ОСОБЕННОСТИ ПРЕДУПРЕЖДЕНИЯ УГРОЗ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ, СВЯЗАННЫХ С СОЗДАНИЕМ И ЭКСПЛУАТАЦИЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

***Гарбук Сергей Владимирович**, кандидат технических наук*

В статье рассматриваются угрозы национальной безопасности Российской Федерации, связанные с широким применением программного обеспечения в органах государственного управления, различных отраслях промышленности, Вооруженных силах. Показано, что эффективное парирование всего комплекса возникающих угроз не может быть обеспечено только за счет нормативного закрепления требований по отечественному происхождению программного обеспечения, а предполагает реализацию ряда дополнительных мероприятий, инвариантных к стране – разработчику.

***Ключевые слова**: национальная технологическая безопасность, отечественное программное обеспечение.*

FEATURES PREVENTING THREATS OF NATIONAL SECURITY ASSOCIATED WITH THE CREATION AND MAINTENANCE OF SOFTWARE

***Sergey Garbuk**, Ph.D.*

Threats to the national security of the Russian Federation related to the widespread use of software in government, various industries, the armed forces are considered.

The effective elimination of all complex emerging is discussed. The additional measures for process of national technological security invariant to country are analyzed.

***Keywords**: national security technology, domestic softwar.*

1. Характеристика угроз национальной безопасности, связанных с созданием и эксплуатацией программного обеспечения

С началом использования автоматизированных систем и, в частности программного обеспечения автоматизированных систем (далее – ПО), связано появление специфических угроз национальной безопасности, нарушающих состояние защищенности личности, общества и государства. До настоящего времени основное внимание уделялось парированию угроз, связанных с нарушением информационной безопасности при создании и эксплуатации ПО. Однако по мере повышения значимости программного обеспечения в современном мире, все более отчетливо начинают проявляться и другие связанные с ним угрозы, например, угроза технологической безопасности страны.

В данной статье предпринята попытка рассмотреть совокупность угроз национальной безопасности, проявляющихся на различных стадиях жизненного цикла ПО, как комплексную проблему, решение которой может быть обеспечено за счет реализации системы нормативных, организационных и технических мероприятий.

Классификация угроз национальной безопасности, связанных с созданием и эксплуатацией ПО, представлена на рисунке 1. По механизму реализации и вызываемым последствиям угрозы могут быть связаны:

- с нарушением информационной безопасности (нарушение целостности, доступности и конфиденциальности обрабатываемой информации[1], способное привести к негативным последствиям для отдельного человека, общества или государства в целом);

