ИМПОРТОЗАМЕЩЕНИЕ

# Создание доверенной аппаратно-программной платформы на базе решений компании «Доломант»

**Алексей Боровиков, Денис Стулов, Олег Маслов** (г. Пенза)

**В статье изложен один из подходов по созданию аппаратно-программной платформы на базе решений компании ЗАО «НПФ «Доломант», предназначенной для построения средств вычислительной техники, обрабатывающих информацию ограниченного доступа, которая обеспечивает необходимый уровень доверия. Указаны проблемы, с которыми сталкивается разработчик, и предложены способы их решения.**

При создании средств вычислительной техники (СВТ) в частности и автоматизированных систем в целом, предназначенных для обработки информации ограниченного доступа и её защиты, перед разработчиком возникает вопрос выбора аппаратно-программной платформы, которая не должна нарушать заданный алгоритм обработки информации и вносить функции, не предусмотренные особенностями функционирования целевой системы.

Подавляющее большинство подобных средств вычислительной техники построено на аппаратно-программных платформах импортного 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.

В настоящее время вопрос повышения уровня доверия к средствам вычислительной техники, применяемым в автоматизированных системах для обработки информации ограниченного доступа, а также её защиты, является одним из приоритетных ввиду необходимости обеспечения в системах заданных характеристик безопасности информации, таких как конфиденциальность, целостность, доступность. С этой целью в каждой системе сертификации средств защиты информации, действующей на территории Российской Федерации, создаются и совершенствуются требования, предъявляемые к средствам вычислительной техники, в том числе к аппаратно-программным средам их функционирования, выполнение которых обеспечивает необходимый уровень доверия к ним. Данные требования, к примеру, изложены в требованиях к межсетевым экранам, действующим в системах сертификации ФСТЭК России и МО РФ, а также в нормативных документах ФСБ России, определяющих требования к средствам криптографической защиты информации (СКЗИ) и требования к мультипротокольному оборудованию (МПО).

Дополнительно стоит отметить, что, помимо требований, приведённых в нормативно-правовых актах и руководящих документах, действующих в системах сертификации, необходимость применения доверенной аппаратно-программной среды функционирования в средствах вычислительной техники определяется условиями эксплуатации сертифицированных средств защиты информации, например аппаратно-программных модулей доверенной загрузки (АПМДЗ).

В общем случае для обеспечения соответствия необходимому уровню доверия и соответствия предъявляемым требованиям по безопасности информации для средств вычислительной техники, применяемых в указанных автоматизированных системах, необходимо выполнение следующих обязательных условий:

- гарантия проектирования и наличие конструкторской документации на аппаратную платформу;
- наличие исходного кода, программной документации и гарантированное отсутствие опасных функциональных возможностей в микропрограммном обеспечении аппаратной платформы;
- применение сертифицированных по требованиям безопасности информации общесистемного, прикладного и специального программного обеспечения по соответствующему уровню контроля отсутствия недекларированных возможностей;
- 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 данных средств вычислительной техники необходимо обеспечить наличие конструктивных средств защиты от несанкционированного доступа к внутренним цепям, аппаратному обеспечению и внешним разъёмам, 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.

Учитывая распространённость, доступность, технические характеристики и стоимость аппаратных платформ на базе системной логики Intel, в большинстве случаев для создания средств вычислительной техники разработчики выбирают именно эти платформы. Ниже описан подход, позволяющий повысить уровень доверия к аппаратно-программной платформе на базе системной логики фирмы Intel.

