Доверенная программно-аппаратная платформа «Эльбрус». Отечественное решение для АСУ ТП КВО

В настоящее время особую актуальность приобретает обеспечение информационной безопасности автоматических систем управления производственными и технологическими процессами (АСУ ТП). Это особенно важно в отношении критически важных объектов (КВО), прежде всего, в таких отраслях, как атомная и тепловая энергетика, железнодорожный и воздушный транспорт, химические производства, где удачно проведенная кибератака может иметь самые тяжкие последствия. Ключом к решению проблемы является применение отечественных изделий электроники и сертифицированных программных платформ, специально созданных для ответственных применений.

ЗАО «МЦСТ», г. Москва

Безопасность систем управления технологическими процессами: сегодняшнее состояние

Современный уровень проникновения информационных технологий во все сферы деятельности общества несет не только новые возможности, но и новые угрозы. В последние годы в мире возникло и стало быстро распространяться кибероружие, обладающее трансграничными поражающими факторами.

Множество стран разрабатывают технологии кибернетических атак, которые отличаются скрытностью и эффективностью, позволяя без улик нарушать работу ответственных систем – от АСУ производственными и технологическими процессами предприятий до систем жизнеобеспечения городов. Кибернетические атаки используют уязвимости информационно-коммуникационных и управляющих систем, позволяющие атакующей стороне проникнуть в эти системы и взять их под контроль.

Одновременно с техникой атак развивается промышленный и политический шпионаж. Поэтому количество операций на фронтах киберпространства постоянно растет: ежедневно во всем мире происходят тысячи проникновений, направленных на кражу информации либо нарушение работы объектов инфраструктуры разных стран.

Предтечей кибероружия можно считать компьютерные вирусы. Вирусы также используют уязвимости в программном обеспечении, но в большинстве случаев не обладают должной избирательностью действия и деструктивным эффектом. Однако сохраняющаяся тенденция подключать различные системы к сети Интернет позволяет качественно расширить возможности вирусов, связав их с управляющим центром, и даже обходиться взломом атакуемых систем «на лету», через эксплуатацию уязвимостей в программном обеспечении. Эволюцией вирусов (и уже настоящим применением кибероружия) можно считать проведенную в 2010 году хакерскую атаку на иранские атомные объекты, когда с помощью вирусного червя Stuxnet, занесенного в систему управления, удалось нарушить работу центрифуг для обогащения урана и, по некоторым сведениям, добиться их физического разрушения.

В целом можно отметить, что возникла целая методология под названием Advanced Persistent Threat (APT), которая объединяет различные методы проникновения в единую систему и позволяет эффективно атаковать самые разные объекты. Хорошо спланированная атака способна спровоцировать экономический коллапс или парализовать важнейшие структуры армии или правительства.

Компания Positive Technologies специализируется на исследованиях информационной безопасности различных информационных систем, в том числе промышленных. Ее специалистами был проведен анализ[1] АСУ ТП ключевых зарубежных и российских компаний и промышленных предприятий, имеющих выход в Интернет, результаты которого приведены в табл. 1.

Согласно этой статистике, доля АСУ ТП с уязвимыми программны-

[1] Безопасность промышленных систем в цифрах. М., 2012.

Таблица 1. Данные компании Positive Technologies по уязвимости АСУ ТП в разных странах мира

Страна	Доля уязвимых АСУ ТП, %
Швейцария	100
Чешская Республика	86
Швеция	67
Испания	63
Тайвань	60
Великобритания	60
Российская Федерация	50
Финляндия	50
Италия	42
США	41
Польша	36
Франция	36
Нидерланды	33
Австрия	33
Южная Корея	32
Канада	25
Германия	20
Индия	–
Китай	–

ми компонентами в разных странах сильно различается, причем прямую зависимость показателей уязвимости от общего уровня технологического развития страны констатировать довольно непросто. Достаточно отметить, что, по приведенным данным, в России уязвимы около половины АСУ ТП, информацию о которых можно найти в сети Интернет. В среднем эксплуатация каждой второй уязвимости позволяет злоумышленнику выполнить произвольный код на различных компонентах систем АСУ ТП. Почти треть уязвимостей (36 %) связана с переполнением буфера (Buffer Overflow) – явлением, возникающим, когда компьютерная программа записывает данные за пределами выделенного в памяти буфера.

