Федеральная таможенная служба
Государственное казенное образовательное учреждение высшего профессионального образования
«РОССИЙСКАЯ ТАМОЖЕННАЯ АКАДЕМИЯ»

Ю.И. Сомов, Э.П. Купринов, С.В. Курихин, Л.Д. Зайцева

ЭКОНОМИЧЕСКАЯ ОЦЕНКА И ОПТИМИЗАЦИЯ ЗАТРАТ НА РАЗРАБОТКУ ПРОГРАММНЫХ ПРОДУКТОВ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ТАМОЖЕННЫХ ОРГАНОВ

МОНОГРАФИЯ

Москва – 2014

УДК 004.056
ББК 67.401.114
С 61

Р е ц е н з е н т ы:

А.М. Годин, профессор кафедры экономики и управления Всероссийской государственной налоговой академии Министерства финансов РФ, д-р экон. наук, профессор
Л.А. Филиппова, доцент кафедры информатики и информационных технологий Российской таможенной академии, канд. экон. наук.

Ю.И. Сомов, Э.П. Купринов, С.В. Курихин, Л.Д. Зайцева ЭКОНОМИЧЕСКАЯ ОЦЕНКА И ОПТИМИЗАЦИЯ ЗАТРАТ НА РАЗРАБОТКУ ПРОГРАММНЫХ ПРОДУКТОВ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ТАМОЖЕННЫХ ОРГАНОВ: Монография / Ю.И. Сомов, Э.П. Купринов, С.В. Курихин, Л.Д. Зайцева. – М.: Изд-во Российской таможенной академии, 2014. 186 с.

ISBN 978-5-9590-0823-9

Монография посвящена рассмотрению актуальных вопросов, связанных с экономическими аспектами информатизации деятельности государственных органов на примере Федеральной таможенной службы. Представлена методология экономической оценки информационных продуктов и услуг. На базе проведенных исследований рассматриваются вопросы совершенствования механизма закупок программных средств и оптимизации затрат на защиту информации для таможенных органов.

Издание предназначено для специалистов таможенных органов, научных работников, преподавателей, аспирантов и студентов, обучающихся по специальности «Таможенное дело», экономическим и информационным специальностям.

Оглавление

Обозначения и сокращения

АПС – аппаратно-программное средство

ВИТС – ведомственная интегрированная телекоммуникационная система

ГК РФ – Гражданский кодекс Российской Федерации

ГНИВЦ – Главный научно-информационный вычислительный центр (в настоящее время – Центральное информационно-техническое таможенное управление)

ГТК Белоруссии – Государственный таможенный комитет Республики Беларусь

ГТК России – Государственный таможенный комитет Российской Федерации (в настоящее время Федеральная таможенная служба)

ГУИТ - Главное управление информационных технологий ФТС России

ГФЭУ – Главное финансово-экономической управление ФТС России

ДРОНД - Доклад о результатах и основных направлениях деятельности

ЕАИС – Единая автоматизированная информационная система

ЕЭК – Евразийская экономическая комиссия

ЕЭС – Единая энергетическая система

ИПС – информационно-программное средство

ИПЦ – индекс потребительских цен

ИТ – информационные технологии

КПС – комплекс программных средств

Минкомсвязи – Министерство связи и массовых коммуникаций России

Минпромторг – Министерство промышленности и торговли России

НИОКР - Научно-исследовательские и опытно-конструкторские разработки

НИР – научно-исследовательская работа

НМЦК – начальная (максимальная) цена контракта

НФАП – национальный фонд алгоритмов и программ

ОГВ – орган государственной власти

ПО – программное обеспечение

ПП – программные продукты

ПС – программное средство

ПЭА – поэлементный экономический анализ

УГСиК – Управление государственной службы и кадров ФТС России

ФОТ – фонд оплаты труда

ФСА – функционально-стоимостной анализ

ФТС России – Федеральная таможенная служба

ЦА – Центральный аппарат

ЦИТТУ - Центральное информационно-техническое таможенное управление

ЭВМ – электронная вычислительная машина

Введение

В современных условиях эффективное экономическое развитие общества без использования информационных технологий невозможно. Для таможенных органов, как и для всего аппарата государственного управления, стремительно возрастает роль информации, а в условиях мировой экономической интеграции России, её участия в Таможенном союзе, членства в ВТО значение информационного обеспечения многократно увеличивается. Поэтому важным направлением модернизации таможенных органов Российской Федерации является наращивание применения информационно-коммуникационных систем.

Однако информатизация деятельности таможенных органов несёт в себе и проблемы, которые связаны с особенностями, присущими вновь созданной ситуации. Например, с одной стороны, большое количество информационных продуктов и услуг облегчает деятельность и ускоряет технологические процессы, а с другой, создаётся мешаемый этим процессам, так называемый, «информационный мусор». Создание новых информационных продуктов и услуг нуждается в обосновании затраченных на них средств. Лёгкая доступность к информационным ресурсам диктует необходимость обеспечения их защиты, а значит и обоснования дополнительных затрат. Во многом эти проблемы лежат в области экономики. В связи с этим актуальной становится потребность в определении экономической оценки информационных продуктов и услуг.

Основная идея настоящей работы заключается в разработке методологического подхода к проведению экономической оценки информационных продуктов и услуг, на базе которой возможно исследовать различные аспекты экономики информатизации, и представлении результатов прикладных исследований в сфере приобретения программных продуктов и оптимизации затрат на защиту информации таможенных органов.

В первой главе представлен отечественный опыт расчета экономического эффекта и оптимизации затрат при разработке информационных систем, показана роль информатизации, информационных и программных продуктов, защиты

информации в обеспечении таможенной деятельности, представлена методология экономической оценки информационных продуктов и услуг.

Во второй главе дана оценка российского и мирового рынка программных продуктов в сфере защиты информации. Представлен научно-методический аппарат закупок программных средств для нужд таможенных органов на основе метода функционально-стоимостного анализа. Приведены аргументы по обоснованию рационального механизма обеспечения таможенных органов программными средствами.

В третьей главе дана общая характеристика и анализ проблемы защиты информации в распределенных автоматизированных информационных системах таможенных органов, рассмотрены вопросы управления рисками и инвестициями в обеспечении безопасности информации, представлены методические рекомендации по минимизации затрат на защиту информации таможенных органов Российской Федерации.

Глава 1. Экономические аспекты информатизации таможенной деятельности

1.1. Отечественный опыт расчета экономического эффекта и оптимизации затрат при разработке информационных систем

Под информатизацией таможенной деятельности целесообразно понимать совокупность средств и способов превращения комплекса материально-технических, трудовых, финансовых, информационных ресурсов (первичной информации) в готовый продукт для потребителя (заказчика). Это могут быть самые разнообразные результаты деятельности, как для принятия управленческих решений, так и для исполнения необходимых функций. В данной работе речь идет об информационных продуктах и услугах, программных средствах и средствах защиты конфиденциальной информации.

В современных условиях разработка информационных продуктов и оказание государственных услуг невозможны без автоматизации сбора первичной информации, ее систематизации и агрегации. Широкое распространение автоматизированных систем обработки информации и управления в нашей стране началось в 60-е годы прошлого века. В плановой экономике приоритетными автоматизированными системами были те, которые обеспечивали управление предприятиями, отраслями, народным хозяйством. Естественно, что осуществлялась функционально-стоимостная оценка их эффективности.

Роль стоимостных категорий, показателей затрат живого и овеществленного труда, издержек производства и обращения, себестоимости и прибыли, различных типов цен товаров, услуг и факторов производства, являющихся индикаторами экономичности хозяйственной жизни, во все времена была чрезвычайно велика. Эти показатели являются не только мерилом издержек и результатов, но также выражают экономические и управленческие отношения в обществе. Заметный рост сферы услуг вовлекает в межотраслевую конкуренцию и экономические отношения в народном хозяйстве многочисленных посредников. Их легальная, а часто и нелегальная деятельность, является фактором роста цен товаров и несправедливого перераспределения создаваемой общественной стоимости. Поэтому

особого внимания ученых заслуживают вопросы экономической оценки государственных информационных продуктов и услуг.

Одна из задач настоящей работы состоит в возможности использования позитивного опыта разработки автоматизированных информационных систем в нашей стране в 1960-1980 годы. Экономико-математическая интерпретация объективно действующих закономерностей призвана применять количественные критерии и ориентиры для принятия обоснованных государственных решений по хозяйственному и ценовому регулированию.

Развитие российской экономики и системы управления, как важного фактора этого развития, связаны с необходимостью организации целенаправленного мониторинга, экономико-математического моделирования экономических явлений в народном хозяйстве и внедрения системы прогнозных расчетов, основанных на применении современных информационных технологий и автоматизированных программных продуктов.

Возникновение и развитие моделирования определялось потребностями государства в познании и формализации экономических закономерностей. Необходимость рассмотрения данного вопроса вызывается отрицанием некоторыми экономистами целесообразности использования в механизме государственного управления и регулирования макроэкономических товарных моделей и народнохозяйственных расчетов.

В начале 90-х годов фактически была прекращена масштабная работа по разработке межотраслевых балансов производства и распределения продукции в народном хозяйстве страны. Были прекращены исследования и разработки, проводившиеся ранее Научно-исследовательским экономическим институтом Госплана СССР, другими ведомственными экономическими институтами, в середине 90-х гг. ликвидировали Научно-исследовательский институт по ценообразованию.

Мировой опыт свидетельствует, однако, о повсеместности применения количественных методов, математических моделей, аналитических и прогнозных расчетов в сфере ценообразования и стоимостных показателей на всех уровнях хозяйственной структуры цивилизованного рынка. Моделирование является ат-

рибутом и важным направлением научных исследований в области экономики и её макроэкономического регулирования во многих странах.

Математические исследования отдельных экономических проблем проводились ещё в XIX веке, а попытки формализации некоторых экономических закономерностей осуществлялись ещё ранее. Истоки количественного измерения экономических явлений находятся в теории трудовой стоимости.

В 60-е годы параллельно с разработками межотраслевых балансов в стоимостном выражении, натурально-стоимостном выражении, отчетных, плановых балансов интенсивно разрабатывались оптимизационные модели различных типов и уровней. Авторы этих моделей опять-таки «примеряли» их к системе различных планов в области социалистического директивного планирования. Было создано большое количество оптимальных моделей, на основе которых были составлены, например, оптимальные планы перевозок, эксплуатации подвижного состава транспорта, использования топлива, загрузки оборудования предприятий, планы размещения отдельных отраслей промышленности и предприятий отрасли, оптимальные планы распределения капвложений и другие задачи. В приложении 1 даётся более подробное представление анализа проблемы оптимального моделирования необходимого и прибавочного продукта.

Опыт разработки автоматизированных систем обработки информации в нашей стране заслуживает изучения и творческого заимствования на принципиально новой ступени организации информационно-вычислительных мощностей государственного управления, регулирования и контроля. Это относится и к ФТС России, где создана солидная методическая база в процессе разработки комплексов и отдельных информационных продуктов.

В нынешних условиях целесообразно творчески заимствовать всё положительное в области экономико-математического моделирования, накопленное как в отечественной, так и зарубежной науке. Особенное внимание следует уделить изучению математических моделей, непосредственно связанных с проблематикой государственного регулирования экономики.

1.2. Роль информатизации, информационных и программных продуктов, защиты информации в обеспечении таможенной деятельности

Роль информации в экономике трудно переоценить. Это относится и к директивно-плановой, и к рыночной экономике. Маркетинг, как главный инструмент изучения рынка и целенаправленного воздействия на него, нуждается в постоянном обновлении информации о важнейших его параметрах - количестве и качестве конкретных товаров, о ценах и ценообразующих факторах, о платежеспособном спросе на конкретные виды товаров, работ, услуг. При этом информация непосредственно становится дополнительным фактором развития экономики, внутреннего и мирового рынка.

С начала 90-х годов в современной России актуальной задачей стала разработка систем, обслуживающих торговлю и, прежде всего внешнюю. Большая работа была проведена Федеральной таможенной службой (ФТС России) в новом веке. По мнению специалистов в этом ведомстве создана одна из наиболее эффективных систем информатизации. Современное состояние информационной сферы таможенных органов характеризуется следующими специфическими моментами:

сосредоточением значительного объёма первичной информации, связанной с внешнеэкономической деятельностью (ВЭД);

многообразием информационных ресурсов и производимых на их основе информационных продуктов, используемых для оказания таможенных услуг государству и участникам ВЭД;

автоматизацией обработки информации при осуществлении контроля внешней торговли и других функций таможенной деятельности;

предусмотренным информационным обменом на основе заключаемых соглашений с государственными ведомствами и таможенными администрациями других стран.

На фоне стремительного роста информации становится более очевидной потребность в исчислении стоимости и потребительской ценности её отдельных видов, являющихся результатом переработки первичных данных и становящихся собственно информационными продуктами. Для заказчиков, разработчиков, соб-

ственников этих продуктов важно знать стоимостную оценку каждого из них в составе совокупных расходов на осуществление всей программы информатизации таможенной службы при ее технико-экономическом обосновании. Одновременно существует необходимость научного обоснования расчета параметров, характеризующих полезность информационного продукта как ресурса и фактора эффективной деятельности таможенных органов, выражающих его общую потребительскую ценность.

Для реализации функций таможенных органов в перспективе особую значимость приобретает задача выбора адекватных методов количественной оценки различных информационных продуктов с точки зрения их фактической и прогнозной стоимости, потребительской ценности, что поможет сформировать систему оценочных показателей и критериев, пригодных для принятия управленческих решений в сфере таможенной службы.

Разработка эффективных методов функционально-экономической оценки затрат на разработку информационных и программных продуктов и потребительской их ценности в современных условиях становится актуальной с позиций минимизации расходов государства и повышения действенности контрольных и регулирующих функций в народном хозяйстве, связанных с внешнеторговыми процессами, большим объемом экономической информации о товарах, пересекающих таможенную границу. Данное направление в информационной политике обусловлено финансово – экономическими соображениями и широкого внедрения практики финансирования бюджетной сферы, ориентированной на результаты ее работы.

С развитием производительных сил и производственных отношений информация, наряду с трудовыми, инвестиционными, природными ресурсами, предпринимательскими и управленческими способностями все более становится действенным фактором экономического развития. В государственном управлении происходит рост значимости информации как фактора его эффективности. Обладание информацией как первоначальными сведениями в виде информационных ресурсов и информационных продуктов дает ее собственнику определенные пре-

имущества в реализации своих целей. Одновременно информация становится предметом экономических отношений в качестве продукта управленческой деятельности государственных органов, реализуемого главным образом в виде информационных услуг.

Информационная сфера деятельности таможенных органов в условиях экономической интеграции постоянно расширяется. При этом для собственной разработки (или по заказу) информационных продуктов ФТС России необходимы как специфически подготовленные информационные, организационные, материально-технические ресурсы, так и значительные финансовые средства. Особую актуальность приобретают вопросы, связанные с закупкой госорганами программных продуктов. Это обусловлено их специфическими экономическими свойствами, например, такими как возможностью их практически беззатратного размножения, возможностью создания как уникальных, так и универсальных программных продуктов, многовариантностью решений по созданию одних и тех же, по сути, программ и др. Поэтому требуется методический аппарат для научного обоснования необходимости создания и применения программных средств и контроля со стороны государства за их закупками.

Информационная среда постоянно и объективно расширяется как за счет диверсификации общественного производства, так и за счет усложнения системы управления, включая ее важные функции. Заметной тенденцией стал опережающий рост всех элементов информационной среды перед ростом материальных благ. Это усугубляет противоречие между ограниченностью материальных ресурсов и возросшим числом людей, обладающих информацией по способам удовлетворения потребностей с помощью этих ресурсов, что ведёт к обострению конкуренции за обладание ресурсами и обусловливает актуальность и значимость обеспечения информационной безопасности.

Необходимость специальной защиты определенных категорий информации требует выделения дополнительных ресурсов на ее осуществление. Интерес к такой информации со стороны субъектов экономических отношений продиктован стремлением получить конкурентные преимущества в рыночном пространстве,

являясь смыслом борьбы экономических интересов. Таможенные органы призваны гарантировать равные условия конкуренции во внешней торговле, не допуская утечки важной управленческой и внешнеэкономической информации из своей системы.

1.3. Экономические характеристики таможенных информационных услуг

В современных условиях таможенные органы оказывают участникам ВЭД - юридическим и физическим лицам, государству разнообразные таможенные услуги. Собственно говоря, они также являются частью государственных услуг, как продукты деятельности органов государственного управления. В экономической теории результаты трудовой деятельности выражаются такими категориями, как «продукция», «работы», «услуги». Применительно к таможенной службе более предпочтительным является термин «услуги». Дискуссии в области понятийного аппарата возможны.

Физическим и юридическим лицам таможенные органы оказывают следующие виды услуг:

- самостоятельно определяют фактические свойства товаров, перемещаемых через таможенную границу, и устанавливают их соответствие свойствам товаров, указанных участниками ВЭД в таможенных документах (информационные услуги);

- обеспечивают хранение и перемещение товаров через таможенную границу в соответствии с установленными для них таможенными режимами (организационные услуги);

- взимают таможенные платежи с участников ВЭД (финансовые услуги);

- консультируют участников ВЭД;

- осуществляют другие виды работ и услуг.

Государству в лице конкретных его представителей таможенные органы оказывают следующие услуги:

- обеспечивают безопасность страны тем, что запрещают или ограничивают ввоз и вывоз участниками ВЭД специальными перечнями товаров (организационные услуги);

- обеспечивают сбор и поступление в госбюджет взимаемых таможенных платежей (финансовые услуги);

- участвуют в уничтожении опасных товаров (санитарные услуги);

- реализуют конфискованные товары (торговые услуги);

- участвуют в сборе информации о товарах и участниках ВЭД и представляют ее государству, а также заинтересованным организациям и гражданам обеспечивают информационные услуги.

Таможенные услуги имеют свою специфику. Часть их является обязательной для таможенных органов, так как обеспечивает экономическую безопасность государства. Собственно таможенные органы и создаются государством для этих целей. Другая часть услуг выполняется по просьбе участников ВЭД. Это, в основном, услуги, которые облегчают выполнение указанных обязательных услуг. Их выполнение способствует улучшению ведения международной торговли.

Часть таможенных услуг оказывается участникам ВЭД бесплатно, то есть они не являются товарами в коммерческом смысле слова и не имеют цены. Но они, безусловно, имеют стоимость поскольку выражают количество воплощенного в них индивидуального и общественно необходимого труда, измеряемого рабочим временем. Для таможенных органов эти услуги являются важными, так как в первую очередь обеспечивают им выполнять прежде всего фискальные показатели их деятельности. Другая менее важная для таможенных органов часть услуг может оказываться участникам ВЭД за плату и, таким образом, имеет цену реализации. Она может оказываться как таможенными органами, так и частными фирмами или физическими лицами по лицензиям, выданными ФТС России.

Постоянно увеличивается количество наименований и модификаций товаров, растет число товарных позиций в национальных и внешнеэкономических классификаторах продукции, увеличивается число хозяйствующих субъектов, и, в конечном счете, усиливается конкуренция на различных рынках, что делает ин-

формацию о ВЭД ценным фактором управления и фактором повышения конкурентоспособности. Поэтому особое значение имеют информационные услуги таможенных органов. Среди них стоит выделить информирование и консультирование физических, юридических лиц, органов государственной власти, таможенных администраций мира в части представления информации о ВЭД. Информационные услуги заключаются в том, что для участников ВЭД готовятся востребованные ими информационные продукты.

Уникальность таможенной службы как отрасли государственного контроля состоит в том, что информация возникает и фиксируется непосредственно в процессе таможенного контроля, оформления, то есть в режиме реального времени. Важно за небольшой промежуток этого времени не упустить возможность получить ценные данные об элементах объективного экономического процесса.

Наряду с этим вырастает объем дополнительной управленческой информации, необходимой для обслуживания текущего процесса таможенного оформления, контроля, диагностики, оценки. В процессе обработки текущей информации в информационной системе таможенных органов возникает необходимость в оперативном ее преобразовании, расширении и направлении в специализированные банки данных. Весь этот процесс означает постоянное преобразование информационных ресурсов и создание новых информационных продуктов.

Особое значение в информационной среде таможенных органов приобретают специально разработанные информационные продукты программного характера (программные продукты), которые могут многократно использоваться для выполнения таможенными органами их функций, в частности для решения задач таможенного оформления, контроля и регулирования внешнеторговой и экономической деятельности. При растущих хозяйственных связях, масштабах торговых отношений со странами-партнерами в мировой экономике, при диверсификации общественного производства соответствующий им объем информации растет во многих направлениях и соответственно требует многообразных актуальных программных продуктов.

Заметим, что информационные продукты таможенных органов тесно связанны с их функциями и являются, с одной стороны, результатом, а с другой стороны – необходимым средством выполнения этих функций. Агрегирование частных задач таможенных органов в группы позволяет выделить их определяющие функции: контрольную, фискальную, правоохранительную. Из этих функций следует, что таможенные органы должны аккумулировать и систематизировать как открытую, так и закрытую информацию. Федеральная таможенная служба, как и любая государственная структура, обязана строго исполнять законодательство страны. С одной стороны, речь идет о существенных ограничениях в использовании информации, а с другой – об ее открытости.

Существует тесная взаимосвязь между этими аспектами и основными функциями таможенных органов. Свободный информационный обмен между таможенными органами, участниками ВЭД и другими государственными учреждениями обеспечивает Федеральной таможенной службе роль главного контролера в сфере ВЭД. Относительно закрытый информационный обмен между таможенными органами и участниками ВЭД, безусловно, помогает таможне более качественно исполнять свои функции и определяет то, как, каким именно образом ею будут выполняться задачи, подчиненные общей системе функций. Функции (назначение) информационных продуктов таможенных органов обусловливают направления их использования.

Документированная информация, отнесенная законом к категории ограниченного доступа, по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную. В таможенных органах существует перечень информационных ресурсов, которые с помощью программно-технических средств доступа и обработки приобретают признаки конфиденциальных информационных продуктов. К ним относят базы данных электронных копий таможенных деклараций (ТД), электронных копий таможенных приходных ордеров (ТПО), валютного контроля, профилей рисков, ценовой информации, персональных данных и др.

К открытым информационным продуктам в порядке запросов относятся некоторые базы агрегированных данных ТД, документы внутреннего/международного таможенного транзита, данные таможенной статистики внешней торговли, базы данных о таможенном оформлении автотранспортного средства. Эти продукты предоставляются юридическим и физическим лицам. Общедоступными информационными продуктами таможенных органов также являются разделы таможенной статистики внешней торговли, информация о правовых актах в области таможенного дела, разнообразные списки, перечни, реестры и др.

Информационные продукты, образованные из одних и тех же данных, могут являться как открытыми, так и защищаемыми конфиденциальными информационными продуктами в зависимости от их структуры и содержания. Так, к примеру, информационный продукт, отражающий показатель стоимости ввезенного товара с соответствующим наименованием импортера, не может находиться в открытом доступе, в то время как агрегированные показатели стоимости импортированных товаров по ряду импортеров (например, по одной стране происхождения товаров) предполагают доступ для всех заинтересованных лиц.

Быстрое распространение угроз информационной безопасности вызывает ответную реакцию её собственников на применение систем защиты информации. Необходимо осуществлять затраты на организацию системы защиты информации, в сопоставлении с её потребительской ценностью и с учётом минимизации затрат при достижении заданных уровней безопасности.

1.4. Методология экономической оценки информационных продуктов и услуг

1.4.1. Общие сведения об экономике информатизации

Новые информационно-коммуникационные технологии прочно вошли в нашу жизнь и существенно повлияли на экономику, во многом успешно справляясь с давно ставшими для человечества актуальными вопросами. Однако информатизация принесла не только блага, но и свои проблемы, решение которых позволит обеспечить наше дальнейшее развитие. Информатизация не только изменила классическую экономику, но и грандиозностью своего охвата практически всех

сторон производства благ породила свою собственную экономику, которая нуждается в научном осмыслении.

Целью и задачами исследования в сфере экономики информатизации является изучение сути произошедших изменений интересующих объектов и явлений, взгляд на них с точки зрения экономики и на этой основе выработка научно обоснованных рекомендаций по управлению процессом информатизации.

Особый интерес представляют экономические оценки различных аспектов информатизации. В монографии основное внимание уделено информационным продуктам и услугам, исследованию их ценности, полезности, стоимости и конфиденциальности. Подобное исследование способствует разрешению таких вопросов экономики информатизации как обоснование цены на информационные (программные) продукты, что является весьма важным, например, при их закупке государственными или частными предприятиями и организациями, соотнесении затрат на защиту конкретного защищаемого информационного продукта с учётом его ценности и обосновании затрат на создание и применение систем защиты информации и др.

Отметим самые общие особенности экономики информатизации:

В ней остались базовые классические основы (люди сообща создают и потребляют разнообразные блага, сочетая в себе индивидуальные и общественные интересы, которые могут находиться в противоречии).

Люди стремятся адаптировать новую для них виртуальную среду под привычный уклад экономики (выделение границ собственности, ограничение доступа к ней, исключение анонимности при проведении обмена, привнесение «силового элемента» в отношениях при распределении конкурентных ресурсов в виртуальном мире (выключение сайтов, выведение из строя серверов, разработка специального «компьютерного» законодательства и др.)).

Осуществляется поиск методов соизмерения информационных продуктов друг с другом и с другими товарами для их справедливого распределения, обмена (продажа – покупка) или совместного использования.

Выделяется неотделимая от информатизации отрасль – обеспечение информационной безопасности (защита информации).

Ниже предлагается методологический подход экономической оценки информационных продуктов.

1.4.2. Экономическая оценка

Под экономической оценкой предлагается понимать процедуру, состоящую из следующих действий:

выделение у объекта исследования интересующих экономических свойств (ценность, полезность, стоимость, конфиденциальность информационных продуктов и услуг);

определение того, как будут сравниваться исследуемые объекты по выбранным свойствам, то есть определение своеобразных «единиц измерения и шкалы» («системы координат»), на которой «будут откладываться значения»;

определение собственно значений интересующих свойств объектов исследования в данных «единицах измерений» (определение способов получения значений ценности, полезности, стоимости, конфиденциальности информационных продуктов и услуг) и их «места на шкале»;

определение критерия оценки - отношения исследователя к полученным «значениям» и их «месту на шкале» с целью выработки решения о том, что делать дальше, в каком направлении совершенствовать информационные продукты и услуги.

Данная процедура выполняется в интересах потребителя - лица, принимающего решение относительно приобретения и применения информационного продукта или услуги.

Таким лицом (субъектом) может быть собственник, владелец или пользователь информационного продукта[1].

---

[1] Семененко В.А. Информационная безопасность: Учебное пособие. 2-е изд., стереотип. – М.:МГИУ, 2006. – 277 с. (С. 36).

Заметим, что под субъектом понимается человек, консолидированная группа лиц, общество, которые обладают своими потребностями и могут действовать в направлении получения собственного блага.

Собственник информационного продукта – это субъект, реализующий в полном объёме полномочия владения, распоряжения информационным продуктом. Право распоряжаться информационным продуктом является исключительным правом собственника: никто другой, кроме него, не определяет, кому данная информация может быть представлена для владения или пользования. Собственником информационного продукта чаще всего является его создатель. Но возможна и ситуация, когда информационный продукт создаётся другим лицом, как правило, специализированным производителем сложного в техническом исполнении информационного продукта. В этом случае права собственника передаются заказчику информационного продукта в соответствии с соглашением по обмену (договору или контракту).

Владелец информационного продукта – это субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информационного продукта. При этом право владения подразумевает наличие этого информационного продукта в неизменённом виде, а право пользования – использование его в своих интересах.

Пользователь информационного продукта – это субъект, пользующийся информационным продуктом, полученным от его собственника, владельца или посредника в соответствии с установленными правами и правами доступа к информации либо с их нарушением.

Рассмотрим специфику определения собственников, владельцев и потребителей информационного продукта таможенных органов.

В ЕАИС ТО данные поступают от разнообразных агентов: участников ВЭД, других органов государственной власти, таможенных служб других государств, физических лиц, банков, страховых компаний и др. Агрегированная в системе таможенных органов информация становится собственностью ФТС России.

Владельцами и пользователями информационных продуктов таможенных органов могут быть другие органы государственной власти, таможенные администрации мира, участники ВЭД, страховые компании, банки, физические лица. В этих случаях информационные продукты должны быть переданы им легальным путём.

Теперь перейдём к рассмотрению экономических свойств информационных продуктов, ресурсов, услуг.

1.4.3. Методология экономической оценки информационного продукта

Понятие «продукт» (от лат. – буквально «произведенный») давно используется в экономической практике и во всех школах экономической теории. В английском языке Product означает: 1) продукт, продукция; 2) результат производства.

Заметим, что продукт создаётся именно для использования, т.е. для пользы, для потребления, для удовлетворения потребности.

Отсюда вытекают свойства продукта:

быть необходимым (создаётся для удовлетворения потребности);

быть полезным (выполнять нужную (заданную) функцию);

быть реализуемым;

быть удобным в применении;

быть менее затратным;

в создании продукта участвует человек своим трудом (непосредственно или опосредованно, например, через автоматизированную технологию).

Рассмотрим жизненный цикл продукта с учётом экономических аспектов (рис. 1.1).

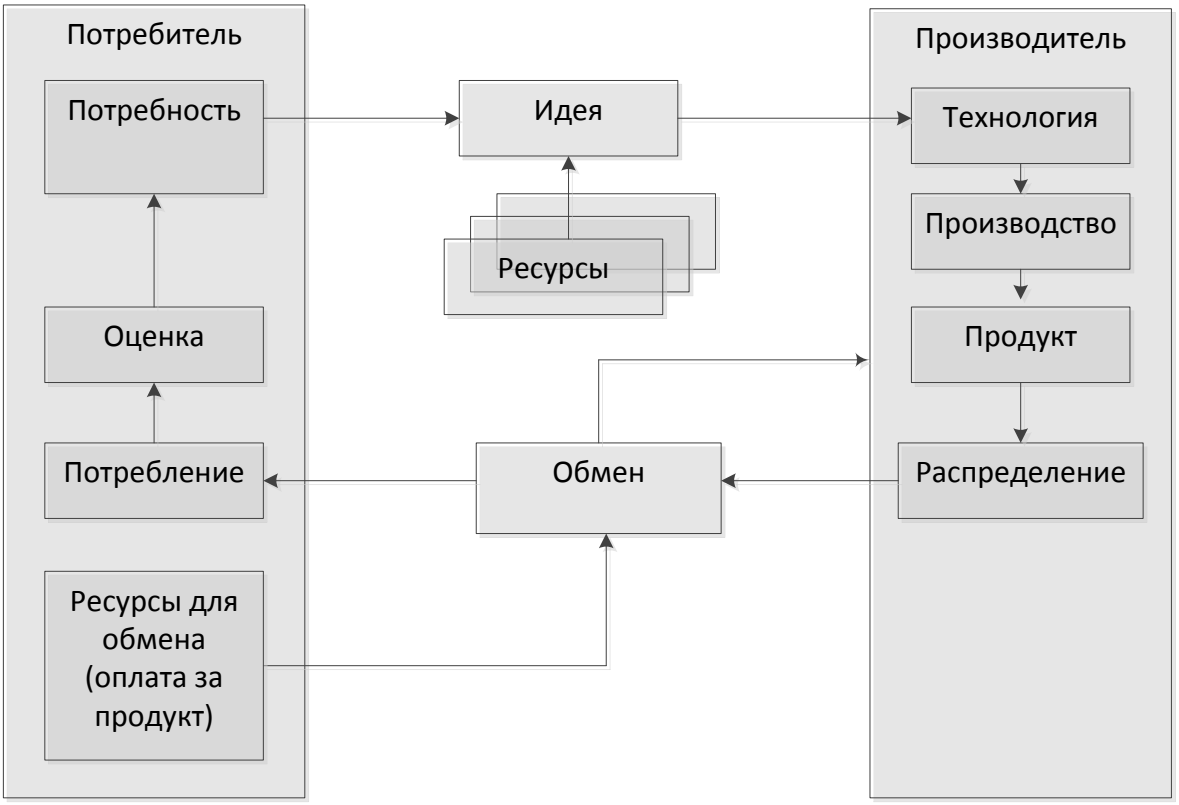

Рис.1.1. Жизненный цикл продукта

Продукт зарождается от потребности субъекта: человека, группы лиц или общества в целом. О том, как удовлетворить потребность должна быть выработана идея, общий замысел, который, опираясь на доступные ресурсы, формулирует средства и способы достижения поставленной цели, которые затем воплощаются в технологию. Технология, в свою очередь, помогает производителю организовать производство продукта. Готовый продукт распределяется и получает своего собственника. Далее происходит обмен продукта на другой товар (обычно – деньги). Таким образом, продукт находит своего потребителя, который его использует. В результате использования продукта потребитель оценивает степень удовлетворения своей потребности и принимает решение относительно дальнейшего использования данного продукта, что в свою очередь влияет на его производство.

Всё сказанное необходимо учитывать при исследовании экономических свойств информационного продукта.

Будем полагать, что информационный продукт – это информация, созданная субъектом: человеком, группой лиц или обществом (непосредственно или опосредованно в составе с другими ресурсами) и специально подготовленная для по-

требления, т.е. для удовлетворения потребности (непосредственно или опосредованно в составе с другими ресурсами).

Информационный продукт для того, чтобы быть полезным должен обладать следующими присущими именно информационному продукту свойствами:

находится в состоянии, удобным для восприятия органами чувств человека;

быть доступным;

быть полученным;

быть понятным;

быть пригодным для применения;

быть новым (ранее не известным потребителю);

быть достаточным (полным);

быть не избыточным;

быть точным;

быть достоверным (истинным, доверенным);

быть своевременным;

соответствовать наличию и доступности других ресурсов, необходимых для удовлетворения потребности.

Информационные продукты обладают большим разнообразием. Дадим им следующую классификацию (рис. 1.2).

Рис.1.2 Классификация информационных продуктов

По функции, с помощью которой используются информационные продукты, их можно подразделить на те, которые непосредственно удовлетворяют потребности человека, например, справочная информация, художественная или научная литература, музыкальные произведения, видеофильмы и т.п. и на те, что удовлетворяют потребности как обеспечивающий ресурс в составе с другими ресурсами (информация как атрибут мира, в котором мы живём, присутствует во всех сферах нашей жизнедеятельности).

По признаку, кем (чем) созданы информационные продукты, они делятся на созданные непосредственно человеком и созданные человеческим трудом опосредованно, например, через средства автоматизации.

Так называемые «носители» информационных продуктов, которые позволяют их передавать от одного субъекта другому и перемещать во времени и пространстве, весьма разнообразны. Выделим основные из них: человек, традиционные бумажные издания, разные типы электронных носителей, которые достаточно быстро видоизменяются.

По тому, через какие органы чувств в настоящее время больше всего воспринимаются информационные продукты из них можно выделить изображение (текст, изображения статические (фотографии и рисунки) и динамические (видеоизображения)) и звук отдельно или вместе с изображением. Отдельно необходимо сказать о программных продуктах. Они удовлетворяют потребности человека не через его органы чувств, а возможностью создавать с помощью технических устройств именно те изображения, звуки и другие ощущения, которые требуются.

Наиболее часто использующимся инструментарием воспроизведения информационных продуктов являются человек, книга, технические средства с программным обеспечением (электронно-вычислительная техника).

По степени доступа потребителей к информационным продуктам последние подразделяются на общедоступные информационные продукты и информационные продукты ограниченного доступа.

В современных условиях особый интерес для проведения экономической оценки представляют информационные продукты, создаваемые в так называемой

«виртуальной среде» с использование средств информатизации. Они не похожи на традиционные продукты и люди ещё только осваивают ту новую экономику, которые они с собой принесли.

Заметим, что при формировании информационных продуктов происходит агрегирование (наращивание) информационных параметров: из простого информационного продукта можно получить более сложный продукт. Если взять пример из таможенного дела, например, рассмотреть базу данных с выборкой двух параметров (код товара по единой Товарной номенклатуре внешнеэкономической деятельности (ТН ВЭД) Таможенного союза и таможенная стоимость товара), то она будет являться более простым информационным продуктом, в то время как при добавлении параметров веса и таможенной пошлины она становится более сложным информационным продуктом.