1 ISO/IEC 27002:2005. Информационная технология. Свод правил по управлению защитой информации.

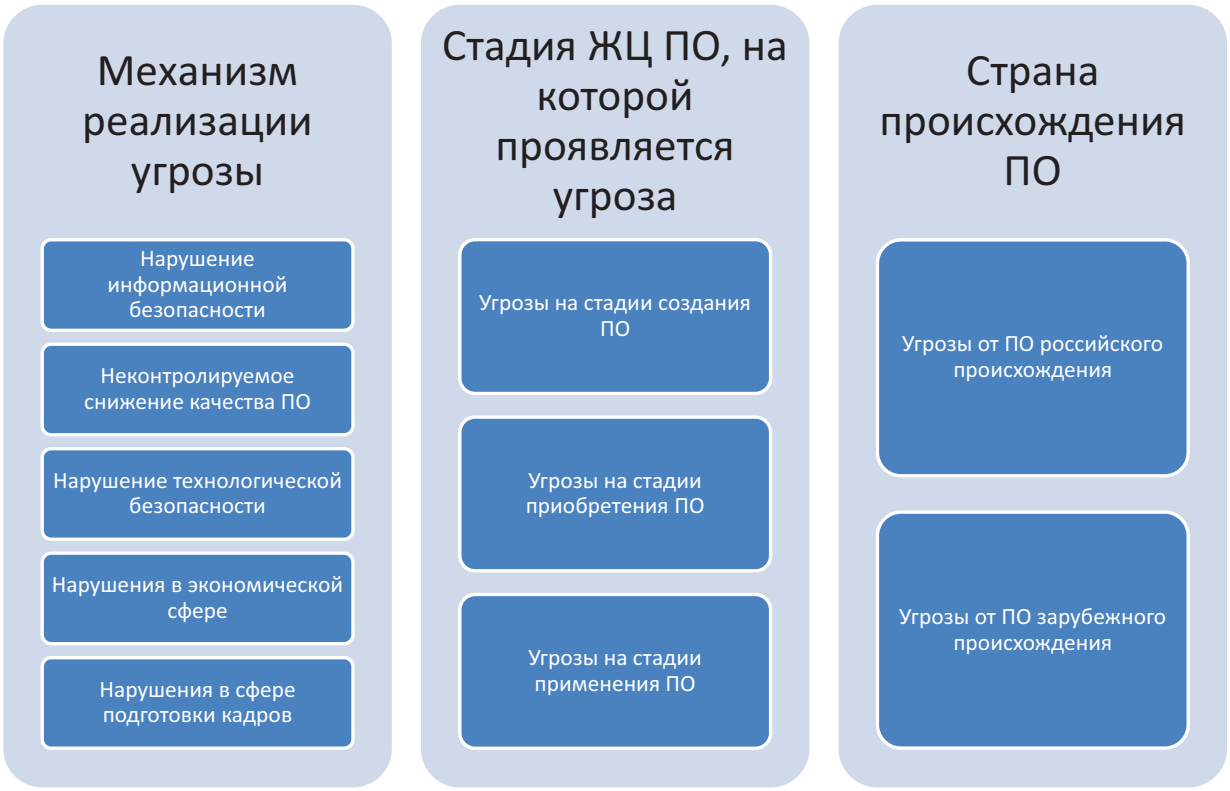

Рис. 1. *Классификация угроз национальной безопасности, связанных с созданием и эксплуатацией программного обеспечения.*

- неконтролируемым снижением качества ПО (снижение степени соответствия совокупности присущих характеристик требованиям, установленным и предполагаемым потребителем ПО или являющимся обязательными[2]);
- нарушением технологической (научно-технологической) безопасности (нарушение безопасности при реализации имеющихся или новых знаний и технологий в производственной и иной экономической деятельности, включая меры и средства, обеспечивающие уровень развития науки и технологий в ключевых направлениях для обеспечения суверенитета, социально-экономического развития государства и его национальной безопасности [1]);
- нарушениями в экономической сфере (угрозы, связанные с неоптимальным расходованием бюджетных средств в процессе приобретения и эксплуатации ПО, при котором не обеспечивается эффективное воспроизводство соответствующих отраслей отечественной промышленности);
- нарушениями в сфере подготовки кадров (угрозы, реализация которых приводит к существенному дисбалансу между количеством и составом выпускников государственных учебных заведений и государственными же потребностями в этих выпускниках).

Из приведенного перечня видно, что вся совокупность угроз проявляется на уровне безопасности государства и общества, в то время как на уровне отдельной личности значимыми являются лишь отдельные из угроз. Поэтому далее основное внимание будет уделяться программному обеспечению, создание и применение которого может вызывать угрозы для государства или общества. Подобное ПО в ходе дальнейшего изложения будет называться «контролируемое программное обеспечение» (КПО), виду того, что выполнение в отношении КПО определенных контрольных процедур государственными регуляторами и общественными организациями позволит устранить соответствующие угрозы национальной безопасности.

К контролируемому ПО, на наш взгляд, следует отнести:

- программное обеспечение, приобретаемое за счет бюджетных средств Российской Федерации;
- ПО, применяемое в государственных и муниципальных информационных системах (в со-

2 ГОСТ Р ИСО 9000-2011. Система менеджмента качества. Основные положения и словарь.

