УДК 004.9

ОБОСНОВАНИЕ ПОДХОДА К СОЗДАНИЮ ДОВЕРЕННОЙ ПРОГРАММНО-АППАРАТНОЙ СРЕДЫ

[1]Жидков И.В., [1]Кадушкин И.В., [1]Шубенин А.А.

[1]3-й Центральный научно-исследовательский институт Министерства обороны Российской Федерации (3 ЦНИИ» Минобороны России), Москва, Россия (*107564, Погонный проезд, д. 10)*

Рассмотрены основные проблемы создания доверенной программно-аппаратной среды и пути их решения.

Ключевые слова: автоматизированные системы, информационная безопасность, доверенная программно-аппаратная среда.

RATIONALE FOR TRUSTED APPROACH TO CREATING SOFTWARE AND HARDWARE ENVIRONMENT

[1]Zhidkov I.V., [1]Kadushkin I.V., [1]Shubenin A.A.

[1] 3rd Central Scientific - Research Institute of Ministry of Defense of the Russian Federation, Moscow , Russia (107564 , Pogonnyi passage, h. 10)

The main problem of creating a trusted hardware and software environment and ways of solving them.

Keywords : automated systems, information security, trusted software and hardware environment .

Созданию доверенной программно-аппаратной среды (ДПАС) для автоматизированных систем управления (АСУ) в последние десятилетия посвящены многочисленные усилия заказчиков и разработчиков. На это прямо или косвенно были нацелены выработка и стандартизация требований к вычислительным системам, к качеству программных средств и информационных систем, к системам менеджмента качества предприятий и организаций, создающих и выпускающих указанную продукцию, создание систем сертификации средств защиты информации, принятие и реализация соответствующих целевых программ в интересах различных министерств и ведомств.

Вместе с тем, проведенные с 90-х годов прошлого века реформы силовых структур, оборонно-промышленного и производственных комплексов, научно-исследовательских институтов и организаций, отсутствие технологической независимости России в области ИТ, первые результаты построения в России электронного правительства, а также проявления глобального экономического кризиса явились источником технологических, экономических, психологических, правовых, финансовых и организационных проблем для создания ДПАС АСУ (см. рис. 1).

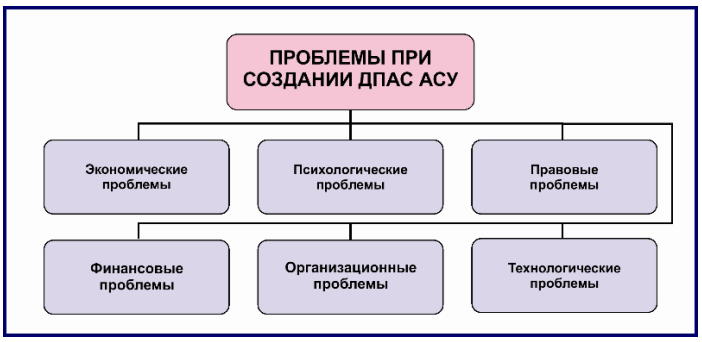

Рис. 1. Проблемы для создания ДПАС АСУ

Технологические проблемы обусловлены отсталостью не только ИТ отечественного производства, но и технологий в тех областях экономики и государственного управления, которые должны обеспечивать процесс создания ДПАС. Эти проблемы обострились в результате либерализации рынка программно-аппаратных средств при одновременном противодействии доступу России к новым информационным технологиям, отсутствия целенаправленной согласованной технической политики в области контроля и обеспечения качества и безопасности программных средств, и АСУ в целом. К примеру, около 90% задействованных в специализированных АСУ аппаратно-программных средств и операционных систем (ОС) разработаны и произведены за рубежом. С другой стороны, военно-политическим руководством ряда государств разработан широкий спектр методов и технологий информационного воздействия как на отдельные средства вычислительной техники, так и на информационно-телекоммуникационные системы России. Сами угрозы носят зачастую скрытый характер и маскируются под случайно пропущенные неумышленные ошибки или злоумышленные воздействия, направленные на снижение качества или угрожающие безопасности. Воздействия выражаются в нарушениях качества или безопасности функционирования систем. Предпринимаются практические шаги по реализации явного или скрытного негативного воздействия.

В свою очередь, процесс разработки, совершенствования (модернизации), сертификации и подготовки к внедрению программных продуктов иногда затянут во времени на долгие месяцы. Сопровождение отечественных средств не всегда соответствует лучшим мировым практикам и современным требованиям.