Подробно говорить о программных продуктах, образующих данные компоненты, излишне. Достаточно отметить, что их очень много и они в большинстве своем проприетарны, то есть разработаны частными компаниями и имеют закрытый исходный код. По статистическим данным, для них характерно большее число уязвимостей и недокументированных возможностей. Более того, у конечного пользователя нет никакой возможности провести аудит исходного кода таких продуктов и наладить процесс поиска и устранения уязвимостей – этот вопрос зависит исключительно от доброй воли поставщика продукции.

Кроме чисто программных атак на системное и прикладное программное обеспечение, потенциальную угрозу для безопасности представляют и присутствующие в аппаратуре практически любого современного компьютера внутренние функции, к которым у пользователей нет прямого доступа (либо пользователи не знают об их существовании). Примером такой функциональности служат процессор и специальное ПО, входящие в состав чипов Trusted Platform Module, сервисных управляющих модулей BMC[2], а также современных интеллектуальных сетевых адаптеров. Обеспечить полноценный аудит функций этих модулей еще сложнее, чем добиться этого от производителей проприетарных операционных систем и прикладного ПО, то есть на практике не представляется возможным.

Пути решения проблемы безопасности АСУ ТП

Очевидный факт: если атакующий владеет более полной информацией об атакуемой системе, чем ее владелец, то у последнего остается немного шансов на успешную защиту. Сложно говорить о защищенном хранении и обработке информации на компьютере, в котором установлена операционная система с закрытым и не прошедшим аудит исходным кодом. Точно так же никакое системное и прикладное программное обеспечение не может обеспечить безопасность системы, если используется аппаратная платформа с закрытой конструкторской документацией, имеющая закрытый исходный код системы начальной загрузки (BIOS) и другие модули, недоступные для инспекции.

Справедливости ради отметим, что сама по себе доступность исходных кодов и конструкторской документации для аудита также не является панацеей. Сложность современных систем, как программных, так и аппаратных, настолько высока, что иногда лишь сам разработчик системы способен полностью разобраться в ее функциональности. Поэтому гарантией безопасности может служить только разработка всей системы силами своей команды разработчиков и тщательный аудит исходных кодов и конструкторской документации. Иначе говоря, безопасность может обеспечить только доверенная вычислительная платформа. Это цель, к которой следует стремиться.

В своем отчете Positive Technologies постулирует: «История безопасности промышленных систем разделяется на два этапа: до и после появления Stuxnet». Но Stuxnet – кибероружие, которое, по мнению многих экспертов, было создано государством против государства. Благодаря инциденту с атакой на иранские атомные объекты проблема информационной безопасности была вынесена на государственный уровень. Поэтому решение вопроса с информационной безопасностью находится тоже на государственном уровне.

Взгляд на информационную безопасность АСУ ТП критически важных объектов (КВО) со стороны государства выражен в руководящем документе Совета безопасности РФ «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации». Появление этого документа свидетельствует о том, что руководящие органы РФ понимают всю актуальность проблемы.

В этом документе есть пункты, включающие в себя импортозамещение и поддержку отечественных разработок в области информационной безопасности. По большому счету, иного выхода, кроме как развивать и внедрять отечественные разработки, просто нет. Нельзя гарантировать, что импортное оборудование и ПО, использованное для создания системы управления, полностью свободно от уязвимостей и закладок, позволяющих по команде извне изменить его функционирование. На иранских ядерных объектах АСУ ТП была построена на базе проприетарных решений с закрытым исходным кодом, поставляемых производителями из недружественных Ирану стран. Результат всем известен.

[2] *От англ.* Baseboard Management Controller (контроллер управления основной платой) – встроенный в платформу автономный микроконтроллер.

