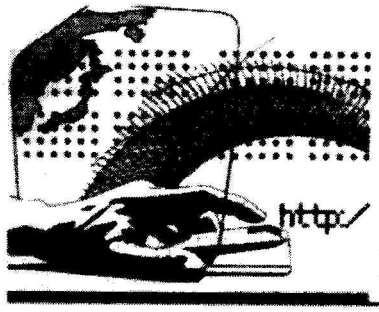
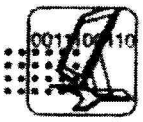


МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



УДК 004.056

А.П. Баранов

ЦБС ФСБ России

О ПРАКТИКЕ ПРИМЕНЕНИЯ В ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ ПРОГРАММНЫХ ПРОДУКТОВ ИНОСТРАННОГО ПРОИЗВОДСТВА

Рассматриваются вопросы применения в отечественных защищенных информационно-телекоммуникационных системах (ИТС) программно-аппаратных средств российского и иностранного производства.

Анализируется соотношение применения как отечественных, так и импортных программно-аппаратных средств с учетом принятия новых законов Российской Федерации, в первую очередь новой редакции закона "Об информации, информатизации и безопасности информации". Обосновывается необходимость совершенствования законодательства в этой области.

Указаны причины, приводящие к необходимости применения в ИТС в ряде случаев импортных, но сертифицированных в России программно-аппаратных средств.

Отмечены особенности сертификации телекоммуникационного оборудования.

A.P. Baranov

PRACTICAL EXPERIENCE OF FOREIGN PRODUCTS' APPLICATION IN SECURE INFORMATION SYSTEMS

This article is dedicated to discussion of problems concerning application of Russian and foreign soft- and hardware in secure informational-telecommunication systems (ITS).

The comparison of Russian and foreign soft- and hardware application is analyzed. The analysis is taken in the scope of new-passed laws of Russian Federation "About information, informatisation and information security". The necessity of the laws' revision are listed.

The reasons leading to the necessity of application in some cases foreign, but certified in Russia soft- and hardware in ITS are listed. Attention is also drawn to specific points in the process of certification.

В отечественных информационно-телекоммуникационных системах (ИТС) в защищенном исполнении применяются как отечественные, так и импортные программно-аппаратные средства. Этот тезис относится к программно-аппаратной части,

обеспечивающей функционирование прикладного уровня, и к части, обеспечивающей работу транспортной, телекоммуникационной составляющей. На предыдущей конференции в докладе автора был представлен спектр основных средств, сертифицированных по требованиям информационной безопасности (ИБ) на трех уровнях: транспортном, операционных систем (ОС), совместно или отдельно с СУБД, и прикладном.

За прошедший год произошел ряд событий, обострivших проблематику обеспечения ИБ и привлекших к этому направлению дополнительное внимание научной и политической общественности. Прежде всего это два новых закона Российской Федерации: по персональным данным и новая редакция, а по существу новый закон "Об информации, информатизации и безопасности информации".

Принято решение и проведен конкурс о развертывании в России двух крупных производств элементной базы на уровне 0,25 мк. Ожидаемое начало производства чипов — 2009 г.

Неожиданно быстро появилась ОС Vista на замену W-XP. По времени это событие совпало с окончанием работ по дополнению Windows XP требуемыми защитными функциями.

Отмеченные моменты и ряд других опять поставили на повестку дня вопрос о применении и соотношении в современных ИТС отечественных и иностранных программно-аппаратных продуктов. Развитие отечественных производителей "подталкивает" идею о законодательном закреплении применения по крайней мере в критических системах только продукции российского производителя. В этом году такой проект закона рассматривался и не был рекомендован к принятию. При этом компьютерное сообщество продолжает наращивать усилия по развитию отечественного высокотехнологического сектора и оказывает отечественным производителям поддержку, вплоть до определенного протекционизма в его трудной борьбе с крупными, эффективными и богатыми иностранными конкурентами.

Однако это не означает отказ или ограничение применения передовых научно-технических достижений, имеющихся в мире. Исторический пример с ЕС ЭВМ многому научил. К настоящему времени ясно, что построить современную, высокоэффективную, в дальнейшем достаточно легко развиваемую и продолжительно эксплуатируемую ИТС только на отечественной базе невозможно. Следовательно, надо научиться правильно, с учетом ИБ, применять как отечественные достижения, так и иностранные технологии. Если применение отечественных технологий в защищенных системах ограничивается их функциональными возможностями и наличием у изготовителя соответствующих функций, в том числе обеспечивающих свойства ИБ, то с иностранными дело обстоит сложнее.

