

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ АТОМНОЙ ЭНЕРГЕТИКИ

А.Г. Полетыкин, Е.Ф. Жарко, И.Н. Зуенкова, В.Г. Промыслов,
М.Е. Бывайков, Н.Э. Менгазетдинов (ИПУ им. В.А. Трапезникова РАН)

Рассматриваются вопросы обеспечения технологической независимости, лицензионной чистоты и безопасности, возникающие при применении программного обеспечения в АСУ ТП АЭС. Исследуются виды зависимости, источники опасности и излагается точка зрения ИПУ РАН на решение этих вопросов. Представлены некоторые программные продукты, разработанные в ИПУ РАН для АСУ ТП АЭС.

Введение

Программное обеспечение (ПО) стало одной из составляющих окружающей среды. Оно работает в мобильных телефонах, домашних компьютерах, в магазинах, медицинских учреждениях, предприятиях, на транспорте, в системах жизнеобеспечения, в системах, важных для безопасности, включая ядерную.

Во многих случаях используется одно и то же ПО. Ярким примером является ОС Windows фирмы Microsoft, применяемая широким спектром пользователей от игровых залов до третьего энергоблока Калининской АЭС.

Рассмотрим точку зрения Института проблем управления им. В.А. Трапезникова РАН на обеспечение технологической независимости, лицензионной чистоты, качества и безопасности ПО в атомной энергетике.

Технологическая независимость и лицензионная чистота

Технологическая зависимость организации А от организации Б возникает при наступлении одного из следующих случаев.

(1) А использует ПО, произведенное Б, но Б не передает А исходные коды ПО;

(2) Б передает исполняемые и исходные коды ПО А, но не производит обучение персонала А в объеме, необходимом для внесения изменений и доработок в ПО;

(3) Б передает исполняемые и исходные коды ПО А, по возможности обучает персонал А правилам внесения изменений и доработок в ПО, но оставляет за собой через лицензионные соглашения права собственности на ПО, которые позволяют Б контролировать применение ПО.

Случай (1) типичен при применении ОС ведущих мировых производителей, SCADA-систем и т. п. Это худшая из всех видов зависимостей. В этом случае пользователь ПО зависит от прихотей производителей, которые по своему усмотрению могут менять ПО, что вынуждает пользователей нести значительные расходы по адаптации нового ПО, его испытаниям и т. п. Кроме этого, при использовании продукции иностранных поставщиков зависимость типа (1) может существенно ограничить применение конечного продукта, в котором используется ПО, например, из-за эмбарго, политических, конкурентных и других причин.

Случай (2) имеет место при использовании ПО "с открытым кодом". К ним, в частности, относятся версии ОС LINUX, компиляторы, Web-браузеры, утилиты и т. п. В этом случае пользователь имеет возмож-

ность получить независимость. Но для этого ему нужно создать группу, лабораторию или целый институт, набрать в него квалифицированных специалистов, которые способны разобраться в исходных кодах ПО и содержать их в течение всего времени эксплуатации данного ПО. Это требует значительных финансовых затрат и под силу либо государству в целом, либо отрасли (Министерство обороны, РОСАТОМ, Академия наук), либо крупной корпорации (РАО ЕЭС, Газпром и т. п.).

Случай (3) — это лицензионная зависимость. Часто она наступает при применении ПО "с открытым кодом", произведенным фирмами США и других стран. Примером может служить продукт Open Office фирмы Sun, который будучи продукцией США не может поставляться в ряд стран и организаций. В этом случае определенная зависимость от фирмы или иностранного государства не может быть устранена полностью, а конечный продукт не будет лицензионно чистым.

Если понимать под А отечественные фирмы-строители АЭС (Атомстройэкспорт, Росэнергоатом), то как им обеспечить технологическую независимость и лицензионную чистоту своей конечной продукции (энергоблоков АЭС) от иностранных фирм-изготовителей ПО и политики чужих государств?