У России есть собственные аппаратные и программные разработки, которые позволяют построить доверенную систему, и сегодня они доступны не только для закрытых применений, но и для гражданской сферы. Именно они являются ключом к построению надежных и безопасных систем АСУ ТП.

Отечественные разработки в области вычислительной техники

Старейшим создателем отечественных средств автоматизации технологических процессов является организованный в 1958 году Институт электронных управляющих машин (ИНЭУМ), который впоследствии получил имя И.С. Брука. За годы существования института в нем были разработаны и запущены в серийное производство многие модели управляющих ЭВМ. В ИНЭУМ была создана первая в СССР серийная управляющая микро-ЭВМ СМ 1803 на микропроцессорной элементной базе. В конце 1980-х годов было разработано семейство управляющих машин СМ 1810, выпускавшееся массовыми партиями. К настоящему моменту спроектированы, серийно выпускаются и постоянно развиваются разнообразные технические и программные средства модели СМ 1820М, относящиеся к четвертому поколению семейства СМ 1800. Несмотря на то что разработчики вынуждены были использовать зарубежную элементную базу, выпуск этих машин позволил институту сохранить коллектив и приобрести определенные позиции на рынке промышленной автоматизации. Среди выполненных проектов на базе СМ 1820М можно отметить систему контроля и управления движением электропоездов Московского метрополитена, подсистемы контроля обстановки и управления технологическим процессом на различных обогатительных фабриках и АЭС, систему транспортировки ядерного топлива на Белоярской АЭС. Подробнее о выполненных проектах и системе СМ 1820М можно узнать на сайте www.sm1820.ru.

В перечисленных выше разработках использовалась импортная электронно-компонентная база. Однако в последние несколько лет появилась возможность для применения отечественной элементной базы в управляющих комплексах АСУ ТП. Эта возможность связана с достижениями компании ЗАО «МЦСТ», с 2006 года работающей в тесном сотрудничестве с ОАО «ИНЭУМ им. И.С. Брука». ЗАО «МЦСТ» было образовано в 1992 году ведущими сотрудниками Института точной механики и вычислительной техники, к тому времени создавшими отечественные высокопроизводительные вычислительные средства для использования в наиболее ответственных и наукоемких областях – космических исследованиях, атомной энергетике, обороне. За 20 лет, прошедших с момента основания ЗАО «МЦСТ», его специалисты разработали ряд универсальных микропроцессоров и вычислительных комплексов на их основе, в настоящее время по своим показателям превосходящих все отечественные разработки в данной области.

▲ Рис. 1. Микропроцессор Эльбрус-2С+

Отечественные программно-аппаратные платформы «Эльбрус» и «МЦСТ-R»

ЗАО «МЦСТ» проектирует и выпускает две линейки процессоров: серии «МЦСТ-R», архитектура которых совместима со стандартной системой команд SPARC, и серии «Эльбрус» с оригинальной архитектурой, обладающей повышенной вычислительной мощностью.

В первой линейке следует выделить два изделия. Это система на кристалле МЦСТ R500S и микропроцессор МЦСТ R1000. Их основные характеристики приведены в табл. 2 и 3. Система на кристалле МЦСТ R500S показывает умеренную производительность и низкую выделяемую мощность. Устройство хорошо подходит для организации программируемых логических контроллеров (ПЛК), терминалов отображения информации, управляющих ЭВМ нижнего уровня. Микропроцессор МЦСТ R1000 имеет умеренную выделяемую мощность, высокую производительность и позволяет эффективно исполнять многопоточные приложения. Его сфера применения – управляющие ЭВМ верхнего уровня, АРМ операторов, файл-серверы и серверы баз данных. Для связи с внешними устройствами МЦСТ R1000 используется совместно с контроллером интерфейсов (южным мостом) КПИ.