Далее заметим, что в классическом понимании любой произведенный товар (продукт) характеризуется стоимостью и потребительной стоимостью. В настоящее время, особенно в прикладной экономике, в квалиметрии, чаще используют категории «полезность», «функциональное качество» товара (услуги). Между оценкой стоимости и полезности товара имеется противоречие. Стоимость как совокупные затраты рабочего времени на производство продукта в их денежной оценке отличается от потребительской оценки полезности продукта на рынке.

Ценность информационного продукта

Информационный продукт имеет ряд специфических свойств:

не убывает при потреблении (использовании);

способен быстро распространяться, если не принимать специальных мер защиты;

сложен в определении объективной оценке его ценности;

создаётся с помощью программно-технических средств доступа и обработки информации.

Ценность информационного продукта – характеристика его значимости, оценка его конкретных свойств, в которых заинтересован пользователь информации или испытывает в нём потребность.

Полезность информационного продукта – его способность удовлетворять потребности.

Стоимость информационного продукта – издержки его производства, выраженные затратами труда и расходом ресурсов.

Потребительские свойства информационных продуктов формируют их полезность, а затраты на производство – их стоимость. Категории стоимости и полезности продукта диалектически связаны друг с другом и определяют его ценность (рис. 3).

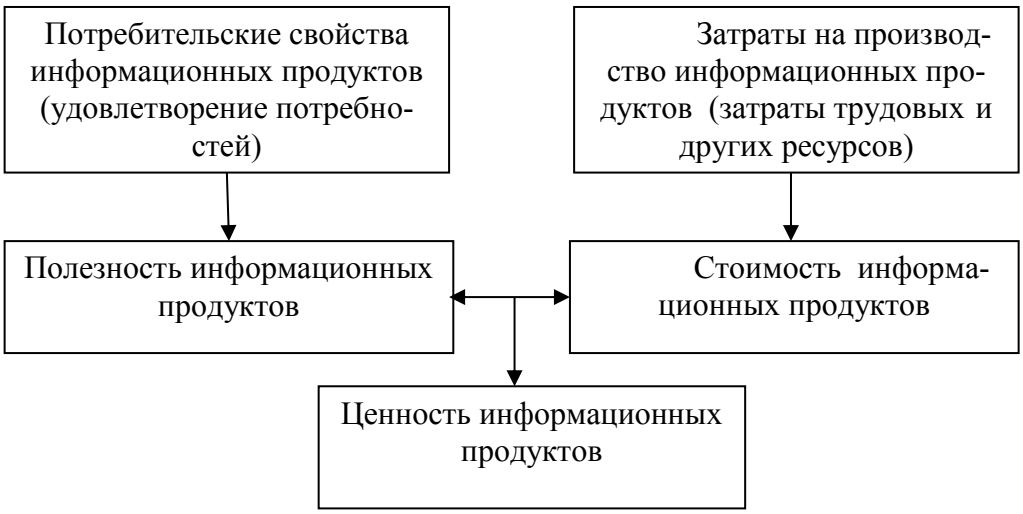

Рис. 1.3. Формирование ценности информационных продуктов

Таким образом, ценность информационного продукта можно выразить через его полезность и стоимость:

$Ц_{ИП} = f\{П_{ИП}, С_{ИП}\}$,

где $Ц_{ИП}$ – ценность информационного продукта;

$П_{ИП}$ – полезность информационного продукта;

$С_{ИП}$ – стоимость информационного продукта.

Если полезность и стоимость информационного продукта выразить в денежной форме, то соотношение между ними можно выразить в абсолютных и относительных величинах:

$Ц_{ИП} = П_{ИП} - С_{ИП}$;

$К_Ц = П_{ИП} / С_{ИП}$,

где $К_Ц$ – коэффициент ценности информационного продукта.

Данные соотношения учитывают существование в экономической теории двух основных направлений исследования рыночной экономики: классической политической экономии и теории неоклассического синтеза («экономикс»). Первое базируется на трудовой теории стоимости, второе – на субъективной полезности (предпочтениях) потребителей и законе спроса и предложения. В отношении информационных продуктов данная зависимость представляется обоснованной. Именно соотношение потребительского эффекта (полезности) с затратами на производство, разработку, обслуживание информационного продукта определяет его ценность. Однако с позиций потребления один и тот же информационный продукт представляет различный интерес для разных пользователей, стремящихся максимально удовлетворить свои потребности.

Информация, заложенная в информационном продукте, способна удовлетворять наши потребности в той мере, в какой позволяют ей объёмы доступных потребляемых ресурсов остальных категорий: пространства, энергии, времени, вещества. Имеется определенная зависимость потребительской ценности информации от наличия и доступности расходуемых ресурсов. Она будет тем выше, чем больше объём таких ресурсов, что означает большее количество раз удовлетворения потребностей. Ограничение потенциально доступных ресурсов возникает при увеличении количества их потребителей, и, следовательно, возникает конкуренция за их обладанием.

Полезность информационного продукта

Полезность информационного продукта можно определить приростом степени удовлетворения потребности, достигнутой благодаря его использованию:

$П_{ИП} = f \{э, Э\}$,

где э – степень удовлетворения потребности без использования информационного продукта;

Э – степень удовлетворения потребности с использованием информационного продукта.

Необходимо отметить, что один и тот же информационный продукт представляет различный интерес для разных пользователей. Он зависит от силы потребности и способности информационного продукта удовлетворить эту потребность.

Существует множество подходов к определению силы потребности для субъекта в тех или иных условиях. Например, согласно теории мотивации А. Маслоу[2] люди в своих мотивах опираются на несколько иерархических видов потребностей. При этом стоящая на более высоком иерархическом уровне потребность становится инструментом мотивирования только после того, как будут удовлетворены более низшие потребности.

Стоимость информационного продукта

Стоимость информационного продукта таможенных органов можно определить на основе анализа затрат на каждой из стадий его создания:

$C = \sum C_n$,

где C_n – затраты на n-ой стадии создания информационного продукта таможенных органов;

n – количество стадий создания информационного продукта таможенных органов.

Основными стадиями создания информационного продукта таможенных органов являются: сбор, обработка, накопление, хранение, формирование и распространение (рис. 1.4).

Необходимо отметить, что в зависимости от характеристик конкретного информационного продукта таможенных органов количество стадий его создания может быть иным.

[2] Пирамида потребностей по А.Маслоу [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org

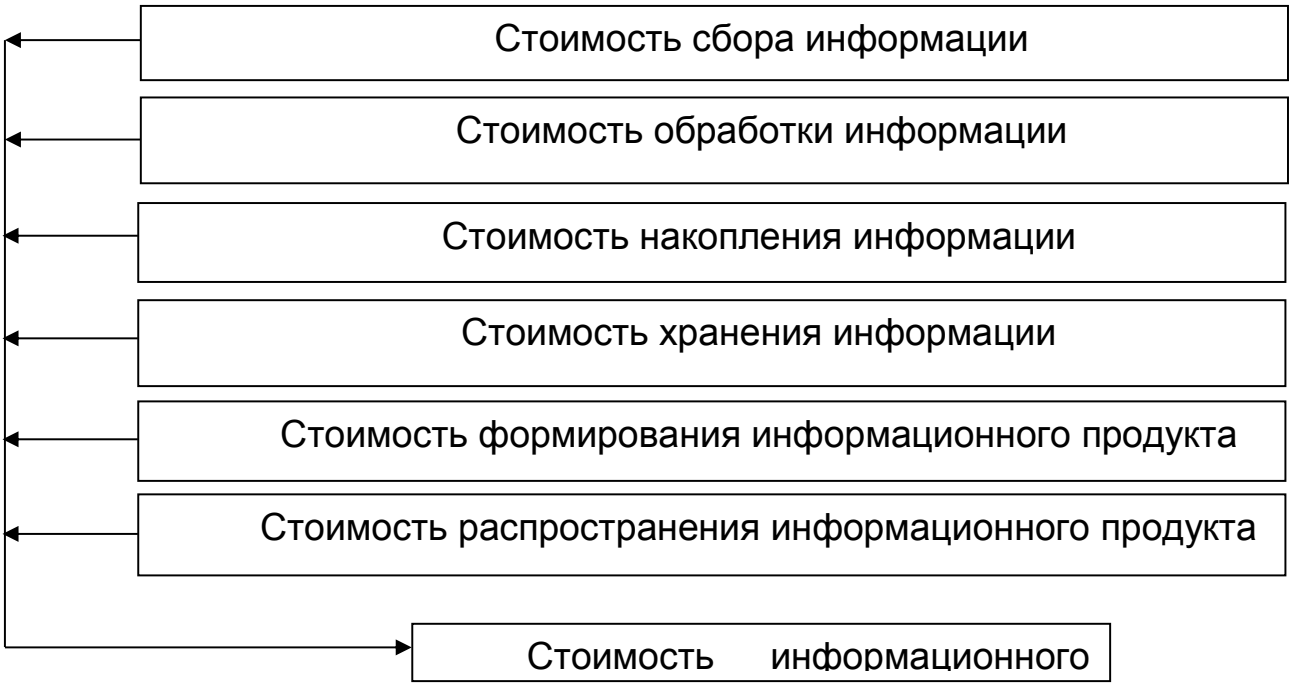

Рис. 1.4. Формирование стоимости информационного продукта по стадиям его создания

В рамках каждой из стадий производства информационного продукта расчет может основываться на калькуляции статей расходов с учетом особенностей данного продукта, например:

1. Затраты и расходы на оплату труда работников.

2. Затраты по сопровождению и гарантийному надзору информационного продукта и устранению недостатков, выявленных в процессе его эксплуатации.

3. Затраты на подготовку и освоение производства информационного продукта.

4. Затраты некапитального характера, связанные с совершенствованием технологии и организации производства информационного продукта, а также с улучшением его качества, повышением его надежности, долговечности и других эксплуатационных свойств, осуществляемыми в ходе производственного процесса.

5. Затраты на обслуживание производственного процесса: по обеспечению производства энергией, инструментарием, программным обеспечением и другими средствами и предметами труда.

6. Затраты по поддержанию основных производственных фондов в рабочем состоянии (расходы на технический осмотр и уход, на проведение текущего, среднего и капитального ремонтов).

7. Затраты по обеспечению нормальных условий труда и техники безопасности.

8. Затраты на информационную безопасность.

Отметим, что расходы на информационную безопасность необходимо выделять отдельной статьей, а также выявлять момент, когда информационный продукт приобретает конфиденциальные свойства. При этом следует предположить, что подобные расходы будут зависеть от ценности информационного продукта за счёт его конфиденциальности.

Необходимо также учитывать, что различные этапы создания информационного продукта могут реализовываться на различных управленческих уровнях госучреждения (в таможенных органах – в управлениях Центрального аппарата, Региональных таможенных управлениях, таможнях, на таможенных постах), в различных ведомствах и частных компаниях, что значительно усложняет калькуляцию себестоимости по общим статьям затрат.

Включение в цену информационного продукта прибыли по средней ее норме правомерно для открытых продуктов, распространяемых на коммерческих условиях.

В отношении открытой общедоступной, а также служебной информации, подлежащей защите, стоимость информационного продукта, как правило, ограничивается себестоимостью, так как подобные объекты не подлежат продаже и создаются не ради извлечения прибыли.

Более подробная информация о полезности и стоимости информационных продуктов представлена в монографии [22].

1.4.4. Экономические аспекты конфиденциальности информации

Помимо полезности и стоимости информационного продукта на его ценность оказывает влияние свойство конфиденциальности. Рассмотрим экономическое толкование этого свойства.

Если какого-либо ресурса не хватает для удовлетворения потребностей всех желающих потребителей, то для увеличения его потребляемой доли собственнику, владельцу или пользователю информации об этом ресурсе целесообразно вводить режим конфиденциальности. Действительно, чем меньше потенциальных потребителей ресурса будет знать о его существовании, тем большая его доля достанется обладателю информации, а, следовательно, он в большей степени (в большем объёме) сможет удовлетворить свои потребности.

Также как и при определении ценности информационного продукта ценность его конфиденциальности зависит и от затрат на обеспечение информационной безопасности. С учётом затрат на систему защиты информации ценность информационного продукта за счёт его конфиденциальности $Ц_{КИП}$ можно представить следующим образом:

$$Ц_{КИП} = f\{\Delta Р_К, С_{СЗИ}\},$$

где $\Delta Р_К$ – разница в долях используемого ресурса:

$С_{СЗИ}$ – стоимость системы защиты информации.

$$\Delta Р_К = Р_{КК} - Р_{КНК},$$

где $Р_{КК}$ – доля ресурса, который достанется обладателю информации при режиме конфиденциальности информации;

$Р_{КНК}$ – доля ресурса, который достанется обладателю информации без режима конфиденциальности информации.

Таким образом, ценность информационного продукта за счёт его конфиденциальности будет тем выше, чем больше будет разность ΔРК и меньше затрат на систему защиты информации.

Методические рекомендации по оценке ценности информационного продукта за счёт его конфиденциальности

Для оценки ценности информационного продукта за счёт его конфиденциальности необходимо выполнить следующие этапы (рис. 1.5.):

определение собственника, владельца или пользователя информации;

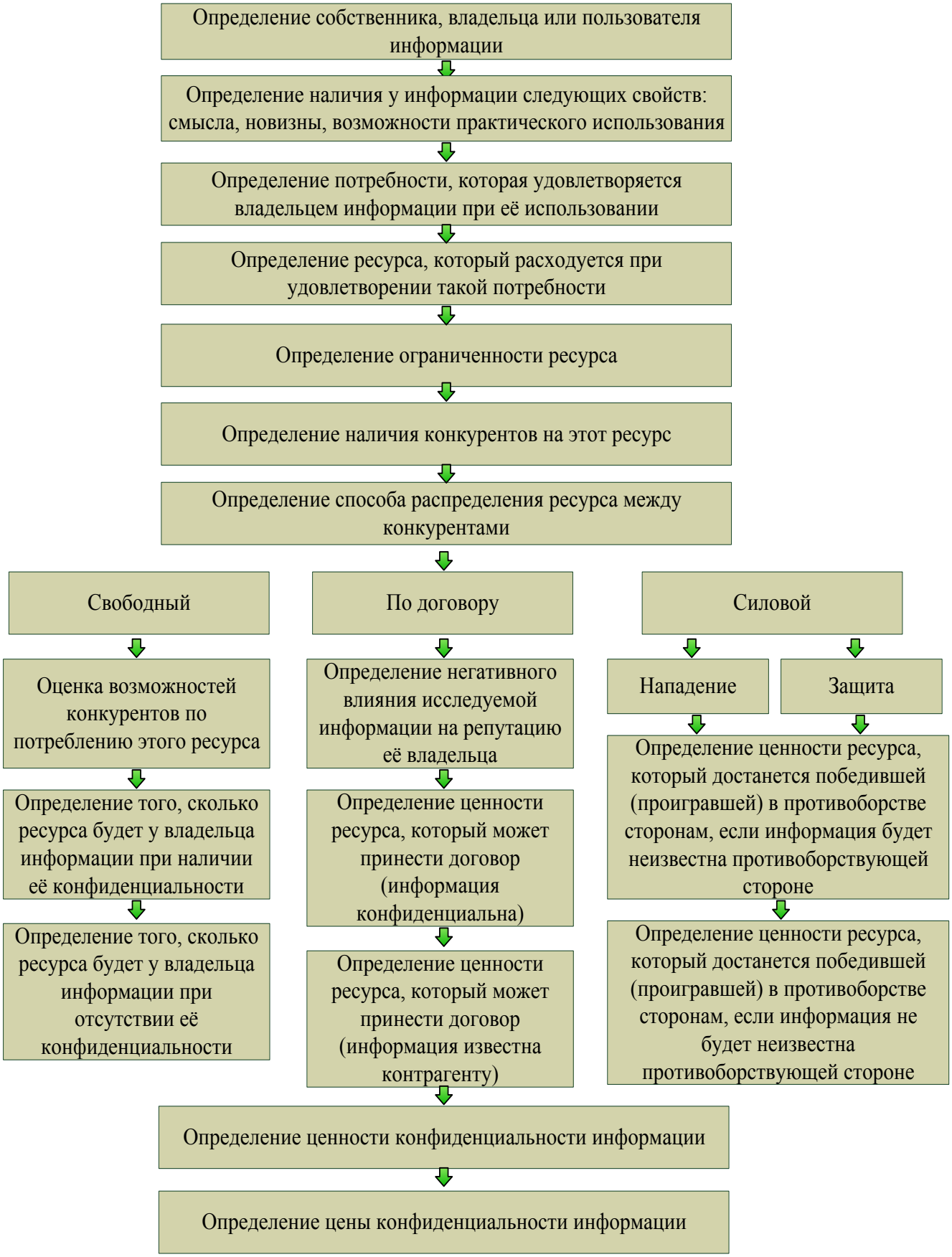

Рис. 1.5. Последовательность определения ценности конфиденциальной информации

определение наличия у информации следующих свойств: смысла, новизны, возможности практического использования;

определение потребности, которая удовлетворяется потребителем информации при её использовании;

определение ресурсов, которые расходуются при удовлетворении такой потребности;

определение ограниченности ресурсов;

определение наличия конкурентов на эти ресурсы (желательно отдельно на каждый ресурс);

определение способа распределения ресурса между конкурентами:

а) свободный

оценка возможностей конкурентов по потреблению этого ресурс;.

определение того, сколько ресурса будет у владельца информации при наличии её конфиденциальности;

определение того, сколько ресурса будет у владельца информации при отсутствии её конфиденциальности;

б) по договору

определение негативного влияния исследуемой информации на репутацию её владельца;

определение ценности ресурса, который может принести договор, если информация не будет известна контрагенту;

определение ценности ресурса, который может принести договор, если информация будет известна контрагенту;

в) силовой (нападение и защита)

определение ценности ресурса, который достанется победившей (проигравшей) в противоборстве сторонам, если информация будет неизвестна противоборствующей стороне;

определение ценности ресурса, который достанется победившей (проигравшей) в противоборстве сторонам, если информация будет известна противоборствующей стороне;

определение ценности конфиденциальности информации.

Рассмотрим подробнее каждый этап.

Задача в целом формулируется так, есть некоторая информация, для которой необходимо определить степень её конфиденциальности.

На начальном этапе необходимо определить, кто является собственником, владельцем или пользователем информации (далее в этом параграфе – «субъект»). Отметим, что самым первым собственником информации является её автор. Но реальное обладание информации по разным причинам и разными способами может перейти к другому лицу. Действительным собственником, владельцем или пользователем информации можно считать того, кто удовлетворяет свои потребностей при применении этой информации, а для собственника и владельца – и в состоянии защитить своё право на обладание ею. Именно такое лицо должно присваивать ей тот или иной статус конфиденциальности, то есть, принимать решение по её защите и нести соответствующие затраты, а значит, быть готовым к рискам и терпеть ущерб в случае реализации информационных угроз. Подразумевается, что дальнейшие этапы по оценке будет проводить именно такое лицо.

Далее необходимо определиться с тем, какая именно информация оценивается на предмет конфиденциальности. Информация может быть представлена в самом разном виде: текстом, звуком, изображением и т.п. Её полезно для лучшего понимания сформулировать в словесной (текстовой) форме. Объём такой информации может быть разным и определяется как предварительным объёмом знаний у владельца информации, так и возможностью его воспринять, понять её и иметь возможность переработать для того, чтобы в дальнейшем её можно было бы применить и получить от неё пользу.

Оцениваемая информация должна быть проанализирована на наличие в ней смысла, новизны, возможности практического использования.

Сформулированная информация должна иметь смысл как для владельца информации, так и для других лиц.

Информация должна нести в себе новые ещё никому не известные знания. Информация, которая известна всем по определению не может считаться конфиденциальной.

Следующим требованием к исследуемой на конфиденциальность информации является возможность её применения с пользой для «субъекта» или других лиц. Таким образом, информация должна нести в себе знания, с помощью которых «субъект» мог бы удовлетворить ту или иную свою потребность.

Подразумевается, что информация должна сохраниться неискажённой после оценки на всём протяжении периода её дальнейшего использования. В противном случае окажется, что проводилась оценка совсем не той информации, которую следовало оценить.

Далее выявляется, какая потребность владельца информации удовлетворяется. Потребность определяется таким образом, чтобы было ясно, какой ресурс при её удовлетворении расходуется.

Таким образом, определяется связка «информация - удовлетворяемая потребность – потребляемый ресурс».

На следующем этапе выявляются конкуренты «субъекта» на этот ресурс. Особенностью здесь является то, что конкуренты стремятся скрыть информацию о себе, которая влияет на исход конкурентной борьбы. Поэтому для собственника, владельца или пользователя информации очень важно организовать получение достоверной, точной и достаточной информации о возможных конкурентах. Этого можно достичь самыми разными способами, например, от сбора информации о конкурентах из открытых источников до скрытого наблюдения за ними и т.п.

Целью получения информации о конкурентах является определение той части ресурса, которую они могут забрать у «субъекта». Поэтому желательно как можно точнее определить количество конкурентов, их возможности по потреблению ресурса. Часто «субъект» в отсутствии сведений о кон-

курентах предполагает, что они обладают такими же возможностями по использованию ресурса, как и он сам.

Заметим, что для более точного анализа надо иметь в виду, что конкуренты могут потреблять ресурс, удовлетворяя отличные потребности от той, что удовлетворяет владелец информации.

На следующем этапе определяется ограниченность (или достаточность) этого ресурса для удовлетворения потребностей владельца информации и конкурентов. С этой целью определяются такие характеристики ресурса, по которым можно определить достаточность его для удовлетворения потребностей: общий объём, способность к воспроизводству, скорость потребления, скорость восстановления и т.д. Выясняется, относится ли данный ресурс к категории ограниченного ресурса. Ресурс считается ограниченным, если его недостаточно для удовлетворения потребностей лиц, использующего его, за некоторый промежуток времени.

В предлагаемом методе предполагается, что ценность информационного продукта за счёт его конфиденциальности определяется степенью удовлетворения потребности её владельца. А с учётом того, что в условиях конкурентного распределения ресурса степень удовлетворения потребности определяется той частью ресурса, который может использовать владелец информации, такой ценностью можно считать разницу между частями ресурса, которые достанутся «субъекту» в условиях, когда информация, которой он владеет, будет конфиденциальной и когда к ней будет доступ конкурентов.

Дальнейшие этапы определения ценности информации за счёт её конфиденциальности имеют свои особенности, которые зависят от способа совместного использования конкурентами ограниченного ресурса. К таким способам относятся:

свободное использование ресурса (ресурс никому конкретно не принадлежит, и им может пользоваться любой желающий);

договор между конкурентами о доли используемого ресурса каждого из них (например, оговаривается закреплённые за конкретным лицом местопо-

ложение, объёмы и время использования и т.п.), здесь в интересах сторон обсуждается та часть ресурса, которая уже известна всем сторонам;

захват силой или защита от силового захвата доли ресурса, который рассчитывает потребить «субъект».

Рассмотрим особенности определения ценности конфиденциальности информации каждого способа.

Если ресурс изначально никому не принадлежит, то владелец информации, первый узнавший о наличии такого ресурса, может рассчитывать, что в случае, если информация о ресурсе будет им сохранена в тайне, то он весь может быть им употреблён для удовлетворения его потребности. Как только у конкурентов на этот ресурс появится информация о его наличии, то они сами начнут использовать этот ресурс, и доля владельца информации будет уменьшаться за счёт долей, используемых конкурентами. Поэтому для определения ценности информации о ресурсе необходимо оценить, сколько ресурса могут потребить конкуренты и вычесть эти доли из того объёма ресурса, который мог бы достаться владельцу информации, если бы информация была бы конфиденциальной. Заметим, что ценность конфиденциальности информации о ресурсе будет уменьшаться соответственно уменьшению доли доставшегося «субъекту» ресурса.

В условиях совместного потребления ресурса особое значение приобретают знания о технологиях его использования. Чем больший объём ресурса такие технологии позволят использовать за определённый срок, тем более ценной является конфиденциальность информации, содержащая знания об этих технологиях. К ценным конфиденциальным знаниям следует отнести и знания о технологиях присвоения ресурса. Таким образом, ценность конфиденциальности информации о технологиях использования ресурса будет определяться разницей в его долях для случаев, когда информация о технологиях конфиденциальна и когда доступна для конкурентов.

Когда конкуренты договариваются о некоторых правилах совместного потребления ресурса, в том числе о размерах потребляемых ими долей ресур-

са, главным становится доверительные отношения сторон по соблюдению договора. При этом надо иметь в виду, что договоры тогда имеют смысл, когда за ними стоит возможность обеспечения их соблюдения и возможности силового понуждающего воздействия на тех, кто не соблюдает договор. Для того чтобы с «субъектом» был заключён договор, он должен иметь хорошую репутацию у своих контрагентов. Если исследуемая на конфиденциальность информация способна негативно повлиять на репутацию «субъекта», то она должна быть признана им как конфиденциальная.

Ценность конфиденциальности такой информации будет определяться разницей в долях ресурса, который мог бы получить «субъект» в случае заключения с ним договора и в случае, когда с ним отказываются заключать договор, иначе говоря, когда информация, влияющая отрицательно на репутацию своего собственника, владельца или пользователя конфиденциальна и когда она общедоступна.

При силовом захвате ресурса конкуренты должны скрывать друг от друга всю информацию, которая будет обеспечивать им победу. Поэтому на следующем этапе необходимо проверить, не повлияет ли знание конкурентом-противником исследуемой информации на победу над «субъектом» в борьбе за конкурентный ресурс. Если будет установлена такая связь, то необходимо определить разницу между долями ресурса, который будет принадлежать владельцу информации, если подобная информация будет держаться в тайне от противника и в случае, если она станет ему известной.

После того, как определяется ценность информации для всех вышеприведённых способах распределения ресурса «субъекту» необходимо определиться с тем, насколько он готов к затратам на защиту информации. Это будет ценой, которую должен заплатить «субъект» за её защиту.

Таким образом, показано, что необходимо делать собственнику, владельцу или пользователю информационного продукта, чтобы обосновать путём определения ценности конфиденциальности информации свою готовность к затратам на её защиту.

Заметим, что готовность к затратам на защиту информации является субъективной оценкой. У разных «субъектов» схожей информации могут быть разные отношения к ценности конфиденциальности и цене защиты информации.

1.4.5. Методология экономической оценки информационных ресурсов

Под ресурсами будем понимать всё, что расходуется при удовлетворении потребности. В самом общем виде к ним относятся: информация, энергия, время, пространство, вещество. Кроме того, для удовлетворения потребности требуется трудовой ресурс, чтобы превратить используемые ресурсы в благо.

Поэтому очевидно, что ценность информационных продуктов определяется не только их полезностью и стоимостью, но также и величиной объёмов расходуемых на удовлетворение потребностей ресурсов, вместе с которыми они используются.

В связи с тем, что указанные выше ресурсы неразрывно связаны между собой и не существуют отдельно сами по себе, можно предположить, что каждый из них определённой своей частью составляет совокупный ресурс, требующийся для удовлетворения потребности (рис. 1.6.).

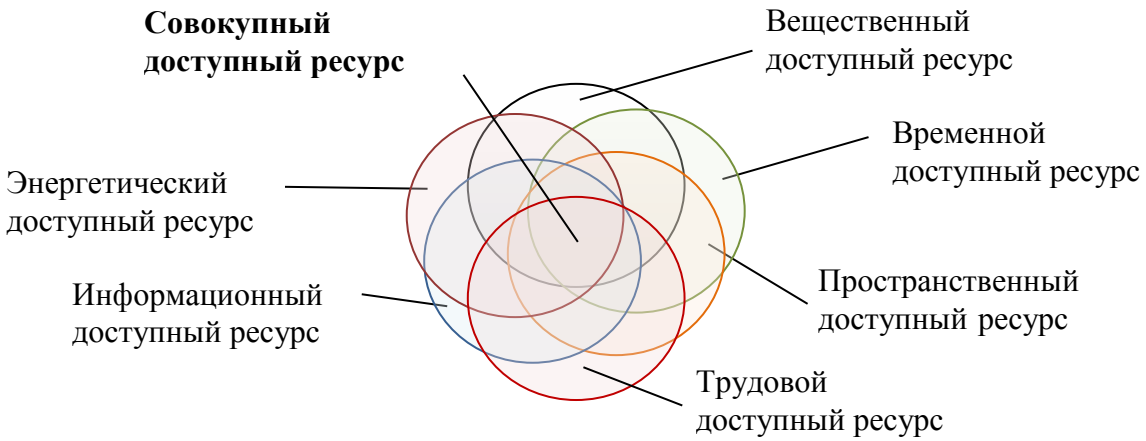

Рис. 1.6. Образование совокупного ресурса для удовлетворения потребности

Из этого следует, что информация, заложенная в информационном продукте, способна удовлетворять наши потребности в той мере, в какой

позволяют ей объёмы других необходимых потребляемых ресурсов. Действительно, имея одну лишь информацию о том, где, когда, каким образом и т.п. можно удовлетворить потребность, без наличия других доступных ресурсов, потребность удовлетворить невозможно.

Ценность информационного продукта с этой точки зрения будет тем выше, чем в большей степени (в большем количестве, в течение более долгого периода времени) будет удовлетворена потребность, что в свою очередь определяется либо большими объёмами доступных ресурсов, либо более эффективным использованием этих ресурсов.

Заметим, что уменьшение потенциально доступных ресурсов возникает при увеличении количества их потребителей, а отсюда следует конкуренция за их обладанием.

1.4.6. Особенности рынка информационных продуктов таможенных органов

Отметим особенности рынка информационных продуктов таможенных органов. В маркетинговом его понимании он не обязательно представляется в форме непосредственной «купли-продажи».

Учитывая особенности деятельности таможенных органов, данное экономическое явление можно называть «рынком» лишь условно. Действительно, государство в лице таможенных органов зачастую является лишь условным «продавцом» информационных продуктов. Рынок же информационных продуктов таможенных органов в маркетинговом его понимании определяется как совокупность их существующих и потенциальных потребителей. Эти особенности приводят к рассмотрению сферы обмена информационными продуктами таможенных органов не только в разрезе взаимоотношений купли-продажи.

Действительно, нельзя говорить о факте купли-продажи в отношении конфиденциальных информационных продуктов, однако существует объективная заинтересованность в них различных субъектов (потребителей) в процессе борьбы экономических интересов. Также нельзя говорить о факте куп-

ли-продажи в отношении открытых общедоступных информационных продуктов или продуктов, используемых, в том числе и в международном информационном обмене, однако данный факт не исключает наличия заинтересованных в них потребителей.

В связи с тем, что информационные продукты таможенных органов по степени доступа к ним подразделяются на общедоступные и с ограниченным доступом, то только лишь по отношению к общедоступным продуктам можно применить механизм ценообразования на товарном рынке с определенной долей допущения. Для, например, услуги по предоставлению данных о таможенном оформлении автотранспортных средств, из информационных ресурсов Единой автоматизированной информационной системы (ЕАИС) таможенных органов, рынок характеризуется признаками двусторонней монополии. Действительно, на рынке данной услуги существует лишь один продавец (таможенный орган) и один покупатель (физическое лицо, заинтересованное в данных о факте таможенного оформления конкретного автомобиля).

Учитывая сказанное, заметим, что, таким образом, отсутствует возможность определения цены для информационных продуктов таможенных органов как рыночной (равновесной) цены, которая теоретически является интегральным выражением ценности продукта для потребителя. Поэтому свободно-рыночный механизм ценообразования должен быть заменен расчетным, при котором в основе ценности информационного продукта будут использоваться как показатели стоимости, отражающие приведенные затраты, так и показатели полезности, выражающие потребительский эффект продукта.

1.4.7. Методология экономической оценки информационной услуги

Предлагается рассматривать услугу как удовлетворение потребности одного субъекта действиями другого субъекта. Подобная ситуация возникает, когда субъект по тем или иным причинам не может или не желает выпол-

нить некоторое нужное ему действие самостоятельно и поэтому вынужден обратиться к помощи другого субъекта, который имеет такую возможность.

Анализ того, с чего зарождается услуга и чем завершается, привёл к формированию схемы, представленной на рис. 1.7. Приведённый ниже вариант соответствует случаю, когда предоставляемая услуга уникальна и требуется только для одного потребителя, а также исполняется одним производителем. Эта ситуация характерна для создания новых информационных услуг.

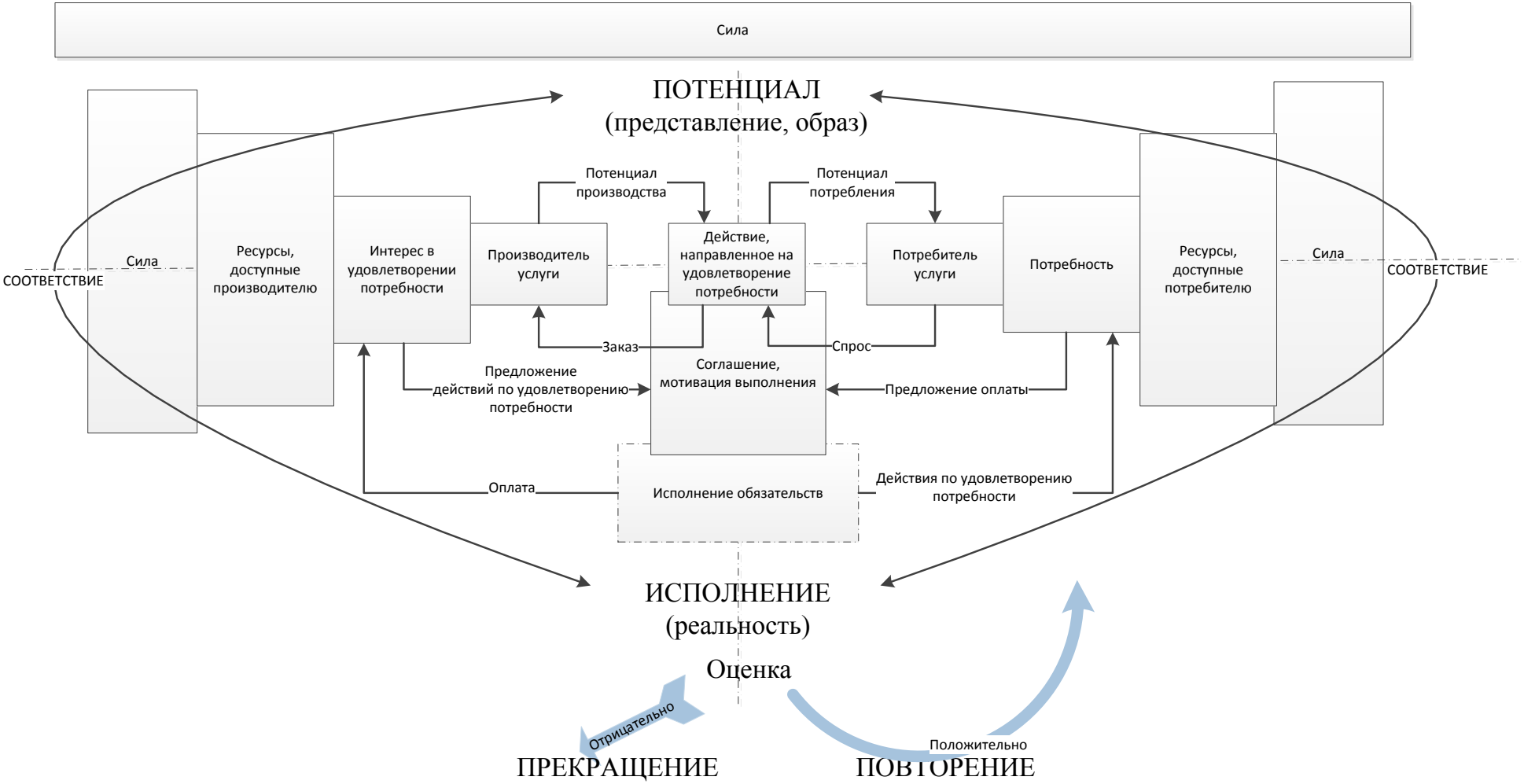

Рис. 1.7. Структурная схема услуги, представленная в виде экономической системы

Рассмотрим эту схему. Её основу составляют два элемента: потребитель и производитель. Каждый из них обладает потенциалом совершения обмена. У потребителя есть неудовлетворённая потребность, которая порождает спрос на услугу. Спрос формирует заказ для производителя. Способов заказа множество, например, путём публикации объявления о необходимости услуги, поиска услуг на рынке, специальным социологическим обследованием и т.д.