Есть только два пути. Первый — заказывать ПО в России либо у подконтрольных заказчику фирм, либо у государственных организаций, недостижимых для недружественных действий. К ним относятся федеральные государственные унитарные предприятия РОСАТОМа, институты РАН, федеральные ядерные центры и другие отечественные организации.

Второй путь связан с преодолением зависимости типов (2) и частично (3). Это можно сделать либо указанным выше способом, либо путем установления контроля над фирмой-поставщиком ПО.

Безопасность ПО

Безопасное ПО — это ПО, выполняющее только возложенные на него владельцем задачи и не выполняющее никаких других. Чтобы проверить выполнение требуемых задач проводятся испытания. Однако выполняет ли ПО непредусмотренные законным владельцем задачи, испытаниями проверить нельзя. Например, как можно проверить отсутствие закладки в ОС, которая содержит суперпароль для входа в систему? Для программиста ответ очевиден: нужно проанализировать исходный код ПО. Иного пути нет.

Иными словами, ПО должно быть подвергнуто операции верификации исходного кода и документа-

ции. Это утверждение носит характер аксиомы для всех, кто занимается ПО для АЭС, поскольку оно содержится в нормативных документах, регламентирующих разработку программного обеспечения для систем важных для безопасности АЭС.

Однако на практике это требование часто нарушается. Так, на третьем блоке Калининской АЭС в системе верхнего блочного уровня (системе, важной для ядерной безопасности) используются ОС MS Windows и Open WMS, верификацию исходного кода которых никто не проводил, то есть используется иностранное ПО, безопасность которого не подтверждена.

Практика применения на АЭС ПО сомнительной безопасности должна быть законодательно запрещена, а само ПО заменено. Какая бы фирма, российская или зарубежная, ни разрабатывала ПО для АЭС, процедура его изготовления должна производиться по методам, обеспечивающим качество и безопасность.

Программные продукты ИПУ РАН для атомной промышленности

ИПУ РАН более 20 лет ведет работы в области ПО для АСУТП АЭС, накопил значительный опыт и создал ряд программных продуктов, которые поставляются различным организациям в России и за рубежом. Они различаются по назначению, области применения, масштабу и комплектности. Вместе с тем, каждый программный продукт является законченным инструментальным средством, которое может применяться как самостоятельно, так и в комплексе с другим ПО.

Все ПО было разработано с соблюдением норм и правил, установленных в РФ, и имеет разрешение государственных надзорных органов для применения на АЭС.

Операционная система LICS

LICS (Linux Institute of Control Science) является универсальным коммерческим продуктом, который может применяться в широком классе систем АЭС, включая офисные приложения, АСУ П и АСУТП [1].

Поддерживает широкий спектр технических средств с процессорами Intel, включая мобильные компьютеры, промышленную вычислительную технику и высокопроизводительные вычислительные комплексы. Поддерживает работы с многодисплейными компьютерами и с резервированными вычислительными сетями.

Основными характеристиками LICS являются: высокая надежность; безопасность; сбалансированность системы и ее компонентов; уникальная встроенная система самодиагностики; отсутствие лицензионных ограничений; совместимость с другими версиями Linux; способность выполнять функции сервера в вычислительных комплексах, где работают компьютеры с другими ОС, включая продукты Microsoft; интегрированность с системой контроля ПТК CENTRIS.

Продукт верифицирован по методикам, применяемым в атомной энергетике в России и Европе. Тестирование продукта производилось в течение двух лет независимыми организациями на полигоне АСУТП АЭС в Научно-исследовательском центре по

безопасности АЭС (г. Электрогорск) и в составе поставочного комплекта системы верхнего блочного уровня АСУТП АЭС "Бушер" (Иран), который был собран в полном объеме в Научно-исследовательском институте измерительных систем им. Ю.Е. Седакова (г. Нижний Новгород).