Экономические проблемы возникают, в основном, в связи с реализацией структурного реформирования Министерств и ведомств. Это приводит к сокращению финансирования на определенных направлениях, а в некоторых случаях и к отказу от дальнейшей работы с исполнителями текущих НИОКР по созданию АСУ. Следствием этого, является утрата наработанного научного и технологического задела, разрушение сложившихся коллективов, потеря преемственности не только в разработках новых средств, но и в

сопровождении уже внедряемых средств. В конечном счете усугубляются проблемы совместимости и обеспечения взаимодействия АСУ.

К **психологическим проблемам** относится неготовность пользователей к дополнительным ограничениям их повседневной деятельности, связанных с особенностями использования средств защиты информации, а также уже сформировавшаяся в обществе устойчивая зависимость от Windows-приложений.

Правовые проблемы возникают в связи с использованием при разработке программных средств на базе «открытого кода», размещаемого в открытом доступе через Интернет (так называемое, «свободное ПО»). Это в основном – устаревшие версии с сопроводительной документацией невысокого качества. Выявление потенциально опасных фрагментов (см. рис. 2) не позволяет получить какие-либо официальные разъяснения и, тем более, не влечет никаких санкций, поскольку все выставлено бесплатно и без каких-либо обязательств. Тем самым размывается ответственность за возможные негативные последствия.

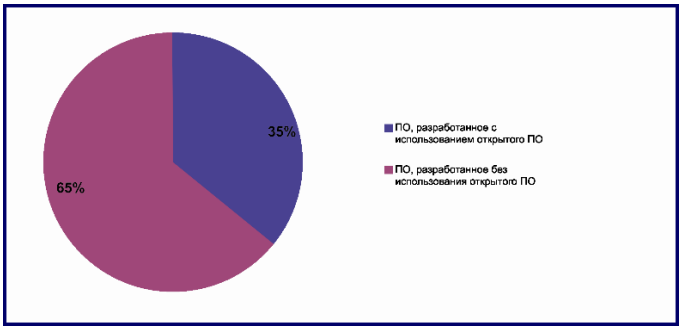

Рис. 2. Процентное соотношение уязвимостей в ПО [1]

Финансовые проблемы возникают в связи с высокой стоимостью внедрения новых информационных технологий (ИТ), ограниченными выделенными средствами и, соответственно, с необходимостью привлечения внебюджетных средств. Например, в условиях финансирования только в рамках заказов Минобороны России поддерживать желаемые темпы развития средств БИЗКТ проблематично. Более того, без использования средств БИЗКТ во всех органах государственного управления данный проект представляется коммерчески неконкурентоспособным по сравнению с продукцией ведущих мировых компаний, поскольку рынок Минобороны России недостаточен, чтобы обеспечить коммерческую эффективность.

Организационные проблемы связаны с необходимостью создания таких структур и механизмов в России, которые на практике обеспечивали бы комплексную организацию и планирование развития ДПАС. Например, существующий порядок корректировки

комплексных целевых программ не позволяет с достаточной оперативностью включать в них (соответственно задавать соответствующие новые НИОКР) создание новых ИТ, появляющихся на мировом и отечественном рынке.

Наиболее опасными являются целенаправленные негативные воздействия на технологии проектирования АСУ, электронно-компонентную базу, аппаратную среду, телекоммуникационную среду, средства аппаратно-программной загрузки, электронные замки, аппаратные средства шифрования и цифровой подписи, системные протоколы и алгоритмы, операционные системы, средства разработки программного обеспечения, приобретаемые (готовые) программные средства, производственную базу, непосредственно на разработчиков и поставщиков, на персонал АСУ.

В итоге, в процессе жизненного цикла АСУ неизбежно возникают угрозы негативного воздействия на программно-аппаратную среду и соответствующие риски [2]. Краткий анализ условий для формирования требуемого качества и безопасности элементной базы, аппаратных и программных средств с учетом реализуемых методов и технологий их контроля и сертификации, способствующих доверию к программно-аппаратной среде АСУ, показал следующее.

Из-за масштабности государственных проектов и отставания отечественной элементной базы имеют место вынужденные приобретения телекоммуникационных и компьютерных элементов и аппаратных средств из стран Юго-Восточной Азии, Европы, США. Оценить их качество и безопасность в полном объеме за приемлемый срок (за недели) невозможно, в лучшем случае применяется выборочный контроль. Тем самым имеет место риск недоверия к используемой элементной базе по степени выполнения требований к качеству и безопасности.

