

**A**втоматизированные системы управления, как правило, имеют общий недостаток – высокую степень уязвимости обрабатываемой информации, существующей в новой электронной форме, и, как следствие, необходимость ее защиты от различных воздействий, в том числе и так называемого «информационного оружия» – одного из компонентов ведения информационных войн. Ряд стран мира ведет интенсивную подготовку к информационным войнам. Уже сейчас элементы этих войн становятся обязательными факторами, предшествующими и сопровождающими силовые формы вооруженной борьбы.

В этих условиях использование отечественных защищенных аппаратно-программных платформ с ограниченными функциональными возможностями, даже если они соответствуют международным протоколам и стандартам, возможно лишь в определенных областях, связанных, как правило, с управлением техническими устройствами (комплексами) и технологическими процессами. Создание на их основе сложных «человеко-машинных» автоматизированных систем весьма проблематично.

Кроме того, использование узкоспециализированных отечественных аппаратно-программных платформ, которые,

но безопасных гетерогенных территориально-распределенных автоматизированных систем специального назначения лежит в области создания ряда (линейки) отечественных унифицированных информационных технологий, которые должны функционировать на различных аппаратных платформах – от «майнфреймов» до встраиваемых систем – в любых условиях обстановки (агрессивные среды, работа в движении и т.д.) и размещения (стационарные и мобильные, наземные, морские, воздушные и космические объекты).

В соответствии с современными взглядами, линейка программных средств представляет собой их широкий набор,

# ОТЕЧЕСТВЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ – ЗАДАЧИ, РЕШЕНИЯ, ПЕРСПЕКТИВЫ

Сергей Маняшин – директор ОАО «Всероссийский научно-исследовательский институт автоматизации управления в непромышленной сфере им. В.В. Соломатина»



**На базе ВНИИНС уже создан и успешно функционирует центр подготовки специалистов из числа разработчиков и обслуживающего персонала АС ВН, должностных лиц органов государственного и военного управления, специалистов научно-исследовательских организаций Министерства обороны и других силовых структур.**

Ни у кого не вызывает сомнения тот факт, что информационная безопасность автоматизированных систем зависит от степени защищенности их аппаратной и программной платформ (в первую очередь операционной системы). В настоящее время многократное возрастание сложности таких платформ – объективный факт. И этот рост не могут ограничить ни необходимость защищенности систем, ни трудности с контролем качества, ни сертификация по требованиям безопасности информации.

Неоспоримо также и то, что недопустимо использовать зарубежные коммерческие платформы для создания автоматизированных систем специального назначения. В свою очередь, конкуренция на рынке информационных технологий (ИТ) лишь частично определяется их защищенностью. Основным критерием конкурентоспособности аппаратно-программных платформ являются их функциональные возможности и потребительский спрос.

в свою очередь, должны обладать требуемыми функциональными возможностями, соответствовать мировым достижениям в сфере ИТ, поддерживать необходимые периферийные устройства и противодействовать средствам известного на момент их создания «информационного оружия», возможно лишь до той поры, пока система управления конкретным техническим комплексом не претерпит изменений. Таким образом, срок «жизни» узкоспециализированных аппаратно-программных платформ определяется сроком «жизни» либо самого технического комплекса, либо его системы управления и никак не связан с развитием ИТ в мире.

Развитие подобных платформ, например «Багет», ориентировано на обеспечение минимума функциональности аппаратуры и операционной системы. Поэтому в автоматизированных системах они могут применяться только для управления окончательными устройствами.

Решение же проблемы информацион-

пронизанный единой идеологией защиты информации и поделенный на уровни от системного до прикладного, с единым интерфейсом как с точки зрения пользователя или администратора, так и с точки зрения разработчика. Такая линейка должна постоянно развиваться и совершенствоваться в соответствии с мировым уровнем. Только в этом случае отечественные программные средства могут позиционироваться как альтернатива зарубежным технологиям.