LICS используется в системе верхнего блочного уровня (СВБУ, разработки ИПУ РАН и НИИИС) и в системе контроля, управления и диагностики (разработки КИАЭ) в АСУТП АЭС "Бушер" (Иран) и "Куданкулам" (Индия). Из применений в России можно назвать систему управления перегрузочной машиной 3-го блока Калининской АЭС и систему РАКУРС исследовательского реактора ПИК в ПИЯФ.

Сформулируем главное преимущество выбора LICS: по сравнению с широким спектром версий Linux, которые за символическую стоимость наводнили рынок, LICS имеет документацию, выполненную по российским нормам, и гарантии от производителя на длительный срок. Это не разнородный набор свободно распространяемых программ, а продукт, качество и безопасность которого подтверждены.

SCADA-система рабочего ПО и Конфигуратора (РПОиК)

Открытая SCADA-система РПОиК разработана для ответственных приложений с уникальными гарантийными обязательствами от производителя высшей категории надежности [2]. Она предназначена для интеграции АСУТП АЭС и построения высокопроизводительных ПТК повышенной надежности с большим периодом эксплуатации.

Система разрабатывалась для АСУТП АЭС, и при ее проектировании закладывались свойства, максимально обеспечивающие надежность и высокую производительность.

Основными функциями системы являются:

- прием и обработка информации о состоянии объекта управления и систем АСУТП;
- обеспечение синхронизации времени всех систем АСУТП;
- регистрация событий с присвоением метки времени с точностью до одной миллисекунды и записью в архив;
- отображение информации на экранах дисплеев в различных форматах (мнемосхемы, диаграммы, графики и т.п.) и протокола текущих событий восьмью способами;
- формирование сигнализации;
- подавление выбросов ложной сигнализации, возникающих вследствие отказов по общей причине;
- обеспечение вывода команд управления технологическим оборудованием с фиксацией времени выдачи команды в АСУТП в архиве.

Основные особенности системы:

- работает на всей линейке вычислительной техники, включая мобильные, бытовые, офисные и промышленные компьютеры;
- совместима с произвольными системами автоматизации российского или зарубежного производства;

Система контроля ПТК CENTRIS

- позволяет создавать интегрированные АСУТП с автоматикой от различных производителей и организовывать обмен информацией между разнотипными системами автоматизации;

- в рамках единого информационного пространства позволяет организовывать АРМ для различных групп оперативного персонала, включая выделенные АРМ для контроля состояния оборудования АСУТП;

- обеспечивает доступ через Web-технологии;

- обеспечивает защищенный от несанкционированного доступа режим работы пользователя;

- содержит систему автоматического проектирования со встроенным языком программирования;

- объем обрабатываемой информации не ограничен (зависит от мощности вычислительных устройств, испытан на объеме в 8 тысяч аналоговых и 250 тысяч дискретных сигналов с потоком в 2 тысячи сигналов в секунду);

- в максимальной конфигурации обеспечивает 100% резервирование всех элементов, включая серверы, рабочие станции, сетевое оборудование и линии передачи данных;

- обеспечивает непрерывную работу АСУТП в течение неограниченного срока с учетом поэтапной замены технических средств, автоматический рестарт после включения электрического питания;

- позволяет производить обновление ПО без останова системы;

- не требует технического обслуживания;

- интегрирована с системой CENTRIS и промышленной ОС LICS;

- гарантия поддержки производителя – 30 лет с возможностью последующей замены на 64-разрядную версию.

РПОиК протестировано на специально созданном полигоне АСУТП в г. Электрогорске, где было установлено оборудование (60%) реальной АСУТП АЭС с реактором ВВЭР-1000. Тест продолжался в течение одного года, по его результатам было получено разрешение на применение РПОиК в системах АСУТП АЭС, важных для безопасности.

РПОиК используется на АЭС "Бушер" (Иран) в качестве основного интегрирующего ПО в составе СВБУ. Ведутся работы по применению РПОиК для двух промышленных АЭС в Индии и тяжеловодного атомного реактора в России.