***Таблица 1**. Соответствие стадий жизненного цикла программного обеспечения.*

Действующий нормативный документ	Стадия создания ПО	Стадия приобретения ПО	Стадия применения ПО
ГОСТ 34.601-90 Автоматизированные системы. Стадии создания	Формирование требований к АС Разработка концепции АС Техническое задание Эскизный проект Технический проект Рабочая документация	Ввод в действие	Сопровождение АС
ГОСТ Р ИСО/МЭК 12207-2010 Информационная технология. Программная и системная инженерия. Процессы жизненного цикла программных средств (ПС)	Процессы реализации ПС (реализации, анализа требований, проектирования архитектуры, детального проектирования, конструирования, комплексирования, квалификационного тестирования)	Процессы соглашения (приобретения и поставки)	Процессы поддержки ПС (менеджмента программной документации, менеджмента конфигурации, обеспечения гарантий качества, верификации, валидации, ревизии, аудита, решения проблем в ПС)
ГОСТ РВ 15.004-2004 Система разработки и постановки продукции на производства. Военная техника. Стадии жизненного цикла изделий и материалов	Исследований и обоснование разработки Разработка Производство	Эксплуатация (в части процессов принятия изделия эксплуатирующей организацией от поставщика, ввода в эксплуатацию)	Эксплуатация (в части процессов приведения в установленную степень готовности к использованию по назначению, поддержания в установленной степени готовности к использованию, хранения и транспортирования при эксплуатации, использования по назначению, вывода из эксплуатации)

ответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. №ФЗ-149),

- ПО, применяемое в ключевых системах информационной инфраструктуры (в соответствии с документами ФСТЭК России, зарегистрированными в Минюсте России в 2007 году),
- ПО, применяемое на объектах критической информационной инфраструктуры (в соответствии с Указом Президента Российской Федерации от 15 января 2013 г. №31с),
- ПО, применяемое в автоматизированных системах управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (в соответствии с поручением Правительства Российской Федерации от 10 декабря 2013 г. №ДМ-П10-8883),
- программные средства военного назначения (по разрабатываемому в настоящее время ГОСТ РВ).

Возвращаясь к классификации, представленной на рисунке1, отметим, что по стадии жизненного цикла (ЖЦ) ПО, могут быть выделены угрозы, специфичные для стадий создания, приобретения и применения (включая поддержание) программного обеспечения. Указанные стадии жизненного цикла ПО получены путем обобщения стадий ЖЦ, установленных различными нормативными документами (табл.1). Подобные укрупненные стадии позволят в дальнейшем выполнить анализ способов парирования угроз, различающихся последствиями и механизмами реализации.

По стране происхождения программное обеспечение, в котором могут проявляться угрозы национальной безопасности, подразделяется на ПО российского и ПО зарубежного происхождения. Отметим, что до настоящего времени в нашей стране эти понятия нормативно не определены, хотя соответствующие работы проводятся очень активно. В частности, рассматриваются альтернативные варианты, один из которых предусматривает, что российским будет считаться ПО, права на который принадлежат лицу, не менее чем на 51% подконтрольному российским резидентам, а другой – ПО, разработанное на предприятии, в котором доля иностранного капитала не превышает 25% минус 1 акция, у которого более 75% выручки генерируется в России, которое является российским налоговым и юридическим резидентом, а доля иностранцев среди его сотрудников не превышает 25% [2]. Еще один подход к определению отечественного ПО заключается в адаптации нормативного документа[3], разработанного ранее для телекоммуникационного оборудования, с учетом специфики процессов создания программного обеспечения.

3 Совместный приказ Минпромторга России N 1032 и Минэкономразвития России N 397 от 17 августа 2011 года.

Таблица 2. Существующие способы парирования угроз на различных стадиях жизненного цикла ПО.