Наивысший уровень производительности обеспечивают микропроцессоры семейства «Эльбрус». На сегодня самой совершенной моделью данного семейства является микропроцессор Эльбрус-2С+ (рис. 1). Несмотря на свою сравнительно низкую тактовую частоту, он обладает однопоточной производительностью на уровне современных импортных процессоров для настольных систем[3]. Его сфера применения – управляющие ЭВМ, требующие повышенной вычислительной мощности и проводящие интенсивные расчеты с плавающей запятой. Примером такой задачи является моделирование сложных процессов в реальном времени. Для связи с внешними устройствами процессор Эльбрус-2С+ также использует контроллер интерфейсов КПИ.

Все вычислительные системы, разработанные на базе линеек процессоров «МЦСТ-R» и «Эльбрус», обладают базовой системой ввода/вывода (BIOS), разработанной также в ЗАО «МЦСТ». Единой программной платформой является операционная система «Эльбрус».

[3] В зависимости от характера решаемой задачи, абсолютная производительность процессора Эльбрус-2С+ может достигать уровня Intel Core 2 с тактовой частотой 1,5 ГГц и выше. Особенно эффективно исполняются на процессорах «Эльбрус» задачи из области цифровой обработки сигналов, в частности интеллектуальная обработка изображений, задачи математического моделирования процессов, криптографические алгоритмы.

Таблица 2. Характеристики СБИС процессоров и систем на кристалле, разработанных в ЗАО «МЦСТ»

Параметр	МЦСТ R500S	МЦСТ R1000	Эльбрус-2С+
Архитектура	SPARC V8 (32-bit)	SPARC V9 (64-bit)	Elbrus (64-bit)
Количество ядер	2	4	2 ядра Эльбрус + 4 ядра DSP
Тактовая частота	500 МГц	1000 МГц	500 МГц
Объем кэш-памяти 2-го уровня	512 КБ (общая)	2 МБ (общая)	2 МБ (по 1 МБ на каждое ядро «Эльбрус»)
Оперативная память	PC2600 (DDR-333)	PC2–6400 (DDR2-800)	PC2-6400 (DDR2-800) (2 канала)
Внешние интерфейсы	PCI, Fast Ethernet, SCSI-2, PS/2, RS-232, IEEE 1284, EBus, LVDS (для межмашинного обмена данными)	3 канала межпроцессорного обмена, 1 канал ввода/вывода (к южному мосту КПИ)	3 канала межпроцессорного обмена, 2 канала ввода/вывода (к южному мосту КПИ)
Диапазон рабочих температур среды	-60…+85 °С	-60…+85 °С	-60…+85 °С
Энергопотребление	5 Вт	15 Вт	25 Вт
Аналог по уровню производительности (при равной тактовой частоте)	ARM 11	ARM Cortex A8, Intel Atom	Intel Core2

Таблица 3. Характеристики контроллера южного моста КПИ

Параметр	Значение
Характеристики канала ввода/вывода для связи с процессором	Дуплексный, пропускная способность 1 Гбайт/с в каждую сторону
Набор поддерживаемых внешних интерфейсов	PCI-Express версии 1.0a x8, PCI версии 2.3, Ethernet 1 Гбит/с, SATA 2.0, USB 2.0, IDE, AC-97, RS-232/485, IEEE-1284, GPIO, I2C, SPI
Диапазон рабочих температур среды	-60…+85 °С
Энергопотребление	6 Вт

Она построена на базе ядра Linux 2.6.33, имеет варианты сборки для всех поддерживаемых архитектур (32-разрядного МЦСТ R500S, 64-разрядного МЦСТ R1000 и 64-разрядного Эльбрус-2С+) из единой базы исходных кодов. ОС «Эльбрус» поставляется в двух исполнениях: обычном и поддерживающем режим жесткого реального времени. В последнем варианте обеспечивается время реакции на прерывание порядка 30 мкс для процессоров Эльбрус-2С+ и МЦСТ R500S, и порядка 10 мкс для процессора МЦСТ R1000. Все дистрибутивы ОС «Эльбрус» проходят обязательную сертификацию по 2-му уровню контроля недекларированных возможностей (НДВ) и 2-му классу защиты от несанкционированного доступа (НСД) в соответствии с руководящими документами Гостехкомиссии при Президенте РФ.