РПОиК используется на АЭС "Бушер" (Иран) в качестве основного интегрирующего ПО в составе СВБУ. Ведутся работы по применению РПОиК для двух промышленных АЭС в Индии и тяжеловодного атомного реактора в России.

В отличие от продуктов "в коробке", по которым не дается никаких гарантий от производителя, РПОиК поставляется с пожизненной гарантией. Эксклюзивность поставки подразумевает заключение долгосрочных партнерских соглашений, в рамках которых может производиться модификация РПОиК под особенности и нужды заказчика, подключение уникальных устройств, реализацию нестандартных алгоритмов, а также при необходимости передачу исходных текстов программ.

Данная система предназначена для оперативного представления информации о состоянии компонентов ПТК, включая инициативное уведомление о неисправностях [3]. CENTRIS обеспечивает непрерывный контроль всех устройств и программ, входящих в комплекс, включая рабочие станции, серверы, сетевое оборудование, принтеры, внешние дисковые накопители, системы единого времени и т.д. Результаты могут выводиться на специализированные пульта контроля, что позволяет эффективно организовать эксплуатацию ПТК и реально улучшить степень их надежности и готовности. Система разрабатывалась для использования на АЭС, и при ее проектировании закладывались свойства, максимально обеспечивающие надежность и высокую производительность.

Основные возможности системы: контроль состояния технических средств и сетевого оборудования, ОС, прикладного ПО, диагностика зависаний; контроль физического проникновения в приборные стойки; контроль целостности ПО (защита от несанкционированной модификации) и точности синхронизации времени.

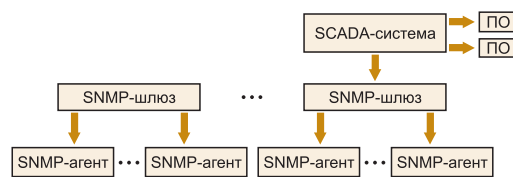
Особенностями системы являются: масштабируемость; поддержка работы с SNMP и NTP; открытый интерфейс с возможностью наращивания путем использования технологии plug-in; дублирование диагностической информации по предоставленным резервным каналам и рабочим местам; ведение единого архива событий; многоуровневый протокол событий; удобный графический интерфейс с пользователем; звуковая сигнализация; установка предупредительных уставок для диагностических сигналов, организации гибкой системы защиты и

предупреждения аварийных ситуаций; настраиваемые средства обновления диагностической информации.

Структура системы имеет три уровня (рисунок). Нижний уровень представлен SNMP-шлюзами, которые производят обмен информацией с SNMP-агентами, функционирующими на технических средствах (эти SNMP-агенты не входят в состав CENTRIS и поставляются производителями оборудования или являются свободно распространяемыми продуктами).

SNMP-шлюзы передают информацию в SCADA-систему по открытому протоколу. Передача осуществляется по циклическому принципу с заданным периодом, который настраивается для различного вида информации. Минимальная продолжительность цикла составляет одну секунду.

Резервированный вариант отличается от представленного на рисунке наличием дублирующих SNMP-шлюзов и SCADA-системы, которые функционируют на отдельных технических средствах и используют резервные линии связи.



Структура CENTRIS
(нерезервированный вариант)

Для средств вычислительной техники собирается следующая основная информация: загрузка процессора; объем свободной оперативной памяти и дисковой памяти; состояние сетевых устройств и др.; состояние замков; температура в процессорном блоке и др.

Для сетевого оборудования собирается следующая основная информация: наличие подключений (по портам); скорость передачи (по портам); наличие неисправностей и др.

Для оперативной системы собирается информация: число открытых сессий и запущенных программ; наличие нарушений целостности системных директорий (результатов взлома) и др.

Для прикладного ПО собирается информация: состояние (программа запущена или нет); специфические данные, зависящие от особенности программы.

CENTRIS представляет собой надежное и безопасное открытое решение для контроля ПТК, где требуется гарантия на поддержку от производителя и/или применяется уникальное оборудование, которое не стыкуется с массовыми программными продуктами.