Стадия ЖЦ ПО	Угрозы в области информационной безопасности	Угрозы в области качества ПО	Угрозы в области технологической безопасности	Угрозы в экономической сфере	Угрозы в сфере подготовки кадров
Создание ПО	Выполнение требований нормативных документов на стадии создания	Выполнение требований стандартов в области качества (серии ИСО 9000, ISO/IEC 14598, ГОСТ Р 12207 и других [3])	Размещение наиболее значимых заказов в государственных организациях, а также разработка требований к «программному обеспечению российского происхождения» с последующим преимущественным приобретением такого ПО		
Приобретение ПО	Формирование к приобретаемому ПО требований по информационной безопасности (сертификация)	Выполнение процедур верификации валидации приобретаемого ПО в рамках требований корпоративных стандартов			
Применение ПО	Выполнение требований руководящих документов в области ИБ на стадии применения	Нет	Нет	Нет	Нет

2. Мероприятия по устранению угроз, связанных с созданием и эксплуатацией программ

Несмотря на существующие различия в реализуемых подходах, все они совпадают в одном: гарантией парирования угроз в технологической, экономической и кадровой сферах считается закрепление отечественного статуса приобретаемого программного обеспечения. При этом механизмы противодействия угрозам национальной безопасности в сфере качества ПО как правило не рассматриваются вовсе, либо в лучшем случае регулируются на корпоративном уровне, а угрозы в области информационной безопасности рассматриваются отдельно от остальных (табл. 2). Характерно, что действующее федеральное законодательство предусматривает следующие способы парирования угроз информационной безопасности: лицензирование отдельных видов деятельности; сертификация ПО по требованиям безопасности информации; применение сертифицированных технических средств защиты информации; аттестация объектов информатизации, а также реализация других организационно-технических мероприятий. Страна происхождения программного обеспечения в руководящих документах государственных регуляторов в области информационной безопасности (ФСТЭК России, ФСБ России и Минобороны России) не учитывается, так как считается несущественной.

По нашему мнению, способы парирования конкретных угроз национальной безопасности определяются, прежде всего, последствиями и механизмом реализации угрозы на конкретной стадии жизненного цикла КПО, и в меньшей степени – страной его происхождения. Последнее обстоятельство объясняется следующим:

- страна происхождения для негосударственных компаний-разработчиков КПО (а таких подавляющее большинство) может неконтролируемо меняться с течением времени;
- российское гражданство собственников компаний и локализация производства КПО на территории Российской Федерации не влечет за собой автоматического устранения угроз национальной безопасности, связанных с созданием и эксплуатацией программного обеспечения, а лишь создает опасную иллюзию защищенности.

Более того, в некоторых случаях попытка ограничиться применением исключительно отечественного программного обеспечения приводит к обострению некоторых угроз. Так, искусственные ограничения на применение ПО, разработанного добросовестными зарубежными производителями (т. е. теми, кто выполняет все условия, предъявляемые Российской Федерацией к контролируемому ПО – некоторые из этих условий будут изложены далее), устраняют фактор здоровой конкуренции, что неизбежно вызывает снижение качества отечественного программного обеспечения.

Таким образом, в большинстве практически значимых случаев «отечественное происхождение» ПО является условием необходимым, но отнюдь не достаточным для эффективного парирования актуальных угроз национальной безопасности, возникающих в связи с его созданием и применением. Эффективное решение вопросов обеспечения национальной безопасности предполагает реализацию комплекса согласованных

мероприятий, направленных на устранение угроз, различающихся последствиями и механизмами их реализации, с учетом стадии жизненного цикла контролируемого программного обеспечения.

В частности, мероприятия по устранению угрозы в области несоответствующего качества поставляемого КПО должны осуществляться с целью обеспечения гарантированного уровня соответствия функциональных характеристик приобретаемого КПО заявленным требованиям. К возможным таким мероприятиям следует отнести:

- квалификационное тестирование программных средств (в качестве примера отметим, что используемые в настоящее время в российской промышленности системы автоматизированного проектирования (САПР), как зарубежные, так и отечественные, подобного квалификационного тестирования не проходят. Не существует даже нормативной базы, обеспечивающей его проведение, и в некотором смысле отечественным инженерам приходится верить разработчикам САПР «на слово». Как правило, из этого неприятного положения выходят, перепроверяя результаты инженерных расчетов на нескольких САПР разных разработчиков);
- страхование ответственности разработчиков за возможные негативные последствия, связанные с несоответствием функциональных характеристик приобретаемого КПО заявленным требованиям.