Реагируя на заказ, производитель услуги, прежде всего, определяет или уточняет свои возможности по его выполнению. Кроме того, он оценивает свои возможные затраты и предполагаемую оплату за предоставление услуги, иначе говоря, определяет свой интерес в случае, если он выполнит эту услугу. Последнее является как бы эквивалентом потребности, но только теперь не у потребителя, а у производителя. Поэтому система симметрична. Примем во внимание тот факт, что без собственного интереса производитель никогда не будет оказывать услугу. Учёт интересов производителя услуги является очень важным фактором. Заметим также, что интерес производителя услуги может проявляться как с положительной мотивацией (например, получение оплаты) так и с отрицательной (например, под угрозой чего-либо опасного или неприятного для производителя). Но в последнем случае необходимо силовое воздействие на производителя.

И у потребителя, и у производителя должны иметься доступные ресурсы, на которые они будут опираться при совершении обмена, то есть у потребителя должны быть средства на оплату услуг, а у производителя – на выполнение определённых действий, составляющих услугу.

Ещё одним важным элементом системы, представленной на рис. 1.7, является сила, стоящая за каждой из сторон. В нашем понимании сила – это способность субъекта различными способами добиться достижения поставленной цели не зависимо от воли других субъектов и даже вопреки

их сопротивлению. Сила присутствует у каждого субъекта услуги в большем или меньшем объёме. Если у одной из сторон её не будет, то и обмена не состоится. Согласно экономическому принципу «меньше затрат – больше пользы» уверенная в своей превалирующей силе сторона присвоит себе то, что принадлежит слабой стороне, без всякого обмена, по так называемому «праву силы». Поэтому для того, чтобы сделка совершалась многократно, нужен примерный баланс сил обменивающихся сторон. За этим, как правило, следит и управляет процессом выравнивания сил более высокая иерархическая структура. Например, государство заинтересовано, чтобы обмен между его гражданами имел место и совершался многократно. Для этого оно создаёт определённые правила в виде нормативных правовых актов и добивается их исполнения от всех членов общества. На схеме (рис.1) вверху показана сила, которая стоит над обеими обменивающимися сторонами.

Баланс сил приводит стороны к необходимости переговоров, в процессе которых сравниваются их ценности относительно своих и пока ещё чужих предметов обмена. Причём каждая из сторон стремиться взять больше, а отдать меньше. В случае если ценности по своей значимости для каждой из сторон станут взаимоприемлемыми, что достигается в процессе торга, то сделка заключается. Договор или соглашение могут иметь самую разную форму, например, устный или письменный договор, главное, чтобы стороны были уверены в исполнении обязательств своим контрагентом.

Затем следует исполнение обязанностей по этому соглашению, при котором стороны получают, то к чему стремились: одна – услугу, другая – оплату за неё.

После чего субъекты сделки оценивают, соответствует ли реальная реализация услуги и оплаты за неё их ожиданиям. При положительной

оценке с каждой стороны сделка по созданию услуги может стать повторяющейся.

Учитывая вышесказанное, можно предложить следующий порядок по созданию новых услуг.

Потребителю услуги необходимо:

Осознать необходимость услуги (определить свою потребность и то, что нужно для её удовлетворения).

Определить, чем он готов за нее расплатиться.

Сделать заказ (оповестить о необходимости услуги ее возможного производителя).

Производителю услуги необходимо:

1. Сформулировать суть услуги (что надо делать, какую функцию выполнять).

2. Убедиться в наличии потребности, которая будет удовлетворяться посредством услуги и оценить масштаб ее применения (спрос).

3. Оценить свои ресурсы (возможности) по выполнению услуги.

4. Определить, что нужно получить взамен услуги.

5. Стороны сопоставляют свои ожидания от обмена и возможности исполнения обязательств сделки.

6. Стороны обеспечивают сделке «силовое прикрытие» (обычно сделка заключается согласно государственным нормативным правовым актам, что и дает гарантии исполнения сторонами своих обязательств).

7. Стороны договариваются о цене сделки (цена понимается в широком смысле и определяется конкретными предметами обмена).

8. Если цена устраивает обе стороны, выполняются услуга и оплата за нее.

9. Стороны оценивают реальный предмет обмена со своими ожиданиями и принимают решение о возможном повторении сделки.

Рассмотрев общую систему, позволяющую проводить детальный анализ услуги для определения её жизнеспособности, рассмотрим особенности информационных услуг, которые стали актуальными с развитием цифровых и коммуникационных технологий.

К их достоинствам можно отнести:

– высокую скорость получения из любой точки сетевой информационной системы;

– массовость применения;

– низкие затраты при доступе к ним и использовании.

К недостаткам информационных услуг относятся:

– возможная сложность применения для неподготовленных пользователей;

– высокая доступность к информационному продукту без защиты информации;

– возможность осуществления подделки услуги и получение за нее оплаты и т.д.

Эти черты информационных услуг потребуют от их производителя:

– ориентирования на уровень возможности пользователя воспользоваться услугой;

– организации регулирования доступа к услуге;

– проведения мониторинга за точностью, своевременностью, полнотой и достаточностью создаваемого информационного продукта;

– решения проблем, связанных с возложением ответственности на должностных лиц по предоставлению информации;

– несения бремени затрат на систему защиты информации и другие мероприятия.

Необходимо отметить, что многие представленные действия при выполнении информационных услуг исполняются практически мгновенно и как бы автоматически. Но так случается, если система услуги «собрана» правильно: все элементы имеются в наличии и между ними есть связи. В этом случае в применении анализа нет необходимости. Однако когда услуга перестает работать или возникают проблемы с её созданием, а хотя бы одна из сторон заинтересована в ней, то проведение предложенного анализа может помочь выявить проблему и решить её.

Рассмотрим применение данной модели, взяв за пример оказание услуги таможенными органами. При этом нас будет интересовать проведение формального анализа именно с точки зрения приведённых выше рассуждений [48].

Само существование таможенных органов обусловлено наличием потребности общества в обеспечении своей экономической безопасности. Поэтому потребителем действий по выполнению таможенных формальностей является общество. Таможенные органы получают от общества своё содержание и обеспечиваются всем необходимым для осуществления своих функций. Таким образом, согласно представленной модели между обществом и таможенными органами заключено соглашение о том, что таможенные органы обеспечивают защиту экономических интересов и безопасность общества, а общество содержит таможенные органы. Это главное и основное условие существования оказания таможенными органами услуги обществу. Все остальные услуги, которые они могут оказывать кому-либо, например, участникам внешнеэкономической деятельности, должны осуществляться без снижения эффективности выполнения своих основных обязанностей перед обществом.

Если же мы рассмотрим нашу систему для случая, когда потребителем услуги выступает участник внешнеэкономической деятельности, у ко-

торого есть потребность сократить издержки, связанные с выполнением необходимых таможенных формальностей, то у него возникает спрос, например, на сокращение времени на проведение таможенных процедур. Таможенные органы могут оказать такую услугу. У государства – их учредителя (поэтому можно сказать и у них) есть интерес в оказании такой слуги, а именно увеличение международного товарооборота. Данная услуга будет стабильно выполняться и совершенствоваться со стороны таможенных органов при условии не снижения эффективности их основной деятельности и реального повышения международного товарооборота. А участники внешнеэкономической деятельности будут повышать товарооборот, если действительно будет сокращаться время прохождения таможенных процедур.

Таким образом, для того, чтобы новые информационные услуги в таможенном деле исполнялись качественно, необходимо соблюдать следующие положения:

выявлять потребности возможных потребителей таможенных услуг и организовывать информационную обратную связь с ними, характеризующую степень удовлетворения потребностей;

обеспечить исполнение этих услуг при сохранении эффективности выполнения таможенными органами своих основных функций;

устанавливать систему экономических показателей «затраты – польза» при оказании услуг и организовывать мониторинг за ними;

обеспечивать поощрение таможенников, непосредственно участвующих в предоставлении услуг, в зависимости от затраченного ими времени на их оказание.

Глава 2. Совершенствование механизма закупок программных средств для нужд таможенных органов

2.1. Обеспечение деятельности таможенных органов программными средствами

2.1.1. Характеристика российского рынка программных средств

Интеграционные процессы в национальной и мировой экономике вызывают значительный рост объема информации. Так, членство России во Всемирной торговой организации, создание Евразийского экономического сообщества и развитие Таможенного союза приводят к аккумуляции информации, порождаемой более интенсивным товародвижением и необходимостью его правового регулирования в современных условиях.

Таможенная интеграция способствует усилению взаимодействия таможенных органов зарубежных стран друг с другом, а также с участниками внешнеэкономической деятельности, что приводит к сосредоточению в ФТС России разнообразной экономической и управленческой информации, которая представляется особенно ценной участникам внешнеторговой деятельности, так как дает возможность получить неоспоримые преимущества на рынке.

Для обеспечения экономической безопасности страны и принципа свободной конкуренции необходима селективная защита информации. Актуальность приобретает обеспечение таможенных органов информационными продуктами и программными средствами (ПС), способными осуществлять качественную защиту этой информации, а также ее сбор, обработку и хранение. Создание комплекса таких специфических продуктов, включая экономические аспекты их приобретения таможенными органами, является актуальным направлением ресурсного обеспечения деятельности таможенных органов в современных условиях.

Для того, чтобы оценить возможность обеспечения потребности Федеральной таможенной службы в программных средствах, необходимо прежде всего исследовать рынок данного вида продукции.

График изменения объема рынка программных средств России представлен на рис. 2.1.

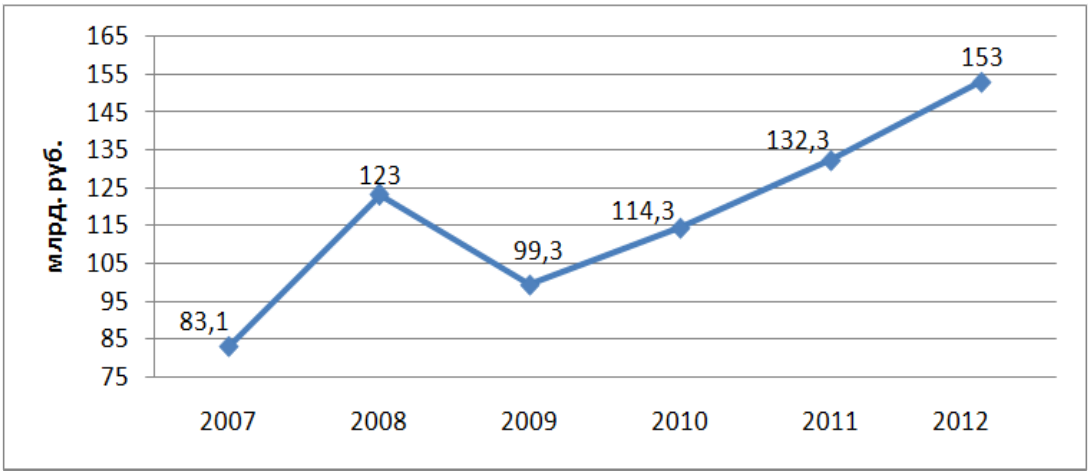

Рис. 2.1. Динамика объема рынка ПС России, млрд. руб.(рассчитано на основе данных Минэкономразвития3)

Резкое снижение объема рынка ПС наглядно демонстрирует негативный эффект от финансово-экономического кризиса 2009 года. Однако в долгосрочной перспективе график характеризуется стабильным ростом стоимостных объемов продаваемых в России программных средств.

Механизм рынка программных средств России, отражающий его внутреннее устройство, представлен на рис. 2.2.

В центре схемы находятся субъекты, чья потребность в программных средствах формирует спрос на рынке: потребители и посредники, занимающиеся перепродажей этого товара для получения прибыли. Объем предложения зависит от возможностей производителей удовлетворить потребности своих клиентов. Разработчики программных средств могут быть как отечественными, так и иностранными в зависимости от того, резидентами какого государства они являются.

[3] Министерство экономического развития Российской Федерации. Режим доступа: World Wide Web. URL: http://www.economy.gov.ru

Государство воздействует на объем предлагаемой на рынке продукции (представлен на рисунке в виде черных квадратов), используя меры налогового и таможенного регулирования. В части внешней торговли эту возможность обеспечивает Федеральная таможенная служба, которая на данном рынке одновременно выполняет функции регулятора и выступает в качестве покупателя.

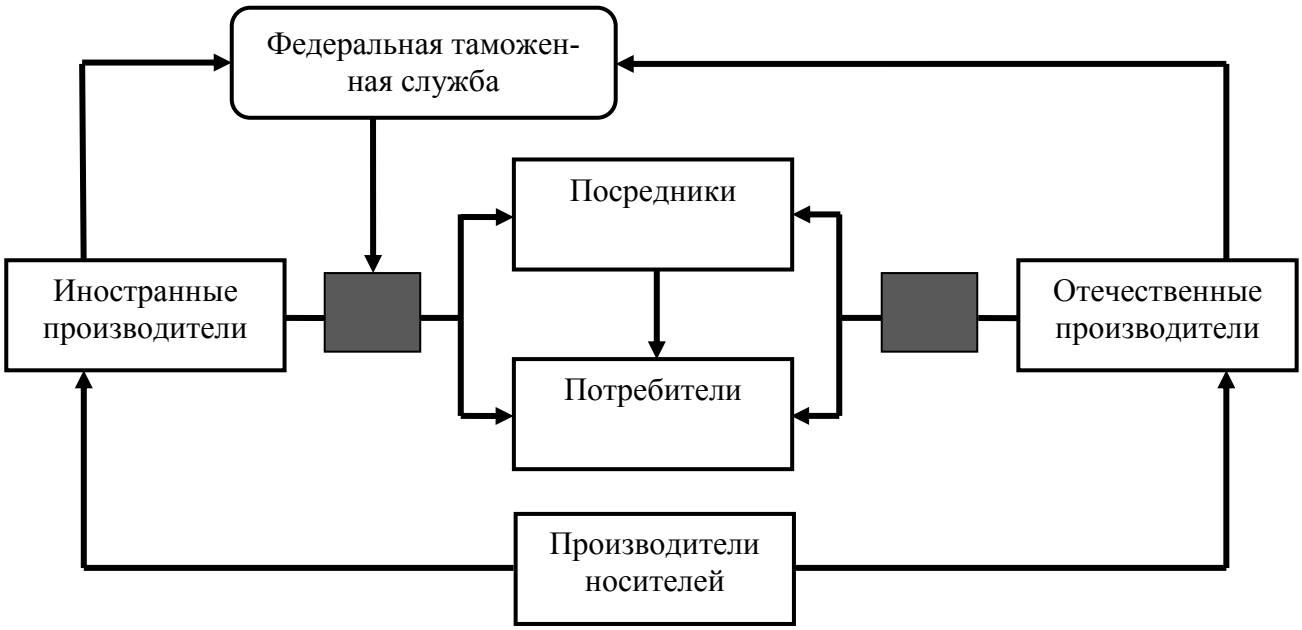

Рис. 2.2. Система субъектов рынка ПС России

С развитием сети Интернет потребность в материальных носителях для передачи ПС постепенно уменьшается, однако данный способ доставки товара покупателю до сих пор весьма популярен.

Поскольку в данном случае рассматривается механизм функционирования именно российского рынка, в схеме специально не был отражен экспорт, который будет рассмотрен далее.

Современные процессы глобализации и интеграция государств в рамках Таможенного союза воздействуют на российскую экономику, встраивая ее в систему международных экономических отношений. Поэтому при исследовании отечественного рынка необходимо учитывать внешнюю торговлю. Как известно, положительное сальдо внешней торговли свидетельствует о высокой конкурентоспособности товара. Поэтому выводы, полученные в

результате анализа статистических данных по объему внешней торговли, предоставят возможность судить о качестве разрабатываемых отечественными компаниями программных средств. Несмотря на то, что имеются подробные сведения по вывозу программных средств (рис.2.3), по ввозу данная информация не собирается.

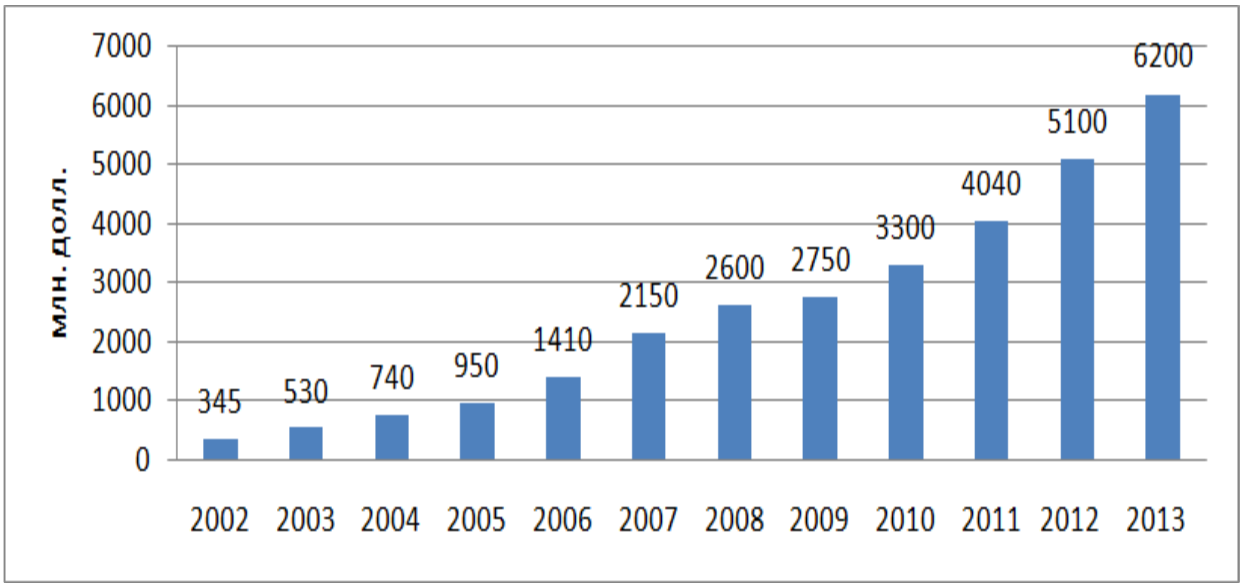

Рис. 2.3. Объем экспорта программных средств из Российской Федерации в 2002-2013 годах[4], млн. долл.

Интересной особенностью является тот факт, что кризис 2009 года практически не повлиял на объемы экспорта, лишь незначительно снизив темпы его роста. Также необходимо отметить, что объем экспорта в денежном выражении в разы превышает заявленный официальной статистикой объем внутреннего рынка ПС России.

В связи с этим, можно достаточно обоснованно заявлять о том, что разработанные российскими компаниями ПС являются конкурентоспособными и востребованными на мировом рынке. Также можно предположить дальнейший рост объема экспорта.

В то же время импорт ПС в Россию характеризуется отсутствием достоверной информации. Однако может быть изучен процесс таможенного ре-

[4] Девятое ежегодное исследование российской индустрии экспортной разработки программного обеспечения. Режим доступа: World Wide Web. URL: http://www.russoft.ru

гулирования данного процесса, для чего он схематично отображен на рис. 2.4.

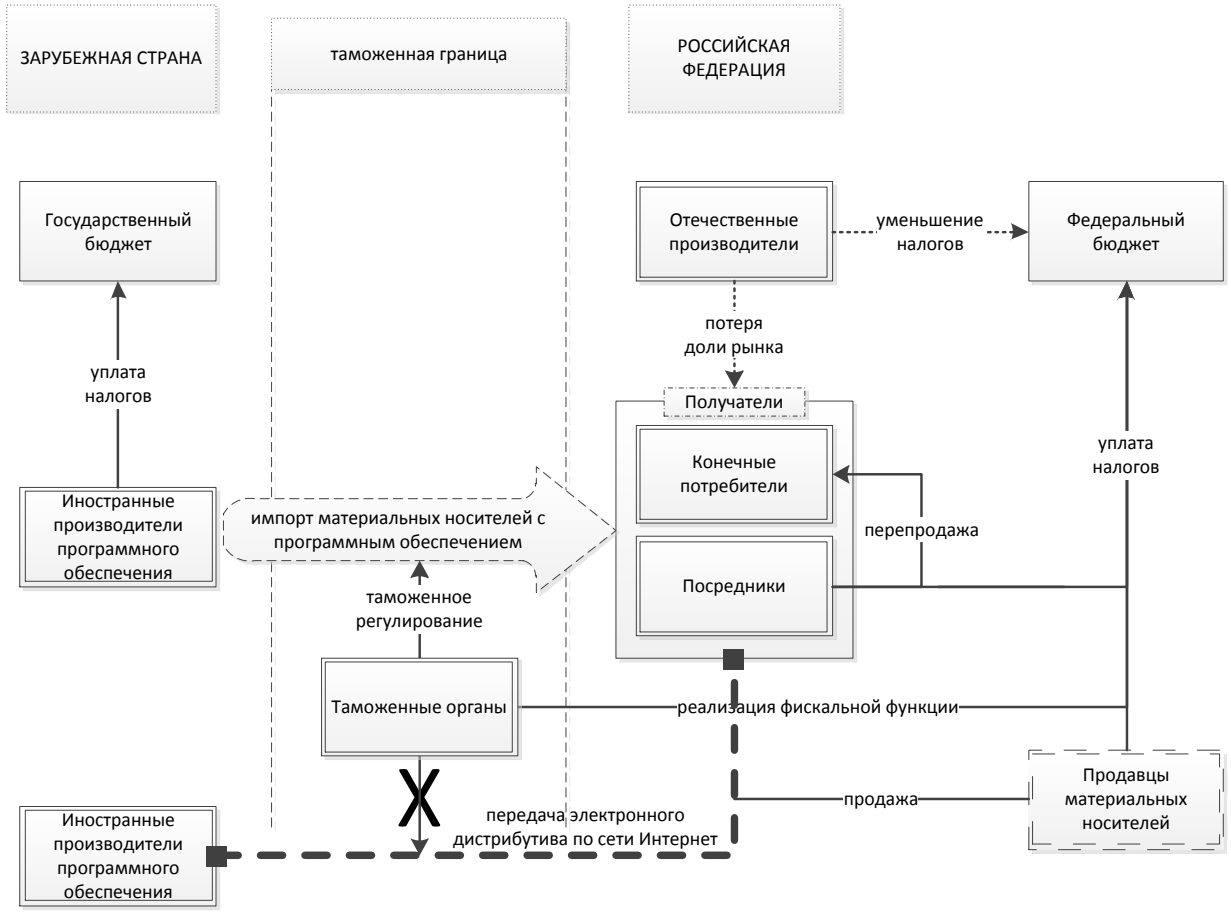

Рис. 2.4. Таможенное регулирование импорта программных средств в Российскую Федерацию

Нематериальная форма продукции обусловливает ряд особенностей таможенного регулирования внешней торговли программными средствами. В российском законодательстве это выражается прежде всего в том, что передача электронного дистрибутива от иностранного производителя отечественному потребителю либо посреднику не подлежит таможенному оформлению[5]. В то же время фактическое перемещение через таможенную границу материальных носителей с записанными на них ПС таможенному оформлению подлежит. Данный подход формирует двойные стандарты в отношении

[5] Письмо ФТС России от 17.03.2006 г. №15-14/8524 «О таможенном оформлении информации, передаваемой по сети Интернет». М.: consultant.ru, 2014. Режим доступа: World Wide Web. URL: http://www.consultant.ru

практически идентичной ситуации, что, несомненно, не способствует предоставлению равных условий участникам внешнеэкономической деятельности.

Характеристика рынка будет неполной без определения важнейших тенденций его дальнейшего развития. В соответствии с результатами опроса, проведенного компанией РУССОФТ, были выделены следующие тенденции развития рынка программных средств:

рост ИТ-аутсорсинга;

увеличение прямых продаж через Интернет;

увеличение доли продуктовых разработок;

рост в области разработки и внедрения программных решений;

увеличение доли разработок на заказ;

внедрение систем управления качеством.

По итогам исследования есть основания утверждать, что в ближайшем будущем рынок ПС ждут стабильные высокие темпы роста. Отечественные разработчики увеличивают занимаемую ими часть мирового рынка не только за счет его значительного увеличения в последнее время, но и благодаря высокому качеству производимой продукции, которое позволяет им успешно конкурировать с известными зарубежными производителями. Можно сделать вывод о том, что у российских разработчиков есть возможность занять достойное место на мировом рынке, способствуя дальнейшей интеграции национальной экономики в мировую.

Также устойчивые темпы роста рынка и высокая конкурентоспособность отечественной продукции позволяют утверждать, что потребность Федеральной таможенной службы в ПС в перспективе может быть полностью удовлетворена российскими разработчиками.

При этом необходимым условием качественного обеспечения таможенных органов программными средствами является эффективный механизм их закупки, определяющую роль в котором играют способы расчета цены контракта.

2.1.2. Анализ практики и научно-методического инструментария экономической оценки программных средств

Обладающий приоритетом при определении цены контракта метод сопоставимых рыночных цен может быть применен лишь в отношении тиражируемых программных средств. Однако существенную долю в структуре затрат Федеральной таможенной службы составляют расходы на закупку уникальных (разрабатываемых на заказ) программных продуктов, в отношении которых используется затратный метод. При этом для его применения необходимо определять трудоемкость разработки программного средства на основе мнений экспертов. Данный подход обладает рядом очевидных недостатков и не способствует объективности получаемой в результате цены контракта.

Следует особо отметить, что экономическая оценка программных средств является важнейшей потребностью при планировании создания, продажи и последующей эксплуатации данного товара. «Неадекватная оценка трудозатрат на разработку системы ведет к срыву сроков и низкому качеству конечного программного продукта»[6]. Это особенно актуально для крупных проектов, к которым относится большая часть заказываемых государственными органами.

Необходимо отметить, что общественные отношения в сфере государственных закупок регулируются федеральным законом № 44-фз «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», который содержит следующие методы обоснования начальной цены контракта:

метод сопоставимых рыночных цен (основан на анализе рынка с целью определения средней цены на идентичные товары);

нормативный метод (использование заранее предусмотренных предельных цен на реализацию предопределенных требований);

---

[6] Научные аспекты инновационных исследований: материалы I Международной научно-практической конференции, г.Самара, 6–8 марта 2013г. – Самара: Изд-во ООО «Инсома-пресс», 2012.– Т.1-2. – С. 39.

тарифный метод (определение цены контракта на основе установленных тарифов на товары, работы и услуги);

проектно-сметный метод (применяется в сфере строительства, реконструкции и ремонта сооружений);

затратный метод (используется, если нет возможности применить прочие методы);

любой иной метод (только в случае обоснованной невозможности применения любого из перечисленных).

В целях экономической оценки ПС могут быть применены метод сопоставимых рыночных цен и затратный метод, а остальные подлежат использованию в отношении иных товаров, работ и услуг.

Метод сопоставимых рыночных цен обладает приоритетом по отношению к остальным и должен применяться ко всем неспецифичным товарам, работам и услугам. Математически его можно отобразить с помощью формулы 2.1.

$$НМЦК = \frac{\sum_{i=1}^{n} Ц_н}{n}, \quad (2.1)$$

где НМЦК – начальная (максимальная) цена контракта (руб.),

$\sum_{i=1}^{n} Цн$ – сумма n – количества контрактов,

n – число контрактов.

При анализе рынка изучаются сделки, заключаемые в отношении идентичных товаров, работ и услуг, то есть тех, которые имеют одинаковые основные признаки. В случае их отсутствия либо невозможности получить имеющиеся по ним сведения, используются данные о сделках с однородными товарами, которые имеют сходные характеристики или компоненты и могут выполнять одинаковые функции, что позволяет им быть взаимозаменяемыми. При этом заказчикам предоставлено право пользоваться обоснованными коэффициентами и индексами, чтобы скорректировать цену контракта для

обеспечения сопоставимости условий сделок и возможности использовать собранную информацию. Обычно при расчете начальной максимальной цены контракта используются данные не менее чем по трем контрактам.

Метод сопоставимых рыночных цен обладает определенными достоинствами, важнейшее из которых – его объективность. Также немаловажным преимуществом является то, что метод опирается на опыт предыдущих закупок.

В то же время имеют место и значительные недостатки. Прежде всего, нельзя исключать возможность завышения цены самых первых контрактов, в результате чего цена заключенного позднее может значительно превышать оптимальную. Также, необходимым условием применения метода является формирование четких критериев классификации для определения идентичных и однородных товаров, работ и услуг. В контексте рассматриваемой темы следует отметить, что для ПС это является значительным препятствием.

Вторым методом, который будет рассмотрен, выступает затратный. Он применяется, когда особенности объекта закупки не позволяют применить иные методы оценки либо в сочетании с ними. Порядок расчета цены контракта можно представить в виде формулы 2.2.

$$НМЦК = \sum_{i=1}^{n} Зi + Пр, \qquad (2.2)$$

где НМЦК – начальная (максимальная) цена контракта,

$\sum_{i=1}^{n} Зi$ – сумма затрат исполнителя контракта,

Пр – средняя для данной сферы норма прибыли.

В структуре затрат учитываются все возможные расходы на этапах производства, реализации, транспортировки, хранения и страхования.

Затратный метод обладает целым рядом недостатков, среди которых следует выделить невозможность проверки заказчиком заявленных исполни-

телем затрат. Также не работает позволяющий снизить цену контракта механизм конкуренции. Поэтому в применении метода заинтересованы прежде всего поставщики, а не заказчики.

В соответствии с законом, за заказчиком остается право применения иных методов определения цены контракта, но лишь в случае невозможности использования указанных в законе.

Методы обоснования цены контракта на приобретение программных средств как для государственных органов, так и коммерческих организаций базируются на различных способах определения стоимости данного вида продукции, всю совокупность которых можно укрупнено представить в виде следующих подходов:

аналитический;

эмпирический;

экспертный.

В основе аналитического подхода лежит идея о том, что определить стоимость программного средства можно, исходя из его размера. При этом для измерения программного средства используются количественные характеристики его кода и предусмотренные функциональные возможности.

Число строк, длина и объем кода являются стандартными показателями для измерения программного средства.

На основе числа строк кода стоимость разработки ПС определяется посредством следующей формулы 2.3:

$$С = К * П * Ц, \quad (2.3)$$

где С – стоимость разработки программы (ден. ед.);

К –число строк кода (строки кода);

П – временная производительность персонала (ч.);

Ц – удельная стоимость трудозатрат (ден.ед./ч.).

Подобный подход мотивирует программистов писать необоснованно большое число строк кода в ограниченные сроки, что приводит к низкому качеству программного продукта и завышению стоимости его разработки. Также необходимо учитывать, что с ростом профессионализма программисту для реализации одного и того же проекта требуется написать меньшее количество строк кода, что тоже влияет на стоимость разработки продукта. Нельзя забывать о том, что существует множество языков программирования, одному и тому же функционалу в которых соответствует разное число строк кода.

Другими показателями для определения размера ПС являются длина и объем кода, предложенные М.Х. Холстедом. Длина кода определяется по формуле 2.4:

$$N = N_1 + N_2, \tag{2.4}$$

где N – длина кода (операторы),

N_1 – количество операторов (выполняющее действие неделимое приложение) в программе,

N_2 – количество операндов (элементов) в программе.

Объем кода (V) определяет необходимый для хранения программы объем памяти и вычисляется на основе формулы 2.5:

$$V = N \log (N_1 + N_2) \tag{2.5}$$

Сразу же после появления метод Холстеда подвергся критике как еще более затруднительный, чем оценка числа строк кода, и практически не используется.

Необходимо отметить, что в настоящее время определение стоимости разработки программного средства на основе количественных характеристик

его кода многими исследователями признается устаревшим и неэффективным способом.

Наиболее известной и удачной альтернативой числу строк кода при измерении программного продукта являются функциональные точки - блоки программы, выполняющие самостоятельную функцию и по этой причине способные рассматриваться отдельно от прочих. Первая версия метода была разработана Аланом Альбрехтом в середине 70-х годов XX века, а его усовершенствованный вариант – в 1984 году. Два года спустя была сформирована Международная Ассоциация Пользователей Функциональных Точек (International Function Point User Group — IFPUG), которая опубликовала несколько версий метода.

Если сложность реализации проекта не может быть отражена с помощью сформулированных требований, применяется модифицированный вариант метода функциональных точек – точки свойств, позволяющие корректировать оценку размера ПС с учетом сложности его алгоритмов. Для этого к представленным ранее типам функциональных точек добавляется еще один класс - алгоритмы.

В отличие от рассмотренных ранее, эмпирический подход заключается в использовании сведений о ранее разработанных продуктах.

При этом базой оценки являются фактические данные, стоимостные результаты предыдущих проектов. С одной стороны, это облегчает обоснование затрат на приобретение ПС, с другой – подобрать продукт, аналогичный приобретаемому, зачастую оказывается непросто. Также нельзя забывать, что стоимость первых заключенных контрактов на закупку ПС может быть завышена, что создает предпосылки для сохранения данной диспропорции в дальнейшем. Это обстоятельство является, несомненно, важнейшим недостатком подхода.

Обычно эмпирический подход применяют, когда от заказчика требуется обоснование затрачиваемых на закупку денежных сумм, но собственных

специалистов в сфере разработки ПС организация не имеет. Зачастую подобным заказчиком выступают органы государственной власти.

Третьим рассматриваемым подходом является экспертный. Чаще всего он используется в случае невозможности применения прочих подходов. Его специфика заключается в том, что объем трудозатрат определяют эксперты – лица и организации, обладающие значительным опытом работы в рассматриваемой сфере. Примером экспертного метода является техника PERT. Математически данный метод можно выразить с помощью формулы 2.6:

$$S = \frac{1}{n} \sum_{i=1}^{n} \frac{L_i + H_i + 4M_i}{6}, \quad (2.6)$$

где S – размер программного средства (строки кода);

L_i – нижняя оценка размера (строки кода);

H_i – верхняя оценка размера (строки кода);

M_i – наиболее вероятный размер (строки кода).

Классическим примером метода, основанного на экспертном подходе, является Дельфи. Суть метода заключается в многократном повторении экспертизы вплоть до тех пор, пока не будет достигнут консенсус в оценках с допустимой степенью точности.

Также при планировании стоимости программного продукта основанием для определения цены контракта могут служить бюджет заказчика и заявленные затраты исполнителя.

В первом случае эксперты определяют доли бюджета, затрачиваемые на приобретение тех или иных ПС. В случае недооценки качество разработанного исполнителем ПС с высокой степенью вероятности может оказаться низким. В случае завышения стоимости разработки неэффективно расходуются средства бюджета.

Стоимость, определенная исходя из затрат разработчика, в большей степени учитывает интересы исполнителя контракта, а не заказчика, по-

скольку зачастую осуществить проверку затрат не представляется возможным.

Необходимо отметить, что методы на основе аналитического подхода не позволяют адекватно прогнозировать трудозатраты на разработку ПС. В то же время эмпирический и экспертный подходы обладают неоспоримым преимуществом – простотой применения, и поэтому пользуются большей популярностью. Хотя это не отменяет присущих им недостатков.

Характеристика российского рынка программных средств в сочетании с анализом практики и научно-методического инструментария оценки программных средств позволяет перейти к завершающему этапу исследования обеспечения деятельности таможенных органов программными средствами – провести анализ существующего механизма закупок данного вида продукции. Однако прежде в работе будет представлен перевод руководства по применению метода функциональных точек на примере его версии FPA IFPUG (Function Point Analysis International Function Point User Group), поскольку позднее данная методика будет использована при формировании усовершенствованного механизма закупок ПС для ФТС России.