Система верхнего уровня АСУТП

СВБУ АСУТП – это современное комплексное решение для автоматического сбора, хранения и представления информации о текущем состоянии технологического объекта управления и автоматизированного дистанционного формирования команд управления механизмами и алгоритмами АСУТП АЭС [4].

СВБУ создана для достижения: централизации контроля и управления ТП; экономически эффективного производства продукции; соблюдения эксплуатационных пределов, условий безопасной эксплуатации оборудования; улучшения характеристик ТП и работы технологического оборудования; уменьшения трудоемкости эксплуатации оборудования, улучшения ремонтнопригодности технических средств, снижения численности обслуживаемого персонала, улучшения потребительских характеристик элементов АСУТП; улучшения условий труда персонала, сокращения его числа и уменьшения последствий от ошибочных действий операторов.

На основе теоретических исследований существующих методов управления, а также в результате анализа мирового опыта были сформулированы следующие основные задачи СВБУ:

- регистрация текущего состояния и технологических событий, аварийных и переходных процессов;
- представление обобщенной информации по готовности технических систем безопасности;
- ведение протокола текущих событий;
- представление информации о режимах работы оборудования и автоматики; информации по расчетным задачам и задачам анализа оперативного состояния и диагностики;
- сбор данных о командах персонала;
- отображение мнемосхем, видеogramм на графических дисплеях и информации для управления на видеодисплеях;

- аварийная и предупредительная сигнализация на видеодисплеях;

- регистрация приема, выдачи и обработки управляющих воздействий в архиве СВБУ с присвоением им меток времени, введенных при помощи ключей индивидуального управления;

- архивация ресурса работы оборудования и диагностики его работы;

- регистрация и архивация состояния, ремонтов и замен технологического оборудования, записей операторов;

- распечатка данных за смену и периодических отчетов;

- управление локальными регуляторами с рабочих станций;

- контроль и управление режимом технологической защиты (технологической блокировки), управление программами логического управления с рабочих станций; управление контрольными и диагностическими задачами;

- сбор и обработка информации о состоянии средств и систем АСУТП;

- диагностика технических и программных средств АСУТП;

- ведение единого времени и присвоение метки времени при сборе данных;

- информационная поддержка управления штатным функционированием системы;

- операторское управление функционированием СВБУ;

- автоматическое управление в части автоматического реконfigurирования резервируемых элементов СВБУ и рестарта системы после отказа по общей причине (обесточивания);

СВБУ представляет собой распределенный ПТК, основными элементами которого являются АРМ, дублированные серверы, локальная вычислительная сеть и шлюзовые устройства. Взаимодействие СВБУ со смежными ПТК АСУТП осуществляется через шлюзы, подключенные к ЛВС СВБУ, в которых на программном уровне обеспечивается информационная совместимость с СВБУ.

Особенностью взаимодействия элементов СВБУ является применение технологии "клиент-сервер", в результате чего алгоритм функционирования каждой подсистемы разбивается на совокупность алгоритмов функционирования шлюзов, серверов и рабочих станций, решающих соответствующие им задачи внутри себя и обменивающихся между собой сетевыми сообщениями.

СВБУ испытана для обработки не менее 8 тысяч аналоговых и 250 тысяч дискретных сигналов, при этом объем обрабатываемой информации может быть увеличен. Система обладает следующими показателями временной задержки прохождения сигналов: на команду оператора $\leq 2,0$ с; на запрос оператора о представлении оперативной технологической информации на экране дисплея $\leq 2,0$ с. Обеспечивает следующие показатели надежности: средняя наработка на отказ $\leq 10^5$ час; коэффициент неготовности $\leq 1 \cdot 10^{-5}$.