Парирование угрозы в области технологической безопасности (технологической независимости) предполагает гарантированное обеспечение заданного минимального срока поддержания КПО при его поставке отечественным потребителям. В качестве возможных механизмов устранения подобной угрозы могут быть использованы:

- обязательное включение в договора поставки КПО сроков, на протяжении которых разработчик (поставщик) обязуется поддерживать поставляемое программное обеспечение;
- страхование ответственности разработчиков (поставщиков) КПО, связанной с преждевременным прекращением его поддержания при поставке отечественным потребителям;
- создание на территории Российской Федерации репозиториев для хранения исходных текстов и дистрибутивов КПО, обеспечивающих необходимую поддержку программного обеспечения. Подобная мера наиболее эффективна в отношении «коробочных» программных продуктов, в то время как для крупных программных систем, требующих регулярных обновлений, более действенным представляется указанный выше механизм, связанный со страхованием ответственности.

Требования к КПО, направленные на устранение угроз в сфере экономической безопасности, устанавливаются с целью повышения возвратности бюджетных средств, расходуемых на приобретение КПО, за счет налоговых отчислений организаций – разработчиков этого программного обеспечения. Такие требования могут предусматривать, что разработчики (поставщики) КПО должны являться резидентами Российской Федерации. Очевидно, нормативное регулирование подобных вопросов должно быть увязано с осуществляемыми в настоящее время работами по государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий.

Угроза национальной безопасности, связанная с созданием и приобретением ПО в сфере подготовки кадров является хотя и неявной, но в перспективе – едва ли не самой опасной. Проявление подобной угрозы заключается в разрушении существующих и не появлении новых отечественных научно-технических школ в области создания высокотехнологичного ПО. Одной из причин этого является то, что приобретение КПО за счет бюджетных средств осуществляется в компаниях с зарубежными разработчиками, а выпускники отечественных технических ВУЗов, обучение которых осуществляется также за бюджетные средства, одновременно с этим трудоустраиваются в зарубежные компании и начинают заниматься разработкой ПО, никак на связанного с государственным заказом.

Для устранения угрозы в кадровой сфере необходимо установить требования, направленные на обеспечение сбалансированности потребностей в сфере разработки КПО и планов подготовки специалистов по разработке соответствующего программного обеспечения в государственных аккредитованных учебных заведениях. Подобные требования могут предусматривать, что в штате организации – разработчика КПО должно состоять не менее 50-75% (например) работников, имеющих профильное высшее образование (с соответствующими кодами направлений подготовки по приказу Минобрнауки России от 12 сентября 2013 г. №1061), полученное в российских учебных заведениях.

3. Зарубежный опыт государственного регулирования вопросов создания и приобретения программного обеспечения

В контексте рассматриваемого вопроса определенный интерес представляет опыт зарубежных стран по регулированию госзакупок. В Китае основными нормативными документами в этой сфере являются закон о госзакупках (The Government Procurement Law of the People's Republic of China) от 29 июля 2002 года и положение о тендерах (Tendering Regulation). Закон о госзакупках обязывает государственные учреждения покупать отечественные товары и услуги. При этом в первоначальной редакции закона отсутствовало определение «отечественные товары» («domestic goods»). Вместо определения закон отсылал к «соответствующим постановлениям Государственного Совета». Согласно положению о тендерах, компании, участвующие в аукционах по госзакупкам, должны быть «отечественными поставщиками», если иное не установлено законом. Термин «отечественный поставщик» также не определяется. В январе 2010 г. правительство выпустило проект поправок к закону о госзакупках. «Отечественный продукт» там определяется как «произведенный в границах Китая, заводская себестоимость которого превышает определенный процент от конечной цены» (на практике чаще всего 50%). Также отечественными считаются проекты и услуги, произведенные гражданами и компаниями Китая. Главным признаком, определяющим «отечественный продукт», служит факт непрохождения его через таможню КНР.