Доверенная аппаратно-программная платформа (ДАПП) – это 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 объёме, согласованном с регулятором, и получены соответствующие разрешительные документы на программные компоненты, в

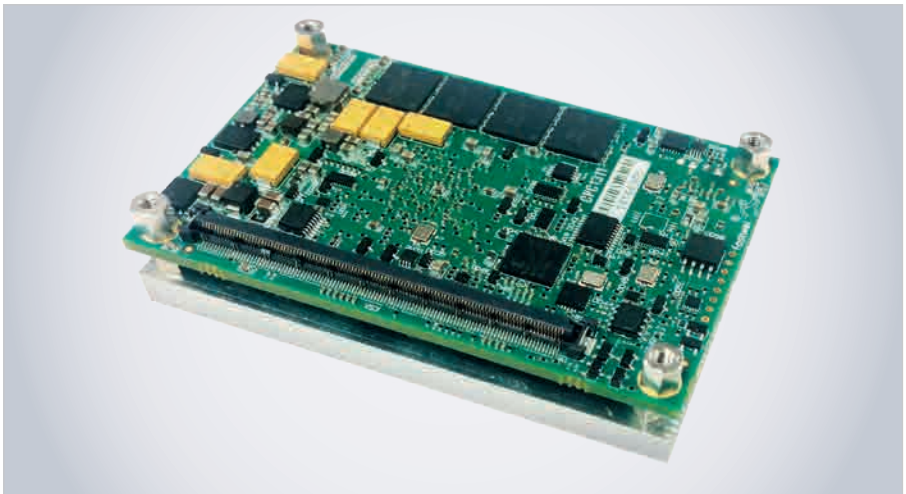
том числе на микропрограммное обеспечение. Для ДАПП однозначно должны выполняться следующие условия.

*Гарантия проектирования и наличие конструкторской документации на аппаратную платформу*. Для выполнения данного условия при проведении сертификационных испытаний по требованиям безопасности информации разработчику необходимо подтвердить, что аппаратная платформа выпускается на территории РФ и на неё имеется необходимая конструкторская и эксплуатационная документация, содержащая сведения о её составе, условиях эксплуатации, ограничениях по применению. Учитывая тот факт, что на российском рынке присутствуют аппаратные платформы отечественного производителя ЗАО «НПФ «Доломант», которые могут быть применены в ДАПП, обеспечить выполнение данного условия возможно в полном объёме.

*Наличие исходного кода, программной документации и гарантированное отсутствие опасных функциональных возможностей в микропрограммном обеспечении аппаратной платформы.* Для выполнения данного условия при проведении сертификационных испытаний по требованиям безопасности информации разработчику необходимо представить исходный код и документацию на микропрограммное обеспечение аппаратной платформы в объёме, достаточном для проведения соответствующих исследований, и при необходимости обеспечить доработку микропрограммного обеспечения, позволяющую гарантировать отсутствие опасных функциональных возможностей и уязвимостей в указанном программном обеспечении.

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

*Применение сертифицированных по требованиям безопасности информации общесистемного, прикладного и специального программного обеспечения по соответствующему уровню контроля отсутствия недекларированных возможностей*. Для выполнения данного условия разработчику необходимо обеспечить наличие соответствующих сертификатов по требованиям безопасности информации на общесистемное, прикладное и специальное программное обеспечение.



**Компьютерный модуль CPC1311**

На российском рынке присутствуют отечественные операционные системы ЗОСРВ «Нейтрино» (ООО «СВД Встраиваемые Системы»), ОС «Astra Linux» (АО «НПО РусБИТех») и другие. Данные операционные системы имеют соответствующие сертификаты и могут быть применены в ДАПП. Прикладное и специальное программное обеспечение имеет исходный код и документацию, пригодную для проведения сертификационных испытаний и получения соответствующих сертификатов. Таким образом, обеспечить выполнение данного условия возможно в полном объёме.

*Применение сертифицированных аппаратно-программных или программных средств защиты информации и средств антивирусной защиты для обеспечения невозможности работы несанкционированных пользователей и замкнутости программной среды*. Для выполнения данного условия разработчику необходимо обеспечить наличие соответствующих сертификатов по требованиям безопасности информации на средства защиты информации от НСД и средства антивирусной защиты. Учитывая тот факт, что на российском рынке присутствуют отечественные операционные системы, которые могут быть использованы в качестве средств защиты информации от НСД, и отечественные средства антивирусной защиты АО «Лаборатория Касперского» и «Доктор Веб», которые имеют соответствующие сертификаты и могут быть применены в ДАПП, обеспечить выполнение данного условия возможно в полном объёме.