СВБУ является полностью российским изделием, разработано на основе собственных программных компонент ИПУ РАН и свободно распространяемых продуктов, которые верифицированы и аттестованы для применения в атомной энергетике для систем, важных для безопасности. Система построена на основе только отечественных комплектующих, аттестованных Минобороны РФ. Техническая документация разработана по российским нормам. Испытания СВБУ проводились на специально построенном полигоне, приемка осуществлялась межведомственной комиссией. Все технические решения и ПО обладают полной лицензионной чистотой, что позволяет гарантировать поддержку системы в течение всего срока жизни. СВБУ производства поставлена на АЭС "Бушер" (Иран) и готовится к поставке на АЭС "Куданкулам" (Индия).

Полетыкин Алексей Григорьевич — канд. техн. наук, и.о. заведующего лабораторией 31,
Жарко Елена Филипповна — канд. техн. наук, ст. научный сотрудник,
Зуенкова Ирина Николаевна — научный сотрудник,

Промыслов Виталий Георгиевич — канд. физ-мат. наук, ст. научный сотрудник,
Бывайков Михаил Евгеньевич — канд. техн. наук, ст. научный сотрудник,
Менгазетдинов Надир Энверович — ст. научный сотрудник
Института проблем управления им. В.А. Трапезникова РАН.

Контактный телефон (495) 334-75-71. E-mail: poletik@ipu.rssi.ru [Http://www31.ipu.rssi.ru](http://www31.ipu.rssi.ru)

СОЗДАНИЕ СИСТЕМЫ РАДИАЦИОННОГО КОНТРОЛЯ НА БАЗЕ SCADA-СИСТЕМЫ MASTERSCADA

В.И. Чернышев (ЗАО "НПП "Доза")

Рассмотрены этапы развития проекта создания полноценной системы радиационного контроля (СРК) специалистами ЗАО "НПП Доза". Обоснованы причины выбора SCADA-системы MasterSCADA для использования в современной версии СРК. Кратко представлен первый проект с использованием MasterSCADA, реализованный для ФГУП ИРМ (г. Заречный).

ЗАО "НПП Доза" занимается разработкой и производством приборов и оборудования радиационного контроля с 1991 г. В мае 2006 г. предприятие отметило свой 15-летний юбилей. С 1999 г. в недрах фирмы заговорили о проекте создания полноценной системы радиационного контроля (СРК). В это же время возникла задача реализации пакета программ верхнего уровня (ВУ) для этой системы. В первую очередь были сформулированы основные требования, предъявляемые к такому пакету программ: надежность работы; наглядность и однозначность отображения измеряемой информации; своевременность подачи предупреждающих сигналов; сохранность ключевых измерений для последующего анализа; возможность построения пользовательских отчетов; настраиваемость, масштабируемость.

Для обеспечения надежности работы программно-аппаратного комплекса ВУ применяются:

1. промышленные, высоконадежные серверы в качестве серверов БД и компьютеров-шлюзов информации нижнего уровня (НУ); промышленные рабочие станции в качестве центрального пульта управления и критически важных АРМ операторов;
2. "горячее" и "холодное" резервирование серверов, дублирование АРМ операторов;
3. "горячее" резервирование каналов связи НУ с ВУ.

Список литературы

1. Масолкин С.И., Промыслов В.Г., Жарко Е.Ф., Антонов А.В., Промыслова О.А., Степанянц А.С. Системное ПО LICS как компонент подсистем АСУТП АЭС // Автоматизация в промышленности. 2004. №10.
2. Полетыкин А.Г., Бывайков М.Е., Менгазетдинов Н.Э., Байбулатов А.А. Основные решения по созданию системы верхнего (блочного) уровня АСУТП АЭС // Тр. ИПУ РАН том XVIII. 2002.
3. Масолкин С.И., Промыслов В.Г., Менгазетдинов Н.Э. Диагностика программно-технических средств с использованием интеллектуальных агентов // Доклад на II Международной конференции "Идентификация систем и задачи управления". 2003.
4. Полетыкин А.Г., Бывайков М.Е., Менгазетдинов Н.Э., Байбулатов А.А. Основные решения по созданию системы верхнего (блочного) уровня АСУТП АЭС // Ядерные измерительно-информационные технологии. 2004. №1-2.