Метод функциональных точек

Метод позволяет оценить размер ПС в специальных единицах измерения, функциональных точках. В его основе лежит алгоритм, который отображен далее (рис. 2.5).

Определение типа осуществляемой оценки в зависимости от стадии, на которой находится процесс разработки ПС, является первым шагом при определении его размера. Выделяют три типа:

разрабатываемый продукт (новое, ранее не существовавшее ПС);

улучшаемый продукт (доработка готовой программы с целью изменить ее функциональные возможности);

готовый продукт (уже разработанное и используемое ПС).

Следующим шагом является определение границ ПС для выделения области оценки. Выбранному ранее типу оценки соответствуют следующие области:

все реализуемые функции (для разрабатываемого ПС);

только добавляемые, изменяемые или удаляемые функции (для улучшаемого ПС);

фактически используемые или все имеющиеся функции (для готового ПС).

При подсчете количества нескорректированных функциональных точек (UFP) необходимо учитывать следующие две характеристики данных и операций:

место хранения данных (внутри или за пределами продукта);

исходная и конечная точки операции, ее влияние на ПС и поддержка внутренних данных.

Рис. 2.5. Последовательность этапов при измерении размера программного средства методом функциональных точек

Логические данные программы можно классифицировать на две группы:

ILF (Internal logical file, внутренний логический файл);

EIF (External interface file), внешний интерфейсный файл).

ILF – распознаваемый пользователем логически организованный ряд данных или блок управляющей информации, который поддерживается внутри программы.

EIF – распознаваемый пользователем логически организованный ряд данных или блок управляющей информации, на который ссылается программа, но он поддерживается за ее пределами.

Для подсчета количества функциональных точек, связанных с данными, следует оценить их сложность. Необходимым условием в данном случае выступает изучение следующих показателей:

DET (data element type) – неповторяемое уникальное поле данных;

RET (record element type) – логическая группа данных, носит обобщающий характер для DET.

На основе их количества в ILF/EIF определяется сложность логической группы данных. Критерии для ранжирования указаны в матрице сложности, представленной в таблице ниже (табл. 2.1).

Табл. 2.1.

Матрица сложности данных

	1 – 19 DET	20 – 50 DET	50+ DET
1 RET	Низкая	Низкая	Низкая
2 – 5 RET	Низкая	Средняя	Высокая
6+ RET	Средняя	Высокая	Высокая

Оценка количества нескорректированных функциональных точек осуществляется по-разному для EIF и ILF. Этот подход отражен в таблице ниже (табл. 2.2).

Табл. 2.2.

Оценка UFP для ILF и EIF

Сложность данных	Количество UFP	
	ILF	EIF
Низкая	7	5
Средняя	10	7
Высокая	15	10

Одновременно с подсчетом функциональных точек для данных, аналогичная процедура осуществляется в отношении операций, осуществляемых пользователем.

Операция (также называется транзакцией) – «элементарный неделимый замкнутый процесс, представляющий значение для пользователя и переводящий продукт из одного консистентного состояния в другое».

В соответствии с методом FP выделяются три типа операций, который могут быть связаны с программным продуктом:

EI (external inputs) – внешние входные транзакции, целью которых является поддержка ILF или изменение поведения системы;

EO (external outputs) – внешние выходные транзакции, целью которых является предоставление обработанных данных пользователю;

EQ (external inquiries) – внешние запросы, целью которых является предоставление информации пользователю.

На практике могут возникать затруднения при определении группы, к которой следует отнести классифицируемую операцию. Далее приведена сравнительная характеристика присущих им функций, которая дает возможность облегчить процесс принятия решения при отнесении операции к тому или иному типу (табл. 2.3).

Табл. 2.3.

Основные характеристики операций

Функция	Тип транзакции		
	EI	EO	EQ
Изменяет поведение системы	основная	дополнительная	-
Поддержка одного или более ILF	основная	дополнительная	-
Представление информации пользователю	дополнительная	основная	основная

По аналогии с данными, оценка сложности операции базируется на изучении ее показателей:

FTR (file type referenced) – ссылки на модифицируемые и/или считываемые файлы ILF и EIF;

DET (data element type) – неповторимое уникальное поле данных.

Для оценки сложности операции применяются матрицы, изображенные ниже (табл. 2.4. и табл. 2.5.). Необходимо отметить, что для входных и выходных операций применяются различные критерии определения степени сложности.

Табл. 2.4.

Матрица сложности внешних входных операций (EI)

	1 – 4 DET	5 – 15 DET	16+ DET
0 – 1 FTR	Низкая	Низкая	Средняя
2 FTR	Низкая	Средняя	Высокая
3+ FTR	Средняя	Высокая	Высокая

Табл. 2.5.

Матрица сложности внешних выходных операций и внешних запросов (EO и EQ)

	1 – 5 DET	6 – 19 DET	19+ DET
0 – 1 FTR	Низкая	Низкая	Средняя
2 - 3 FTR	Низкая	Средняя	Высокая
4+ FTR	Средняя	Высокая	Высокая

Для перевода сложности представленных в матрицах показателей операции в функциональные точки используется следующая таблица 2.6.

Табл. 2.6.

Оценка UFP для операций

Сложность данных	Количество UFP	
	EI и EQ	EO
Низкая	3	4
Средняя	4	5
Высокая	6	7

Отобразить взаимосвязь данных и операций можно с помощью рис.2.7.

По окончании этого процесса производится суммирование количества полученных нескорретированных функциональных точек, связанных с данными и операциями (формула 2.6).

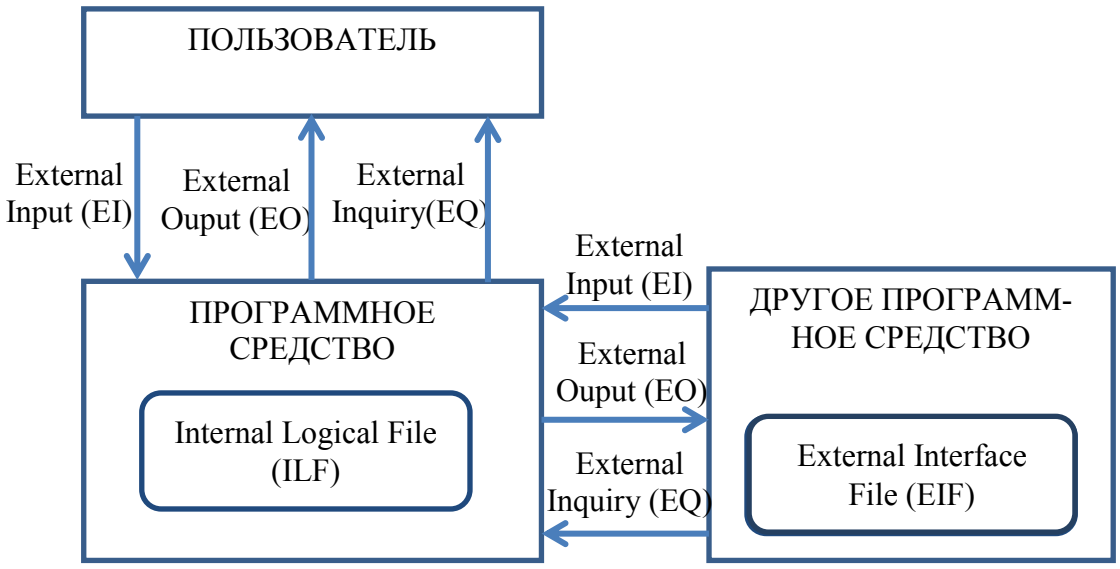

Рис. 2.6. Взаимосвязь данных и операций, учитываемых при определении количества функциональных точек

$$UFP = \sum_{ILF} UFPi + \sum_{EIF} UFPi + \sum_{EI} UFPi + \sum_{EO} UFPi + \sum_{EQ} UFPi, \quad (2.7)$$

где UFPi – количество нескорректированных функциональных точек, полученных при подсчете данных (ILF и EIF) и операций (EI, EO, EQ).

Параллельно с подсчетом количества связанных с данными и транзакциями нескорректированных функциональных точек осуществляется определение величины корректирующего фактора (VAF), для расчета которого четырнадцати важнейшим параметрам программного продукта присваиваются

значения, характеризующие степень их воздействия на процесс разработки. К этим параметрам относятся: передача данных, распределенная обработка данных, производительность, влияние используемой конфигурации, операционная скорость, ввод данных в режиме онлайн, эффективность работы конечного пользователя, интерактивное обновление, сложность обработки, многократное использование, удобство установки, легкость эксплуатации, переносимость, легкость внесения изменений.

Расчет значения VAF осуществляется посредством следующей формулы (формула 2.8):

$$VAF = (\sum DI * 0{,}01) + 0{,}65, \quad (2.8)$$

где VAF – величина корректирующего фактора;

DI (degrees of influence) – влияние параметра корректирующего фактора.

Последним шагом метода является расчет количества скорректированных функциональных точек в зависимости от выбранного на первом этапе типа оценки. Для оценки готового продукта перемножается количество нескорректированных функциональных точек и величины корректирующего фактора. При определении размера разрабатываемого продукта также учитывается количество нескорректированных функциональных точек, которые потребуются при установке продукта.

Поскольку метод позволяет наглядно продемонстрировать заказчику взаимосвязь между требованиями к функциональности программы и ее стоимостью, функциональные точки активно используются в ИТ-сфере.

2.1.2. Анализ существующего механизма закупок программных средств для нужд таможенных органов

«Ускорение научно-технического прогресса, без которого невозможен рост конкурентоспособности, требует ускоренного обновления продукции,

внедрения гибкой технологии и сопровождающего ее программного обеспечения»[7].

Динамика расходов на закупку программных средств для ФТС России представлена на рисунке далее (рис. 2.7).

Источником информации послужили данные, представленные на сайте Центрального информационно-технического таможенного управления в разделе, посвященном результатам конкурсных торгов. Для анализа была выделена часть расходов ФТС России, непосредственно связанная с приобретением программных средств.

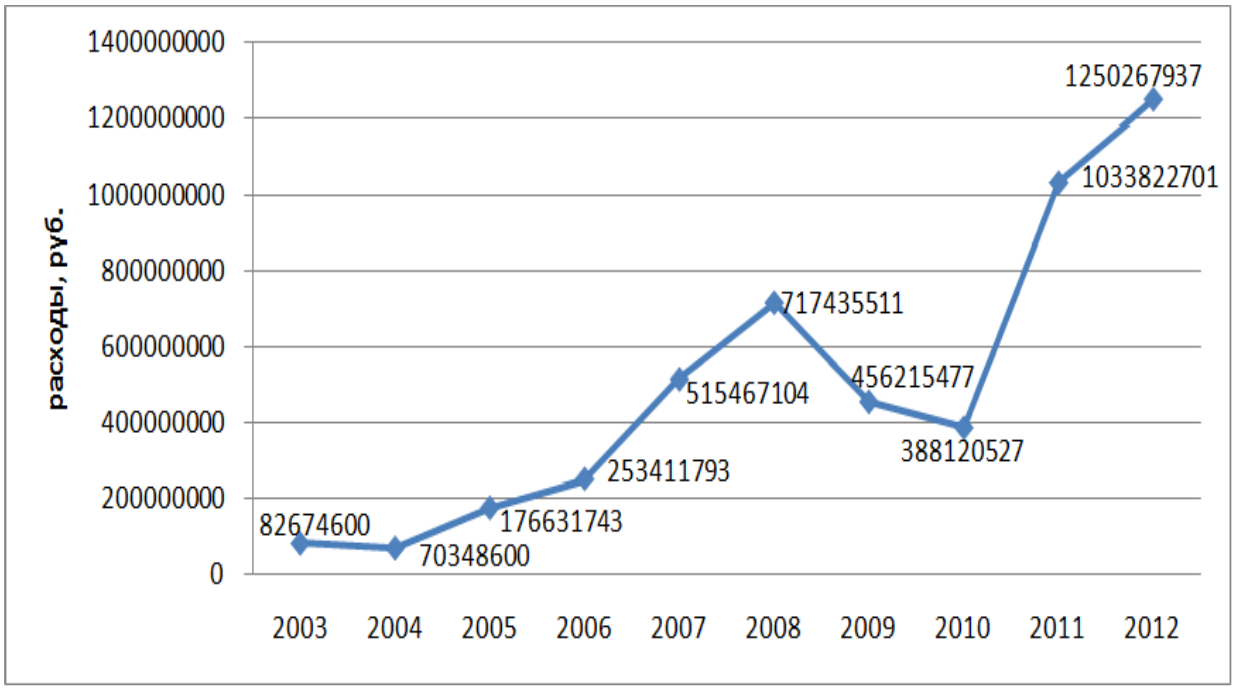

Рис. 2.7. Суммарные расходы на закупку программных средств для ФТС России, руб.[8]

График демонстрирует значительные колебания, объяснить которые можно изменением экономической ситуации в стране. Наглядно отображены «провалы»: практически незаметный в 2004 и значительный в 2009 – 2010 годах. Связать данные изменения в общей тенденции роста можно с кризисами, которые происходили в это время в мировой экономике. Так, 2004 год

[7] Скалкин В.В. Управление внедрением программного обеспечения технологической подготовки производства на машиностроительном предприятии: авт. дисс. … канд. экон. наук. / Государственная ордена Трудового Красного Знамени Академия Управления имени Серго Орджоникидзе. – М., 1993 г. – С.7.

[8] Результаты конкурсных торгов. Центральное информационно-техническое таможенное управление. Режим доступа: World Wide Web. URL: http://edpc.customs.ru

ознаменовался банковским кризисом в России, послужившим причиной ухудшения имиджа страны в глазах импортеров и зарубежных инвесторов. Помимо этого, произошел энергетический кризис, приведший к падению объемов производства большинства стран. Аналогичная ситуация сложилась и в 2009 – 2010 годах, когда произошел мировой финансово-экономический кризис, повлиявший на многие сферы деятельности государства. В этих условиях расходы на закупку программных средств не могли остаться неизменными. Впрочем, уже с 2011 года объем затрат вернулся на докризисный уровень и даже превысил его.

Неудивительно, что ряд исследователей называет «обеспечение современными программными средствами одной из важнейших стоящих перед таможней задач»[9].

Изучение затрат на обеспечение ПС деятельности ФТС России было бы неполным без рассмотрения их структуры, в которой можно выделить три основных направления: внедрение, модернизация и сопровождение.

Внедрение подразумевает под собой приобретение новых ПС, а модернизация – придание ранее закупленным непредусмотренных изначально функций. Сопровождение осуществляется организациями в отношении поставленных ими средств и заключается в обновлении, настройке и технической поддержке. Соотношение затрат на реализацию этих направлений в относительных величинах отображено в Приложении 7, а в абсолютных – на рисунке далее (рис. 2.8).

[9] Липатова Н.Г., Вялов М.А. Информационные технологии и современная таможня. Таможенная служба России на защите экономических интересов страны: Материалы докладов Всероссийской научно-практической конференции. – М.: Изд-во Российской таможенной академии, 2003. – С. 339.

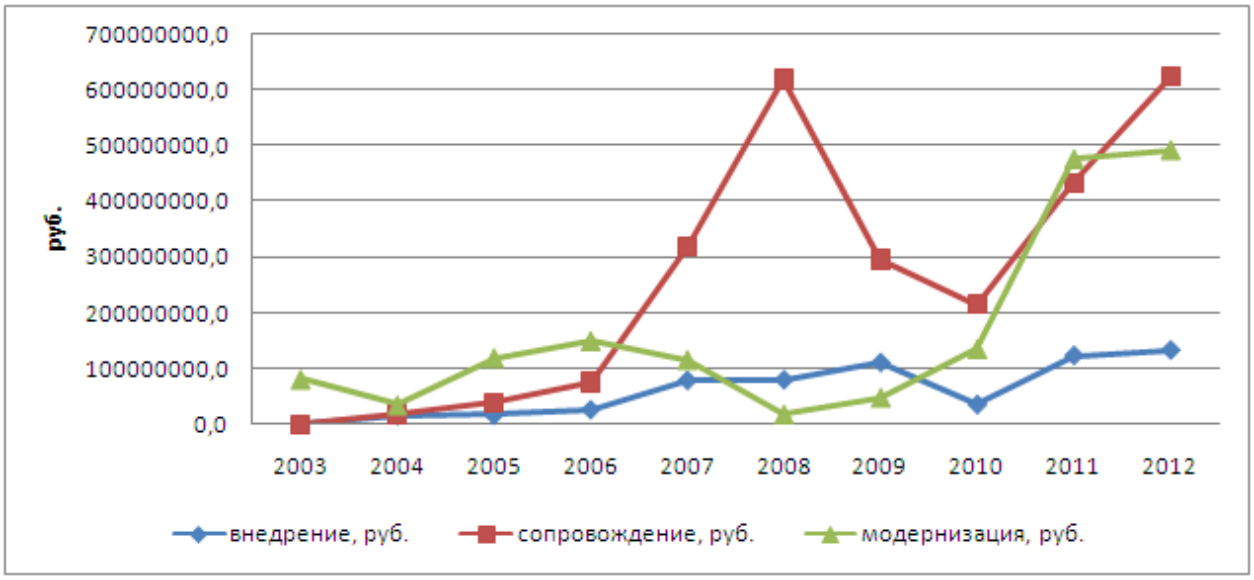

Рис. 2.8. Динамика затрат на внедрение, модернизацию и сопровождение закупаемых для ФТС России программных средств, %

В сравнении с прочими процессами объем затрат на внедрение ПС оставался более стабилен в абсолютных величинах в течение всего исследуемого периода. Возрастание его доли в кризисные годы можно объяснить уменьшением объемов денежных средств, выделяемых на другие направления информатизации, а также приоритетом внедрения новых программ. Процессы модернизации и сопровождения являются обратно пропорциональными: рост одного из них сопровождается уменьшением другого. Помимо этого, есть некоторая взаимосвязь с приобретением новых ПС. Так, до 2008 года процесс внедрения был прямо пропорционален сопровождению, а после – модернизации.

Рост объемов расходов на закупку ПС для ФТС России данную статью затрат как несомненно важную и обладающую тенденцией к увеличению в долгосрочной перспективе. При этом особая, нематериальная форма данного вида продукции обусловливает риск неэффективного расходования средств федерального бюджета, который может реализоваться в виде завышения стоимости приобретаемого ПС. В этих условиях особую актуальность приобретает изучение механизма закупок ПС для ФТС России с целью выявить присущие ему недостатки для их последующей ликвидации. Для этого в процессе исследования были изучены представленные на официальном сайте госу-

дарственных закупок[10] материалы, содержащие сведения о приобретении ПС для ФТС России.

По результатам данного действия было установлено, что механизм закупок значительно различается в зависимости от таких характеристик ПС, как уникальность и комплектность. При этом под уникальностью следует понимать степень неповторимости ПС, его разработку в соответствии с требованиями конкретного заказчика. Комплектность является признаком, характеризующим программу как поставляемое совместно либо отдельно от оборудования, предназначенного для его применения.

Основными отличительными характеристиками тиражируемого ПС являются его завершенность как готового для продажи товара и отсутствие конкретных, определенных ранее, покупателей (либо в их качестве предполагается широкий круг лиц). Заказные программы, соответственно, являются антиподами тиражируемого: покупатель определен заранее, объект сделки непосредственно в момент заключения контракта не готов (определена основная концепция его создания либо планируется доработка в соответствии с потребностями заказчика). Особое место в классификации занимает поставляемое с оборудованием программное обеспечение, которое может быть как тиражируемым, так и заказным.

Функционирующий в настоящее время механизм обеспечения ФТС России ПС представлен на рис. 2.9.

Следует заметить, что в зависимости от того, к какой группе ПС в соответствии с классификацией принадлежит объект закупки, таможенными органами применяется тот или иной алгоритм его приобретения.

[10] Портал закупок. Режим доступа: World Wide Web. URL: http://zakupki.gov.ru.

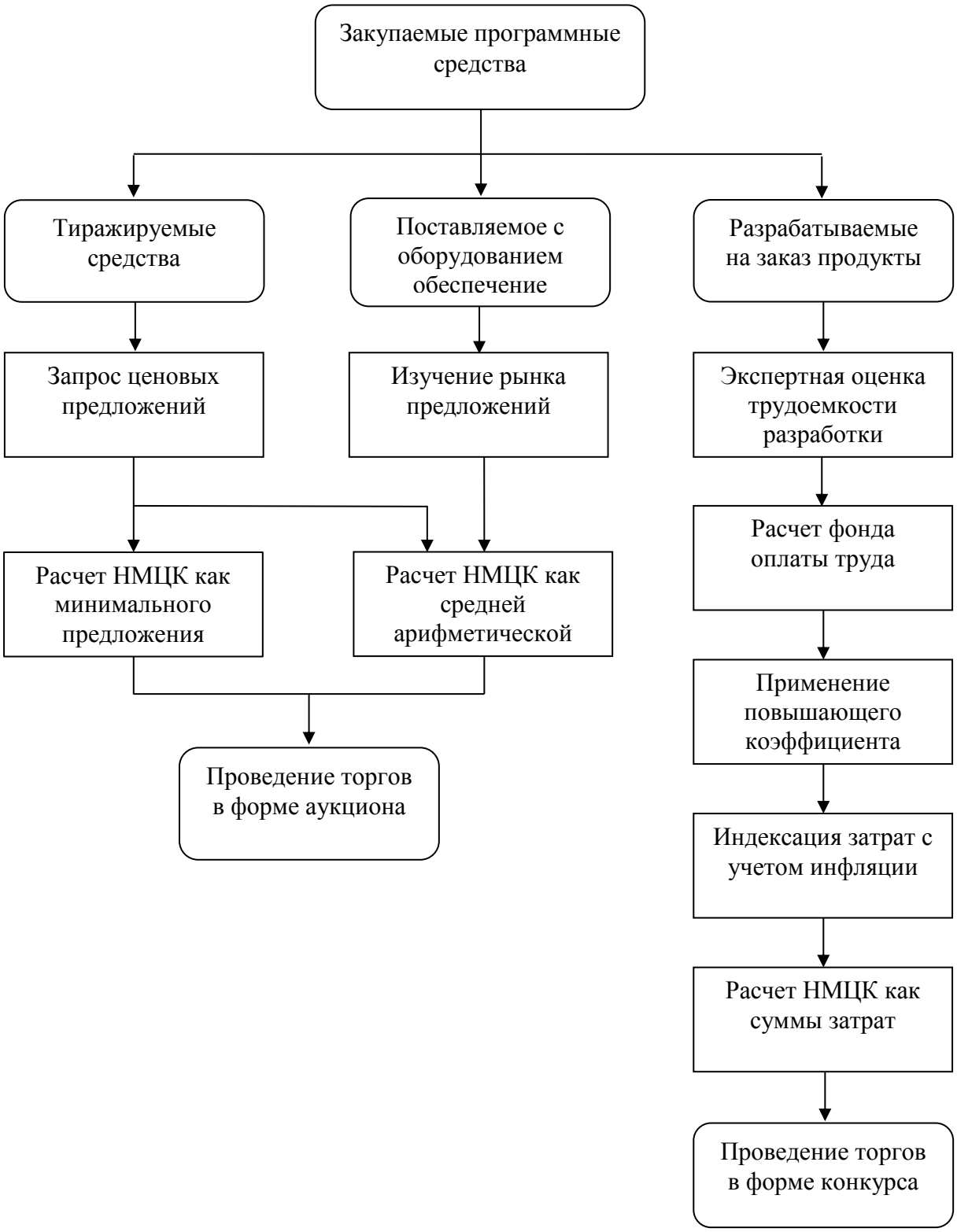

Рис. 2.9. Механизм закупок ПС для ФТС России

Рынок тиражируемых ПС характеризуется значительным количеством продавцов, развитостью и широким ассортиментом продукции. Данное обстоятельство позволяет уполномоченным лицам ФТС России определять

НМЦК путем запроса ценовых предложений у потенциальных поставщиков. Для этого ЦИТТУ направляет запросы с необходимыми для оценки условиями контракта в организации, предоставляющие данный вид услуг. После получения не менее трех ответов осуществляется расчет НМЦК на основе одного из двух следующих подходов:

выбор минимального ценового предложения;

расчет средней цены предложения.

На практике первый подход чаще всего используется в случае комплексной закупки, когда запланировано приобретение более одного ПС; а второй, соответственно, в остальных случаях.

Завершающим этапом обоснования НМЦК для тиражируемого ПС является математическое округление в меньшую сторону, после чего проводятся торги в форме аукциона.

Практически полностью повторяет рассмотренный алгоритм последовательность действий, осуществляемых при закупке поставляемых совместно с оборудованием ПС. Классическим примером подобной закупки является приобретение вычислительных машин (компьютеров и ноутбуков) с предустановленными на них операционными системами.

Для этого осуществляется изучение рынка предложений в сети Интернет, после чего проводится расчет НМЦК как средней арифметической с последующим округлением в меньшую сторону и посредством аукциона определяется победитель. Данный алгоритм обладает двумя особенностями:

Во-первых, в настоящее время для расчета НМЦК используются представленные на сайтах продавцов цены, которые учитывают суммарную стоимость как оборудования, так и ПС без их разделения.

Во-вторых, алгоритм начинается с изучения рынка, в отличие от запроса ценовых предложений, применяемого в отношении тиражируемых ПС. Данный подход позволяет подобрать в большей степени соответствующий потребностям ФТС России как заказчика аппаратно-программного средства (АПС).

Последним будет рассмотрен алгоритм приобретения для Федеральной таможенной службы заказных (уникальных) ПС, которые включают в себя как принципиально новые, так и модернизированные программы.

В данном случае основной статьей затрат выступает фонд оплаты труда (далее - ФОТ), для обоснования расчета которого необходимо иметь данные о трудоемкости реализации проекта.

Данный показатель определяется в таможенных органах методом экспертной оценки, позволяющим получить приблизительное значение количества необходимых для работы трудочасов.

При этом стоимость единицы времени, одного трудочаса рассчитывается, исходя из полученных от Федеральной службы государственной статистики Российской Федерации данных, в которых содержатся сведения о среднемесячной начисленной заработной плате в расчете на одного работника по следующим видам деятельности: «Разработка программного обеспечения и консультирование в этой области» и «Прочая деятельность, связанная с использованием вычислительной техники и информационных технологий».

Последующие простейшие математические операции позволяют рассчитать размер ФОТ. Для оптимизации расчета НМЦК в отношении ПС таможенными органами применяется повышающий коэффициент, который призван увеличить стоимость проекта для покрытия накладных расходов, социальных отчислений, налогов и обеспечить прибыль исполнителю контракта. Также для учета инфляции проводится индексация полученной суммы.

Полученная в результате величина затрат устанавливается как НМЦК для последующих торгов в форме конкурса. Данный способ определения победителя, вводя дополнительные критерии оценки предложений (такие как сроки реализации и квалификация исполнителя) и специальные коэффициенты, позволяет снизить значимость субъективно определенной цены контракта.

Изучение механизма обеспечения таможенных органов ПС позволяет выделить следующие его недостатки:

Во-первых, это субъективизм при определении трудоемкости разработки ПС, что приводит к необходимости непосредственно перед каждой закупкой получать данные из других органов государственной власти. Также возникает потребность в проведении торгов именно в форме конкурса, чтобы снизить значимость цены контракта как критерия определения победителя. Для этого применяются определенные экспертами коэффициенты, что опять же повышает субъективизм оценки расходов. При этом «исторически сложилось так, что разработку информационных систем, программных комплексов, программных задач ведут отдельные фирмы программистов без учета системного подхода и видения ФТС как целостной системы»[11].

Во-вторых, применение повышающего коэффициента к сумме рассчитанного ФОТ, который должен покрыть накладные расходы, отчисления в фонды, налоги и обеспечить прибыль разработчику. Для повышения обоснованности стоимости приобретаемого ПС необходима детализация всех затрат исполнителя.

В-третьих, непроработанный алгоритм закупки поставляемых с оборудованием ПС. В современных условиях, когда происходит активное развитие рынка данного вида продукции и появляются все новые типы оборудования, появляется возможность раздельного приобретения данных товаров. Это обстоятельство должно быть учтено при совершенствовании научно-методического аппарата механизма закупок ПС для ФТС России.

В-четвертых, имеет место двойственный подход к расчету НМЦК при закупке тиражируемых ПС. Необходимо изучить целесообразность их применения в различных ситуациях и выбрать наиболее соответствующие интересам таможенных органов и, соответственно, государственного аппарата.

[11] Гусев С.Л. Совершенствование архитектуры Единой автоматизированной информационной системы ФТС России. Актуальные проблемы теории и практики таможенного дела и пути их решения: сборник материалов Международной научно – практической конференции: в 2 ч. Ч. 2. М.: Изд-во Российской таможенной академии, 2010. – С. 35.

Дальнейшее исследование должно быть направлено на ликвидацию выявленных недостатков, для чего необходимо совершить следующие действия:

найти альтернативу используемому в настоящее время способу расчета стоимости разработки уникального ПС;

доработать научно-методический аппарат в части закупок тиражируемых и поставляемых с оборудованием ПС;

сформировать практические рекомендации по реализации выдвинутых предложений.

2.2. Разработка научно-методического аппарата закупок программных средств для нужд таможенных органов

2.2.1. Понятийный аппарат и характеристика программных средств таможенных органов как особого рода товара

Изучая нормативно-правовые акты, учебные и научные источники, можно обратить внимание на тот факт, что некоторые исследователи используют как синонимы такие понятия, как «программное изделие», «программа для ЭВМ», «программное средство», «программный продукт» и «программное обеспечение».

Также, например, А.Н. Степанов писал, что «логика развития программного обеспечения систем управления проектами привела к тому, что программные средства этого класса хорошо приспособлены для обработки информации по проектам предприятия»[12]

Ермаков И.А. проводит параллели между такими понятиями, как программная продукция и программное изделие. В своей диссертации он отмечал: «программная продукция разрабатывается (а не изготавливается в процессе промышленного производства), а стоимость программного изделия

[12] Степанов А.Н. Инновации в области применения программного обеспечения систем управления проектами: дисс. … канд. эконом. наук / ГОУ ВПО Государственный университет управления. – М., 2003. – С. 5.

определяется стоимостью инженерной деятельности, а не производственной»[13].

Выявление различий между перечисленными понятиями позволяет аргументированно использовать их, способствует пресечению возможных споров в процессе их толкования в нормативно-правовых актах и его предлагается учесть при разработке усовершенствованного механизма закупок ПС для ФТС России.

Представленная далее таблица содержит понятия, а также список регламентирующих их нормативно-правовых актов (табл. 2.8).

Таблица 2.8

Понятия и содержащие их нормативно-правовые акты

№	Понятие	Нормативно-правовой акт
1	программа	Приказ ФТС России от 28.12.2006 № 1378 «О внесении изменений в отдельные правовые акты ФТС (ГТК) России». Приказ Минздравсоцразвития РФ от 14.10.2011 № 1175н «Об утверждении Межотраслевых типовых норм времени на работы по сервисному обслуживанию оборудования телемеханики, сопровождению и доработке программного обеспечения». ГОСТ СССР 19.781-90 (уст. Постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 27.08.1990 г. № 2467)
2	программа для ЭВМ	«Гражданский кодекс Российской Федерации (часть четвертая)» от 18.12.2006 № 230-ФЗ
3	программное изделие	ГОСТ СССР 19.004-80 (уст. Постановлением Государственного комитета СССР по стандартам от 08. 05.1980 г. № 2051)
4	программное средство	Межгосударственный стандарт ГОСТ 28806-90 (уст. Постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 25.12.1990 г. № 3278)
5	программный продукт	Межгосударственный стандарт ГОСТ 28806-90 (уст. Постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 25.12.1990 г. № 3278)
6	программное обеспечение	Межгосударственный стандарт ГОСТ 19.781-90 (уст. Постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 27.08.1990 г. № 2467)

[13] Ермаков И.А. Логистическая поддержка процесса разработки интеллектуальной продукции в сфере производства программного обеспечения: дисс. … канд. эконом. наук / ГОУ ВПО ГУУ. – М., 2004. – С. 166.

Количество нормативно-правовых актов, содержащих рассматриваемые понятия, действительно велико. Необходимо также учитывать, что представленный в таблице список документов не полон. Следует отметить, что толчком к развитию понятийного аппарата, результатом которого стало появление большей части новых терминов, послужило принятие регулирующих данную сферу стандартов в СССР в 1980-1990-х годах.

Наиболее общим понятием, производным от которого являются все остальные представленные в таблице, выступает слово «программа». Им определяют целый спектр объектов и процессов.

Наглядным примером устаревания отдельных элементов понятийного аппарата служит термин «программное изделие». Он был закреплен в стандарте СССР № 19.004 в 1980 году. При этом под программным изделием понималась единичная или логически связанная совокупность программ, обладающая следующими важнейшими характеристиками: является результатом промышленного производства, снабжена сопутствующей документацией, предназначена для широкого распространения, записана на носителях информации. Если ранее термин активно применялся, то с момента его закрепления в стандарте он вызвал критику исследователей, указывавших на слишком грубое понимание промышленного характера программирования. Поэтому уже в 1990 году ГОСТ 19781, принятый взамен ГОСТ 19.004, данного понятия не содержал.

Законом «О правовой охране программ для электронных вычислительных машин и баз данных», принятым Верховным Советом Российской Федерации в 1992 году, был определен новый объект правовой охраны – «программа для ЭВМ». В соответствии с современным законодательством, это «представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготови-

тельные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения»[14].

В научной литературе придерживаются следующего определения: «программа для ЭВМ – объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин и других компьютерных устройств с целью получения определенного результата»[15].

Однако нельзя не отметить, что термин ЭВМ (электронная вычислительная машина) в настоящее время почти вытеснен из бытового употребления и употребляется чаще всего только в юридических документах либо материалах исторической направленности. Это дает основания говорить о том, что понятие постепенно устаревает и выходит из повседневного оборота, а основной причиной, по которой его до сих пор используют, является некоторое отставание развития правового поля от современных общественных отношений. Можно предположить, что со временем словосочетание разделит участь термина «программное изделие».

Определенные сложности возникают при разграничении определений программного продукта, средства и обеспечения. Отнюдь не способствует решению этого вопроса постоянное развитие механизма правового регулирования, так как в результате данного процесса появляются все новые интерпретации изучаемых понятий. Чтобы преодолеть это препятствие, рассмотрим, какое содержание вкладывал в эти понятия законодатель изначально. Для этого необходимо обратиться к стандартам СССР, закрепившим их определения.

Программное обеспечение – «совокупность программ системы обработки информации и программных документов, необходимых для эксплуата-

[14] «Гражданский кодекс Российской Федерации (часть четвертая)» от 18.12.2006 № 230-ФЗ. М.: consultant.ru, 2014. Режим доступа: World Wide Web. URL: http://www.consultant.ru

[15] Проблемы совершенствования правовой системы информационной безопасности таможенного дела: монография / М.И. Агабалаев, А.Н. Дюков, Н.М. Кожуханов и др. М.: Изд-во Российской таможенной академии, 2009. – С. 146.

ции этих программ»[16]. Необходимо отметить, что с точки зрения экономической теории под обеспечением понимается прежде всего процесс, что дает повод усомниться в достаточной обоснованности рассматриваемого термина. Однако его закрепление на законодательном уровне позволяет использовать его и в настоящей работе.

Программное средство – «объект, состоящий из программ, процедур, правил, а также, если предусмотрено, сопутствующих им документации и данных, относящихся к функционированию системы обработки информации»[17]. При этом в пояснениях к терминам стандарта отмечается, что объем понятия, выражаемого производным термином «программные средства», включает в себя как частный случай объем понятия «программное обеспечение».

«Термин «продукт» давно используется в экономической практике и во всех школах экономической теории. В маркетинговой теории и практике этот термин присутствует как атрибут потребительского рынка»[18]. При этом программный продукт – «программное средство, предназначенное для поставки, передачи, продажи пользователю»[19].

Для наглядного представления можно графически изобразить взаимосвязь понятий с помощью кругов Эйлера.