Основными законодательными актами, регулирующими государственные закупки в США являются The Buy American Act (BAA) и The Trade Agreements Act (TAA). Акт BAA, принятый в 1933 году, применяется к закупкам товаров стоимостью выше 3 тыс. долл. США, предназначенных для использования на территории США. При этом Buy American Act не применяется к услугам. На практике большинство закупок товаров и ИТ-продуктов регулируются актом Trade Agreements Act, принятым в 1979 году. Применение обоих законов подразумевает определение страны происхождения конечного продукта, критерии определения которых в BAA и TAA различаются.

В BAA присутствуют два критерия, используемые для определения страны отнесения продукта к категории «отечественного» («domestic end products»): он должен быть произведен в США; стоимость добытых, изготовленных или произведенных в США компонентов («domestic construction materials») должна превышать 50% стоимости всех компонентов продукта. Несмотря на кажущуюся простоту подхода, сложность однозначного толкования термина «произведенных компонентов», которому в BAA не дается определения, привела к трудностям применения этого подхода на практике. Кроме того, следует отличать соответствие BAA и признание продукта «Made in America». Регулированием использования маркировки «Made in America» занимается Федеральная торговая комиссия США. Продукт может отвечать критерию 50%-го порога стоимости компонентов, но не быть «полностью или почти полностью» отечественным, как того требует статус «Made in America».

Вступивший в силу в 2004 году The Omnibus Appropriations Bill (Pub.L. No. 108–109) освободил госзакупки ИТ-продуктов от ограничений BAA и стало возможным иностранное ПО при госзакупках рассматривать на равных основаниях с американской продукцией. Однако действенность этого послабления на практике была ограничена, так как закупки ИТ-продукции, как правило, регулируются актом Trade Agreements Act. Как правило, TAA применяется к закупкам продуктов и услуг стоимостью свыше 204 тыс. долл. США. В отличие от BAA, который направлен на формирование преференций использования американских продуктов, TAA разрешает использование только продуктов, произведенных в США («US-made end product») или в странах из оговоренного перечня, в который входит около 100 стран («designated countries»). Это страны, подписавшие соглашения World Trade Organization Government Procurement Agreement, Free Trade Agreement, страны Карибского бассейна и слабо развитые страны (в основном Африканского континента). В перечне отсутствуют Российская Федерация, КНР, Индия, Бразилия.

При определении возможности закупки конечного ИТ-продукта согласно TAA могут быть применимы два альтернативных критерия:

- он должен быть добыт, изготовлен или произведен в США или в стране из оговоренного перечня;
- он должен быть существенно переработан в новый продукт – предмет торговли – в США или в стране из оговоренного перечня. Новый продукт должен отличаться от исходного названием, характеристиками или назначением.

В TAA страна происхождения продукта обычно определяется по месту выполнения «существенной переработки» продукта. Определение «су-

щественной переработки» может представлять сложную задачу и зависит от рассматриваемого случая и определяется по «совокупности обстоятельств». При определении страны происхождения компьютерного оборудования, отмечаются страны, где была собрана аппаратная часть, было разработано и загружено ПО. Например, изделия, собранные в США из иностранных комплектующих с загруженным на них американским ПО, признаются «отечественными» продуктами как претерпевшие «существенную переработку». Вместе с тем, существуют прецеденты, когда загрузка ПО не становилась определяющей. Например, в случае загрузки американского ПО в электронные модули в Китае с последующей досборкой продукта и загрузкой системного ПО в США страной происхождения признавались США, а запись американского микропрограммного кода и завершающая 7-минутная сборка в Мексике принтеров компании HP не были признаны существенной переработкой компонентов произведенных и предварительно собранных в Китае.