4. полнофункциональное тестирование ПО, в том числе на запредельных нагрузках.

Наглядность отображения измеряемой информации обычно реализуется в ПО оператора с помощью: мнемосхем, трендов, таблиц и отчетов. Однозначность отображения ситуации закладывается на этапе проектирования системы с учетом специфики предприятия, измерителей, измеряемых величин и персонала.

Своевременность подачи предупреждающих сигналов обеспечивается:

1. асинхронной передачей информации от измеряющего блока по готовности (без использования идеологии опроса);
2. мгновенным отображением соответствующей информации по факту формирования события и формированием исполнительной команды для сигнализирующих устройств и релейных схем;
3. использованием ОС РВ и БД РВ.

Механизм очередей событий и команд, а также пропускная способность каналов передачи данных при максимальной нагрузке должны обеспечивать пропускную способность заведомо больше расчетной.

Сохранность измерений достигается введением специализированного сервера БД в состав ПО ВУ, обеспечивающего поддержку работы со встроенными аппаратными архивами, с таблицами измерений

ДЕКОНТ-Ех

**Многофункциональный
взрывозащищенный
комплекс**



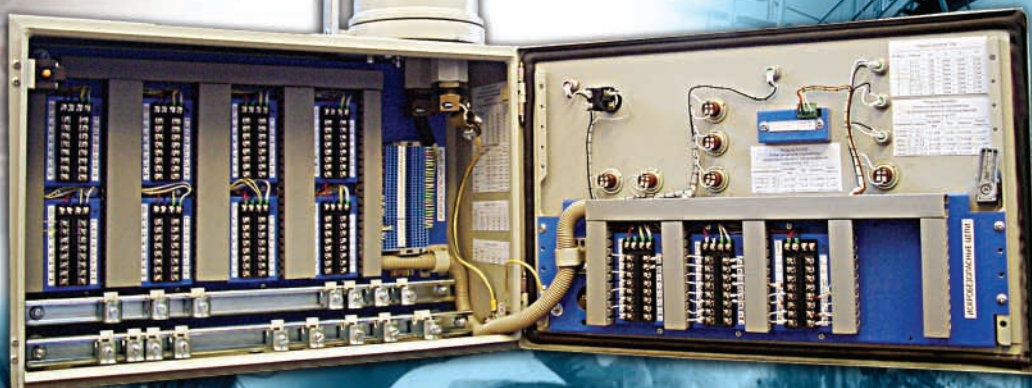
- Компактная модульная конструкция
- Низкое энергопотребление
- Индивидуальная маркировка взрывозащиты модулей



PO Exia/0ExiaIICt6



PB Exd[ia]
/1Exd[ia]IICt6



Компания
ДЭП
www.dep.ru
(495) 995-00-12

ЕЩЁ НАДЁЖНЕЕ!

**Повышенная
устойчивость к вибрации**



ПРОМЫШЛЕННЫЕ ПК НА ЗАКАЗ



- + Дополнительные крепления для плат любого формата
- + 100% выходное тестирование
- + Широчайший выбор конфигураций

Только в ПРОСОФТ вы можете заказать промышленные ПК с дополнительными креплениями, которые реально обеспечивают повышенную виброустойчивость

PROSOFT®

МОСКВА
С.-ПЕТЕРБУРГ
ЕКАТЕРИНБУРГ
САМАРА

Телефон: (495) 234-0636 • Факс: (495) 234-0640 • E-mail: info@prosoft.ru • Web: www.prosoft.ru
Телефон: (812) 448-0444 • Факс: (812) 448-0339 • E-mail: info@spb.prosoft.ru • Web: www.prosoft.ru
Телефон/факс: (343) 376-2820/376-2830 • E-mail: info@prosoftsystems.ru • Web: www.prosoftsystems.ru
Телефон: (846) 277-9165 • Факс: (846) 277-9166 • E-mail: info@samara.prosoft.ru • Web: www.prosoft.ru