Инструменты разработчика, доступные на обеих платформах, включают в себя: компилятор с языков Си, Си++, Фортран, разработанный собственными силами компании, отладчик gdb, профилировщики, математические и системные библиотеки. Имеется графическая среда Xorg, различные офисные приложения, в том числе LibreOffice, СУБД, веб-сервер Apache и множество других программных пакетов. Все они также проходят сертификацию и включены в дистрибутив.

Защищенность от эксплуатации уязвимостей

Следует подчеркнуть, что сертификация продукта сама по себе не гарантирует его полной безопасности. Дело в том, что значительная часть атак пользуется уязвимостями в ПО, которые не были своевременно выявлены разработчиками. Сертификация также не в состоянии выявить их в полном объеме. Поэтому немаловажным является вопрос: что будет, если злоумышленник все же обнаружит уязвимость в продукте и попытается воспользоваться ею?

Современная технология взлома опирается на отработанные и общеизвестные инструменты, такие как Metasploit Framework, разрабатываемые совместно хакерами всего мира по модели croudsourcing. Metasploit содержит базы известных уязвимостей в популярных программных продуктах, фрагменты кода для атакуемых платформ (так называемый shell code), позволяющие доставить вредоносную нагрузку на компьютер-жертву, и прочие подручные инструменты, необходимые хакерам для успешного и незаметного взлома. Значительная часть этих инструментов привязана к архитектуре процессора атакуемой системы. Но есть закономерность: чем менее популярна и распространена платформа или приложение, тем меньше инструментов для нее наработано. Взлом таких систем становится дороже с точки зрения трудозатрат, а риск разоблачения — выше: эксплуатация уязвимости, по сути, вызывает сбой в работе приложения, и если она проведена неудачно, программа «падает», в работе системы регистрируется сбой, который может привлечь внимание администраторов и спровоцировать организационные меры по защите от атак на данное приложение. С этой точки зрения платформа SPARC, будучи малораспространенной, находится в выигрышном положении по сравнению с более популярными платформами Intel x86, ARM, MIPS, PowerPC. Но платформа «Эльбрус», на практике еще не получившая распространения, в отношении сложности взлома находится вне конкуренции. Кроме того, что наработанной базы эксплоитов для нее сейчас не существует, есть и определенные архитектурные особенности, которые затрудняют применение популярной техники эксплуатации уязвимостей под названием Return Oriented Programming (ROP). Именно эта техника часто применяется при эксплуатации уязвимости типа «переполнение буфера».

Итак, можно констатировать, что выбор процессорных архитектур SPARC или «Эльбрус» позволяет усложнить потенциальным злоумышленникам задачу взлома системы.

Специализированное ПО для организации АСУ ТП на базе отечественных программно-аппаратных платформ

Для применения в сфере АСУ ТП крайне важно специализированное программное обеспечение, позволяющее быстро и качественно настраивать алгоритмы управления технологическим процессом. Доступное сегодня коммерческое ПО