Приведенные определения в сочетании с диаграммой, изображенной выше (рис. 2.10), позволяют сделать следующие выводы.

[16] Межгосударственный стандарт ГОСТ 19781-90 «Обеспечение систем обработки информации. Программное» (утв. постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 27 августа 1990 г. № 2467) . М.: consultant.ru, 2014. Режим доступа: World Wide Web. URL: http://www.consultant.ru

[17] Межгосударственный стандарт ГОСТ 28806-90 «Качество программных средств. Термины и определения» (утв. постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 25 декабря 1990 г. № 3278) . М.: consultant.ru, 2014. Режим доступа: World Wide Web. URL: http://www.consultant.ru

[18] Бизин С.В. Информационные продукты таможенных органов: классификация, стоимость, потребительская ценность. Вестник Российской таможенной академии № 2. М.: Изд-во Российской таможенной академии, 2010. – С. 131 – 138.

[19] Там же.

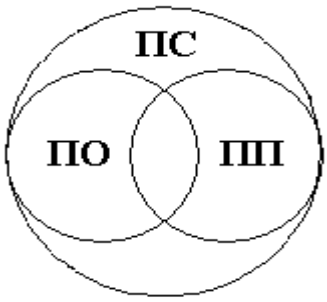

Рис. 2.10. Отображение взаимосвязи программных средств, продуктов и обеспечения с помощью кругов Эйлера

Во-первых, общим понятием выступает программное средство, а программные продукты и обеспечение являются его частными случаями.

Во-вторых, выбор применяемого понятия зависит от контекста ситуации. Если рассматривается продажа программы, то правильнее использовать словосочетание «программный продукт», если же в разговоре или тексте подразумевается программа, необходимая для выполнения оборудованием предусмотренных функций, лучше применять понятие «программное обеспечение». Термин «программное средство» может использоваться во всех случаях, поскольку носит обобщающий характер.

Разумеется, понятийный аппарат изучаемой сферы состоит не только из рассмотренных ранее понятий. В качестве примеров можно привести «программный комплекс», «АПС», «программно-техническое средство» и целый ряд других. Зачастую они не имеют законодательного закрепления либо имеют несколько неоднозначных определений, которые могут быть подвергнуты критике.

Таким образом, в настоящее время активно развиваются информационные технологии, на рынке появляются все новые виды высокотехнологичной продукции. Вследствие этого понятийный аппарат данной сферы характеризуется значительным обновлением, что ведет к недостаточно обоснованному использованию терминов.

Полученные в настоящем параграфе выводы и результаты послужат основой для выработки принципов экономической оценки закупаемых таможенными органами программных средств.

2.2.2. Экономическая оценка закупаемых таможенными органами программных средств

По результатам изложенного выше анализа было установлено, что в настоящее время механизм закупок программных средств для таможенных органов обладает рядом недостатков. Это обстоятельство обусловливает потребность в его усовершенствовании, и одним из первых шагов в данном направлении должна стать выработка методических принципов, на которых будет базироваться усовершенствованный механизм.

При этом под методическими принципами в данном случае понимаются наиболее общие теоретические положения, выражающие выявленные в процессе изучения функционирующего в настоящее время механизма закупок ПС для ФТС России закономерности, которые должны быть учтены при его последующем совершенствовании.

Можно выделить следующие методические принципы:

дифференциации;

объективности;

единого подхода;

эффективности;

необходимой квалификации;

самостоятельности;

последовательности.

К данной группе может быть отнесен принцип дифференциации, который диктует необходимость разделять государственные закупки в зависимости от типа приобретаемого ПС. Изучение практики приобретения программ в целях обеспечения таможенных органов позволяет выявить значительные различия в процедурах расчета НМЦК и определения победителя при осуществлении закупок. Данная специфика обусловлена особенностями приобретаемой продукции и побуждает в качестве первого шага исследования и развития методических основ сформировать классификацию ПС, после чего на ее основе можно дифференцировать осуществляемые закупки. Классифи-

кация даст возможность выявить последовательности действий, характерные для различных видов закупок, и позволит совершенствовать непосредственно сам механизм их проведения. Поэтому рассмотренный принцип является первоочередным в их перечне.

Важнейшим недостатком функционирующего в настоящее время механизма является субъективизм при определение трудоемкости разработки программного средства. Совокупность мер, направленных на его снижение, определяется принципом объективности. Среди данных мер следует особо выделить снижение значимости экспертного метода определения трудоемкости разработки заказных программных продуктов, а по возможности – полностью отказаться от его применения, заменив объективной методикой. Реализация данной возможности позволит обоснованно планировать затраты на информатизацию таможенных органов и регулировать очередность закупок. В сочетании с первым рассмотренным, данный принцип является важнейшим в деле совершенствования механизма закупок программ.

Принцип единого подхода актуален в отношении закупок тиражируемых программных средств. В процессе изучения представленной на сайте «Госзакупки» документации было выявлено, что расчет НМЦК в данном случае осуществляется двумя способами: посредством определения средней арифметической для ценовых предложений потенциальных поставщиков или путем выбора минимального предложения и его последующего установления в качестве цены контракта. Каких-либо объективных причин применения того или иного способа не было выявлено. Указанный недостаток должен быть устранен путем установления условий применения метода расчета НМЦК.

Принцип эффективности применяется к закупкам поставляемого с оборудованием программного обеспечения. Функционирующий механизм обеспечения таможенных органов программными средствами не предусматривает рассмотрение программ, поставляемых совместно с оборудованием, как самостоятельный объект сделки. В то же время в условиях научно-технического прогресса появляется значительное количество различного

оборудования и выпускается множество версий программного обеспечения. Возможность их раздельного приобретения и последующего совмещения зачастую существует. Более того, выпускается немало некоммерческих бесплатных аналогов лицензионных программ, которые по своим функциональным возможностям не уступают тиражируемым, а по степени защищенности от угроз извне даже превосходят их. В этих условиях объективной мерой становится расчет НМЦК раздельно на оборудование и совместимое с ним программное обеспечение. Однако нельзя забывать, что целью любой государственной закупки является удовлетворение потребностей органа государственной власти с минимальными издержками для федерального бюджета. Не редка ситуация, когда рассчитанная совместно НМЦК окажется минимальной либо раздельная оценка попросту невозможна. Поэтому определять начальную стоимость поставляемого АПС следует раздельно и совместно одновременно, после чего следует выбрать наименьшую из них.

Необходимым для определения стоимости заказного программного продукта является наличие специально подготовленных оценщиков. Данная потребность реализуется в рамках принципа квалификации. Расчет НМЦК является непростой задачей, которая требует подготовленные кадры. Помимо этого, совершенствование экономического механизма обеспечения таможенных органов программными средствами невозможно без тщательной подготовки по причине его сложности и значимости в структуре затрат федерального бюджета. Принцип квалификации обусловливает многие следующие далее практические рекомендации: проведение НИР, обучение должностных лиц таможенных органов.

Неразрывно связан с предыдущим принцип самостоятельности. Большая часть объективных методик определения стоимости заказных программных средств довольно сложна и требует значительных знаний в данной сфере. Основная идея принципа заключается в том, что привлечение независимых оценщиков без подготовки собственных чревато для таможенных органов негативными последствиями, среди которых можно отметить: увеличе-

ние расходов для федерального бюджета, завышение стоимости в случае заинтересованности осуществляющего оценку лица, отсутствие единого подхода к оценке разных программ. Поэтому объективной необходимостью становится подготовка группы оценщиков в рамках Федеральной таможенной службы.

Исходя из выявленных возможностей для совершенствования механизма обеспечения таможенных органов программными средствами сформулируем основные направления дальнейшего исследования:

нахождение либо разработка методики, позволяющей с большей точностью определять трудоемкость разработки программного продукта;

доработка научно-методического аппарата в части закупок тиражируемых и поставляемых с оборудованием программных средств;

формирование практических рекомендаций по реализации выдвинутых предложений.

2.2.3. Теоретическое обоснование механизма закупок программных средств для нужд таможенных органов

Как следует из ранее полученных выводов, важнейшим направлением совершенствования механизма обеспечения ФТС России должно стать повышение объективности расчета стоимости разработки уникального ПС.

«Несмотря на существование большого числа моделей оценки затрат на разработку ПО, эта область продолжает оставаться недостаточно хорошо изученной, вызывающей растущий интерес специалистов по программным проектам»[20]. Однако анализ научно-методического аппарата и практики экономической оценки ПС показал, что среди существующих в настоящее время подходов наиболее перспективным является аналитический, в рамках которого следует выделить метод функциональных точек.

Необходимо отметить, что определение размера программы на основе объема его функциональных возможностей имеет значительный потенциал.

[20] Амелина О.В. Управление качеством проектов по созданию продуктовых инноваций (на примере разработки программного обеспечения): дисс. … канд. экон. наук. / Орловский государственный технический университет. – Орел, 2003 г. – С. 88.

В частности, полная независимость оценки от оборудования, на котором планируется использование программы, и единый подход в отношении предназначенных для разных направлений деятельности продуктов. Метод широко распространен в зарубежных странах, для его поддержки и совершенствования была создана организация, которая готовит и предоставляет всем заинтересованным лицам необходимые для применения метода материалы. Более того, модифицированный вариант метрики (MK II FPA) принят в качестве национального стандарта в Великобритании[21]. Его применение на государственном уровне в развитых странах Европы стало возможным благодаря способности к доработке в соответствии с конкретными потребностями потребителя. Это обстоятельство позволяет говорить о применимости метода и в российских условиях, в том числе и в сфере государственных закупок.

Однако методу присущи и недостатки, среди которых можно выделить следующие:

наличие статистики трудозатрат на реализацию функциональных точек является необходимым условием применения;

лучшие результаты достигаются при оценке однотипных проектов одной командой;

требуется квалифицированный оценщик для подробной проработки технического задания.

Метод дает возможность определить размер продукта в специальных единицах измерения – функциональных точках, которые позволяют сделать вывод об объеме заложенных в программе возможностей для пользователя, так называемом функционале. Если данные по затратам на создание одной функциональной точки отсутствуют, составить план расходов на реализацию проекта невозможно.

[21] ISO/IEC 20968 Software engineering - Mk II Function Point Analysis—Counting Practices Manual. Режим доступа: World Wide Web. URL: https://www.iso.org

Метод применим в отношении самых разных программ, но самый точный прогноз количества функциональных точек осуществляется при оценке однотипных проектов одной командой.

В настоящее время существуют четыре наиболее известные вариации метода функциональных точек (метрики):

FPA IFPUG (наиболее распространенная модель в рамках метода, данная версия поддерживается упомянутой ранее международной организацией);

FPA MK II (целью разработки было получение упрощенной версии метода функциональных точек, принят в качестве национального стандарта в Великобритании);

COSMIC (гибрид FPA IFPUG и FPA MK II, был предназначен для оценки систем реального времени, а также космических проектов);

COCOMO II (получена в результате объединения FPA IFPUG и COCOMO, использует в качестве единиц измерения как функциональные точки, так и строки кода).

Среди перечисленных метрик наибольшим потенциалом применения в сфере государственных закупок обладают FPA MK II и FPA IFPUG, поскольку позволяют планировать расходы на самых ранних этапах и не используют такие субъективные показатели, как число строк кода. Первая из методик менее распространена, материалы по ней носят разрозненный характер и распространены не широко. Поэтому было принято решение в рамках исследования изучить возможность применения второй методики.

Внедрение методики FPA IFPUG в сферу закупок ФТС России не позволит рассчитать стоимость разработки продукта, но отразит его размер в функциональных точках, которые могут быть переведены в соответствующие им число строк кода с учетом языка программирования. Зная средние трудозатраты одного программиста на написание определенного числа строк кода, можно рассчитать время, необходимое для создания всех функциональных точек продукта. Определить фонд оплаты труда позволяют рассчитываемые

Федеральной службой государственной статистики Российской Федерации сведения о среднемесячной заработной плате программиста. Графически данная последовательность действий может быть отражена посредством следующего рисунка (рис. 2.11).

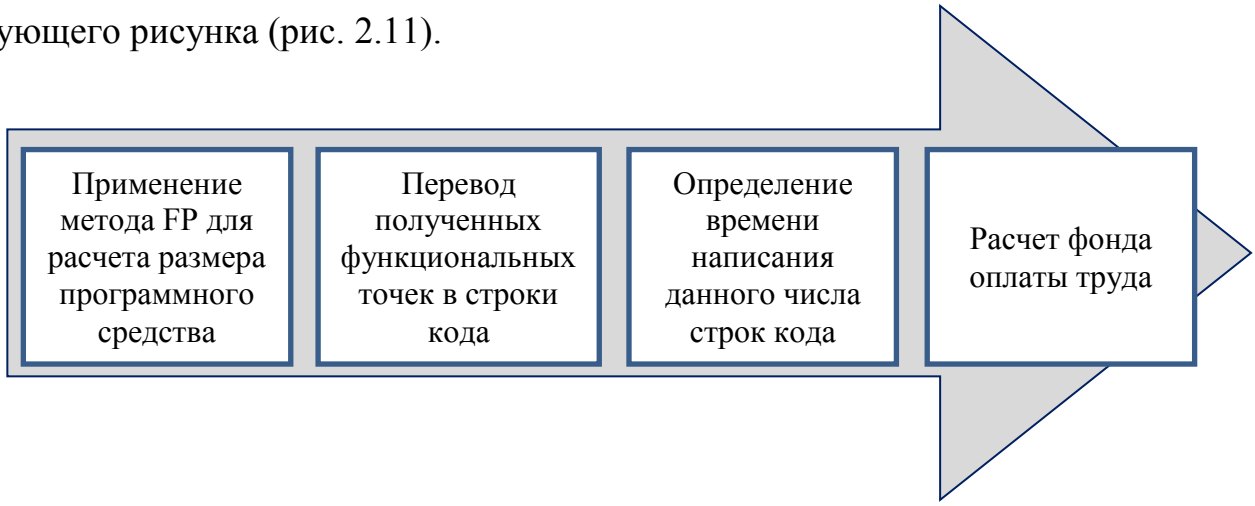

Рис. 2.11. Расчет фонда оплаты труда разработчиков программного продукта с применением метода функциональных точек

Данный подход позволяет рассмотреть метод функциональных точек через экономическую призму, раскрывая его возможности в определении стоимости разработки программного средства. Необходимо отметить, что в науке данная специфика применения метода ещё не отражена, что не способствует внедрению его в практику.

Для разрешения этого противоречия предлагается закрепить данный способ применения метода FP и назвать его функционально-стоимостной оценкой, которая математически может быть отражена посредством формулы 2.9:

$$Cd = p * l * t * w, \qquad (2.9)$$

где Cd – стоимость разработки программного продукта;

p – количество функциональных точек, полученное в результате применения метрики FPA IFPUG;

l – число строк кода, соответствующее одной функциональной точке для данного языка программирования и направления внедрения ПС;

t – время, необходимое программисту на написание одной строки кода на данном языке или системе программирования (ч);

w – стоимость одного трудочаса работы программиста (руб./ч.).

При этом возможность перевести в строки кода полученные в результате измерения программного средства функциональные точки дают возможность полученные эмпирическим путем сведения (табл. 2.9).

Таблица 2.9

Число строк кода для разных языков и систем программирования[22]

№ п/п	Язык программирования	Число строк кода на функциональную точку
1	Basic Assembler	320
2	Macro Assembler	213
3	Basic	107
4	Pascal	91
5	C ++	53
6	Java	53
7	Oracle, Sybase	40
8	Access	38
9	Delphi	29
10	Oracle Developer / 2000	23
11	Smalltalk	21
12	Cobra	20
13	HTML 3,0	15
14	SQL (ANSI)	13
15	Excel	6

Время, необходимое программисту на написание одной строки кода, должно быть рассчитано на основании значительной выборки. При этом необходимо учитывать язык программирования и квалификацию программиста.

Сведения о стоимости одного трудочаса работы программиста будут поступать, как и прежде, из Федеральной службы государственной статистики.

[22] Калайда В.Т. Технико-экономическое обоснование стоимости программных систем: методическое пособие по выполнению экономической части выпускной квалификационной работы для студентов специальности 230105 «Программное обеспечение вычислительной техники и автоматизированных систем». – Томск: ТУСУР, 2009. – С. 11.

При окончательном расчете фонда оплаты труда следует учитывать, что поставленные перед должностными лицами разных подразделений таможенных органов задачи и условия их достижения существенно различаются, вследствие чего имеет место неравная сложность используемых при этом ПС. Поэтому стоимость разработки одного и того же числа строк кода не должна быть одинаковой для всех ПС. Необходима классификация направления применения программ, позволяющая рассчитать собственную, присущую именно ей, стоимость одной функциональной точки. Помимо учета специфики последующего применения разрабатываемого ПС, данный коэффициент позволит покрыть накладные расходы, отчисления в фонды, налоги и обеспечить прибыль разработчику.

На основе изучения операций, осуществляемых должностными лицами таможенных органов, может быть сформирована следующая классификация направлений применения ПС:

регулирующая (таможенное оформление и таможенный контроль, система управления рисками, тарифное регулирование, валютный контроль);

экономическая (таможенная стоимость, таможенные платежи, финансово-хозяйственная деятельность);

управленческая (стратегические цели);

хозяйственная (инфраструктура, логистика);

статистическая (таможенная статистика);

кадровая (штат);

координирующая (взаимодействие с участниками ВЭД, другими органами государственной власти и прочими контрагентами).

Разумеется, данное распределение направлений применения ПС на блоки не является полным и может вызвать обоснованную критику. Однако на данный момент эта классификация представляется наиболее соответствующей цели исследования и учитывающей полученные ранее научные результаты. Несомненно, дальнейшие исследования в данном направлении с боль-

шим учетом специфики деятельности таможенных органов позволят уточнить данный перечень.

Для того чтобы отобразить изменения после внедрения функционально-стоимостной оценки в механизм обеспечения ФТС России программными средствами, на следующем далее рисунке отображены функционирующий в настоящее время и предлагаемый алгоритмы закупки данного вида продукции (рис. 2.12).

Чтобы доказать возможность внедрения функционально-стоимостной оценки в практику, необходимо прежде всего оценить применимость метода функциональных точек на примере используемого в деятельности таможенных органов программного средства.

Для обеспечения удобства проведения расчетов объект оценки не должен обладать излишней сложностью, но в то же время сочетать в себе разнообразные функции, чтобы продемонстрировать применение методики в отношении всех типов функциональных точек.

Исходя из описанных выше соображений, в качестве предмета оценки была выбрана программа «Заполнитель документов», разработанная компанией Альта-Софт[23].

Программа предназначена для извлечения данных из электронных документов произвольного формата и переноса их в программы оформления (заполнения). В первую очередь, эта задача касается товарных перечней, поступающих от отправителей. Дело в том, что эти перечни могут поступать в самых разнообразных форматах (MS Word, MS Excel, DBF, Internet Explorer и др.), притом в виде таблиц произвольного вида.

[23] Альта – Софт. Заполнитель документов. Режим доступа: World Wide Web. URL: http://www.alta.ru/zapolnitel.php

Рис. 2.12. Функционирующий в настоящее время (слева) и предлагаемый (справа) алгоритмы закупки заказных программных продуктов для ФТС России

Место программы в процессе заполнения документов иллюстрирует рис. 2.13.

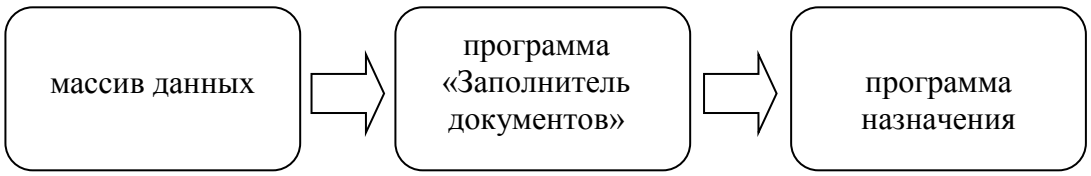

Рис. 2.13. Место программы в процессе заполнения документов для целей таможенного оформления

Программа должна правильно распознать содержимое входного файла и перенести эти данные в программу назначения. Таким образом, исключает-

ся ручной ввод и связанные с ним ошибки, а также значительно ускоряется заполнение при работе с большими списками.

Очевидно, что «Заполнитель документов» занимает важное место в процессе заполнения документов для целей таможенного оформления и может быть рассмотрен в качестве примера для определения возможности применения метода функциональных точек. Несмотря на то, что ПС обрабатывает значительные массивы данных и реализует множество операций, большая часть из них однотипны. Поэтому подсчет суммарного количества функциональных точек в данном случае нецелесообразен. Оценка отдельных групп данных и операций будет в большей степени соответствовать логике исследования.

«Заполнитель» предполагает работу с полученными извне данными, поэтому большая часть логических данных системы представлена внешними интерфейсными файлами (External Interface Files, EIFs). Пример расчета количества функциональных точек, связанных с внешними файлами, представлен на рисунке 2.14.

В качестве примера была выбрана статистическая форма учета перемещения товаров в рамках Таможенного союза, предназначенная для ФТС России. В данном случае вся совокупность данных распределена в пределах двух логических групп: «Заголовок документа» и «Таблица». Первая группа включает 117 уникальных полей, а вторая - 36. То есть рассматриваемый EIF включает 2 RET и 153 DET. В соответствии с методикой, такой массив данных определяется как сложный и оценивается в 10 функциональных точек. Аналогичным образом могут быть оценены остальные группы данных.

Следующим шагом в применении методики на практике будет подсчет количества функциональных точек, связанных с операциями. Поскольку все реализуемые программой операции метод классифицирует на три типа, логичным представляется рассмотреть соответствующие каждому из них примеры.

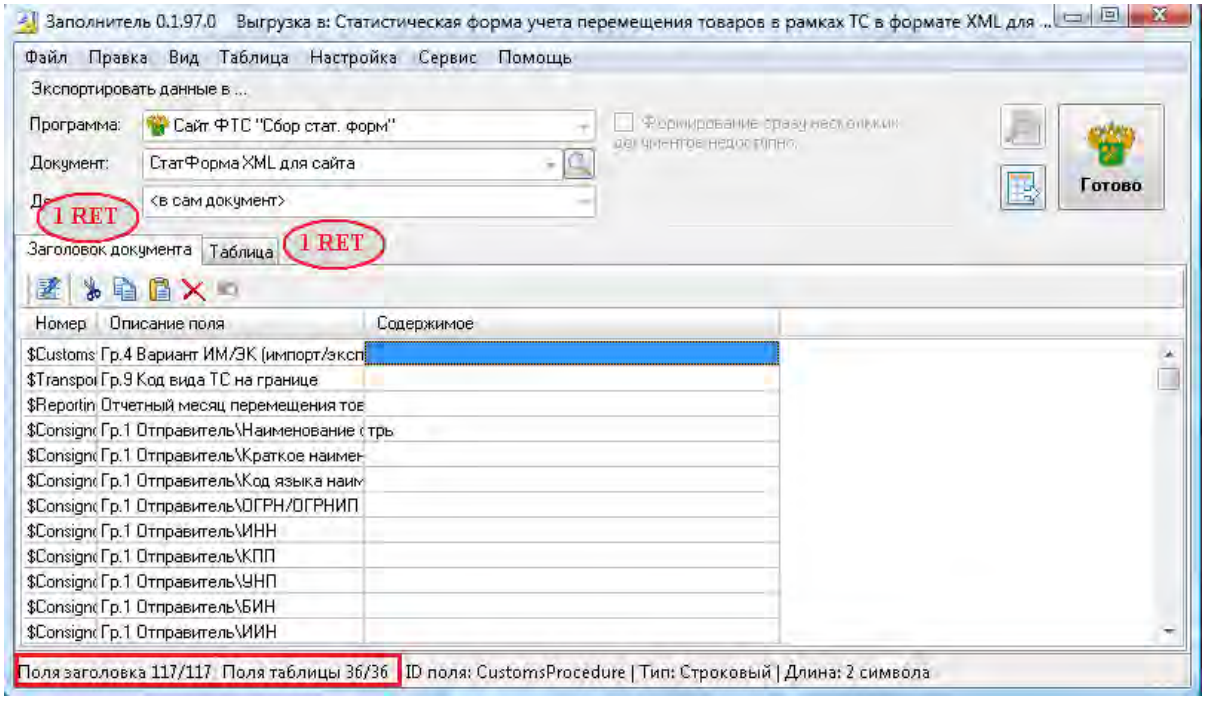

Рис. 2.14. Пример подсчета функциональных точек, связанных с внутренними логическими файлами (External Interface Files, EIF)

Пример оценки внешней входной операции (External Inputs, EI) демонстрирует рис. 2.15, на котором представлена операция по изменению оформления программного средства. Изменяемая при этом управляющая информация представляет из себя единый блок и модифицирует 1 ILF. Поэтому рассматриваемой операции соответствует 1 FTR в сочетании с 9 DET. Сложность подобной операции оценивается как средняя, которой соответствуют 4 функциональные точки.

Второй будет оценена внешняя выходная операция (External Outputs, EO) по распознаванию полей. Ее задачей является генерация информации об используемых пользователем полях. При этом осуществляется расчет частоты использования полей, то есть имеет место обработка данных.

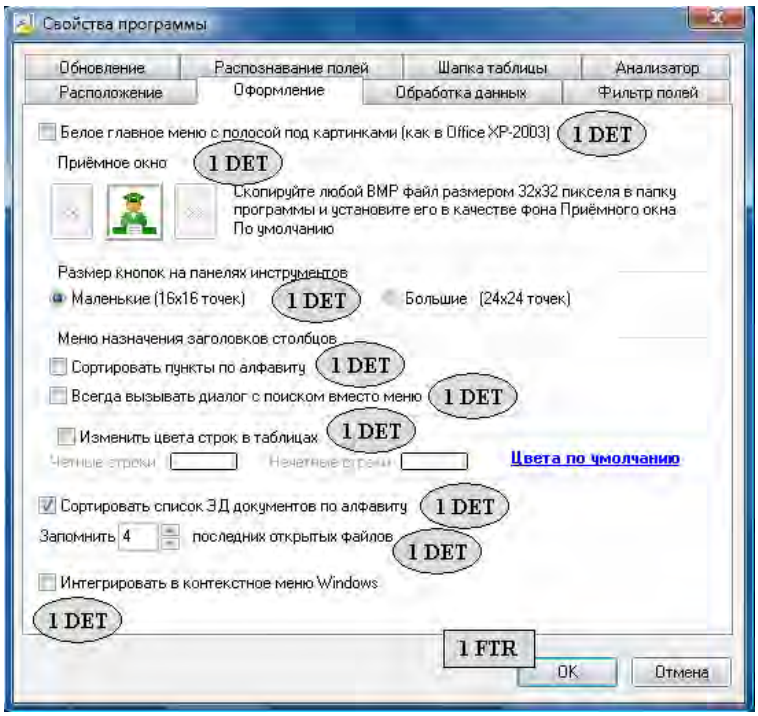

Рис. 2.15. Пример оценки сложности операции внешнего входа (External Input, EI)

Рассматриваемой операции (рис. 2.16) соответствует 1 FTR и 4 DET. Сложность данной операции оценивается как низкая, которой соответствуют 3 функциональные точки.

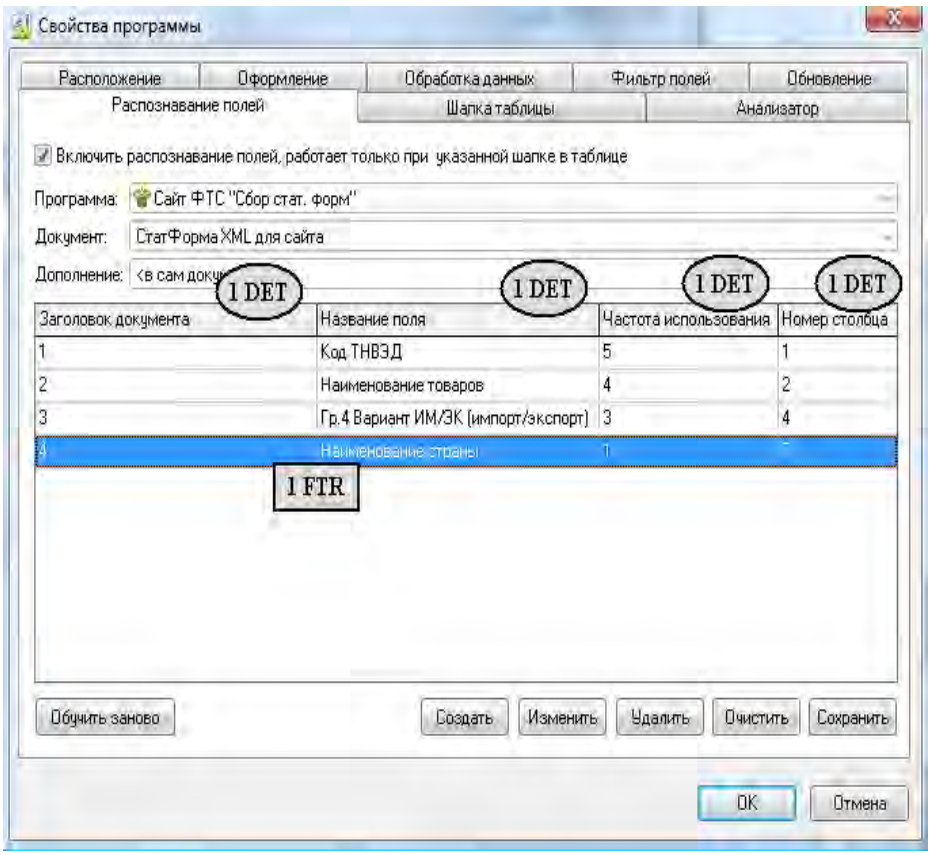

Рис. 2.16. Пример оценки сложности операции внешнего выхода (External Output, EO)

Последней рассматриваемой операцией выступает внешний запрос (External Inquiries, EQ) данных для экспорта в документ «Инвойс» программы «Альта ГТД». Пример иллюстрирует рис. 2.17.

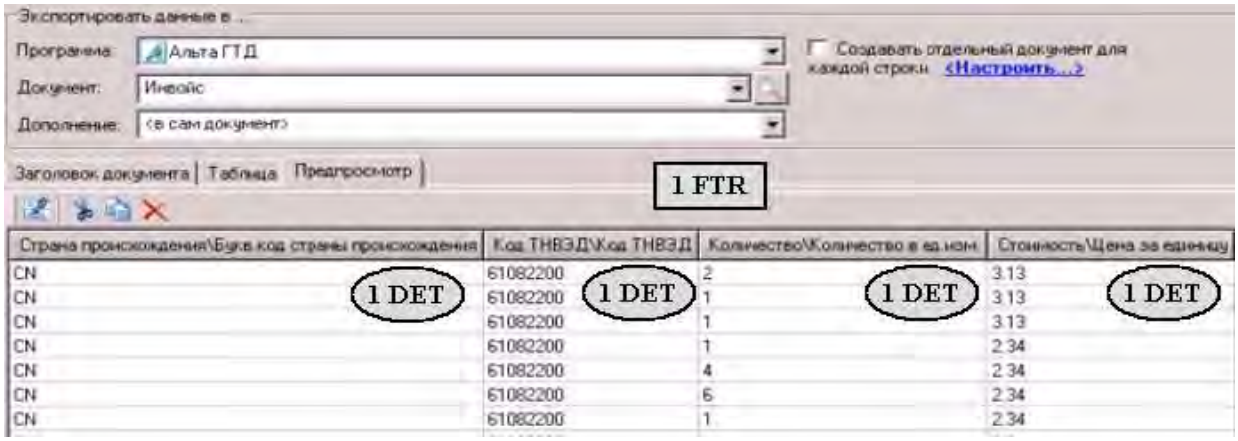

Рис 2.17. Пример оценки сложности операции внешнего запроса (External Inquiries, EQ)

Запрос оценивается в 1 FTR, 4 DET и характеризуется низкой сложностью, которой соответствуют 3 функциональные точки.

Параллельно с определением количества связанных с данными и операциями функциональных точек, должен осуществляться расчет величины корректирующего фактора (VAF). Данный показатель отражает общесистемные требования, которые ограничивают разработчиков в выборе решения и увеличивают сложность разработки. Значение фактора VAF зависит от 14 параметров (DI), которые оцениваются по шкале от 0 до 5 в зависимости от степени влияния. Их суммарный эффект (total degree of influence, TDI) определяется суммированием (формула 2.10):

$$TDI = \sum DI \qquad (2.10)$$

Расчет величины корректирующего фактора (VAF) производится по формуле 2.11:

$$VAF = (TDI * 0.01) + 0.65 \qquad (2.11)$$

Программное средство «Заполнитель документов» по своим общесистемным требованиям соответствует следующим параметрам: передача данных – 5; распределенная обработка данных – 4; производительность – 3; влияние используемой конфигурации – 0; операционная скорость – 0; ввод данных в режиме онлайн – 5; эффективность работы конечного пользователя – 3; интерактивное обновление – 3; сложность обработки – 0; многократное использование – 5; удобство установки – 5; легкость эксплуатации – 0; переносимость – 3; легкость внесения изменений – 2.

Завершающим шагом в применении методики FPA IFPUG является расчет количества скорректированных функциональных точек на основе формулы 2.12:

$$AFP = VAF * UFP = (38 * 0{,}01) + 0{,}65 = 1{,}03 * UFP \qquad (2.12)$$

Можно сделать вывод о том, что на примере программного средства «Заполнитель документов» была доказана возможность применения методики FPA IFPUG для определения его размера. Показанный на основе зарубежного и отечественного опыта потенциал, а также возможность применения на практике метода FP служит достаточно убедительным доказательством того, что приведенный ранее измененный алгоритм определения стоимости заказных ПС может быть реализован. Это обстоятельство позволяет представить усовершенствованный механизм закупок ПС для ФТС (рис. 2.18). Сравнение представленных выше усовершенствованного и функционирующего в настоящее время механизма закупок программных средств для ФТС России наглядно демонстрирует его изменение в сторону усложнения в части расчета НМЦК и в то же время приведение осуществляемых впоследствии торгов к общей форме – аукциону.

Определение стоимости разработки ПС посредством функционально – стоимостной оценки дает возможность повысить объективность рассчитываемой НМЦК, отчасти ликвидируя важнейший недостаток функционирующего в настоящее время механизма.

Рис. 2.18. Усовершенствованный механизм обеспечения ФТС России ПС

Также для заказных ПС появится возможность их приобретения не посредством конкурса, а в форме аукционов. Данный подход должен обеспечить более эффективное расходование средств федерального бюджета. Такие характерные для конкурса критерии определения победителя, как квалификация и опыт работы исполнителя, срок реализации проекта и прочие должны выступать ограничителем при допуске к торгам организаций, желающих заключить контракт с государственными органами.

Предлагаемые для внесения в механизм изменения затрагивают алгоритм расчета НМЦК не только для заказных ПС, но и поставляемого с оборудованием ПО. Изучение рынка предложений раздельных и совместных АПС с последующим выбором наименьшей из рассчитанных НМЦК позволит минимизировать издержки для федерального бюджета.

Алгоритм приобретения тиражируемых ПС остался неизменным по причине отсутствия в нем недостатков по результатам проведенного исследования. Однако необходимо отметить, что расчет НМЦК как средней арифметической обоснован лишь тогда, когда осуществляется закупка однотипного товара; в противном случае, если имеет место приобретение нескольких лотов одновременно, следует осуществлять выбор минимального ценового предложения для каждого объекта закупки.

2.3. Рекомендации по совершенствованию механизма закупок программных средств для нужд таможенных органов

2.3.1. Рекомендации по оценке условий внедрения механизма в практику

Поскольку для применения метода функциональных точек необходимы специальные знания и навыки, возникает вопрос о возможности проведения функционально-стоимостной оценки программных продуктов должностными лицами таможенных органов. Особую актуальность данному вопросу придает тот факт, что затраты на государственные закупки занимают важнейшее место в структуре расходов федерального бюджета, и неправильно рассчи-

танная цена контракта может нанести значительный ущерб экономическому состоянию страны. По этой причине необходимо привлечь специализированную исследовательскую организацию для формирования рекомендаций по внедрению функционально-стоимостной оценки в механизм закупок ПС для ФТС России.

