Нейтрино» и ДОС РВ «ТрастОС».

6. Разработана программная документация на ПО ЗОС Горизонт, по составу и содержанию обеспечивающая возможность сопровождения проектов, в которых будет использоваться модуль процессора СРС1311 с ПО ЗОС Горизонт, и проведения соответствующих исследований по требованиям безопасности информации.

7. Определена возможность постановки серийного производства и поставок модулей процессора СРС1311 с ПО ЗОС Горизонт с приемкой 5.

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

9. 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.

Заключение

В ходе проведения исследовательских работ был получен способ создания доверенной аппаратно-программной платформы на электронной компонентой базе иностранного производства фирмы Intel, обеспечивающей противодействие компьютерным атакам, направленным на использование уязвимостей в ПО BIOS.

Промышленная применимость данного способа является разработанная и серийно-выпускаемая ПФ АО «НТЦ «Атлас» доверенная аппаратно-программная платформа – блок вычислительный БВ001 ЦИАТ.467444.251 на базе модуля процессора 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 описанный способ создания доверенной аппаратно-программной платформы на электронной компонентой базе иностранного производства может быть в полной мере применим для аппаратно-программных платформ на электронной компонентной базе отечественного производства. Для этого необходимо обеспечить выполнение рассмотренных в данной работе условий доверия (УД1 – УД5), реализовать во встроенном программном обеспечении меры защиты от несанкционированного доступа и функции выявления неисправностей аппаратного обеспечения, а также обеспечить отсутствие в нем опасных функциональных возможностей.

В настоящее время ведущими специалистами ПФ АО «НТЦ «Атлас» ведутся работы по дальнейшему развитую ПО ЗОС Горизонт и созданию доверенных аппаратно-программных платформ на электронной компонентой базе отечественного производителя АО «МЦСТ» (процессор «Эльбрус»).

Таким образом, полученные результаты в рамках работ позволяют сделать вывод о возможности создания доверенной аппаратно-программной платформы на электронной компонентной базе иностранного и отечественного производства для её применения в специализированных изделиях и средствах вычислительной техники информационных систем специального назначения.

СПИСОК ЛИТЕРАТУРЫ:

1. Авезова Я.Э., Фадин А.А., Вопросы обеспечения доверенной загрузки в физических и виртуальных средах // Вопросы кибербезопасности. 2016. № 1. С. 24–30. DOI: http://dx.doi.org/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. URL: http://www.okbsapr.ru/library/publications/lydin_2016_1 (дата обращения: 20.11.2021).

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. URL: http://cyberleninka.ru/article/n/sovremennye-ugrozy-bezopasnosti-obrabotki-informatsii-so-storony-vstroennogo-programmnogo-obespecheniya-bios (дата обращения: 21.11.2021).
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. URL: https://npo-echelon.ru/doc/BIT-2019.pdf (дата обращения: 21.11.2021).
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. DOI: http://dx.doi.org/10.17586/0021-3454-2018-61-1-41-46.
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. P. 865–869. DOI: http://dx.doi.org/10.3103/S0146411619080224.
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. URL: http://jisp.ru/volume/metody-i-sredstva-obespecheniya-informacionnoj-bezopasnosti-4 (дата обращения: 22.11.2021).
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. (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. P. 346–353. DOI: http://dx.doi.org/10.5220/0006165603460353.
10. Гефнер И.С., Марков А.С. Механизмы реализации атак на уровне базовой системы ввода/вывода. // Защита информации. Инсайд. 2017. № 5. С. 80–83. URL: http://inside-zi.ru/pages/5_2017/80.html (дата обращения: 21.11.2021).
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. P. 1031–1036. DOI: http://dx.doi.org/10.1109/RusAutoCon49822.2020.9208037.
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. P. 657–662. URL: https://fruct.org/publications/acm20/files/Ogo.pdf (дата обращения: 22.11.2021).
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. URL: https://cyberleninka.ru/article/n/primenenie-vychislitelnyh-sistem-otechestvennogo-proizvodstva-kak-sredsvopovysheniya-informatsionnoy-beropasnosti-vuza (дата обращения: 20.11.2021).
14. Алексеев Д.М., Иваненко К.Н., Убирайло В.Н. Доверенная загрузка как механизм информационной безопасности // сборник статей по итогам Международной научно-практической конференции «Влияние науки на инновационное развитие». 2017. С. 19–20. URL: http://os-russia.com/SBORNIKI/KON-154.pdf (дата обращения: 22.11.2021).
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. DOI: http://dx.doi.org/10.24411/2409-5419-2018-10223.
16. Yao J., Zimmer V. Building Secure Firmware: Armoring the Foundation of the Platform. New York: Apress. 2020. P. 930 ISBN: 978-1-4842-61-06-4.