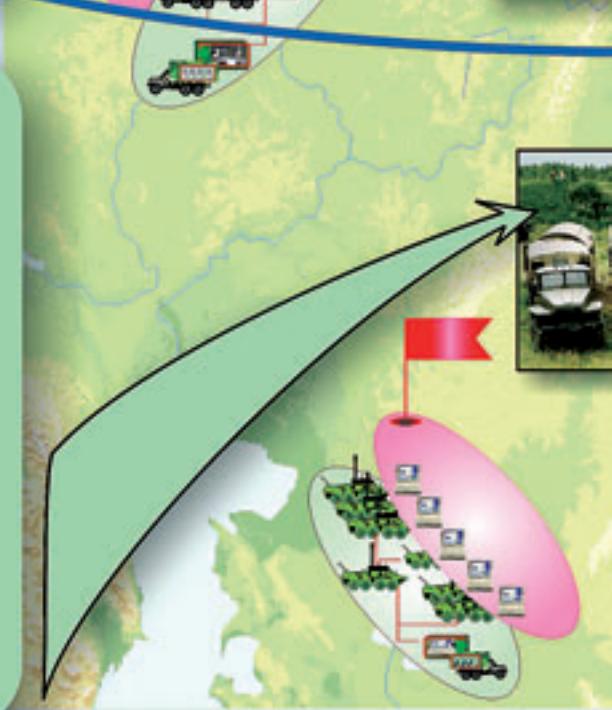
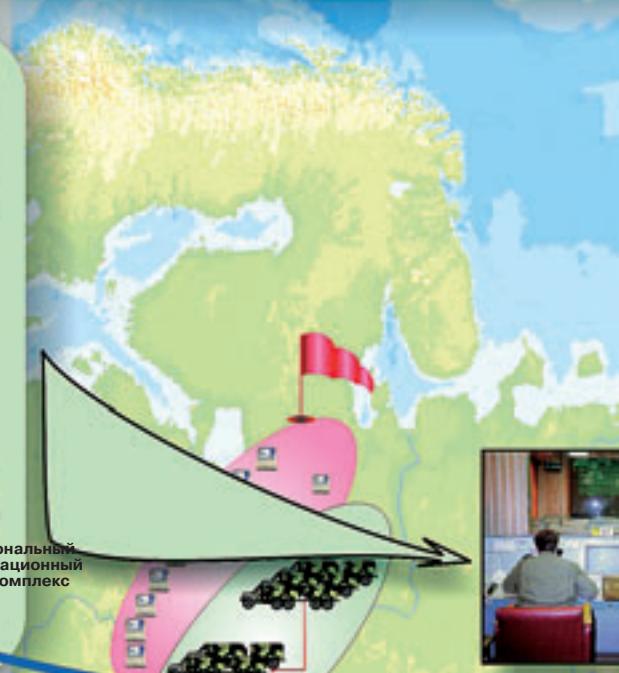
Однако создание отечественных конкурентоспособных программных продуктов – экономически емкий процесс, который должен иметь общегосударственный характер. Но и в этом случае сделать «все свое от начала до конца» – почти невыполнимая задача, требующая колоссальных временных и финансовых затрат. Именно поэтому такая работа может проводиться только строго в соответствии с перспективными планами (программами), поэтапно и с активным использованием результатов мирового научно-технического прогресса в области информационных технологий.

Практика доказала, что в отечественной программной продукции наиболее целесообразно ориентироваться на программное обеспечение с открытым исходным кодом, что позволило сформировать новую, более эффективную организационную модель разработки, за счет более тщательного тестирования повысить качество операционных систем, со-

## СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ

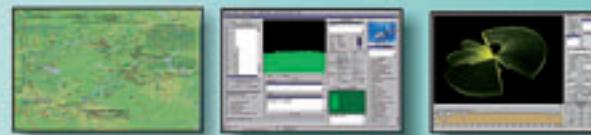
## БАЗОВЫЕ ИНФОРМАЦИОННЫЕ ЗАЩИЩЕН

- доверенные средства разработки
- геоинформационная система
- комплекс программ обеспечения
- защищенные средства гипертекс
- защищенная система управления
- защищенная операционная систе



# ОВАННЫХ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ

ОБЕСПЕЧЕНИЕ



НЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ:

п о в с е д н е в н о й д е я т е л ь н о с т и  
т о в о й обработки информации  
б а з а м и д а н н ы х  
м а

СИСТЕМА ОБЕСПЕЧЕНИЯ  
БЕЗОПАСНОСТИ  
ИНФОРМАЦИИ



кратить количество ошибок и стоимость, сроки освоения сложных проектов. Это оценили и специалисты ведущих фирм мира (IBM, Novell, Oracle, SAP, People Soft и др.). И перевод программных продуктов этих фирм на программное обеспечение с открытыми кодами стал катализатором его развития.

Недостаточная защищенность и надежность корпоративных операционных систем (ОС) типа Windows, регулярно обнаруживаемые изъяны, а также агрессивная лицензионная политика фирмы Microsoft вынудили государственные организации (включая силовые ведомства) Японии, Франции, Германии, Англии, Китая, Индии искать альтернативные операционные системы с открытым кодом на базе ОС Linux. В США государственные структуры также переходят на эту систему. Мощным ударом по позициям Microsoft стало объединение усилий разработчиков Китая и Японии по созданию ОС Asianix для государственных нужд этих стран и стран Азиатского региона.