Результатом работы данной научно-исследовательской организации должен быть Отчет о научно-исследовательской работе, содержащий логически обоснованную последовательность практических рекомендаций по внедрению функционально-стоимостной оценки разрабатываемых для таможенных органов программных продуктов.

Представленная далее схема (рис. 2.19) отображает наиболее важные этапы внедрения усовершенствованного механизма закупок ПС в практику деятельности таможенных органов России. При этом основными подразделениями таможенных органов, в компетенции которых будет реализация этих рекомендаций, являются Главное Управление информационных технологий (ГУИТ) и Центральное информационно-техническое таможенное управление (ЦИТТУ). Как видно из схемы, всю последовательность действий, связанную с совершенствованием механизма закупок ПС, можно укрупнено представить в виде следующих этапов: подготовительного, основного и завершающего.

В рамках подготовительного этапа должны быть определены наиболее эффективные способы осуществления дальнейших действий по внедрению метода функционально-стоимостной оценки в механизм закупок программных продуктов для ФТС России.

Как уже отмечалось ранее, объективной потребностью таможенных органов на данном этапе выступает обращение к специализированной исследовательской организации, способной провести НИР по данному направлению. В настоящее время экономические и юридические вопросы информатизации таможенных органов, снабжения их информационными и программными продуктами, а также средствами защиты активно изучаются сотрудниками Научно-исследовательского института Российской таможенной академии.

Рис. 2.19. Совокупность действий по внедрению усовершенствованного механизма обеспечения ФТС России ПС

Так как подготовительный этап является определяющим для всего дальнейшего процесса, его подробная проработка играет важнейшую роль в том, насколько успешно будут реализованы мероприятия по совершенствованию механизма закупок ПС для ФТС России. В связи с этим представляется необходимым определение вопросов, которые впоследствии будут изучены исследовательской организацией.

При этом при формулировании этих вопросов должны учитываться обстоятельства, которые могут оказать воздействие на процесс реализации предлагаемых практических рекомендаций.

Во-первых, необходимо учитывать тот факт, что в рамках метода функциональных точек существует множество его вариаций, различающихся методикой расчетов и, соответственно, сложностью применения.

Во-вторых, деятельность Федеральной таможенной службы характеризуется спецификой по сравнению с другими органами государственной власти и, тем более, коммерческими организациями. Очевидно, что данное обстоятельство находит свое отражение в трудоемкости разработки программных продуктов.

В-третьих, внедрение функционально-стоимостной оценки потребует затрат средств федерального бюджета и может повлечь за собой такие экономические последствия, как, например, значительное изменение цен контрактов на закупаемые для таможенных органов программные продукты.

Исходя из вышеперечисленного, можно сделать вывод о том, что исследовательская организация должна в своей работе осуществить следующие действия:

выбрать из разработанных в настоящее время вариаций метода функциональных точек такую, которая в наибольшей степени соответствует потребностям и возможностям ФТС России в расчете НМЦК на закупаемые ПС;

оценить применимость выбранной ранее вариации метода функциональных точек в отношении программных продуктов, закупаемых таможенными органами;

оценить целесообразность внедрения функционально-стоимостной оценки в практику закупок ПС для ФТС России (на основе расчета затрат и экономического эффекта от внедрения метода);

сформировать практические рекомендации по совершенствованию механизма закупок ПС для Федеральной таможенной службы.

На основании полученных рекомендаций должен осуществляться следующий, основной этап внедрения функционально-стоимостной оценки. При этом основной задачей таможенных органов будет получение данных о стоимости одной функциональной точки программного продукта для всех направлений деятельности ФТС России. Для достижения поставленной задачи необходимо осуществить следующую последовательность действий:

определить количество направлений деятельности таможенных органов (ранее в настоящем исследовании было выделено семь направлений деятельности, в которых могут применяться купленные для ФТС России программные средства);

для каждого направления выбрать определенное количество ПС, которые позднее будут подлежать экономической оценке (предлагается отобрать по три ПС для каждого направления);

обратиться к организации, способной оценить стоимость данных программных средств;

определить размер этих ПС в функциональных точках и строках кода силами;

посредством простейших математических операций рассчитать, сколько строк кода соответствует одной функциональной точке для каждого направления, а также определить стоимость ее создания.

Таким образом, первоочередными задачами в рамках данного этапа являются определение стоимости и измерение посредством метода функцио-

нальных точек программных средств из разных направлений деятельности таможенных органов.

Как уже отмечалось ранее, для применения метода функциональных точек необходимы специальные знания, и в настоящее время найти в России специалистов, на профессиональной основе занимающихся измерением программных продуктов этим методом, довольно проблематично. Можно назвать три подхода к решению данной проблемы:

создание экспертного центра на уровне государства, целью которого будет измерение методом функциональных точек всех программных продуктов, разрабатываемых по заказу органов государственной власти;

обучение кадров методу функциональных точек каждым органом государственной власти (в том числе и Федеральной таможенной службой) самостоятельно;

привлечение для проведения оценки независимой организации.

Перечисленные подходы имеют преимущества и недостатки, которые более подробно рассмотрены далее (табл. 2.10).

Создание экспертного центра на государственном уровне, равно как и обучение должностных лиц, потребует наличия профессионалов в штате организации. Подготовить кадры в настоящее время затруднительно, поскольку метод функциональных точек еще не приобрел значительного уровня распространения в России, но возможно. Существуют специализированные организации, обучающие методике FPA IFPUG, хотя их количество на данный момент невелико.

Создание экспертного центра характеризуется значительными преимуществами, среди которых следует отметить общий подход к оценке ПС для всех органов государственной власти. То есть будет исключена возможность неоднозначного толкования заложенных в методике принципов, а программы разных ОГВ можно будет сравнивать как по сложности разработки, так и по стоимости. Помимо этого, обеспечение функционирования одного

подразделения в рамках государства будет обходиться дешевле, чем обучение специалистов каждым ОГВ по отдельности.

Таблица 2.10

Сравнение подходов к привлечению квалифицированных оценщиков

	Создание Экспертного центра	Обучение должностных лиц	Привлечение независимой организации
Требования	квалифицированные эксперты в штате организации		способы оценки квалификации экспертов
Преимущества	общий подход к определению НМЦК на закупаемые ПС для всех ОГВ; обеспечение одного подразделения дешевле, чем создание независимых в каждом ОГВ	больший учет специфики деятельности ОГВ; более тесное взаимодействие с подразделениями ОГВ	снижение затрат за счет отсутствия необходимости содержать штат оценщиков;
Недостатки	большой объем работ; неполный учет специфики деятельности ОГВ; затрудненное взаимодействие с подразделениями ОГВ	суммарные расходы на содержание экспертов во всех ОГВ больше чем затраты на обеспечение работы Экспертного центра	в настоящее время трудно найти квалифицированных экспертов; крупные расходы в случае большого объема работ

Рассматриваемый подход обладает и недостатками, важнейшим из которых является большой объем работ, который будет необходимо выполнить оценщикам. Это может привести к увеличению штата и снижению эффекта экономии денежных средств для федерального бюджета. Также, будет затруднено взаимодействие с заинтересованными в закупке ПС подразделениями ОГВ. Данное обстоятельство может привести к недостаточно подробной детализации технического задания и, следовательно, снижению точности оценки при заказе ПС.

Обучение должностных лиц в отдельном ОГВ обладает преимуществами и недостатками, противоположными ранее рассмотренным. Достоинствами подхода являются больший учет специфики деятельности ОГВ и более тесное взаимодействие с подразделениями, заинтересованными в закупке ПС. В то же время, затраты на содержание штата профессионалов будут

иметь постоянный характер, а в случае внедрения метода во все ОГВ приведет к росту затрат для федерального бюджета, суммарно большему, чем для обеспечения функционирования Экспертного центра.

Привлечение независимых экспертов для осуществления оценки стоимости ПС снижает затраты для федерального бюджета, поскольку в данном случае они не носят постоянного характера. Однако данное преимущество исчезает в случае большого объема запланированной работы. При этом особую важность приобретает вопрос обеспечения уровня квалификации оценщика. Чтобы его проверить, необходимо разработать методику, позволяющую определить профессионализм оценщика. Также нельзя забывать о том, что найти специалиста, способного на профессиональной основе измерять программные средства методом функциональных точек, в настоящее время непросто. По этим причинам наиболее перспективными выглядят первые два описанных подхода привлечения оценщиков.

Очевидно, что с позиции экономии средств федерального бюджета в долгосрочной перспективе преимуществами обладает подход, заключающийся в создании общего для всех органов государственной власти экспертного центра. Однако проведение настолько значимых изменений в механизме государственных закупок без подготовки может повлечь за собой неблагоприятные последствия. Поэтому более рациональным видится внедрение метода функционально – стоимостной оценки в практику закупок программных продуктов на примере отдельного органа государственной власти, в качестве которого может быть принята Федеральная таможенная служба. После чего, в случае успешного проведения данного эксперимента, предстоит создание экспертного центра по определению цен контрактов на закупаемые программные средства для всей системы государственных органов.

Следовательно, определение размера программных средств таможенных органов в функциональных точках и строках кода должно осуществляться должностными лицами таможенных органов самостоятельно. В связи с этим необходимым действием со стороны таможенных органов является ор-

ганизация обучения сотрудников ФТС России методу функциональных точек.

Также будет необходимо организовать торги для экономической оценки программных средств, используемых в деятельности Федеральной таможенной службы, с целью определения их стоимости.

Исходя из всего вышесказанного, второй этап внедрения функционально – стоимостной оценки в практику закупок программных средств для таможенных органов можно условно разделить на два подэтапа. В рамках первого из них будет осуществляться оценка программных средств, применяемых в разных направлениях деятельности таможенных органов, и проводиться обучение кадров ЦА ФТС России методу функциональных точек. Как отмечают эксперты,, «затраты на информационные технологии требуются постоянные и в больших объемах, но если использовать их возможности не полностью, не подготовить персонал к работе с внедряемыми технологиями, то все вложения будут напрасны»[24]. Суть второго подэтапа заключается в том, что получившие необходимые знания и навыки должностные лица таможенных органов начнут самостоятельно проводить функционально-стоимостную оценку программных продуктов, применяемых в деятельности ФТС России.

Заключительным этапом выступает применение метода в отношении программных средств, запланированных к закупке для таможенных органов.

2.3.2. Рекомендации по организации взаимодействия подразделений таможенных органов

Внедрение функционально-стоимостной оценки в практику закупок программных средств для таможенных органов может привести к необходимости внесения изменений в организационную структуру и систему информационного взаимодействия подразделений Центрального аппарата ФТС

[24] Никитченко И.И., Павлюченков К.А., Соколов С.М. Оценка эффективности внедрения информационных технологий – приоритетная задача оптимизации деятельности таможенных органов Российской Федерации. Актуальные проблемы теории и практики таможенного дела и пути их решения: сборник материалов Международной научно – практической конференции: в 2 ч. Ч. 2. М.: Изд-во Российской таможенной академии, 2010. – С. 111.

России (далее – ЦА ФТС России). Для того чтобы оценить масштаб этих изменений, следует определить, какие подразделения будут ответственны за реализацию представленных ранее практических рекомендаций, а также обеспечение последующего функционирования усовершенствованного механизма.

По состоянию на 01.04.2014 года ЦА ФТС России включает в себя двадцать одно структурное подразделение, в том числе:

восемь Главных управлений (организационно-инспекторское, информационных технологий, организации таможенного оформления и таможенного контроля, по борьбе с контрабандой, тылового обеспечения, федеральных таможенных доходов и тарифного регулирования, финансово-экономическое, таможенного контроля после выпуска товаров);

тринадцать Управлений (таможенных расследований и дознания; правовое; торговых ограничений, валютного и экспортного контроля; управление делами; государственной службы и кадров; по связям с общественностью; по противодействию коррупции; таможенного сотрудничества; таможенной статистики и анализа; контрольно-ревизионное; товарной номенклатуры; аналитическое; рисков и оперативного контроля).

В настоящее время подразделения ЦА ФТС России образуют сложную систему, охватывающую самые разные направления деятельности таможенных органов. Те из них, которые примут непосредственное участие в совершенствовании механизма закупок программных средств для ФТС России, можно разделить на две группы:

непосредственные участники (подразделения, для которых данное направление является приоритетным в силу возложенных на них функций и поставленных задач);

обеспечивающие подразделения (подразделения, в силу специфики своей деятельности не участвующие в совершенствовании механизма, но необходимые для обеспечения его функционирования).

К группе непосредственных участников из всей структуры ЦА ФТС России может быть отнесено:

Главное управление информационных технологий (далее – ГУИТ). В соответствии с приказом ФТС России от 17.01.2007 г.[25] данное подразделение реализует комплекс самых разнообразных задач в сфере развития информационных технологий таможенных органов, планируя их оснащение средствами информатизации и внедрение результатов НИОКР;

Центральное информационно-техническое таможенное управление (далее – ЦИТТУ), специализированное подразделение ФТС России, деятельность которого направлена на осуществление информационного обеспечения и программно-технической поддержки эксплуатации компонентов автоматизированных систем на всех уровнях таможенных органов.

В качестве обеспечивающих подразделений ЦА ФТС России могут быть выделены такие, как Главное финансово-экономическое управление (ГФЭУ) и Управление государственной службы и кадров (УГСиК).

ГФЭУ осуществляет функции главного распорядителя и получателя средств федерального бюджета. Поэтому в части экономического обеспечения внедрения усовершенствованного механизма закупок ПС для ФТС России данное подразделение будет играть важную роль.

УГСиК занимается вопросами профессиональной подготовки должностных лиц таможенных органов. Поэтому реализация второго этапа внедрения практических рекомендаций должна проходить с участием данного подразделения.

Данные управления характеризуются разной степенью участия в реализации предложенных ранее практических рекомендаций. Отобразить ее можно с помощью рисунка (рис. 2.20)

Регламенты подразделений ЦА ФТС России, представленные на его официальном сайте, дают возможность разграничить обязанности по реали-

[25] Приказ ФТС России от 17.01.2007 № 55 «Об утверждении Положения о Главном управлении информационных технологий». М.: consultant.ru, 2014. Режим доступа: World Wide Web. URL: http://www.consultant.ru

зации практических рекомендаций, разработанных с целью внедрения усовершенствованного механизма закупки ПС.

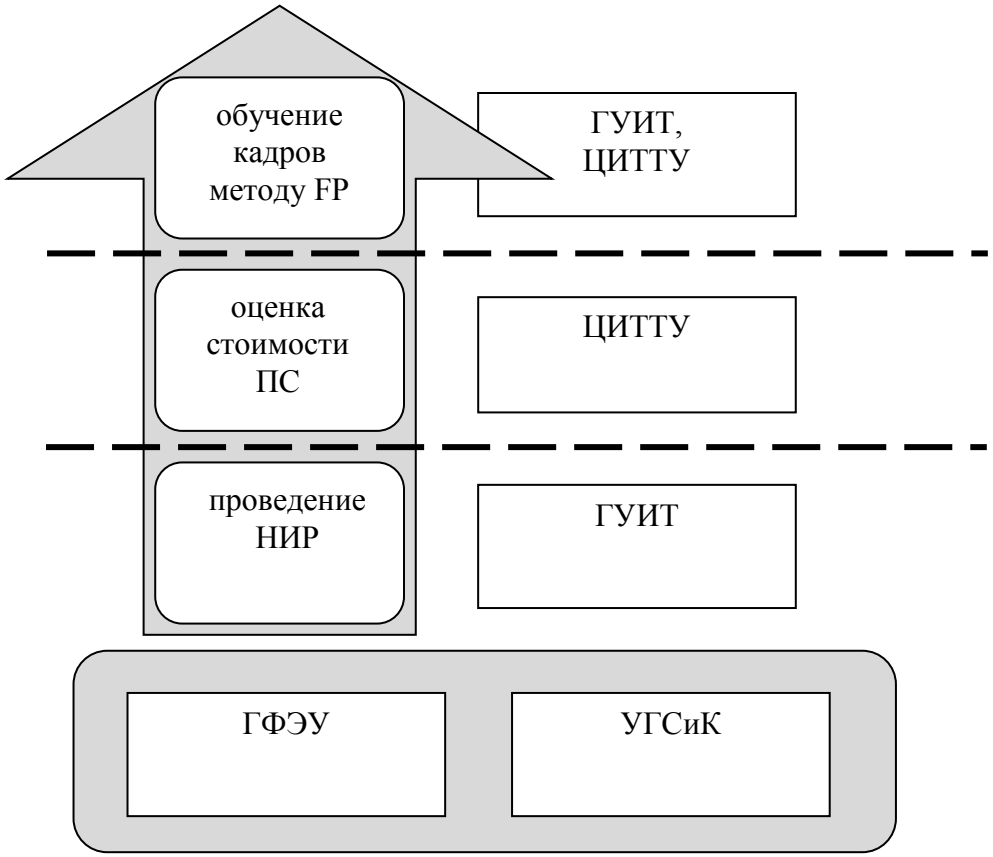

Рис. 2.20. Распределение обязанностей подразделений ЦА ФТС России по реализации практических рекомендаций по внедрению усовершенствованного механизма закупки ПС

Непосредственными задачами ГУИТ являются научно-техническое развитие таможенных органов и осуществление мер по оптимизации расходов и обеспечению эффективного использования средств, выделяемых на содержание и развитие таможенных органов, в части затрат на приобретение информационно-технических средств. В соответствии с регламентом, управление выполняет функции генерального заказчика научно-исследовательских и опытно-конструкторских работ (далее – НИОКР), а также организует обоснование, планирование, контроль выполнения и внедрения полученных результатов. Исходя из поставленных задач и определенных функций, реализация первого этапа внедрения усовершенствованного механизма закупки ПС, проведение НИР, входит в компетенцию ГУИТ.

Следующий этап, оценка стоимости ПС, должен быть выполнен ЦИТТУ. Данное подразделение ЦА ФТС России размещает государственные заказы и заключает государственные контракты на поставку товаров, выполнение работ, оказание услуг в пределах доведенных бюджетных ассигнований и лимитов бюджетных обязательств в соответствии с российским законодательством. Учитывая тот факт, что рассмотренную ранее государственную закупку на оценку балансовой стоимости применяемых в деятельности таможенных органов ПС организовало ЦИТТУ, логичным представляется реализация второго этапа данным подразделением.

Обучение должностных лиц таможенных органов по вопросам, связанным с информационными системами и технологиями входит в компетенцию ГУИТ. Однако нельзя не учитывать того, что обучению методу функциональных точек требует наличия специальных знаний у обучаемых. В то же время технические знания и практический опыт в части внедрения, модернизации и сопровождения информационно-программных средств в большей степени характерен для сотрудников ЦИТТУ, в то время как ГУИТ решает задачи, связанные с экономическим обеспечением информатизации деятельности таможенных органов. Данное обстоятельство дает возможность предложить распределить контингент обучающихся методу функциональных точек на две группы. Одна из них, численностью три человека, будет представлена должностными лицами со стороны ЦИТТУ; другая, состоящая из двух человек – соответственно, со стороны ГУИТ. Реализация данного предложения может повысить объективность и независимость проводимых ими впоследствии оценок.

Реализация мер по организационному взаимодействию подразделений ЦА ФТС России позволит внедрить функционально – стоимостную оценку в механизм закупок ПС для таможенных органов. Однако для обеспечения его функционирования необходимо организовать обучение должностных лиц ФТС России методу FP внутри подразделений ЦА ФТС России. Формирова-

ние кадрового резерва является в данном случае несомненно важным условием обеспечения функционирования усовершенствованного механизма.

Организация обучения внутри подразделений ЦА ФТС России позволит обеспечить им независимость от обучающих организаций, что сократит расходы, и передавать опыт по оценке применяемых в сфере деятельности именно таможенных органов программных средств.

Логичным шагом было бы возложение обязанности по проведению по результатам обучения квалификационного экзамена на УГСиК. Данное подразделение обособленно от обучающихся и в его функции входит подготовка кадрового резерва.

Определение условий внедрения функционально - стоимостной оценки в практику деятельности таможенных органов в сочетании с проработкой организационного взаимодействия с целью обеспечения функционирования усовершенствованного механизма позволяет перейти к экономической оценке затрат на реализацию разработанных ранее практических рекомендаций.

2.3.3. Экономическая оценка затрат на внедрение усовершенствованного механизма

Реализация практических рекомендаций по внедрению функционально–стоимостной оценки потребует затрат со стороны ФТС России. Их расчет позволит обосновать расход денежных средств из федерального бюджета, а также посредством соотнесения суммы затрат и получаемых выгод принять положительное или отрицательное решение по применению метода FP при оценке стоимости заказного ПС. В рамках данного исследования ставится задача составить прогноз затрат, а также подготовить математический аппарат для их последующего более подробного расчета.

Вся совокупность затрат, которые понесут таможенные органы, связана с тремя необходимыми для внедрения метода действиями:

заказ проведения научно-исследовательской работы;

заказ услуг по определению стоимости ранее купленных таможенными органами программных продуктов;

обучение должностных лиц Центрального аппарата ФТС России.

Для определения стоимости проведения научно-исследовательской работы необходимо найти информацию по ранее заключенным контрактам на аналогичные исследования. При этом существенными условиями, определяющими критерии выбора аналогичных исследований, являются сложность научно-исследовательской работы (которую можно определить, изучив содержание Отчета о НИР) и уровень заказа (для федерального органа исполнительной власти). После отбора нескольких подобных работ рассчитать среднюю арифметическую, которая и будет являться прогнозируемой ценой контракта.

Применение метода невозможно без данных о стоимости разработки одной функциональной точки ранее приобретенного ПС. Стоимость имеющихся в распоряжении таможенных органов ПС определялась различными поставщиками, зачастую поставляемый продукт не имел самостоятельного характера, приобретался в комплекте с прочими товарами либо представлял собой не более чем обновление уже установленной программы. По этой причине необходима оценка стоимости нескольких ПС одним исполнителем. В данном случае определить общие расходы можно, умножив затраты на оценку одной программы на их количество.

Расходы на обучение лиц Центрального аппарата до уровня, позволяющего им использовать метод функциональных точек при определении начальной (максимальной) цены контракта (НМЦК), определяются произведением числа направляемых на обучение человек на стоимость обучения одного человека.

То есть суммарные затраты на внедрение функционально-стоимостной оценки в механизм закупок ПС для ФТС России можно определить по следующей формуле (2.12):

$$C = \frac{r_1 + r_2 + \cdots + r_n}{n} + p * s * e + q * t, \qquad (2.12)$$

где C – суммарные затраты на внедрение функционально стоимостной оценки в механизм закупок ПС для ФТС России (cost, руб.);

r – цена контракта на проведение научно-исследовательской работы, сопоставимой по уровню сложности с описанной в данном исследовании ранее (research, руб.);

n – количество учтенных научно-исследовательских работ (number, работ);

p – количество программных средств, которое необходимо оценить для одной направления применения (program, программ);

s – число направлений применения ПС, для которых различается стоимость одной функциональной точки (sphere, сфер);

e – расходы на определение стоимости одного ПС (expense, руб.);

q – количество человек, которые пройдут обучение методу функциональных точек (qualification, человек);

t – стоимость обучения методу функциональных точек одного человека (training, руб.).

Поскольку для обеспечения эффективности деятельности государственным органам особенно важно внедрение современных достижений науки, среди государственных закупок значительную долю составляют затраты на приобретение средств информатизации деятельности. Вследствие этого на официальном сайте госзакупок представлена значительная база данных по заказам на выполнение НИР.

Следует отметить, что ценовой диапазон на выполняемые по заказу государственных органов НИР по состоянию на 01.04.2014 очень широк: от 88060,28 руб. (закупка № 31300460296, анализ устаревших нормативных документов), до 1163200000,00 руб. (закупка № 0173100009511000016, разработка и экспериментальное исследование прорывных решений для двигателей самолетов и вертолетов).

Очевидно, что стоимость контрактов на выполнение данных НИР напрямую зависит от экономического эффекта от полученных результатов. Однако рассчитать его в настоящее время не представляется возможным в большинстве случаев по причине недостаточной развитости научно-методического аппарата.

Тем не менее, на основе изучения данных по госзакупкам уже сейчас можно сделать некоторые выводы. Так, стоимость контракта зависит от сферы деятельности, в которой планируется применение ее результатов. Выполнение НИР, результаты которой используют в сфере экологии или истории, стоит дешевле, чем аналогичная работа в области, например, авиастроения. Подобный подход позволяет, пусть и приближенно, определить ценовой диапазон закупок. После чего, убрав наибольшие и наименьшие значения, появляется возможность определить приблизительную стоимость контракта, отобрав наиболее соответствующие научно-исследовательской работе контракты и рассчитав на их основе среднюю арифметическую.

В случае с заказом НИР, посвященной анализу возможности внедрения метода функциональных точек в механизм закупок ПС для ФТС России, сферой применения результатов является экономика и управление. В соответствии с представленными ранее аргументами были выбраны НИР, сведения о которых представлены далее (табл. 2.11).

Таблица 2.11

Сведения о НИР, использованных для экономической оценки затрат

№ п/п	№ заказа	Наименование	Дата публикования	НМЦК, руб.
1	31300619766	Выполнение НИР «Совершенствование методики для расчетов балансовой надежности ЕЭС России»	21.10.2013	2006000,00
2	0173100009512000351	Выполнение НИР «Комплексный анализ реализации программ инновационного развития и технологических платформ, находящихся в сфере ведения Минпромторга России, а также разработка предложений по их учету в реализации государственной программы «Развитие промышленности и повышение ее конкурентоспособности»»	29.12.2012	3000000,00

№ п/п	№ заказа	Наименование	Дата публикования	НМЦК, руб.
3	31300499023	Выполнение НИР «Подготовка методических рекомендаций по разработке разделов плана объектов транспортной инфраструктуры метрополитена»	16.08.2013	2063018,17
4	0173100009512000097	Выполнение НИР «Разработка методологии организации и проведения независимой экспертизы хода выполнения и результатов НИОКР»	23.03.2012	4625000,00
5	0195100000313000014	Выполнение НИР по теме: «Совершенствование методики оценки эффективности использования иностранной рабочей силы»	31.01.2013	1400000,00

Направления применения ПС в деятельности таможенных органов были определены ранее: регулирующая, экономическая, управленческая, хозяйственная, статистическая, кадровая, координирующая. Несомненно, впоследствии их число будет уточнено по мере дальнейшего исследования в данном направлении, но в настоящее время оно равно семи.

Для каждого направления применения необходимо определить количество ПС, стоимость которых будет оценена. Реализация данного действия даст возможность получить начальную стоимость одной функциональной точки с учетом разного приоритета и сложности реализации ранее закупленных ПС. Предлагается установить в качестве оптимального количества подлежащих оценке ПС по три для каждого направления применения.

Стоимость оценки одного ПС можно определить на основе изучения представленной на официальном сайте госзакупок информации о запросе котировок на «Оказание услуг по проведению оценки балансовой стоимости объектов интеллектуальной собственности (программа для ЭВМ), из состава информационно-расчетной системы контроля таможенных платежей» от 30.10.2013 № 0173100015213000047 по заказу ЦИТТУ. В качестве НМЦК для данных торгов была установлена сумма 500000 руб., при этом осуществлялась оценка стоимости восьми объектов интеллектуальной собственности из состава информационно-расчетной системы контроля таможенных платежей (ИРС «Доход»): АПС «Задолженность», КПС «Обмен данными», КПС

«Имущество», АПС «Штрафы», КПС «Применение льгот», АПС «Платежи-Анализ», АПС «Лицевые счета», АПС «Платежи-Модель».

В соответствии с требованиями заказчика победитель контракта оказывал ему следующие услуги:

1) проведение анализа исходных документов, имеющихся у государственного заказчика по объектам интеллектуальной собственности;

2) оценка балансовой стоимости объектов интеллектуальной собственности;

3) подготовка Отчета об оценке каждого объекта интеллектуальной собственности;

4) выдача Сертификата на каждый объект интеллектуальной собственности.

Представленные сведения позволяют рассчитать расходы на оценку стоимости одного ПС, поскольку алгоритм действий исполнителя, а также сущность оказываемых услуг идентичны предусмотренным в документации.

Так как имеются все сведения, необходимые для прогноза затрат на оплату услуг по оценке стоимости ранее приобретенных ПС, следующим шагом выступает определение расходов на обучение должностных лиц Центрального аппарата ФТС России.

Метод функциональных точек в настоящее время недостаточно широко применяется в деятельности российских разработчиков ПС, и поэтому организаций, обучающих его применению, немного. В качестве примера можно привести компанию Tekama, разрабатывающую учебные программы и проводящую тренинги по обучению различным способам оценки ПС[26].

Основной целевой аудиторией выступают руководители проектов, команд разработчиков, функциональных отделов, а также специалистов, которым необходимо проводить оценки проектных работ. Важнейшим требованием, предъявляемым к участникам тренинга, является понимание процесса

[26] Академия Cisco при ЯрГУ им. П.Г. Демидова. Режим доступа: World Wide Web. URL: http://www.cisco.yar.ru/links/Tekama.php

разработки ПС. То есть направляемые на обучение должностные лица таможенных органов должны обладать необходимыми знаниями.

Компания заявляет, что по завершении тренинга его участники приобретут знания и навыки применения метода функциональных точек.

При этом продолжительность обучения составляет 16 часов, а стоимость равна 8700 руб. с учетом НДС[27]. Также предоставляется скидка в размере 7% при единовременном обучении пяти человек.

Документом, удостоверяющим прохождение обучения, является сертификат TEKAMA, выдаваемый участникам после успешного прохождения проверки полученных знаний по завершении тренинга.

Чтобы определить количество человек, которых необходимо направить на обучение, обратимся к Федеральному закону «О контрактной системе» №44-ФЗ. В соответствии с данным нормативно-правовым актом, число членов аукционной или конкурсной комиссии должно быть не менее пяти человек. В сочетании с фактом того, что на данное количество человек обучающей организацией выдается скидка, примем его за оптимальное.

Затраты на реализацию данных рекомендаций представлена в табл. 2.12.

Соотношение долей затрат на реализацию предварительных действий по внедрению функционально-стоимостной оценки в механизм обеспечения ФТС России ПС представлено на рис. 2.21.

Диаграмма отображает, что большую часть расходов потребует проведение НИР, поскольку тщательная проработка последующих мероприятий позволит избежать необоснованных затрат федерального бюджета и просто необходима.

[27] Стоимость дана на июнь 2014 г.

Таблица 2.12

Экономическая оценка затрат на реализацию практических рекомендаций

<table>
<tr><th>№ п/п</th><th>Цель затрат</th><th>Формулы для расчета затрат</th><th colspan="4">Данные для расчетов</th><th>Затраты, руб.</th></tr>
<tr><td rowspan="7">11</td><td rowspan="7">Выполнение научно-исследовательской работы (C_1)</td><td rowspan="7">$C_1 = \frac{r_1 + r_2 + \cdots + r_n}{n}$,
где C_1 – суммарные затраты на выполнение научно-исследовательской работы (руб.);
r – цена контракта на проведение научно-исследовательской работы, сопоставимой по уровню сложности с описанной в данном исследовании ранее (руб.);
n – количество учтенных научно-исследовательских работ (работ).</td><td>№ контракта, i</td><td colspan="2">Цена контракта, руб.</td><td>Дата опубликования</td><td rowspan="7">2618803,6</td></tr>
<tr><td>r_1</td><td colspan="2">3000000</td><td>29.12.2012</td></tr>
<tr><td>r_2</td><td colspan="2">2006000</td><td>21.10.2013</td></tr>
<tr><td>r_3</td><td colspan="2">1400000</td><td>31.01.2013</td></tr>
<tr><td>r_4</td><td colspan="2">2063018,17</td><td>16.08.2013</td></tr>
<tr><td>r_5</td><td colspan="2">4625000</td><td>23.03.2012</td></tr>
<tr><td colspan="4">n = 5 шт.</td></tr>
<tr><td rowspan="2">22</td><td rowspan="2">Определение стоимости ранее купленных ПС (C_2)</td><td rowspan="2">$C_2 = p * s * e$,
где C_2 – суммарные затраты на определение стоимости ранее купленных для ФТС России программных средств (руб.);
p – количество программных средств, которое необходимо оценить для одной сферы применения (программ);
s – число сфер применения ПС, для которых различается стоимость единицы размера проекта, одной функциональной точки (sphere, сфер);
e – расходы на определение стоимости одного ПС (руб.).</td><td>Количество ПС, ед.</td><td>Число сфер внедрения, ед.</td><td>Расходы, руб.</td><td rowspan="2">1312500</td></tr>
<tr><td>3</td><td>7</td><td>62500</td></tr>
<tr><td rowspan="2">33</td><td rowspan="2">Обучение должностных лиц таможенных органов (C_3)</td><td rowspan="2">$C_3 = q * t$,
где C_3 – суммарные затраты на обучение должностных лиц таможенных органов (руб.);
q – количество человек, которые пройдут обучение способу оценки размера ПС методом функциональных точек (человек);
t – стоимость обучения методу функциональных точек одного человека (руб.).</td><td colspan="2">Количество обучаемых, чел.</td><td>Стоимость обучения, руб.</td><td rowspan="2">43500</td></tr>
<tr><td colspan="2">5</td><td>8700</td></tr>
<tr><td colspan="7">СУММА ЗАТРАТ ($C_1 + C_2 + C_3$):</td><td>3974803,6</td></tr>
</table>

Доля затрат на оценку стоимости ПС может значительно снизиться в результате торгов, так как исполнитель будет обязан выполнять однотипные повторяющиеся действия и, соответственно, нести меньшие расходы в среднем на оценку стоимости одного ПС, чем если бы объектом заказа выступал один ПС.

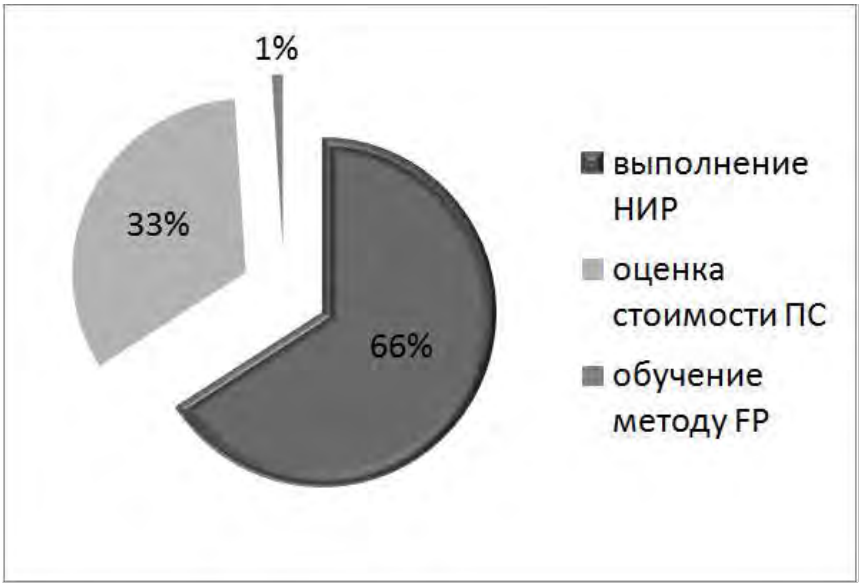

Рис. 2.21. Структура затрат на реализацию рекомендация по внедрению функционально-стоимостной оценки в механизм закупок ПС для ФТС России

Обучение должностных лиц потребует наименьших расходов в общей структуре затрат, однако обязательным условием успешной реализации данного процесса является наличие у обучаемых специальных знаний, навыков и умений.

Глава 3. Оптимизация затрат на защиту информации таможенных органов

3.1. Общая характеристика и анализ проблемы защиты информации в распределенных автоматизированных информационных системах таможенных органов

3.1.1. Роль информации в экономике современного общества

В современном обществе повсеместно внедряются наукоемкие и информационно-ёмкие технологии. Происходит бурный рост индустрии знаний, в которую перемещается все больше и больше людей и ресурсов. Под влиянием увеличивающегося потока информации в сфере образования, области научных исследований, технических разработок, сфере телекоммуникаций и компьютерной деятельности, средствах массовой информации, книгопечатании производится более половины национального продукта высокоразвитых стран.