Исходя из вышеизложенного, можно сделать вывод, что основной проблемой при создании ДАПП на базе системной логики фирмы Intel является получение ПО BIOS в исходных кодах и документации на него, достаточной для проведения сертификационных испытаний по требованиям безопасности информации. С целью определения возможности решения данной проблемы ведущими специалистами ПФ ФГУП «НТЦ «Атлас» и ЗАО «НПФ «Доломант» был проведён ряд исследовательских работ:

- выбор аппаратной платформы для ДАПП (ПФ ФГУП «НТЦ «Атлас» и ЗАО «НПФ «Доломант»);
- замещение ПО BIOS на программное обеспечение загрузчика операционной системы (ПО ЗОС), включающее в себя программу начальной инициализации и конфигурации аппаратного обеспечения, для выбранной аппаратной платформы (ПФ ФГУП «НТЦ «Атлас»);
- проведение функционального тестирования аппаратной платформы с ПО ЗОС (ПФ ФГУП «НТЦ «Атлас» и ЗАО «НПФ «Доломант»);
- определение возможности поставок аппаратной платформы с ПО ЗОС (ЗАО «НПФ «Доломант»).

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). Исходя из данного критерия, в качестве базового модуля для аппаратной платформы выбран компьютерный модуль CPC1311 (см. рис. ) 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 жёстких условиях окружающей среды.

СРС1311 построен на базе индустриального многоядерного процессора Intel Atom семейства BayTrail с 64-разрядной архитектурой. Отличительными особенностями данных процессоров являются крайне низкое энергопотребление (до 10 Вт), поддержка памяти ECC и мощный графический контроллер. В СРС1311 используются два исполнения процессора: высокопроизводительное на базе 4-ядерного процессора E3845 с частотой 1,91 ГГц и энергоэффективное на базе 2-ядерного E3825 с частотой 1,33 ГГц. Использование процессора с 4 ГБ оперативной памяти DDR3L с поддержкой ECC и твердотельным диском 8 ГБ позволяет использовать изделие в качестве самодостаточного встраиваемого компьютера, способного решать большинство прикладных задач.

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

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

Все компоненты СРС1311 расположены непосредственно на плате, что обеспечивает высокую стойкость изделия к ударным и вибрационным нагрузкам. Возможно исполнение модуля с влагозащитным покрытием. Диапазон рабочих температур СРС1311 составляет от –40 до +85°С. Компьютерный модуль СРС1311 по надёжности, производительности и возможности его применения в жёстких условиях эксплуатации в полной мере подходит для построения изделий доверенного управления СКЗИ и межсетевого экранирования.

В результате проведения исследовательских работ:

1. Разработано и проведено функциональное тестирование ПО ЗОС для компьютерного модуля СРС1311. Компьютерный модуль СРС1311 с ПО ЗОС реализует начальную инициализацию и конфигурацию аппаратной платформы и обеспечивает загрузку операционных систем, таких как ЗОСРВ «Нейтрино», Astra Linux и Windows 7.
2. Из ПО ЗОС исключены потенциально опасные функциональные возможности встроенного в центральный процессор микроконтроллера Intel Trusted Execution Engine (TXE), эксплуатация которых может привести или создать условия для нарушения заданных характеристик безопасности обрабатываемой информации.
3. Определена возможность производства и поставки компьютерных модулей СРС1311 с ПО ЗОС с 5-й приёмкой.
4. Программная документация на ПО ЗОС, по составу и содержанию обеспечивающая возможность проведения сертификационных испытаний по требованиям безопасности информации в системах сертификации МО РФ и ФСТЭК России, находится на заключительной стадии разработки. Ориентировочные сроки получения соответствующих сертификатов по требованиям безопасности информации – первый квартал 2020 года.
5. Разработано методическое и технологическое обеспечение по разработке и отладке ПО ЗОС для компьютерного модуля СРС1311, позволяющие существенно ускорить разработку ПО ЗОС для аппаратных платформ с меньшим EOL (5–7 лет). В ближайшей перспективе планируется разработка ПО ЗОС для компьютерного модуля СРС1304 (с центральным процессором Intel Xeon E3), на базе которого возможно построение высокопроизводительных и высоконадёжных вычислителей для автоматизированных рабочих мест оператора.