Ряд программных средств (например, BIOS) поставляются без исходных текстов и соответствующей документации, позволяющей провести их полноценную сертификацию по требованиям безопасности. В свою очередь, сертификация хоть и выявляет дефекты ПО, идентифицируемые как критические уязвимости, а также дефекты безопасности [1], но не дает 100%-ной гарантии отсутствия закладок и выявления недекларированных возможностей (см. рис. 3).

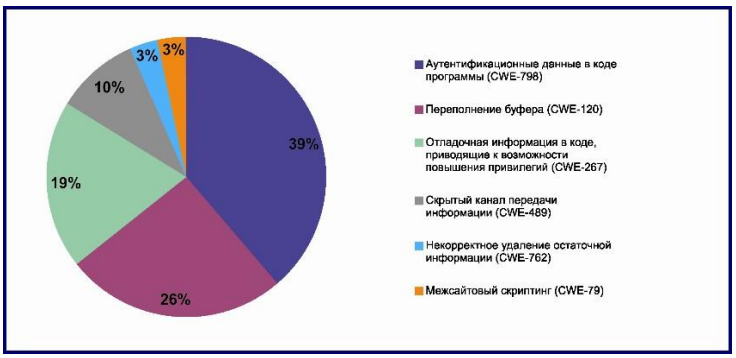

Рис. 3. Статистика по типам уязвимостей

Например, в испытательных лабораториях, как правило, строятся тестовые примеры, далеко не покрывающие все возможные ветви программ. Уровень покрытия 75% с помощью инструментальных средств тестирования является показателем сравнительно высокого качества проводимого тестирования. Сами сертификационные испытания занимают в среднем несколько месяцев. Более длительная сертификация (год - полтора) сдерживает реальную эксплуатацию и приводит к моральному устареванию и потере конкурентных преимуществ программ. Все инструментарии для анализа исходных текстов программ на закладки позволяют лишь выявить подозрительные места по тем формальным критериям, которые заложены в их алгоритмы.

Выявленные потенциально опасные фрагменты анализируются человеком – специалистом испытательной лаборатории. Это – как минимум, сотни фрагментов. Работа испытателя должна выполняться программистами высокой квалификации, владеющего несколькими алгоритмическими языками, обладающим соответствующим опытом построения и контроля сложных программных проектов, следящим за изменениями в области ИТ, периодически повышающим уровень квалификации в современных отечественных и международных центрах обучения ИТ для понимания логики построения современных программ зарубежными специалистами и способного провести адекватный семантический анализ выявленных фрагментов за несколько месяцев испытаний, удерживая в голове сложные структурные построения программ. Подобные специалисты востребованы по всем сертифицируемым программам. На практике уровень компетенции специалистов испытательных лабораторий не столь высок. В итоге, с учетом «человеческого фактора» на практике при сертификации нередко применяется выборочный контроль. Т.е. объективно существует опасность пропуска закладок или неверной логической интерпретации декларируемых и недекларированных функций, выполняемых потенциально опасными фрагментами. Аналогичная картина с программными средствами, создаваемыми отечественными разработчиками. Разница лишь в том, что в России

существует принципиальная возможность получения официальных разъяснений и исправления выявленных недостатков. Т.е. при сопоставимом уровне качества и безопасности за счет потенциальных возможностей контакта непосредственно с разработчиками программных средств с учетом реальной ответственности сторон по российскому законодательству уровень доверия к отечественным программным средствам изначально более высокий.

Тем самым риск недоверия к используемым программным средствам (в т.ч. сертифицированным) по степени выполнения требований к качеству и безопасности должен быть признан как объективная реальность, вызванная сложившимися условиями их разработки. В свою очередь, недоверие к программным и программно-аппаратным средствам вызывает недоверие к методам и технологиям их применения, используемым с их помощью информационным ресурсам, что сдерживает практические возможности создания, функционирования и развития АСУ, их подсистем и составных компонентов с задаваемым уровнем качества и безопасности.