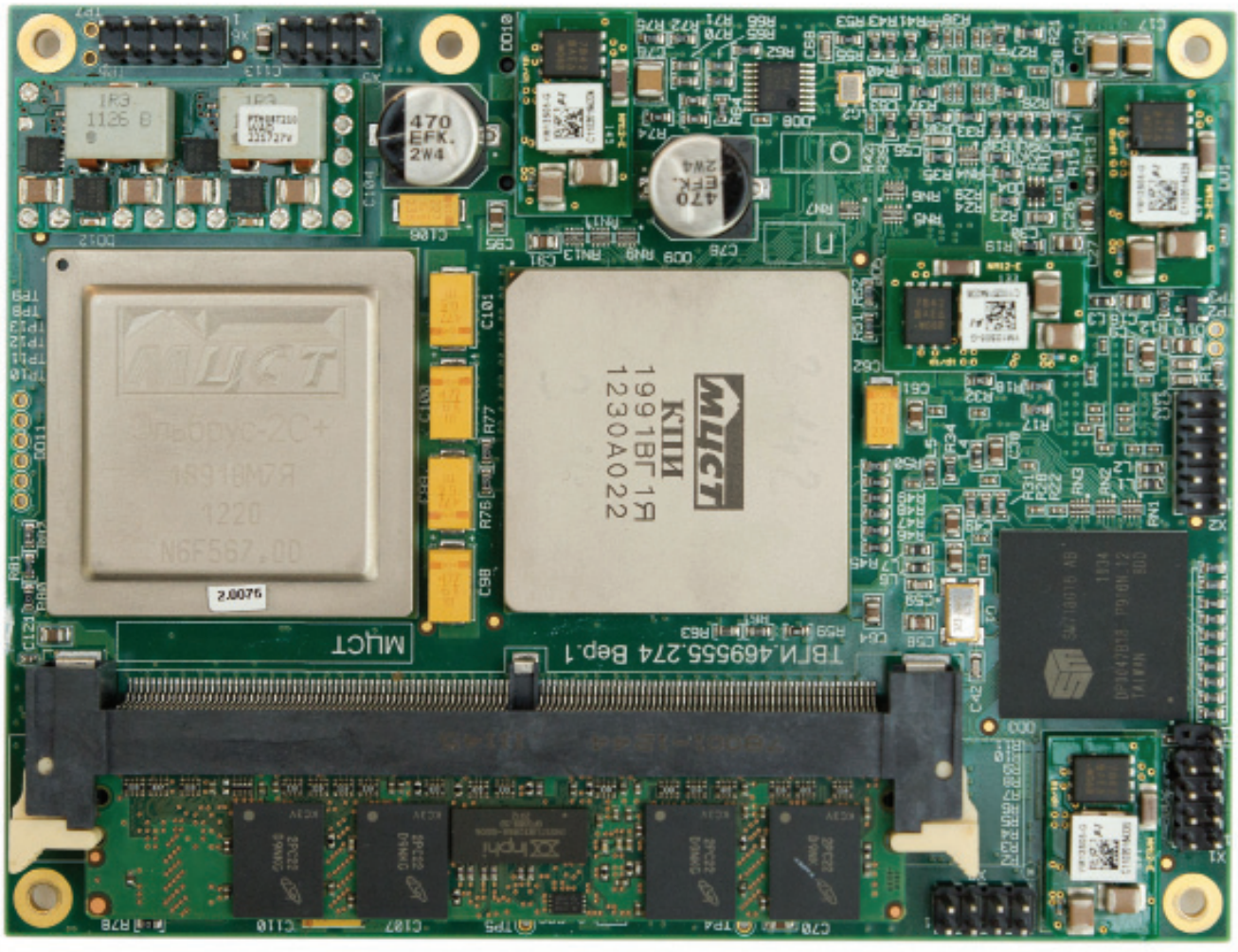

Рис. 2. Компактный вычислительный модуль КУБ-COM

управления технологическими процессами (такое как WinCC) нельзя запустить на не подходящей для него программно-аппаратной платформе. Возможный выход из положения – применить кросс-платформенное ПО с открытым исходным кодом, которое можно перекомпилировать на новую платформу с использованием стандартных компиляторов. Примером могут служить проекты OpenSCADA и Beremiz. Последний рассмотрим подробнее.

Beremiz представляет собой интегрированную среду разработки (IDE) прикладных программ для целевых устройств на языках стандарта IEC 61131-3. Основными компонентами Beremiz являются:

- редактор PLCOpen для текстовых (IL и ST) и графических языков (FBD, LD, SFC) стандарта IEC 61131-3;
- компилятор MatIEC, преобразующий логику и алгоритмы программных модулей (из которых состоит прикладная программа), описанных на языках стандарта IEC 61131-3, в эквивалентный C-код;
- механизм плагинов, позволяющий связывать внешние источники данных, такие как модули УСО (их параметры, состояния), SCADA-системы с логикой и алгоритмами программных модулей;
- средства отладки прикладной программы в режиме исполнения;
- элементы для создания человекомашинного интерфейса управления прикладной программой.