Таким образом возможно создать доверенную аппаратно-программную платформу на базе аппаратных решений компании ЗАО «НПФ «Доломант» для её применения в изделиях, обрабатывающих и осуществляющих защиту информации ограниченного доступа в соответствии с требованиями по безопасности информации в системах сертификации МО РФ, ФСТЭК России и ФСБ России.

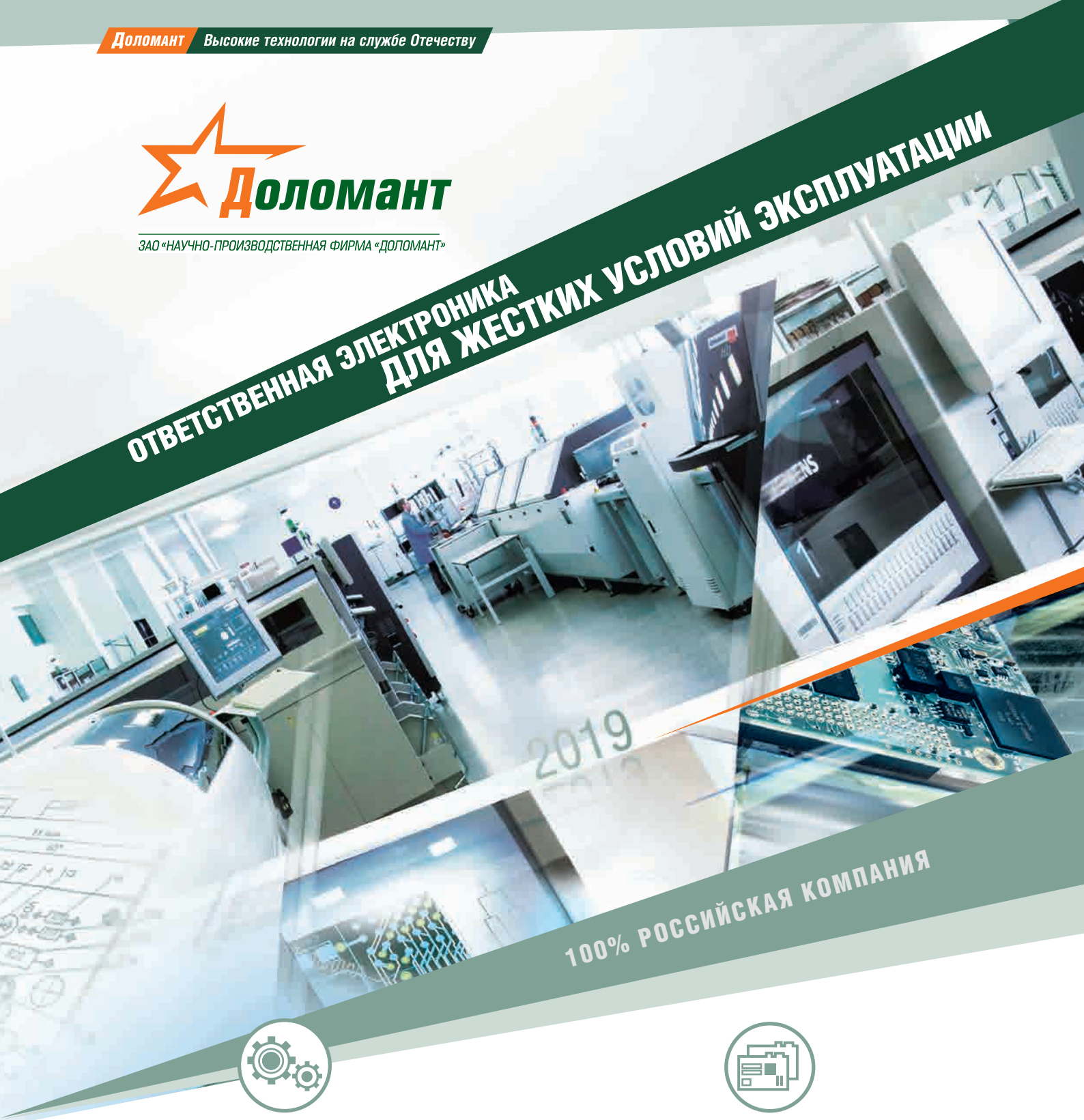
## Литература

1. *Агеев Е.Л.* UEFI замена BIOS. Гагаринские чтения 2018. 2018. С. 46–47.
2. *Сазонов С.А.* Programming ROM BIOS Extension of a personal Computer. RSDN Magasine. 2008. № 4. С. 12–16.
3. *Лыдин С.С.* О средствах доверенной загрузки для аппаратных платформ с UEFI BIOS. Вопросы защиты информации. 2016. № 3. С. 45–50.
4. *Иванников П.В., Алтухов Н.О.* Современные типы атак на BIOS. Молодёжный научно-технический вестник. 2015. № 6. С. 20.
5. *Счастный Д.Ю.* Перспективы развития средств доверенной загрузки. Взгляд разработчика. Вопросы защиты информации. 2017. № 3. С. 27–28.
6. *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.
7. *Добросердов К.О.* Сравнительный анализ возможностей унифицированного расширяемого микропрограммного интерфейса. ИТ-СТАНДАРТ. 2015. № 3. С. 54–62.
8. *Попов К.Г., Шамсутдинов Р.Р.* Актуальные вопросы технических наук: теоретический и практический аспекты. – М.: Аэтерна, 2015. С. 57–72.
9. *Алексеев Д.М., Иваненко К.Н., Убирайло В.Н.* Доверенная загрузка как механизм информационной безопасности. Влияние науки на инновационное развитие. 2017. С. 19–20.
10. *Чепанова Е.Г.* Формирование критериев сравнения модулей доверенной загрузки. Вопросы защиты информации. 2014. № 4. С. 60–63.