Информацию наряду с веществом и энергией рассматривают в качестве важнейшей сущности мира, в котором мы живем. Однако, если задаться целью формально определить понятие «информация», то сделать это будет чрезвычайно сложно. Считается, что «информация» (от латинского «information» – ознакомление, разъяснение, понятие) является одним из основных исходных, фундаментальных понятий в современной науке и поэтому не может быть строго определено через элементарные понятия. Можно лишь обращаться к различным аспектам этого понятия, пояснять и иллюстрировать его смысл, различая научное понятие информации и обыденное представление о получении сведений.

Развитие техники связи остро поставило задачу измерения количества передаваемой информации. Ее решение выдвинуло более широкую концепцию информации как снимаемой, уменьшаемой неопределенности в результате получения сообщения. Такое понимание информации представ-

лялось сначала очень общим, даже фундаментальным, чему способствовала общность математического аппарата количественной теории информации и термодинамики.[28]

Однако в дальнейшем, особенно в связи с развитием кибернетики, ЭВМ, с широким распространением информационного подхода в науке, на первый план стали выходить семантические (смысл), прагматические (использование) стороны информации, т.е. ее зависимость от особенностей получателя. Действительно, информация на чужом языке (или непредусмотренном коде) не снимает неопределенности, но информацией является. Далее, рост информированности человека в соответствии с данной концепцией должен однозначно вести к увеличению определенности его решений и мнений. Однако в жизни наблюдается и обратное. Ограниченные люди высказывают очень определенные суждения, а информированные, глубокие видят массу неясностей в казалось бы, простом вопросе. Стало ясно, что важнейшие характеристики информации, трактуемой как снимаемая неопределенность, в том числе и ее количество, относительны, зависимы от системы, в контексте которой информация рассматривается, от природы информационно взаимодействующих объектов.

Для информации исходными являются понятия, близкие друг другу по смыслу, а именно: разнообразие, неопределенность, структурность, сложность, неоднородность. Количество информации при этом характеризует меру разнообразия, сложности. Элементарное разнообразие, различие – это различие типа «есть – нет», «это – не это». Отсюда вытекает достаточность двоичной системы исчисления информации, двоичного алфавита. Вместе с тем опора в теории информации на сложность, структурность, отражаемую численно, прямо говорит о близости этой теории к науке об

[28] Глушков В.М. Мышление и кибернетика // Вопросы философии. – 1963. – №1. – с. 36

исчислении и структурности мира, т.е. к математике. Не случайно вычислительная математика столь тесно сплетена с информатикой, а в теории информации так эффективна математическая статистика. Чтобы выразить численно разнообразие какого-либо явления, процесса, необходимо измерение. Оно переводит исходное, естественное разнообразие в числовой код. Таким образом, число как универсальное средство точного, количественного познания мира есть одновременно и универсальное средство отображения информации. [29]

Разнообразие (структурность) может быть статической и динамической. Статическая, запечатленная информация есть разнообразие (структура) в аспекте пространства. Ее обычно характеризуют как память и перемещают во времени. Динамическая, процессуальная информация есть разнообразие (структура) в аспекте времени, информация в изменении. Этот вид информации называют обычно сигналом и перемещают в пространстве. Вместе с тем, противопоставлять память и сигнал нельзя, поскольку они взаимосвязаны и взаимно переходят друг в друга в процессах записи и считывания информации.

При этом информацию нельзя рассматривать односторонне, т.е. либо только как свойство, либо только как отношение, либо только как процесс. Статическая информация может интерпретироваться как свойство материи, динамическая – как процесс. Рассмотрение информации как отношения необходимо, если исследуется процесс ее передачи (информационное взаимодействие). Вместе с тем нельзя, видимо, считать совершенно равноправными характеристики информации как свойства, отношения и процесса. Информация есть фундаментальное свойство материи, характеризую-

[29] Сифоров В.И. Наука об информации и ее проблемы / В.И. Сифоров. – М.: Наука, 1992. – 289 с.

щее сравнительное разнообразие и вещей, и процессов, но по-разному проявляющееся в их отношениях.

Таким образом, можно выделить следующие определения информации:

сообщение, осведомление о положении дел, сведения о чем-либо, передаваемые людьми;

уменьшаемая, снимаемая неопределенность в результате получения сообщений.

сообщение, неразрывно связанное с управлением, сигналы в единстве синтаксических, семантических и прагматических характеристик;

передача, отражение разнообразия в любых процессах и объектах.

Информация имеет свойства: полезность, полнота, достоверность, новизна и ценность. Информация может быть полезной и бесполезной. Но так как границы между этими понятиями нет, то следует говорить о степени полезности применительно к нуждам конкретной информационной системы. Чтобы решить поставленную задачу, система должно иметь полную информацию. Но информация никогда не бывает полной (так же, как решение задачи – оптимальным). Поэтому следует иметь в виду степень полноты. Еще одно свойство: достоверность, которая уменьшается с уменьшением полноты. Причем здесь зависимость не прямая, а логическая: первые разрозненные факты мало о чем говорят, и первоначально увеличение их количества мало отражается на природе достоверности; потом, после определенного уровня, начинается пропорциональный рост, который по достижении следующего критического уровня начинает замедляться и затем вовсе прекращается – новые факты сверх избыточны и ничего не добавляют. Чтобы собрать полную и достоверную информацию, требуется время, а информация стареет. Поэтому информация имеет еще одно свойство – новизну. Если разделить информацию на стратегическую

и тактическую, то закономерностью является более быстрое старение тактической информации. Сопоставив два показателя – полноту и новизну, получим оптимальное соотношение, когда информация является уже достаточно полной и еще достаточно свежей. При этом гарантируется достаточно высокий уровень достоверности.

Из ценности информации следует, что она может становиться особым видом продукта с присущими ему всеми свойствами товара. Информационный товар может использоваться для обмена, на него существует спрос, и при этом он должен быть в ограниченном количестве. Информация и знание стали товаром, дающим самый высокий экономический эффект, Отнесение информации к категории товара также юридически закреплено законом об авторском праве.

В то же время многие виды информации предоставляются потребителю бесплатно. Их производство осуществляется государством или некоммерческими организациями. Информация как вид знаний, формирует у граждан экономическую, социальную и политическую позиции. Без развитого самостоятельного мышления, без умения анализировать информацию из вышеназванных областей не может быть сформирована личность в современном обществе. Свободное общество строится на свободном доступе к информации, способности к ее переработке.

Информация в современном обществе является определяющей категорией в экономическом развитии. Информация, знания выходят на первое место в системе общественных ценностей, а их приобретение становится основной задачей общества. Информация сегодня превратилась в мощный ресурс, имеющий даже большую ценность, чем природные, финансовые, трудовые и иные ресурсы. Она стала товаром, который продается и покупается. Информация превратилась в оружие, возникают и прекращаются информационные войны. Активным образом развивается и входит в нашу

жизнь трансграничная информационная сеть Интернет. Все это серьезно изменяет жизнь личности, общества, государства. Именно информация стала важнейшим стратегическим ресурсом мирового сообщества, от которого зависит настоящее и будущее человечества.

Для таможенных органов значение информации в условиях экономической интеграции стремительно возрастает. Накопление в информационных системах таможенных органов значительного объёма различной информации, связанной с осуществлением внешнеэкономической деятельности, заставляет решать проблемы переработки информации, ее хранения, использования и защиты.

Таможенные органы, как и многие государственные органы, не производят материальных благ. Результатом таможенной деятельности является выработка решений, предоставление услуг, создание информационных продуктов. С другой стороны, информация для государственных органов является критически важным ресурсом. Это и персональные данные физических лиц, и информация участников ВЭД, и персональные данные сотрудников таможенных органов, и информация, поступающая из таможенных органов других государств, а также внутренние приказы, решения, распоряжения, статистическая и аналитическая информация. Определенная часть данной информации является конфиденциальной, а ее огромная доля сосредоточена в виде баз данных в ЕАИС таможенных органов. Также указанные сведения могут передаваться по внешним неконтролируемым вычислительным сетям общего доступа (например, через Интернет).

Особое значение приобретают специально разработанные информационные продукты, которые могут многократно использоваться для исполнения таможенными органами своих функций, в частности решения задач таможенного контроля и регулирования внешнеторговой и экономической деятельности.

Очевидно, что при растущих хозяйственных связях, масштабах торговых отношений со странами-партнерами в мировой экономике, при диверсификации общественного производства соответствующий им объем информации растет по многим направлениям. Постоянно увеличивается количество наименований и модификаций товаров, растет число товарных позиций в национальных и внешнеэкономических классификаторах продукции, увеличивается число хозяйствующих субъектов, и, в конечном счете, усиливается конкуренция на различных рынках, что делает информацию о ВЭД ценным фактором управления и повышения конкурентоспособности.

В растущих объемах встречных товарных поставок стран-участниц мирового рынка определенную долю составляют контрафактные виды продукции. Они, наряду с увеличивающимся потоком подлинных товаров, еще более увеличивают информационную и функциональную нагрузку на таможенную службу. При этом усиливается потребность в более действенном контроле за товарами и транспортными средствами, пересекающими границу. Информационное сопровождение товародвижения в мировой экономике присутствует во многих управленческих действиях.

На макроэкономическом уровне государственного регулирования актуализируются задачи по оптимизации принимаемых решений, в том числе в сфере внешнеэкономических отношений, при соблюдении принципов национальной безопасности. Расширенное воспроизводство отраслей национальной экономики, включая такую отрасль, как внешняя торговля, порождая экономическую информацию в разрезе товаров (товарных групп) и транспортных маршрутов их перевозки, представляется глобальным приоритетом развития экономического базиса страны. Этому направлению должна соответствовать система государственного регулирования с возрастающей в условиях экономической интеграции ролью таможенной

службы, что также обусловлено диверсификацией мировой экономики и увеличением экономических и информационных преимуществ и рисков в условиях общей либерализации международной торговли.

Уникальность таможенной службы как отрасли государственного регулирования состоит в том, что информация идентифицируется (фиксируется, возникает) в системе непосредственно в процессе таможенного контроля, оформления, то есть в режиме реального времени. Очень важно за небольшой промежуток этого времени не упустить возможность получить ценные данные об элементах объективного экономического процесса. Наряду с этим вырастает объем дополнительной управленческой информации, необходимой для обслуживания текущего процесса таможенного оформления, контроля, диагностики, оценки. В процессе обработки текущей информации в информационной системе таможенных органов возникает необходимость в оперативном ее преобразовании, расширении и представлении в специализированные банки данных и т.п.

3.1.2. Информационные технологии в деятельности таможенных органов

Федеральная таможенная служба является уполномоченным федеральным органом исполнительной власти, осуществляющим в соответствии с законодательством Российской Федерации функции по выработке государственной политики и нормативному правовому регулированию, контролю и надзору в области таможенного дела, а также функции агента валютного контроля и специальные функции по борьбе с контрабандой, иными преступлениями и административными правонарушениями. Руководство деятельностью ФТС России осуществляет Правительство Российской Федерации.[30]

[30] Постановление Правительства Российской Федерации от 26 июля 2006 г. №459

Основными функциональными задачами таможенной службы Российской Федерации является обеспечение поступлений в бюджет (фискальная функция), обеспечение экономической и национальной безопасности (защитная функция), содействие торговле и создание благоприятных условий для привлечения иностранных инвестиций. При этом таможенные органы в настоящее время сталкиваются с целым рядом проблем. Механизмы международной торговли усложняются, ширится применение информационных и коммуникационных технологий (ИКТ), таких как прямой ввод данных, банковские услуги через Интернет. Сроки таможенного оформления часто неоправданно затягиваются, что дорого обходится торговле (краткосрочные кредиты, издержки по длительному хранению нереализованной продукции). Кроме того, таможенные администрации все чаще сталкиваются с необходимостью интеграции своих систем с глобальными логистическими сетями международных торговых и транспортных операторов.

Чтобы справиться с этими проблемами, основным направлением развития современных таможенных служб является использование информационных технологий (ИТ). Разрабатываются и создаются информационные таможенные системы, адаптированные для удовлетворения национальных потребностей. На протяжении многих лет такие системы были усовершенствованы, упрощенны, а в некоторых отношениях стандартизированы в соответствии с передовой международной практикой. Многие таможенные администрации используют автоматизацию для поддержки таких основных функций как обработка таможенных деклараций, оценка стоимости, сбор налогов, управление рисками и документооборот.

В связи с вступлением во Всемирную торговую организацию основной задачей информационных таможенных технологий является управление информацией внутри таможенной системы для повышения эффектив-

ности таможенного оформления и контроля, создания максимально благоприятных условий для участников внешнеэкономической деятельности (ВЭД), обеспечение правоохранительной деятельности в таможенной сфере. При выборе форм таможенного контроля необходимо использовать систему управления рисками, внедрять предварительное информирование и электронное декларирование.

Условно, внедрение информационных технологий таможенными органами различных стран можно разбить на три этапа. Каждый этап в этой эволюционной модели требует более широкого использования информационных технологий в сочетании с применением современных административных систем и процедур.

На первом этапе, таможенное администрирование сосредоточено на физическом контроле товаров, полагаясь на физический осмотр и проверку представленной бумажной документации. Компьютеризация используется, как правило, только для обработки деклараций и оценки стоимости. Во многих случаях эти системы просто дублируют существующие ручные процессы и процедуры. Сотрудники таможен часто выполняют функции ввода данных после получения бумажной документации, что достаточно трудоемко и приводит к большому количеству ошибок. Недостаточно внимания уделяется анализу, а управление рисками часто ограничено или вообще отсутствует. Акцент делается на обеспечение максимальных доходов, и мало внимания, как правило, уделяется упрощению процедур для торговли. Немало таможенных органов развивающихся стран и стран с переходной экономикой находятся на этом этапе.

На втором этапе работа таможни сосредотачивается на сборе и анализе информации, на основе которой принимается решение об оценке стоимости товара, а также о вмешательстве на основе системы управления рисками. Такие подходы требуют более широкого внедрения информаци-

онных систем, как внутри таможенных органов, так и в рамках торгового сообщества. Особенность таких систем - прямой ввод деклараций импортерами или таможенными брокерами, а также ограниченный электронный обмен информацией с другими государственными органами. Длительность таможенного оформления грузов, как правило, сокращается, и внимание сосредоточивается на торговых сделках, которые представляют самый большой риск. Такой подход используется для достижения баланса между физическим контролем и содействием внешней торговле. Этот этап характеризует нынешнюю ситуацию в большинстве развитых стран и стран со средним уровнем дохода.

На третьем этапе, таможенное администрирование в значительной степени основано на информационных системах учёта и контроля. Весь обмен информацией происходит в электронном виде, а решения о досмотре грузов производится на основе системы управления рисками. Особое внимание уделяется контролю соответствия предъявляемых документов и сведений, а также модернизации услуг (например, концепция одного окна). Таможенные службы переходят от трудоемких, неэффективных операций во время прибытия груза к упрощению процедур, используя предварительное информирование и контроль после выпуска товара, ускоряя, таким образом, процесс таможенного оформления и выпуска грузов. Все таможенные администрации в развитых странах в настоящее время реорганизуют свои системы к этим более эффективным стратегиям и методам работы.[31]

Таможенные организации стран используют различные пути компьютеризации:

разработка внутренней национальной системы;

передача разработки на аутсорсинг третьей стороне;

[31] Модернизация таможен. Справочное руководство / Под редакцией Люка де Вульфа и Хосе Б. Сокола. Всемирный банк реконструкции и развития. 2005. – 327с.

приобретение существующей системы на рынке.

Каждый вариант имеет свои преимущества и недостатки, в зависимости от местных условий ведения бизнеса и технологической среды, в которой действует организация. Федеральная таможенная служба Российской Федерации (ФТС России РФ) развивает и поддерживает свои собственные национальные системы. Разработка внутренней системы, будь то путем использования имеющихся ресурсов, либо через механизм внешнего подряда, имеет определенные преимущества, такие системы могут легко удовлетворить специфические потребности таможенной службы, а также таможенные органы полностью контролируют программное и техническое обеспечение систем.

В соответствии с Федеральным законом от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях. Технические и программные средства, используемые для автоматизации деятельности ФТС России, объединены в единую автоматизированную информационную систему таможенных органов (ЕАИС ТО). Она содержит множество подсистем, предназначенных для автоматизации различных направлений деятельности подразделений таможенной службы. ЕАИС ТО - организационно-техническая система, обеспечивающая выработку и принятие решений на основе автоматизации информационных процессов и технологий на всех уровнях организационной структуры таможенных органов.

ЕАИС ТО имеет иерархическую структуру, и ее уровни соответствуют уровням организационной структуры таможенных органов и их функциональным предназначением (центральный аппарат, региональное

таможенное управление, таможня, таможенный пост) (рис. 3.1).

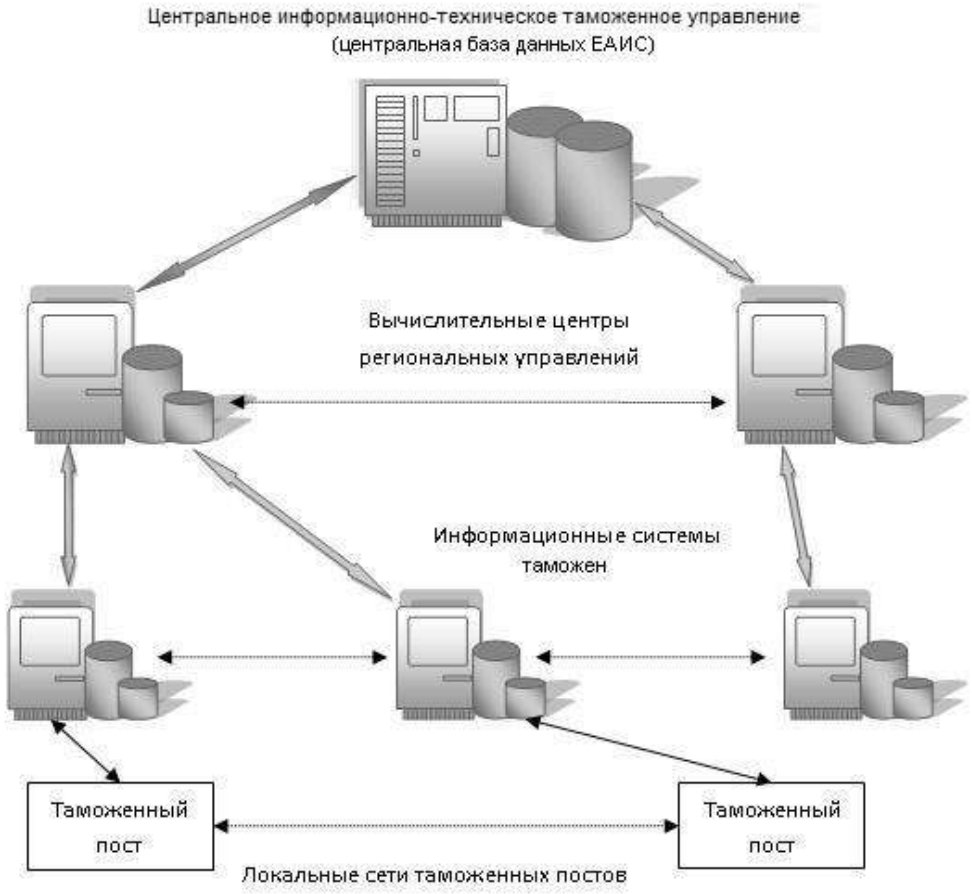

Рис. 3.1. Организационная структура ЕАИС ФТС России

Основными элементами ЕАИС являются локальные вычислительные сети (ЛВС), совокупность компьютерных баз данных, программные комплексы и объединяющая их ведомственная интегрированная телекоммуникационная сеть (ВИТС). ЕАИС ФТС России является распределенной автоматизированной информационной системой и охватывает всю территорию Российской Федерации, включая в себя Центральное информационно-техническое таможенное управление (ЦИТТУ), семь региональных вычислительных центров и транспортную подсистему ВИТС. Каждая таможня имеет собственную информационно-вычислительную сеть. Всего эксплуатируется более 10 тыс. ЛВС и более 300 комплексов специальных про-

граммных средств, объединенных логически в более чем 50 подсистем. Для информационного взаимодействия с участниками ВЭД, государственными и коммерческими структурами, информационными таможенными системами других государств ЕАИС ТО включает в свой состав автоматизированную систему внешнего доступа (АСВД) и систему ведомственных удостоверяющих центров таможенных органов на базе программного комплекса «КриптоПро УЦ».[32]

Каждая подсистема ЕАИС, как правило, предназначена для работы по определенному направлению деятельности таможенных органов. Функциональные задачи, которые решают подсистемы ЕАИС:

таможенное оформление и таможенный контроль;

контроль таможенных платежей;

таможенно-банковский валютный контроль;

обеспечение правоохранительной деятельности таможенных органов;

контроль таможенного транзита и таможенной стоимости;

контроль за таможенным оформлением транспортных средств;

формирование таможенной статистики внешней торговли Российской Федерации;

информационный обмен с министерствами и ведомствами Российской Федерации, таможенными службами зарубежных государств;

обеспечение информационно-аналитической деятельности таможенных органов;

обеспечение финансово-хозяйственной деятельности таможенных органов;

[32] Федоров В.В. Информационные таможенные технологии: Учебник. – М.: РИО РТА, 2007. – 216с.

иные вспомогательные и обеспечивающие функции таможенных органов.

Информационная система таможенных органов – одна из крупнейших информационных систем в стране. Отдельные ее компоненты включены в Перечень критически важных информационных государственных систем Российской Федерации. Автоматизированные системы такие как: электронное декларирование, предварительное информирование, система контроля таможенного транзита, система обеспечения уплаты таможенных платежей, кадры-2, система финансово-хозяйственной деятельность и другие – требуют высокого уровня централизации обработки и хранения информации. Это предъявляет повышенные требования к режиму круглосуточной доступности информационной системы.

Пользователями ЕАИС являются должностные лица таможенных органов, потребителями информации из ЕАИС или источниками информации могут быть информационные системы внешних организаций (например, участники внешнеэкономической деятельности, таможенные службы иностранных государств, министерства и ведомства Российской Федерации, Банк России, и т.д.).

Центральное информационно-техническое таможенное управление (ЦИТТУ) и подчиненные ему региональные центры предназначены для обработки и хранения накопленной информации, управления передачей данных и обслуживания запросов к базе данных. Центральная база данных ЦИТТУ ФТС России - это архивы оформляемых деклараций на товары плюс специализированные базы данных документов контроля доставки товаров и транспортных средств, таможенных приходных ордеров, сертифи-

катов и нормативно-справочной информации, а также база данных по участникам внешнеэкономической деятельности.[33]

Специально для таможенных целей используется ряд документов, которые являются основными элементами информационной составляющей ЕАИС ТО. Это электронные копии таможенных документов: декларация на товары, транзитная декларация, пассажирская таможенная декларация, декларация на транспортное средство и др.

База данных деклараций на товары (ДТ) - центральный элемент комплексной системы таможенного оформления. Каждый товар, приходящий на границу, имеет множество сопроводительных, документов – предварительная информация по товару, накладные, контракт, паспорт сделки, которая предваряет поставку, книжки перевозчиков и т. п. Вся информация из этих документов сводится в один – декларацию на товары; этот документ в настоящее время наиболее важен в работе таможенных служб. В ДТ описывается сам товар, его отправитель, получатель, указывается таможенная стоимость, вес, способ доставки и т. п. Форма этого документа вписана в структуру БД, и каждое его поле имеет под собой информационную поддержку.

ЕАИС поддерживает два формата представления электронной копии ДТ и указанных выше документов - внешний и внутренний. Внешний формат документов используется при декларировании для представления участником ВЭД в таможенный орган сведений в электронном виде. Внутренний формат разработан на базе внешнего формата и включает сведения, заполняемые не только участником ВЭД, но и уполномоченным должностным лицом таможенного органа, а также включает служебную инфор-

[33] Федоров В.В. Информационные таможенные технологии: Учебник. – М.: РИО РТА, 2007. – 216с.

мацию и атрибуты, используемые в целях обеспечения технологии сбора и обработки информации в рамках ЕАИС.

Не менее важной проблемой электронного декларирования является придание сведениям, содержащимся в электронном пакете документов юридической силы. При электронном декларировании декларант должен снабдить электронную версию декларации на товары электронной подписью (ЭП)[34], которая должна быть им предварительно получена в удостоверительном центре ЦИТТУ ФТС России. Система ведомственных удостоверяющих центров обеспечивает реализацию организационных и технических мероприятий для обеспечения использования участниками внешнеэкономической деятельности или иными лицами, осуществляющими информационное взаимодействие при представлении сведений таможенным органам в электронной форме, средств криптографической защиты и электронной подписи конфиденциальной информации.

КПС «Электронное декларирование товаров и транспортных средств» действует следующим образом: декларант формирует в электронной форме и подписывает своей электронной подписью ДТ. Затем вместе с комплектом документов ее направляют на сервер информационно-технической службы таможенного управления. Должностное лицо таможенного поста через систему КПС «ЭДТ и ТС» подключается к серверу и проверяет подлинность ЭП декларанта, правильность заполнения электронной формы ДТ и наличие электронных копий необходимых документов. Если не обнаружено ошибок, инспектор ставит свою ЭП и передает все на обработку в систему КАСТО «АИСТ РТ-21», которая производит все дальнейшие операции, вплоть до выпуска. Реальное ускорение и упро-

[34] Электронная подпись - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. [ФЗ РФ «Об электронной подписи» от 6 апреля 2011 г. N 63-ФЗ]

щение таможенных процедур при использовании ЭП дает участникам ВЭД возможность значительно повысить товарооборот и сократить накладные расходы.

Система электронного декларирования с использованием сети Интернет требует от декларанта только подключения к сети Интернет и осуществления защиты информации. Это дает возможность осуществления удаленного декларирования товаров участниками ВЭД в любой таможенный орган.

Система предварительного информирования дает таможенным органам возможность получать сведения о ввозимых грузах в электронном виде до прибытия груза на границу, что позволяет сотрудникам таможенных органов проверить эти сведения, спланировать необходимые мероприятия по контролю груза, существенно сократить время обработки документов, увеличить пропускную способность таможенных пунктов.

Одним из основных направлений развития современных отечественных и зарубежных информационных таможенных систем является внедрение технологий электронного декларирования и предварительного информирования, интегрированных с системой управления рисками. Применение систем управления таможенными рисками требует широкомасштабной открытой интеграции информационных систем таможни с информационными системами других министерств и ведомств, с силовыми структурами других стран.

Система управления рисками позволяет перейти от тотального досмотра товара на границе к контролю информации о товаре, выявляя возможные риски еще на этапе таможенного оформления, обеспечив тем самым достижение максимального эффекта ограниченными ресурсами. Методы таможенного контроля применяются там, где велики риски недостоверного декларирования, занижения веса и стоимости товара, с заведомо

неправильно указанным кодом товарной номенклатуры, чтобы уменьшить размер или уклониться от уплаты таможенных платежей. А также товары, в отношении которых велика вероятность подделки и незаконного использования товарного знака, то есть наиболее подверженные контрафакции и пиратству.

Основу системы управления рисками составляют правила отнесения тех или иных товаров, участников ВЭД или операций к группе риска. Эти правила, в свою очередь, формируются на основе формализованных критериев риска. В случае высокой вероятности рисков программная система выдаст указания таможенному инспектору о мерах реагирования (запрос у декларанта дополнительных документов, обязательное проведение досмотра и др.)

Еще одним важным направлением работы таможенных органов является обеспечение правоохранительной деятельности в таможенных структурах. Здесь ЕАИС применяется для информационной поддержки расследования дел о таможенных правонарушениях, контрабанде, для проведения таможенного аудита.

Новый механизм организации контроля таможенной стоимости товаров целесообразно организовать на базе предварительных сведений о таможенной стоимости товаров, который с учетом внедрения типовых задач факторного анализа и прогнозирования цен в автоматизированном режиме в составе системы «Мониторинг-Анализ» Единой автоматизированной информационной системы ФТС России может быть реализован в ближайшее время. При этом возможно сокращение административных издержек на осуществление таможенного контроля и повышение вероятности достоверного декларирования таможенной стоимости товаров.

С августа 2012 года вступил в действие единый таможенный тариф и единая товарная номенклатура внешнеэкономической деятельности Тамо-

женного союза в составе России, Казахстана и Беларуси[35]. В этой связи возрастает роль передовых технологий, таких как Интернет-декларирование, предварительное информирование и предварительное декларирование, а также производных от этих технологий - удаленный выпуск и разделенный выпуск.

Информационно-коммуникационные технологии могут существенно способствовать тому, чтобы таможенная деятельность была все более эффективной. Они должны быть адаптированы к реальным потребностям страны и таможенных органов, чтобы наилучшим образом использовать новые открывающиеся возможности.

3.1.3. Автоматизированные информационные системы таможенных органов как объекты защиты информации

Цели и задачи защиты автоматизированных информационных систем таможенных органов

Сегодня таможенные органы не только поддерживают различные информационные процессы, связанные со сбором, хранением, обработкой и поиском таможенной информации, но и предлагают услуги с удаленным доступом к Единой автоматизированной информационной системе ФТС России. Расширение объемов таможенных информационных ресурсов требует проведения большого объема работ по их обработке, ведению, проведению аналитической работы, регистрации и администрированию пользователей, а также по организации технологического процесса защиты.

С ростом киберпреступности и угроз для важнейших информационных ресурсов возрастает важность защиты информации, хранящейся и обрабатываемой в ЕАИС, с целью обеспечения ее конфиденциальности, це-

[35] Решение Совета Евразийской экономической комиссии от 16.07.2012 N 54 "Об утверждении единой Товарной номенклатуры внешнеэкономической деятельности Таможенного союза и Единого таможенного тарифа Таможенного союза"

лостности и доступности, а значит и для защиты национальных интересов государства. Для решения этой задачи используются системы защиты информации, входящие в ЕАИС в качестве подсистем.

В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.[36]

В соответствии с Доктриной информационной безопасности Российской Федерации, утверждённой Президентом Российской Федерации 9 сентября 2000 г. , и Концепцией обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года, утвержденной приказом ФТС России от 13 декабря 2010 г. №2401[37], обеспечение необходимого уровня безопасности ЕАИС ТО и информационных ресурсов, их целостности и конфиденциальности основывается на применении требований защиты информации от утечки, от несанкционированного преднамеренного или непреднамеренного воздействия, от разглашения, от несанкционированного доступа, а также на использовании сертифицированных отечественных средств предупреждения и обнаружения компьютерных атак и защиты информации, разрабатываемых и производимых организациями, получившими в установленном порядке необходимые лицензии.

[36] Приказ ФСТЭК РоссииРоссии от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

[37] 7. Концепция обеспечения информационной безопасности тамо-женных органов Российской Федерации на период до 2020 года (утв. Приказом ФТС России от 13 декабря 2010 г. № 2401).

Цель обеспечения защиты информации таможенных органов состоит в совершенствование ведомственной системы информационной безопасности таможенных органов в целом, в соблюдении прав и свобод граждан в области получения и использования таможенной информации, в развитии современных информационных таможенных технологий, обеспечении их безопасности и защиты от несанкционированного доступа, а также в контроле состояния обеспечения информационной безопасности и технической защиты информации таможенных органов.

Основными направления деятельности по обеспечению информационной безопасности и технической защите информации являются:

обеспечение защиты информации, составляющей государственную тайну от утечки по техническим каналам;

обеспечение защиты Ведомственной интегрированной телекоммуникационной сети ТО;

обеспечение защиты информационных систем персональных данных и служебной информации ограниченного распространения;

обеспечение информационной безопасности при авторизации пользователей на автоматизированных рабочих местах, включенных в Доменную структуру Единой службы каталогов ЕАИС таможенных органов Российской Федерации;

обеспечение информационной безопасности при использовании информационных телекоммуникационных сетей международного информационного обмена (Интернет);

обеспечение функционирования системы антивирусной защиты информации;

контроль обеспечения информационной безопасности и технической защиты информации.

Составными частями любой системы защиты информации являются (рис. 3.2):

нормативно-правовая база (дисциплинарные, гражданско-правовые, уголовно-правовые меры);

структура подразделений таможенных органов, обеспечивающих защиту информации;

организационные меры (стратегия и политика информационной безопасности);

программно-технические методы, способы и средства защиты информации (например, антивирусные программы, системы разграничения полномочий, программные средства контроля доступа).

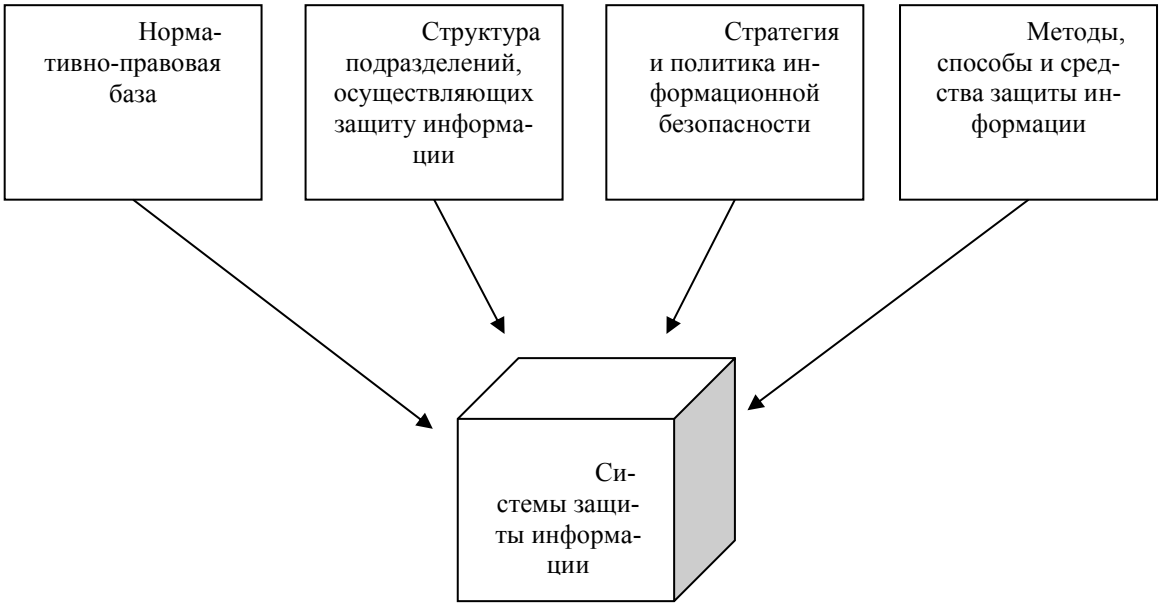

Рис. 3.2. Составные части системы защиты информации

В общем случае, обеспечение защиты информации в автоматизированных информационных системах необходимо рассматривать как совокупность программно-технических и организационных мер для предотвращения или нейтрализации угроз при создании и эксплуатации АИСТ.

Нормативно-правовая база обеспечения защиты информации в таможенных информационных системах

Нормативно-правовое обеспечение защиты информации в таможенных органах относится к законодательным и организационным средствам обеспечения безопасности информации в автоматизированных информационных системах таможенных органов. К настоящему времени утвержден целый ряд нормативно-правовых документов, определяющих направления развития информационных и телекоммуникационных технологий в Российской Федерации на среднесрочную и долгосрочную перспективу.

Структура нормативно – правовой и методической базы обеспечения информационной безопасности таможенных органов Российской Федерации включает в себя:

Федеральные и конституционные законы, Указы Президента Российской Федерации, постановления Правительства Российской Федерации, руководящие документы ФСТЭК Россиии ФСБ России;

Международные нормативные правовые акты;

Правовые акты по обеспечению информационной безопасности таможенных органов Российской Федерации (в целом, центральный аппарат ФТС России, уровень регионального таможенного управления);

Государственные стандарты и технические регламенты.