Гибкость в изменении существующих и добавлении новых компонентов достигается с помощью языка Python (и соответствующих библиотек для пользовательского интерфейса, работы с сетью и т.д.) и xsd (XML Schema) файлов, применяемых для описания компонентов среды разработки: модулей работы с компиляторами целевой архитектуры, плагинов внешних источников данных и т.д.

Подробнее о возможностях использования пакета Beremiz можно узнать в соответствующих статьях на сайте ОАО «ИНЭУМ им. И.С. Брука». Кросс-платформенность позволяет применять Beremiz на всех платформах, выпускаемых ЗАО «МЦСТ».

Вычислительные модули для организации АСУ ТП на отечественной элементной базе

Выше была приведена краткая характеристика элементной базы и комплект общего программного обеспечения, разработанные в ЗАО «МЦСТ».

В продукции ЗАО «МЦСТ» и ОАО «ИНЭУМ им. И.С. Брука» реализованы компактные вычислительные модули, созданные на базе собственных микропроцессоров. Прежде всего, для промышленной автоматизации можно применять модули МПЯ2, МПУ-COM, КУБ-COM (рис. 2), имеющие формат ETX и COM Express.

В качестве комплекта разработчика можно рассматривать эти же модули, установленные на стандартные платы-носители (например,

Таблица 4. Характеристики модулей МПЯ2, МПУ-COM, КУБ-COM, Монокуб, МПУ-ATX, МПУ-MPC

Характеристика	МПЯ2	МПУ-COM	КУБ-COM	МПУ-MPC	МПУ-ATX	Монокуб
Форм-фактор	ETX	COM Express type 2	COM Express type 2	PCI/104	microATX	miniITX
Процессор	МЦСТ R500S	МЦСТ R1000	Эльбрус-2С+	МЦСТ R1000	МЦСТ R1000	Эльбрус-2С+
Оперативная память	Напаянная, 512 КБ DDR-266	miniDIMM ECC DDR2-266	miniDIMM ECC DDR2-266	miniDIMM ECC DDR2-266	DIMM ECC DDR2-800	2 × DIMM ECC DDR2-800
Видеоконтроллер	Встроенный на базе ПЛИС	Silicon Motion SM718	Silicon Motion SM718	нет	Silicon Motion SM718	Silicon Motion SM718
Встроенные интерфейсы	Fast Ethernet, 2 × RS-232, 2 × IDE, Audio (вх./вых./микр.), Video VGA+LVDS, 2 × PS/2, 4 × USB 1.0	PCI-Express 1.0 × 8, Gigabit Ethernet, PCI 32/33, 4 × SATA 2.0, 8 × USB 2.0, Video VGA, Video LVDS, Audio AC'97	PCI-Express 1.0 × 8, Gigabit Ethernet, PCI 32/33, 4 × SATA 2.0, 5 × USB 2.0, Video VGA, Video LVDS, Audio AC'97	PCI/104, 3 × Gigabit Ethernet, SATA 2.0, IDE (CompactFlash), 2 × USB 2.0, RS-232, RS-485/422	PCI-Express 1.0 × 8, 2 × PCI 32/33, Gigabit Ethernet, 2 × RS-232, 4 × SATA 2.0, 2 × IDE, 8 × USB 2.0, Video VGA, Video DVI, Audio (вх./вых./микр.), 6 × GPIO	PCI-Express 1.0 × 8, Gigabit Ethernet, RS-232, 4 × SATA 2.0, IDE (CompactFlash), 8 × USB 2.0, Video VGA, Video DVI, Audio (вх./вых./микр.), 6 × GPIO
Диапазон рабочих температур*, °C	-30…+55	0…+55	0…+45	0…+55	0…+55	0…+55

* Рабочий диапазон температур модуля определяется техническим заданием, выданным на его разработку. При необходимости для каждого модуля можно подобрать элементную базу, выдерживающую индустриальный диапазон температур (от –40 до +85 °C).