11. *Беляева Е.А.* Комплексная оценка функциональных возможностей аппаратно-программных модулей доверенной загрузки. Безопасность информационных технологий. 2013. № 1. С. 81–82.
12. *Беляева Е.А., Модестов А.А.* Классификация функциональных возможностей аппаратно-программных модулей доверенной загрузки. Безопасность информационных технологий. 2013. № 3. С. 75–77.
13. *Хрусталёв А.О.* Аппаратно-программный модуль доверенной загрузки. Аллея науки. 2017. № 10. С. 800–804.
14. *Zimmer V.* Embedded Firmware Solutions. 2015. NY: A-Press One. С. 55.
15. *Sallibun D.* BIOS Ninjutsu Uncovered. 2006. NY: A-Press One. С. 720.

Доломант

ЗАО «НАУЧНО-ПРОИЗВОДСТВЕННАЯ ФИРМА «ДОЛОМАНТ»

# ОТВЕТСТВЕННАЯ ЭЛЕКТРОНИКА ДЛЯ ЖЕСТКИХ УСЛОВИЙ ЭКСПЛУАТАЦИИ



100% РОССИЙСКАЯ КОМПАНИЯ

## ЗАКАЗНЫЕ РАЗРАБОТКИ

**Разработка электронного оборудования по ТЗ заказчика в кратчайшие сроки**

- Модификация КД существующего изделия
- Разработка спецвычислителя на базе COM-модуля
- Конфигурирование модульного корпусированного изделия
- Сборка магистрально-модульной системы по спецификации заказчика
- Разработка изделия с нуля

## КОНТРАКТНОЕ ПРОИЗВОДСТВО

**Контрактная сборка электроники уровней: модуль / узел / блок / шкаф / комплекс**

- ОКР, технологические консультации и согласования
- Макеты, установочные партии, постановка в серию
- Полное комплектование производства импортными и отечественными компонентами и материалами
- Поддержание складов, своевременное анонсирование снятия с производства, подбор аналогов
- Серийное плановое производство
- Тестирование и испытания по методикам и ТУ
- Гарантийный и постгарантийный сервис

(495) 232-2033 • WWW.DOLOMANT.RU • (495) 739-0775