Долгое время Таможенная и пограничная служба США (U.S. Customs and Border Protection) избегала жесткого регулирования подходов к определению страны происхождения ПО, несмотря на то, что неоднократно издавались нормы и правила применительно к ПО, загружаемому в компьютерное оборудование и записываемому на различные материальные носители. В 2012 году Таможенная и пограничная служба США издала разъяснения (консультативное постановление HQ H192146 от 8.06.2012) как определять страну происхождения ПО, не привязанного к аппаратным компонентам, в том числе в случае, если оно частично было разработано в стране, не связанной с США торговым соглашением. На примере определения страны происхождения СУБД и ПО прикладного интерфейса рекомендовалось в качестве места существенной переработки определить страну, где осуществлялась «сборка программного обеспечения» (software build). При этом под сборкой программного обеспечения понимался «процесс методичного конвертирования файлов исходного кода в отдельные строки кода, программы и подпрограммы программного объектного кода, который может выполняться с помощью компьютера». Сам процесс создания ПО был представлен в виде 7 последовательных этапов: исследования; разработки графического пользовательского интерфейса; разработки спецификаций и архитектуры; программирования; программной сборки; тестирования и валидации; записи на сервер для последующей загрузки с него при покупке ПО. Как пояснялось в консультативном постановлении, программирование включает создание «компонентов, которые будут использованы для разработки машинно-исполняемого ПО, но не являются конечным программным продуктом, а именно – исполняемым на компьютере программным кодом».

Предложенный подход облегчает определение страны происхождения ПО, по сравнению с ранее предпринимавшимися попытками оценить происхождение по месту написания программного кода, что представляло собой крайне сложную задачу, так как программу могли писать люди разных национальностей, находящиеся в разных частях мира, часто с использованием программных элементов неизвестного происхождения (открытые коды).

В опубликованном в 2013 году новом консультативном постановлении (HQ H243606 от 11.12.2013), касавшемся определения страны происхождения пакета прикладного ПО DocAve для Microsoft SharePoint, Таможенная и пограничная служба США также использовала 7-этапное представление процесса создания ПО, и местом существенной переработки продукта была признана страна, где была осуществлена программная сборка.

Таким образом, анализ зарубежного опыта, в особенности американского, свидетельствует о стремлении локализовать исходные тексты ПО на территории своего государства, что в соответствии с предложенной выше классификацией позволяет парировать угрозы информационной, технологической безопасности и в экономической сфере.

При этом предупреждению других угроз также уделяется соответствующее внимание. Для организации процессов контроля качества ПО наиболее широко используется серия стандартов ISO 9000. Специально для обеспечения процессов разработки программных систем организацией ISO разработано руководство ISO 9000-3, которое формулирует требования модели качества ISO 9001 к организации процесса разработки программного обеспечения. Недостатком стандарта ISO 9000, связанным с его универсальностью, является сложность измерения уровня качества процесса разработки программного обеспечения в соответствии с предложенной моделью качества. На этом фоне в 2013 году был разработан стандарт ISO/IEC/IEEE 29119 (некоторые части этого стандарта в текущий момент еще

находятся на стадии согласования, в частности методика проектирования тест-планов), описывающий исключительно процессы тестирования ПО, однако и он не в полной мере отвечает на вопрос функционального соответствия ПО, а не формального выполнения тест-плана, особенно в случае, когда компоненты разработаны разными организациями.

Данная проблема достаточно давно беспокоит различные организации, для которых качество ПО является критически важным. Так, например, в министерстве обороны США существует стандарт MIL-STD-498, описывающий единые требования для разработки программного обеспечения и документации; стандарт NASA-STD 8739.8 описывает контроль программного обеспечения и компьютерных систем. На этом фоне за рубежом возникает желание создать некий единый стандарт, применимый в конкретной предметной области. Здесь можно отметить успехи в области стандарта обмена программными данными модели изделия – STEP. Сейчас он используется для обмена данными между САПР, автоматизации производственных процессов, автоматизированного проектирования (CAD/CAE), моделирования данных, управления данными об изделии. Стандарт STEP описывает требования к данным о продукте, геометрическим размерам и допускам. Помимо непосредственно стандарта STEP, существует международный консорциум PDES (Product Data Exchange Using Step), накладывающий ограничение на взаимодействие предприятий исключительно в рамках данного стандарта. Данный консорциум зародился в США, однако сейчас его можно назвать полноценно международным – во главу угла ставится не «отечественность» разработчика или производителя, а его соответствие указанным критериям.