1. Почему приходится применять импортное ПО

1. Высокий уровень развития прикладного ПО обусловлен тем, что его разработкой на основе нескольких базовых ОС занимается весь мир, т. е. миллионы высококвалифицированных программистов. Поэтому применение ОС вызвано не только свойствами самой ОС, но в первую очередь широтой и развитостью прикладного ПО.

Организовать отечественную разработку такого объема и масштаба пока не удалось. Похоже, что одной стране, какая бы она ни была, это и не удастся сделать, несмотря на неоднократные попытки.

2. Очень большое опережение, мирового "чипостроения", по сравнению с российским по элементной базе и получение рядом производителей ПО информации о новых чип-сетах заранее до их массового выпуска. Сращивание ПО и "железа", внедрение низкоуровневых программ непосредственно в кристальную часть. Примеры:

чипы интеллектуальных карт, микросхемы, реализующие значительную часть физического транспортного протокола, содержат большую фиксированную программу часто непосредственно в кристалле; микропроцессоры общего назначения значительную часть команд также содержат в центральном ядре и т. д.

Ряд иностранных программистских фирм непосредственно участвует в создании и разработке чип-сетов. Это Microsoft и Intell, SUN Microsistem, HP и др.

Поэтому даже для поддержания современного прикладного уровня ИТС придется применять иностранную технику, в том числе и для создания защищенных ИТС.

2. Для защищенных ИТС приходится применять иностранные, но сертифицированные по российским требованиям к обеспечению ИБ ПО и аппаратные компоненты

При построении защищенной ИТС сначала рассматривается и применяется отечественное оборудование физического уровня, например SDH:

а) выше уровня первичной сети существует отечественное оборудование только ISDN в ЦАТС;

б) выше TCP/IP пока только импорт;

в) поэтому для обеспечения надежности работы предлагается реализовывать компонент повышенной устойчивости.

Рассмотрим сертификацию ПО, имеющую наибольший опыт. Сертифицировать следует только ПО, по которому представляется вся архитектурно-конструкторская документация и документированные с пояснениями исходные тексты. Опыт имеется: Windows XP, Solaris 10 (Trusted), Linux.

Экспертная организация, работающая совместно с лицензионно-сертификационным органом ФСБ России по вопросам направлений и проведения тематических исследований, взаимодействует с организациями-лицензиатами ФСБ России, имеющими право на работу с государственной тайной. Это связано с тем, что требования составляют государственную тайну и ТЗ, как правило, имеет пометку "Для служебного пользования". Поэтому, если фирма-производитель не является лицензиатом ФСБ России в этой области, то ей целесообразно подобрать отечественного представителя и заключить с ним соответствующий договор, включающий взаимные обязательства о неразглашении сведений конфиденциального характера. Если производитель — инофирма, рекомендуется получить разрешение национального правительства на передачу в Россию указанной выше конструкторской документации для проведения исследований и сертификации. Фирма-лицензиат-представитель готовит ТЗ на тематические исследования рассматриваемого продукта либо для себя, если у нее есть лицензии на проведение тематических исследований, либо для другого лицензиата. ТЗ необходимо для согласования объема работ, чтобы эксперты по ходу работ не требовали проведения дополнительных исследований. Экспертная организация рассматривает результаты тематических исследований и готовит заключение. Выписка из заключения может быть представлена фирме-лицензиату-представителю. Сертификат предоставляется заявителю.

По имеющемуся опыту на изучение развитой ОС с определенным набором прикладного продукта уходит 3–5 лет. Продукт живет, как правило, около 10 лет, т. е. 5 лет он используется с поддержкой и еще 5 лет — по инерции. Как только сертификация продукта закончена, следует начинать разработку следующей версии. Таким образом, задержки в применяемом продукте составляют около 5 лет.

Аналогичная ситуация, насколько известно, наблюдается и в развитых странах, несмотря на то, что производители работают в этих странах. Видимо, дело в существенном различии ПО для защищенных ИТС и общего применения. Как правило,

применяемые в защищенных ИТС ОС и прикладные продукты имеют некоторые дополнения, которые усиливают их защитные свойства.

3. Особенности сертификации телекоммуникационного оборудования

Общая схема такая же, как и для ПО. Имеющийся опыт сертификации показывает, что различия в объеме работ с иностранными заявителями или отечественными производителями практически нет. Например, DX-500 сертифицировалось около 5 лет, вместе с доработками. "Hicom" — 3 года, но для обработки несекретной информации и по низкому классу устойчивости. Сейчас на сертификации — "Квант ЕУ". Работа продолжается уже 3 года и процесс не закончен. Платформа Т-7 — 3 года для обработки открытой информации по требованиям устойчивости, как для "Hicom".