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: http://dx.doi.org/10.21681/2311-3456-2016-1-24-30 (in Russian).
[2] Lydin S.S. O sredstvah doverennoi zagruzki dlya apparatnyh platform s UEFI BIOS. Voprosy zashity informacii. 2016. № 3. S. 45–50. URL: http://www.okbsapr.ru/library/publications/lydin_2016_1 (accessed: 20.11.2021) (in Russian).

[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 URL: http://cyberleninka.ru/article/n/sovremennye-ugrozy-bezopasnosti-obrabotki-informatsii-so-storony-vstroennogo-programmnogo-obespecheniya-bios (accessed: 21.11.2021) (in Russian).

[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. URL: https://npo-echelon.ru/doc/BIT-2019.pdf (accessed: 21.11.2021) (in Russian).

[5] Ogoluk A.A., Shabalin A.V. Analiz bezopastnosti udalennogo dostupa sredstvami Intel Management Engine. Izvestiya vyshih uchebnyh zavedenii. Priborostroenie. 2018. T. 61. № 1. S. 41–46. DOI: http://dx.doi.org/10.17586/0021-3454-2018-61-1-41-46 (in Russian).

[6] I.D. Pankova, A.S. Konopleva, 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, P. 865–869. DOI: http://dx.doi.org/10.3103/S0146411619080224.

[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. URL: http://jisp.ru/volume/metody-i-sredstva-obespecheniya-informacionnoj-bezopasnosti-4 (accessed: 22.11.2021) (in Russian).

[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 (accessed: 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. P. 346–353. DOI: http://dx.doi.org/10.5220/0006165603460353.

[10] Gefner I.S., Markov A.S. Mehanizmy realizacii atak na urovne bazovoi sistemy vvoda/vyvoda. Zashita informacii. Insaid. 2017. № 5. S. 80–83. URL: http://inside-zi.ru/pages/5_2017/80.html (accessed: 21.11.2021) (in Russian).

[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. P. 1031–1036. DOI: http://dx.doi.org/10.1109/RusAutoCon49822.2020.9208037.

[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. P. 657–662. URL: https://fruct.org/publications/acm20/files/Ogo.pdf (accessed: 22.11.2021).

[13] 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. URL: https://cyberleninka.ru/article/n/primenenie-vychislitelnyh-sistem-otechestvennogo-proizvodstva-kak-sredsvopovysheniya-informatsionnoy-beropasnosti-vuza (accessed: 20.11.2021) (in Russian).

[14] Alekseev D.M., Ivanenko K.N., Ubirailo V.N. Doverennaya zagruzka kak mehanizm informacionnoi bezopastnosti. Vliyanie nauki na innovacionnoe razvitie. 2017. S. 19–20. URL: http://os-russia.com/SBORNIKI/KON-154.pdf (accessed: 22.11.2021) (in Russian).

[15] 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 DOI: http://dx.doi.org/10.24411/2409-5419-2018-10223 (in Russian).

[16] Yao J., Zimmer V. Building Secure Firmware: Armoring the Foundation of the Platform. New York: Apress. 2020. P. 930 ISBN: 978-1-4842-61-06-4.

Поступила в редакцию – 18 октября 2021 г. Окончательный вариант – 2 декабря 2021 г.
Received – October 18, 2021. The final version – December 2, 2021.