Наличие систем качества на зарубежных предприятиях-поставщиках программно-аппаратных средств подтверждается в лучшем случае сертификатом соответствия требованиям стандарта ИСО 9001 (чаще – местными сертифицирующими органами. Если сравнивать страны Европы и Юго-Восточной Азии, то степень доверия к сертифицирующим органам из этих стран также различная). Построение системы непрерывного контроля качества на зарубежных предприятиях в интересах российских приобретателей практически невозможно или потребует неоправданных затрат. Кроме того, сертифицируются зачастую лишь системы менеджмента качества, а не сама продукция, поскольку стандартизация требований к качеству программных средств (например, на уровне стандартов ИСО/МЭК 9126, 12119, 12207, 14598, 15504, стандартов серии 25000) не развита ни в одной стране мира и находится в стадии становления. Редкий поставщик позволяет инспектировать систему качества на своем предприятии российским потребителям (к таковым редким исключениям формируется особое доверие). Следовательно, к самим предприятиям – поставщикам программно-аппаратных средств по перечисленным выше причинам изначально существует недоверие (в т.ч. к компаниям, сертифицированным зарубежными органами по требованиям ИСО 9001). Это не может не сказываться на повышении риска недоверия к качеству и безопасности поставляемой продукции.

Проведенный анализ подходов к управлению рисками применительно к различного рода системам, функционирующим в условиях возможного негативного воздействия, показал следующее:

1) В жизненном цикле остаточный системный риск будет иметь место всегда. На уровне законодательных и нормативно-методических документов для обеспечения безопасности объективно востребованы определение, анализ и контроль рисков и принятие управляющих воздействий для поддержания целостности в результате сравнения прогнозируемого и допустимого рисков. Для приложений, в которых уже были многочисленные факты трагедий с гибелью людей - в сфере промышленной, пожарной, радиационной, ядерной, авиационной безопасности - требования к допустимым рискам выражены количественно, как правило, на вероятностном уровне, и качественно на уровне необходимых требований к исходным материалам, используемым ресурсам, технологиям и начальным состояниям, условиям эксплуатации.

2) Для иных приложений - в сфере химической, биологической, транспортной, экологической безопасности, безопасности зданий и сооружений, информационной безопасности, в т.ч. в условиях террористических угроз – требования к допустимым рискам задаются преимущественно на качественном уровне в форме требований к выполнению конкретных условий. Это означает невозможность корректного на сегодня решения обратных задач обоснованного управления безопасностью исходя из задаваемого уровня допустимого риска. То есть, упреждающие меры для того или иного сценария угроз должны иметь количественное обоснование. Для определения уровня допустимых рисков до получения убедительной статистики в соответствующих приложениях целесообразно использование прецедентов в других приложениях.

3) Во всех случаях эффективное управление рисками для любого рода систем при штатных начальных состояниях возможно и целесообразно на основе:

а) использования исходных ресурсов и защитных технологий с более лучшими характеристиками с точки зрения безопасности, в т.ч. для восстановления целостности;

б) рационального применения адекватной системы ситуационного анализа потенциально опасных событий, эффективных способов контроля и мониторинга состояний и оперативного восстановления целостности;

в) рационального применения мер противодействия рискам (включая избегание рисковых ситуаций).

4) Существующие модели для анализа рисков неидентичны (поэтому понятие допустимых рисков логически не сравнимо), они не позволяют решать в режиме упреждения обратные задачи обоснования требований к системам сбора и анализа информации, параметрам контроля и мониторинга и мер противодействия рискам при ограничениях на выделяемые средства и допустимые риски. А это не позволяет утверждать об эффективности управления рисками.

Таким образом, решение проблемы создания доверенной программно-аппаратной среды для АСУ заключается в поиске путей и разработке способов снижения рисков недоверия к разрабатываемым и поставляемым техническим (аппаратным), программным и программно-аппаратным средствам с целью обеспечения практических возможностей создания, функционирования и развития на этой основе АСУ, их подсистем и составных компонентов с задаваемым уровнем качества и безопасности. В общем случае при создании ДПАС целесообразно стремиться к эффективному управлению рисками в жизненном цикле АСУ в условиях целенаправленного негативного воздействия со стороны злоумышленников.

Список литературы

1. Марков А.С., Цирлов В.Л. Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопансости. 2013 №1(1). С.44-46.

2. Методическое руководство по оценке качества функционирования информационных систем [Текст]: 3 ЦНИИ МО РФ – М., 2003. – 352 с.

3. Жидков И.В., Шубенин А.А., Поздняков С.Ю., Кочегаров П.Ю. Проблемы создания доверенной программно-аппаратной среды для автоматизированных систем управления. Информационные и математические технологии в науке и управлении / Труды XIX Байкальской Всероссийской конференции «Информационные и математические технологии в науке и управлении». Часть II/ - Иркутск: ИСЭМ СО РАН, 2014. – 234 с.