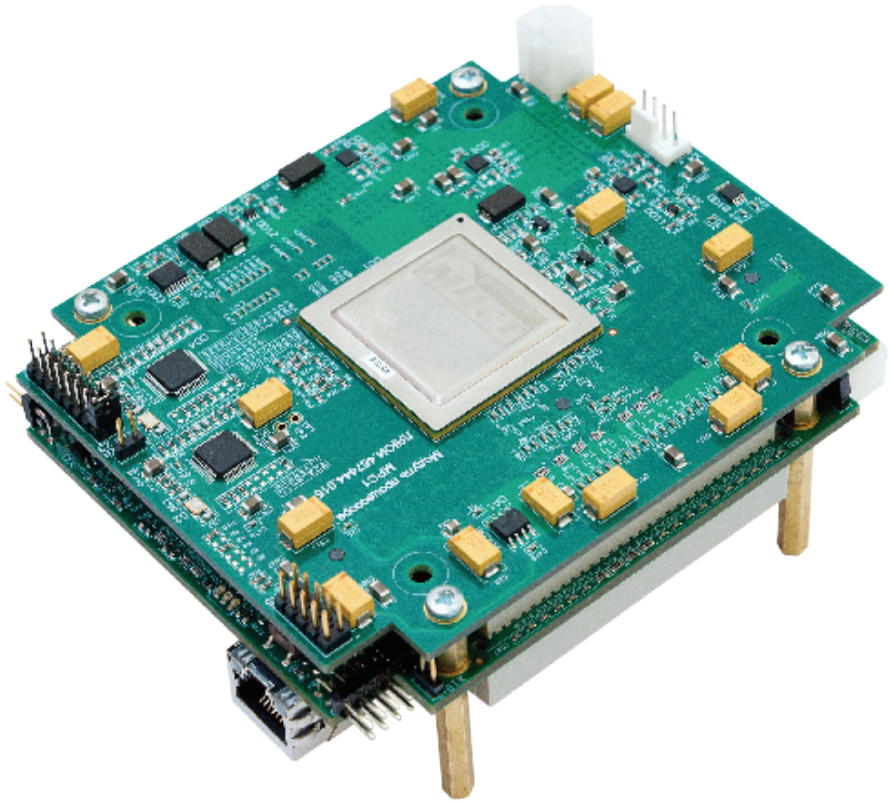

Рис. 3. Модуль МПУ-MPC

на плату COM Express Eval Carrier Type 2 фирмы Kontron). Но имеются и отдельные материнские платы, лучше приспособленные для того же применения. Это плата Монокуб на базе процессора Эльбрус-2С+ и МПУ-ATX на базе МЦСТ-R1000. Для специальных применений имеется модуль МПУ-MPC (рис. 3) в форм-факторе PCI/104. Характеристики модулей и материнских плат приведены в табл. 4.

Заключение

Эта статья начиналась с описания рисков, связанных с информационной безопасностью АСУ ТП, в том числе критически важных объектов. После рассмотрения ее различных аспектов можно сказать, что вычислительные платформы «МЦСТ-R» и «Эльбрус», укомплектованные ОС «Эльбрус», являются доверенными программно-аппаратными средствами и представляют с этой точки зрения наибольший интерес среди всего спектра систем, представленных на отечественном рынке. Их аппаратное и программное обеспечение практически на всех уровнях разработано в России и может быть сертифицировано самым тщательным образом. Таким образом, для сферы АСУ ТП критически важных объектов уже сегодня имеется отечественное решение с уникальными характеристиками.

За дальнейшей информацией обращайтесь на сайты www.mcst.ru и www.ineum.ru.

В. И. Глухов, начальник отделения
ОАО «ИНЭУМ им. И. С. Брука»,
И. Н. Бычков, начальник отдела,
К. А. Трушкин, руководитель отдела маркетинга
ЗАО «МЦСТ», г. Москва,
тел.: (495) 363-9665,
e-mail: mcst@mcst.ru,
www.mcst.ru