Следует отметить, что Россия одной из первых приступила к решению проблемы отечественного информационно-безопасного программного обеспечения. Так, в середине 90-х годов прошлого века по заказу Министерства обороны Российской Федерации в рамках целевой комплексной программы во Всероссийском научно-исследовательском институте автоматизации управления в непромышленной сфере (ВНИИНС) под руководством академика В.В. Соломатина была разработана линейка программных продуктов, получившая впоследствии название «Базовые информационные защищенные компьютерные технологии» (БИЗКТ).

Одной из причин разработки данных технологий, наряду с необходимостью иметь отечественные продукты и быть технологически независимыми, стало достижение высокой степени типизации и унификации системных компонентов. Это дало возможность выделить максимальные людские и финансовые ресурсы на разработку специального программного обеспечения (по мнению зарубежных специалистов, его стоимость составляет до 70% от стоимости системы) автоматизированных систем военного назначения (АС ВН).

Вместе с тем использование в АС ВН серийно выпускаемых продуктов БИЗКТ (типовых программно-технических комплексов, защищенного общего и общесистемного программного обеспечения, унифицированных элементов информационного лингвистического обеспечения, средств защиты информации и объекта ав-

томатизации) позволит не только сэкономить 25–30% финансов, но и создаст условия для интеграции их в единую АСУ Вооруженных Сил РФ и формирования единого информационного пространства.

Основу БИЗКТ составляет линейка взаимодействующих операционных систем MCBC 3.0, «Оливия», «Омоним» на базе открытых кодов, предназначенных для различных аппаратных платформ: S/390, x86, «Эльбрус-90микро», «Эльбрус-3М1», SPARC и MIPS. По своим функциональным возможностям они не уступают зарубежным аналогам.

К настоящему времени накоплен большой опыт создания отечественной программной продукции на базе открытых кодов. Прошли сертификацию по требованиям безопасности информации, принятые на снабжение и серийно выпускаются более 50 программных средств из состава БИЗКТ. Наряду с операционными системами представлены системы управления базами данных, средства разработки приложений, web-средства, офисные программы, картографический редактор и еще ряд программных продуктов, необходимых для АС ВН, обрабатывающих информацию, составляющую государственную тайну.

Однако для АС ВН высоких классов защищенности, помимо доверенного программного обеспечения, потребовалась разработка семейства электронных замков «Цезарь», которые в настоящее время обладают необходимыми сертификатами безопасности ФСБ России. Они серийно выпускаются нашей промышленностью и единственные из разрешенных к применению в Вооруженных Силах.

Наличие полной линейки отечественных взаимодействующих защищенных программных средств позволило руководству Министерства обороны принять решение о переводе всех АС ВН на «Базовые информационные защищенные компьютерные технологии». А положительная оценка, данная Президентом Российской Федерации в 2001 году отечественным программным средствам, разработанным по заказу Министерства обороны, позволила рекомендовать их к применению в автоматизированных системах всех силовых министерств и ведомств России.

Вместе с тем соблюдение всех международных стандартов и протоколов при создании средств БИЗКТ и поддержка ими практически всех применяемых аппаратных платформ позволяют использовать их в автоматизированных системах других органов государственной власти, государственных предприятий, банков и других объектов, для которых

защита информационных ресурсов – необходимое условие успешного функционирования.

Следует отметить, что использование отечественных информационных технологий в автоматизированных системах сдерживается отсутствием необходимого уровня подготовки специалистов по БИЗКТ и российской системой обучения, которая по-прежнему ориентирована на изучение зарубежной корпоративной программной продукции. Экономически это означает, что огромное количество денег в виде лицензий на программное обеспечение, плату за учебные курсы и сертификацию специалистов, а также за техническую поддержку «уходит» из страны и способствует развитию зарубежных компьютерных гигантов.

На базе ВНИИНС уже создан и успешно функционирует центр подготовки специалистов из числа разработчиков и обслуживающего персонала АС ВН, должностных лиц органов государственного и военного управления, специалистов научно-исследовательских организаций Министерства обороны и других силовых структур.

В МИФИ с участием сотрудников ВНИИНС уже более 5 лет студенты обучаются в специализированных группах, читаются курсы лекций в ряде военных академий и училищ. Однако для масштабов нашей страны этого явно недостаточно. Министерству науки и образования необходимо внести изменения в учебные программы и планы вузов страны. Кроме того, требуется создать государственную систему сертификации ИТ специалистов, аналогичную системе фирмы Microsoft, обеспечив ее признание на российском ИТ рынке труда.

В заключение следует отметить, что наличие у государства собственных информационных технологий в определенной степени характеризует уровень его научно-технического потенциала, обеспечивает его технологическую независимость и высокую степень информационной безопасности систем управления критически важными отраслями экономики и вооруженными силами страны. □



ОАО «ВНИИНС»

Россия, 117638, Москва,  
ул. Сивашская, 4, корп. 2  
Тел.: (495) 119 -6842  
Факс: (495) 310 -7097  
E-mail: vniins@vniins.ru