Другим параллельным путем повышения качества ПО, активно используемым в частности в США, является объединение центров разработки в рамках некой единой информационной системы, накладывающей ограничение на используемые инструменты, формирующей требования по функционалу, а также позволяющей коллективно проводить верификацию данных. Среди промышленных систем можно отметить объединения «Model Based Enterprise» и «National Network for Manufacturing Innovation». Также стоит отметить и публичные подобные системы, позволяющие вести коллективную разработку ПО в части открытого кода – GitHub, SourceForge, Google Code, конечно они больше относятся к пользовательским приложениям, но нельзя не отметить факт эффективности контроля качества с помощью подобных инструментов.

Проведенный анализ свидетельствует о том, что для повышения качества ПО за рубежом предпринимаются различные усилия – от попыток унификации требований и коллективного контроля, до наложения ограничений на допуск к информационным системам для организаций, не соответствующих определенным критериям. При этом парирование угрозы несоответствия качества предполагает выполнение функциональных требований, не связанных с национальной принадлежностью организаций.

Выводы

Таким образом, в качестве обобщенного комплекса мероприятий, направленного на устранение в Российской Федерации угроз, связанных с созданием и применением программного обеспечения, могут быть предложены:

- контроль статуса разработчиков (поставщиков) КПО как резидентов Российской Федерации;
- квалификационное тестирование программных средств;
- страхование ответственности разработчиков за возможные негативные последствия, связанные с несоответствием функциональных характеристик приобретаемого КПО заявленным требованиям;
- обязательное включение в договора поставки КПО сроков, на протяжении которых разработчик (поставщик) обязуется поддерживать поставляемое программное обеспечение;
- страхование ответственности разработчиков (поставщиков) КПО, связанной с преждевременным прекращением его поддержания при поставке отечественным потребителям;
- создание на территории Российской Федерации репозиториев для хранения исходных текстов и дистрибутивов КПО, обеспечивающих необходимую поддержку программного обеспечения;
- контроль кадрового состава организаций – разработчиков КПО, обеспечивающий выполнение требований по наличию в штате таких организаций определенной минимальной доли работников, имеющих профильное высшее образование, полученное в российских учебных заведениях.

Литература

1. Война и мир в терминах и определениях. Военно-политический словарь. / Данилевич А.А. и др.; Под общей редакцией Д.О.Рогозина. М.: Вече, 2011. 640 с.
2. Кантышев П. Минпромторг предложил определение софта российского происхождения. // Ведомости, 24 июля 2014 г., URL: http://www.vedomosti.ru/tech/news/29377581/chto-takoe-rossijskij-soft
3. Барабанов А.В. Стандартизация процесса разработки безопасных программных средств // Вопросы кибербезопасности. 2013. № 1(1). С. 37-41.
4. Мошков А.Н. Новые информационные угрозы требуют идти в ногу со временем // Вопросы кибербезопасности. 2014. № 3(4). С. 2-6

References

1. Danilevich A.A. and etc. Voyna i mir v terminakh i opredeleniyakh. Voenno-politicheskiy slovar', by ed. D.O.Rogozin, Moscow, Veche, 2011, 640 p.
2. Kantyshev P. Minpromtorg predlozhil opredelenie softa rossiyskogo proiskhozhdeniya, Vedomosti, 24.07.2014, URL: http://www.vedomosti.ru/tech/news/29377581/chto-takoe-rossijskij-soft
3. Barabanov A.V. Standartizatsiya protsessa razrabotki bezopasnykh programmnykh sredstv, Voprosy kiberbezopasnosti, 2013, N 1(1). pp. 37-41.
4. Moshkov A.N. Novy`e informatcionny`e ugrozy` trebuiut idti v nogu so vremenem // Voprosy` kiberbezopasnosti. 2014. № 3(4). S. 2-6