В 2005 году Всемирной таможенной организацией приняты рамочные стандарты безопасности и содействия международной торговле. Одним из наиболее актуальных вопросов в области деятельности таможенной администрации по осуществлению сотрудничества с таможенными службами зарубежных государств является организация предварительного информирования, предусматривающего обмен сведениями о перемещаемых товарах и транспортных средств, а также обмен информацией, связанной с расследованием административных правонарушений. Отсутствие правово-

го регулирования в этих вопросах приводит к длительным процессам согласования условий информационного взаимодействия.

Одним из главных результатов стандартизации в сфере систематизации требований и характеристик защищенных информационных систем стала Система международных и национальных стандартов безопасности информации, которая насчитывает более сотни различных документов. В последнее время в разных странах появилось новое поколение стандартов в области защиты информации, которое отличается большей формализацией процесса обеспечения безопасности и более детальным комплексным учетом качественно и количественно проверяемых и управляемых показателей информационной безопасности компании. Комплексный учет показателей предполагает комплексный подход к управлению безопасности, когда на соответствие определенным правилам проверяется не только программно-техническая составляющая защиты информации компании, но и организационно-административные меры по ее обеспечению.

В соответствие с международными и национальными стандартами ISO 15408, ISO 17799 (BS7799), BSI; COBIT, SAC, COSO, SAS 78/94 обеспечение информационной безопасности предполагает определение целей обеспечения информационной безопасности компьютерных систем, создание эффективной системы управления информационной безопасностью, расчет совокупности детализированных не только качественных, но и количественных показателей для оценки соответствия информационной безопасности заявленным целям, применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния, использование методик управления безопасностью с обоснованной системой метрик и мер обеспечения информационной безопасности, позволяющих объективно оценить защищенность информационных активов и управлять информационной безопасностью компании.

Основные национальные стандарты в области защиты информации:

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения

ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью.

ГОСТ Р ИСО 7498-2-99 Государственный стандарт Российской Федерации Информационная технология взаимосвязь открытых систем базовая эталонная модель

ГОСТ Р 51241-98 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

ГОСТ Р 50.1.053- 2005 Информационные технологии, основные термины и определения в области технической защиты информации

ГОСТ Р 51188—98 — Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство.

ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта — ISO/IEC 27001:2005.

ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты.

Деятельность таможенных органов Российской Федерации в области обеспечения безопасности информации, подлежащей обязательной защите, регулируется и другими документами, издаваемыми в установленном порядке, в том числе соответствующими постановлениями Правительства Российской Федерации, руководящими документами ФСТЭК Россиии ФСБ России.

Организационно-технические меры защиты информации

В связи с созданием Таможенного союза и вступлением России в ВТО повысилась актуальность внедрения популярных в мире стандартов по организационным основам информационной безопасности серии 27000. Стандарт ГОСТ Р ИСО/МЭК 27001-2006 использует процессный подход для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента информационной безопасности (СМИБ). СМИБ – часть системы менеджмента, основанная на анализе рисков, и включает в себя организационную структуру, политики, план действий, распределение ответственности, осуществление на практике, процедуры, процессы и ресурсы.[38]

Стандарт является руководством по определению, минимизации и управлению угрозами, которым может подвергаться информация и обеспечивает уверенность участников внешнеэкономической деятельности и партнеров в том, что информация защищена должным образом.

В рамках работ по созданию системы менеджмента информационной безопасности можно выделить следующие основные этапы:

принятие решения о создании СМИБ;

анализ рисков;

разработка политик и процедур СМИБ;

внедрение системы менеджмента в эксплуатацию.

Эффективное управление информационной безопасности должно включать в себя:

определение стратегии информационной безопасности;

управление рисками - определение и снижение рисков;

управление активами;

измерение результативности;

[38] ГОСТ Р ИСО/МЭК 27001-2006 Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

оптимизации затрат на информационную безопасность.

Управление информационной безопасностью связано с принятием решений по снижению рисков. Анализ рисков включает в себя:

определение угроз информационной безопасности, характеризующихся вероятностью возникновения и реализации;

выявление уязвимостей системы информационной безопасности, которые влияют на вероятность реализации угрозы;

определение ущерба, возникающего в результате реализации угрозы;

расчет рисков, отражающих предполагаемый ущерб в результате реализации угрозы.

Управление рисками это постоянный процесс выявления рисков информационной безопасности и осуществление планов по их устранению. Зачастую количество активов подверженных риску превышает имеющиеся ресурсы для управления ими. Поэтому крайне важно знать, какие из имеющихся ресурсов можно использовать для смягчения рисков.

Для эффективного решения проблемы управления рисками критически важные активы должны быть определены, документированы и отслежены. Привлечение руководителей таможенных служб к оценке стоимости информационных активов приводит их к пониманию ценности этих активов и организации их безопасности.

СМИБ задает процедуру анализа рисков, в которой определена методология и отражены организационные аспекты по каждой из задач, определяет, кто имеет право принимать решения, и обеспечивает контроль для снижения рисков. А также рекомендует стратегии безопасности. Документ, определяющий стратегию, часто называют концепцией, а документ определяющий тактику - политикой.

В целях совершенствования работы по обеспечению информационной безопасности и технической защиты информации в ФТС России при-

нята Концепция обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года, в которой раскрывается защита национальных интересов государства в информационной сфере деятельности таможенных органов.[39]

Федеральная таможенная служба разрабатывает административные меры обеспечения компьютерной безопасности таможенных органов. Для обеспечения защиты компьютерной информации были приняты следующие приказы:

приказ ФТС России от 02 февраля 2007 № 168 «Об утверждении Порядка предоставления должностным лицам таможенных органов доступа к ресурсам центральной базы данных Единой автоматизированной информационной системы таможенных органов»;

приказ ФТС России от 12 ноября 2007 г. №1393 «Об утверждении Требований по обеспечению информационной безопасности при работе с ресурсами Центральной базы данных Единой автоматизированной информационной системы таможенных органов»;

приказ ФТС России от 28 мая 2007 г. «О системе антивирусной защиты информации в таможенных органах Российской Федерации».

Политика информационной безопасности представляет собой совокупность директив, правил и практик, которые предписывают, как управлять, защищать и распространять информацию. Политика информационной безопасности является важным компонентом управления информационной безопасностью.

Политика информационной безопасности должна быть основана на сочетании соответствующего законодательства, применимых стандартов, и требований руководства, а также клиентов и партнеров.

[39] Концепция обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года (утв. Приказом ФТС России от 13 декабря 2010 г. № 2401).

Политика на уровне управления может включать в себя:

программу обеспечения безопасности и управление этой программой;

должностные инструкции сотрудников, регламентирующие роли и обязанности по выполнению требований СМИБ. Каждый сотрудник должен быть осведомлен о том, что он должен делать для соблюдения режима информационной безопасности;

персональную ответственность каждого сотрудника в отношении соблюдения политики безопасности и последствия ее невыполнения;

классификацию информационных активов и их защиту;

риски информационной безопасности с указанием подверженности риску информационных активов, остаточные риски и сроки оценки риска;

закрепление доступа к активам с указанием прав доступа к категории активов;

образец процесса принятия решений для обеспечения безопасности инвестиций;

стандарты безопасности;

рекомендации по поддержке непрерывности работы;

аварийное восстановление;

взаимодействие со сторонними организациями;

реагирование на инциденты;

информирование и обучение сотрудников правилам безопасности;

оценка уровня безопасности, включающая оценку эффективности и выполнения политики безопасности.

Эффективная система менеджмента информационной безопасности будет показывать тенденции ослабления неблагоприятного воздействия нарушений безопасности. Количественные меры должны также в себя

включать анализ рисков с течением времени, а также измерение, мониторинг и отчетность о процессах обеспечения информационной безопасности

Процесс создания системы менеджмента информационной безопасности достаточно сложен и длителен. Очевидно, что работы по разработке и внедрению этой системы не могут проводиться без привлечения руководителей таможенных органов. Эффективная и реально работающая система управления информационной безопасностью позволит таможенным органам Российской Федерации продемонстрировать надежность своих информационных систем и выйти на новый уровень отношений с участниками ВЭД, таможенными службами иностранных государств и другими государственными органами.

3.1.4. Анализ и оценка рынка средств защиты информации

Информационные потребности разных уровней растут быстрыми темпами, что расширяет возможности информационного обмена, ведет к появлению все новых информационных продуктов, стимулирует развитие всех видов информационной деятельности. Вместе с этим увеличивается число и сложность угроз безопасности информации и случаев их реализации, что в результате стимулирует увеличение вкладываемых инвестиций в индустрию безопасности и ведет к появлению все новых средств защиты на рынке. Рынок технологий и услуг безопасности сегодня один из самым динамично развивающихся.

В ближайшие годы рынок систем безопасности будет одним из самых быстрорастущих сегментов рынка информационных технологий. По мнению аналитиков консалтинговой компании Gartner мировой рынок технологий и услуг безопасности в 2013 году вырос до 67,2 миллиардов долларов, что на 8,7 процента больше по сравнению с уровнем 2012 года.

А к 2016 году объем рынка превысит 86 миллиардов долларов.[40] Российский рынок продуктов безопасности за счет активного регулирующего влияния государства также демонстрирует высокий рост. Совокупный объем российского рынка информационной безопасности составляет около 1,4 миллиардов долларов в год.[41]

На российском рынке представлен широкий спектр аппаратно-программных средств обеспечения безопасности и сохранности информации. Отечественному потребителю предлагаются практически все известные мировые и российские продукты. Разнообразие этих средств определяется, прежде всего, возможными методами противодействия и защиты от угроз безопасности.

Выбор средств защиты информации из всего множества, представленного на рынке, для многих компаний представляет особую сложность. Часто экспертам по безопасности сложно разобраться в таком количестве механизмов защиты, чем они отличаются друг от друга, и какими принципами следует руководствоваться при их выборе. На выбор потребителей может повлиять узнаваемость имени компании производителя, активная маркетинговая политика при представлении нового продукта, аналитические материалы независимых испытательных лабораторий. В результате всех этих манипуляций у участников рынка может сформироваться искаженное представление о продукте.

Все программные и программно-аппаратные средства защиты, представленные в настоящее время на рынке, можно условно разделить на следующие категории:

средства антивирусной защиты;

системы защиты от несанкционированного доступа;

---

[40] http://www.gartner.com/newsroom/id/2512215

[41] Рынок информационной безопасности Российской Федерации http://www.pcidss.ru/files/pub/pdf/Pervoe_expertnoe_issledovanie_rynka_IB.pdf

средства обеспечения сетевой безопасности;

средства контентной фильтрации;

средства криптографической защиты информации;

инструментальные средства анализа защищенности;

системы сбора и анализа событий;

системы идентификации и аутентификации (IAM);

средства контроля утечек (DLP).

Одной из самых известных и обсуждаемых угроз безопасности информации, о которой знает большинство персонала любой организации, являются вредоносные программы-вирусы. К вредоносному программному обеспечению относятся классические файловые вирусы[42], сетевые черви[43,] приложения типа «Троянский конь»[44,] шпионские и рекламные программы, перехватчики ввода с клавиатуры, программы дозвона на платные номера, программы-боты[45,] фишинг[46,] хакерские утилиты и прочие программы, наносящие вред компьютеру и данным. Вирусные эпидемии широко распространились с началом массового использования Интернета. Первоначально вирусы создавались программистами в целях обучения или самоутверждения и открыто проявляли свои действия. Сегодняшние вредоносные программы в основном разработаны с целью кражи персональных и конфиденциальных данных, а также получения финансовой выгоды. Очень часто применяется не один вирус, а их комбинация, например, сочетание вирусов или червей вместе с методами социальной инженерии. Количество

[42] Файловые вирусы - программы, обычно не имеющие собственного исполняемого модуля и присоединяемые к другому файловому объекту.

[43] Черви – программы способные к самовоспроизведению себя через сеть, при этом повреждая файлы.

[44]Трояны или троянские кони - это программы, которые попадают в компьютеры без ведома пользователя и осуществляет различные несанкционированные пользователем действия.

[45] Программы-боты используют зараженный компьютер для выполнения нелегальных операций против третьих сторон: рассылка спама, проведение атак отказа в обслуживании, распространение вредоносного программного обеспечения.

[46] Фишинг - сообщения, которые стараются убедить пользователя рассекретить пароли для доступа к онлайновым сервисам: банкам, электронной почте и др.

и разнообразие вредоносных программ растет из года в год. Вирусные атаки стали заказными и целевыми, жертвами их могут стать как частные, так и физические лица.

С развитием вирусов совершенствуются и средства антивирусной защиты. Современные антивирусные программные продукты являются комплексными платформами с использованием централизованных многофункциональных сред управления, так называемые системы защиты конечных точек (EPP, Endpoint Protection Platform). Эти системы обеспечивают защиту в реальном времени и сочетают в себе функции антивируса, антишпиона, персонального межсетевого экрана (брандмауэр), системы защиты от вторжений (IPS), содержат проактивные технологии анализа аномального поведения процессов и приложений, что позволяет обнаруживать пока неизвестные вредоносные программы. Изменяются и дополнительные сервисы, обеспечивающие ежедневные обновления сигнатур антивирусных баз, техподдержку, клиентские сервисы.

По оценке аналитиков Gartner объем мирового рынка систем защиты конечной точки составил в 2011 г. более 3,2 млрд. долл. и вырос в 2013 г. на 5%. Основные игроки мирового рынка EPP-решений представлены на «магических квадрантах» компании Gartner (рис. 3.3). Квадрант разбит на четыре части, и в правой верхней части расположились ведущие производители с точки зрения возможностей продукта, анализа рынка, опыта заказчиков в работе с решениями производителя и стратегического видения. Лидеры на квадранте занимают большую часть рынка и определяют своей политикой развитие рынка. Лидерами рынка 2013 года стали компании Symantec, McAfee, Sophos, Лаборатория Касперского и Trend Micro, на долю которых приходится около 85% от общего объема этого рынка (рис. 3.3).

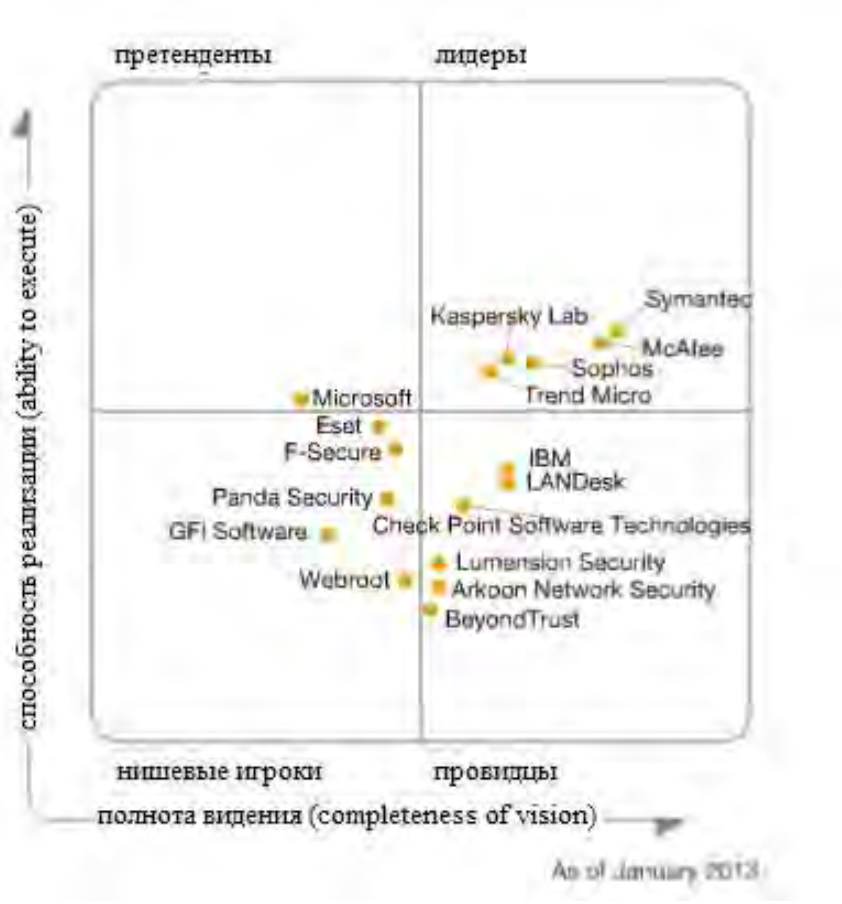

Рис. 3.3. Магический квадрант Gartner игроков рынка систем EPP по состоянию на январь 2013 года

Рынок антивирусного программного обеспечения делится на коммерческие и бесплатные антивирусные решения, а также на персональные и корпоративные продукты. Основной доход большинству производителей приносит корпоративный сегмент антивирусного рынка. Пользователи часто выбирают антивирусное решение по стоимости, техническим характеристикам и обращают внимание на общий уровень защиты антивируса. По данным компании OPSWAT[47] на август 2013 г. самыми популярными антивирусными программами, осуществляющими защиту в реальном времени, стали три бесплатных продукта, которые активно защищают более чем 50% компьютеров в мире. Лидирует программа Microsoft Security

[47] http://www.tomsguide.com/us/best-free-antivirus-software-2013,review-1788.html

Essentials, на втором месте Avast, и AVG на третьем (рис. 3.4). В то время как платные решения теряют долю рынка, бесплатные антивирусные решения продолжают укреплять свои позиции.

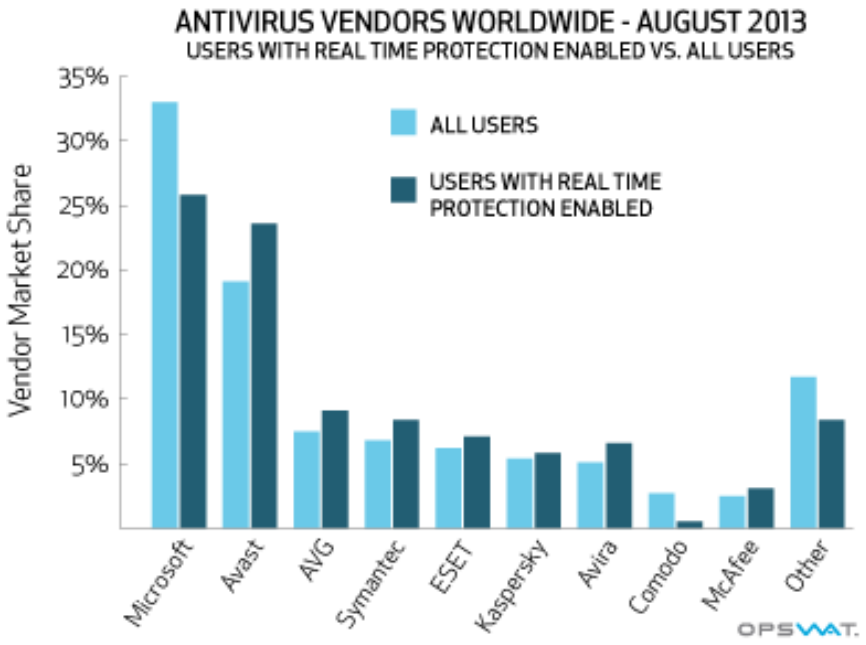

Рис. 3.4. Доли основных игроков мирового рынка антивирусных продуктов на август 2012 года

Любые решения в области безопасности теоретически могут быть обойдены. Несмотря на возрастание защиты от вредоносных программ в последние годы, скорость распространения инфекций остается неизменно высокой. К сожалению, практически не существуют продукты, которые могут обеспечить полную защиту. Результаты испытаний независимых лабораторий неизменно показывают, что практически все антивирусные продукты могут не обнаруживать от 2% до 10% известных угроз безопасности. Сравнительный тест антивирусного программного обеспечения различных производителей на защиту от вредоносных программ из Интернета от независимой некоммерческой организации AV-Comparatives приведен

на рис. 3.5.[48] Хотя на графике некоторые продукты и смогли достичь 100% защиты от распространенных вредоносных образцов, использованных в тесте, это не означает, что эти продукты всегда смогут защищать от всех угроз Интернета.

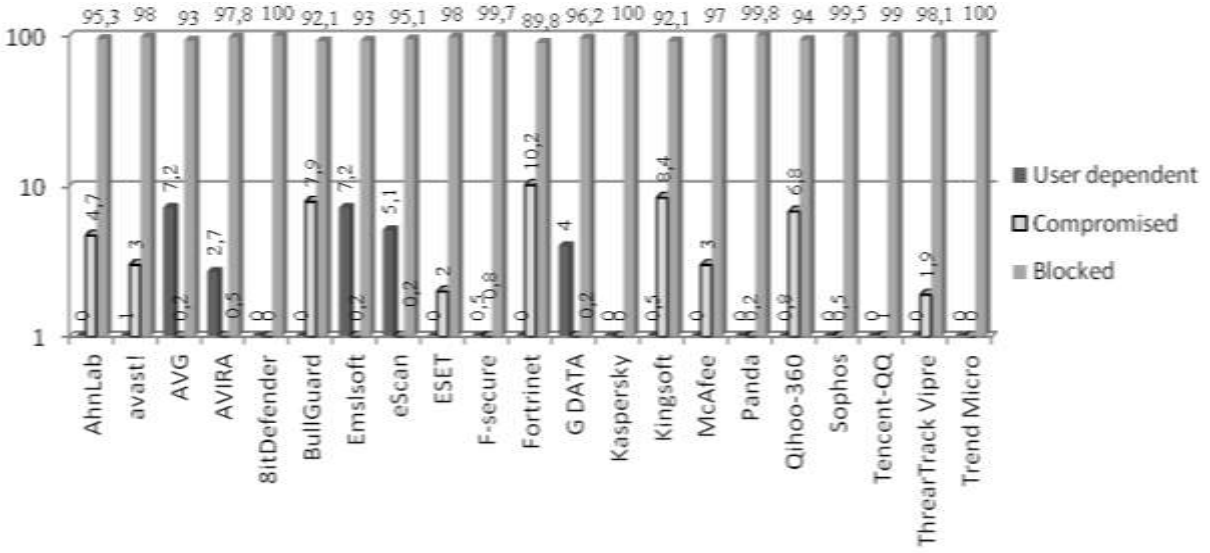

Рис. 3.5. Результаты динамической проверки антивирусных программ на защиту от угроз из Интернета (август 2013 г.)

Российский рынок антивирусных решений также неуклонно растет. Среднегодовой рост российского рынка средств антивирусной защиты с 2005 по 2011 год составил 42%. Объем этого сектора рынка составил в 2010 году 270 миллионов долларов, в 2011 году 334, а в 2012 году достиг 400 миллионов долларов (рис. 3.6).

[48] http://www.av-comparatives.org/wp-content/uploads/2013/09/avc_factsheet2013_08.pdf

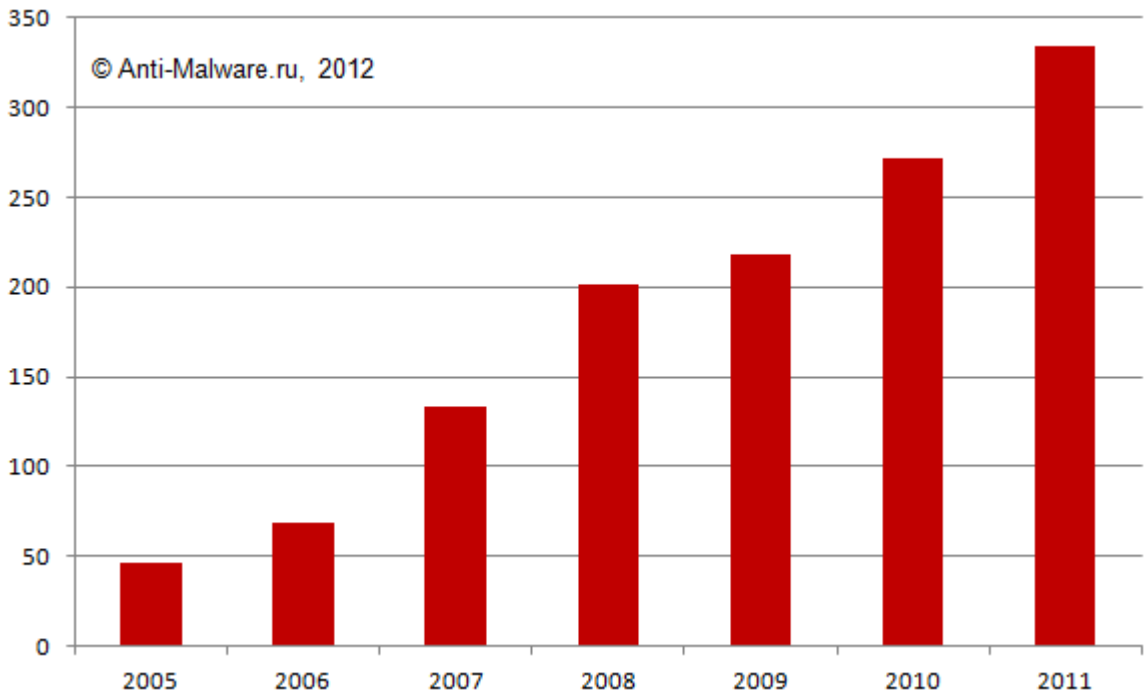

Рис. 3.6. Динамика объема антивирусного рынка в России (млн. долл.)

Данный сегмент рынка средств защиты на сегодняшний день представлен, как отечественными, так и зарубежными средствами. По данным 2012 года лидерами российского рынка являются компании: Лаборатория Касперского и Eset, следом идет еще одна российская компания - Доктор Веб и зарубежные производители - Symantec и Trend Micro. Также на российском рынке представлены и другие производители, такие как Panda Security, Код Безопасности, Microsoft, Aladdin, Agnitum, Avast Software, BitDefender и др. (рис. 3.7).

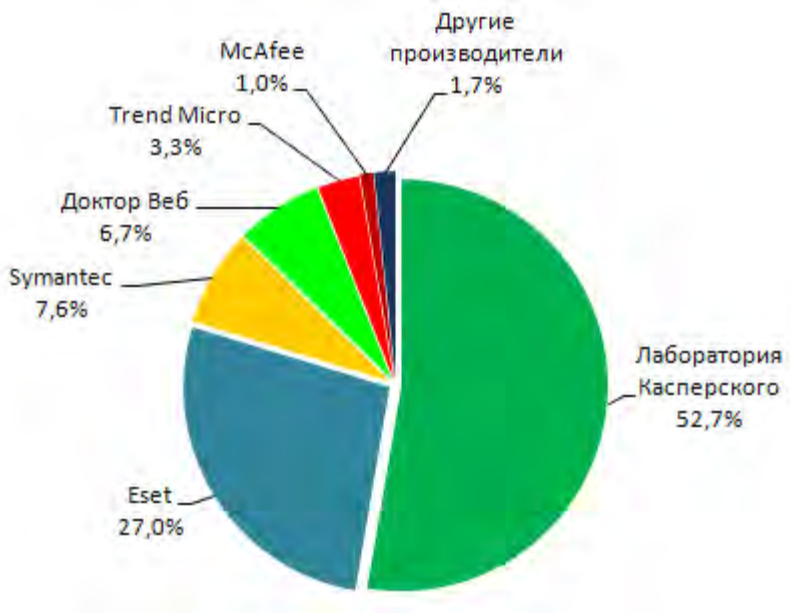

Рис. 3.7. Доли основных участников рынка антивирусной защиты в России

По оценкам экспертов рынок антивирусных продуктов будет продолжать расти и в России, и во всем мире, что обусловлено опережающим ростом регулярно возникающих вирусных эпидемий, широко освещаемых в прессе. Новой сферой применения средств защиты от вредоносного программного обеспечения являются новые технологии, такие как мобильные платформы и облачные хранилища.

Компьютеры, подключенные к глобальной или локальной сети, потенциально всегда более уязвимы. Рынок средств обеспечения сетевой безопасности в России объединяет большое количество различных как российских, так и зарубежных устройств, защищающих информацию в процессе ее передачи по сети, к ним относятся:

межсетевые экраны (МЭ)[49];

системы обнаружения и предотвращения вторжений в сеть (IPS/IDS);

средства шифрования трафика (VPN);

[49] Межсетевой экран - комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

UTM-устройства (Unified Threat Management), объединяющие в одной программно-аппаратной системе функции межсетевого экрана, системы обнаружения и предотвращения вторжений, антивирусного шлюза;

контроль доступа в сеть (NAC) и другие решения.

Лидером продаж на рынке средств обеспечения сетевой безопасности является компания Cisco, ей принадлежит почти четверть мирового рынка. Успех Cisco на рынке сетевой безопасности в значительной степени определяется ее известностью как производителя сетевых решений. Тем не менее, ей приходится постоянно конкурировать с другими ведущими производителями рынка сетевой безопасности: Check Point, Palo Alto Networks, Fortinet, Juniper Networks, McAfee, TippingPoint и др..

Рынок межсетевых экранов, на котором в основном лидирует Cisco, уменьшается, вытесняясь универсальными программно-аппаратными комплексами (UTM), которые объединяют в себе несколько технологий безопасности, таких как межсетевой экран следующего поколения, систему предотвращения вторжений, антивирус, антишпион, антиспам, и фильтрация контента. В настоящий момент рынок сетевой безопасности находится в условиях перехода своих клиентов к следующему поколению технологий. Сфера деятельности UTM-устройств продолжает расширяться, поскольку производители добавляют в них новые функции, такие как противодействие распределенному отказу в обслуживании (DDoS) , защиту от утечки данных (DLP) и др.

По данным аналитиков Gartner, объем мирового рынка UTM-устройств достиг 1,2 млрд. долл. в 2011 году, что на 19,6% больше по сравнению с 2010 годом.[50] Основные игроки этого рынка представлены на рис. 3.8.

[50] http://www.gartner.com/newsroom/id/1991815

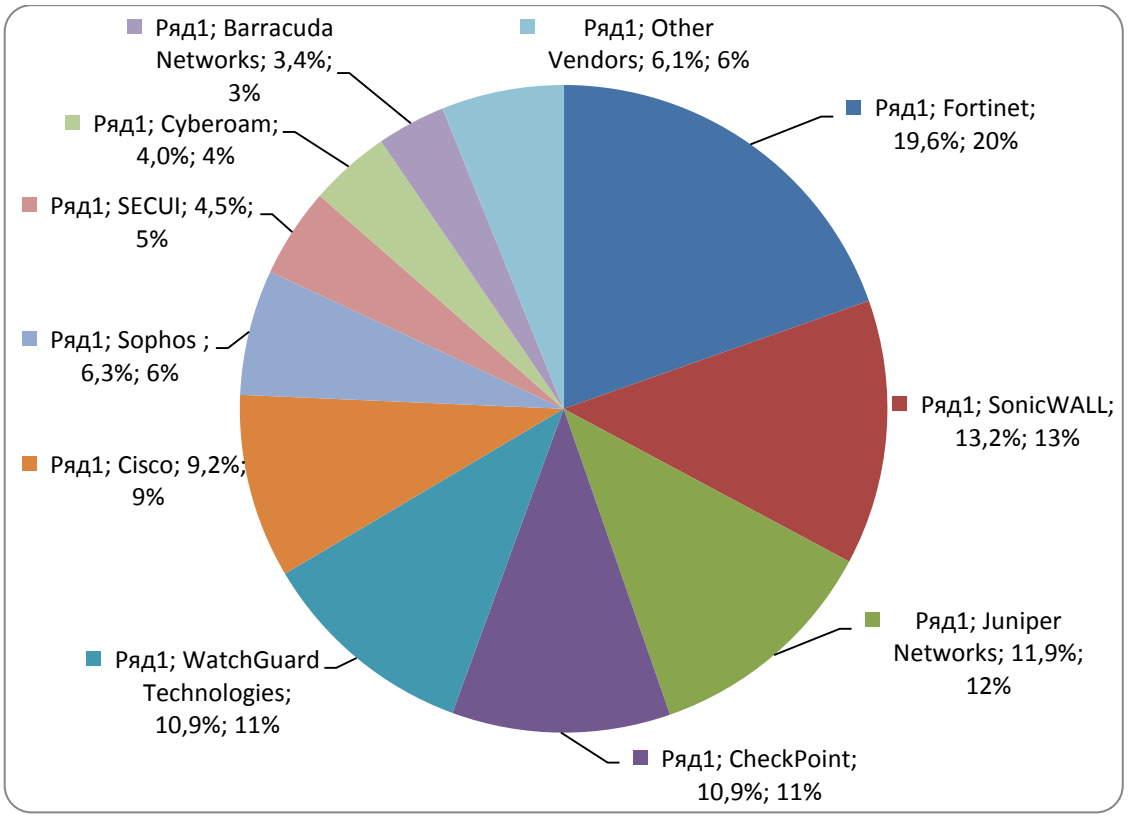

Рис. 3.8. Основные игроки мирового рынка UTM-устройств (2011 г.)

Объем этого рынка и прогноз доходов производителей UTM-устройств на мировом рынке в 2008-2016 годах приведены на рис. 3.9.[51]

Объемы продаж на российском рынке сетевой безопасности достигли в 2013 году 570 млн. долларов. Доходы компаний-производителей на российском рынке сетевой безопасности представлены на рисунке 3.10.

[51] http://www.academia.edu/4374092/Global_UTM_Market_Nov

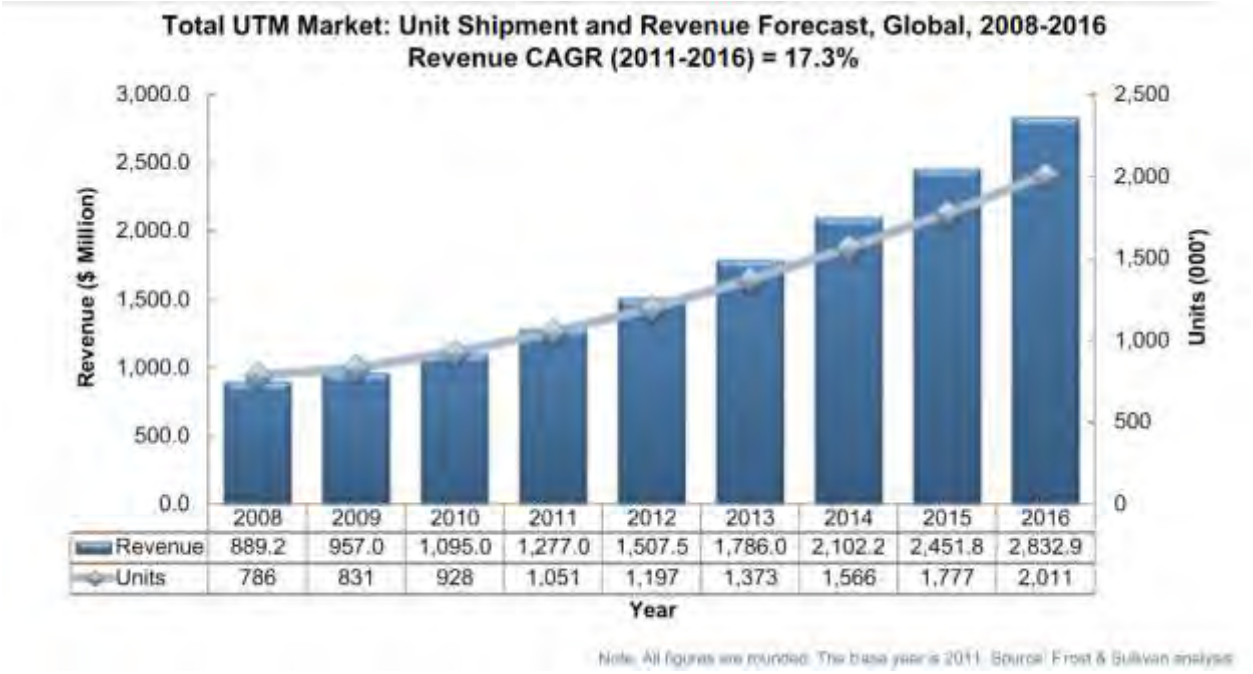

Рис. 3.9. Прогноз доходов производителей UTM-устройств на мировом рынке в 2008-2016 годах

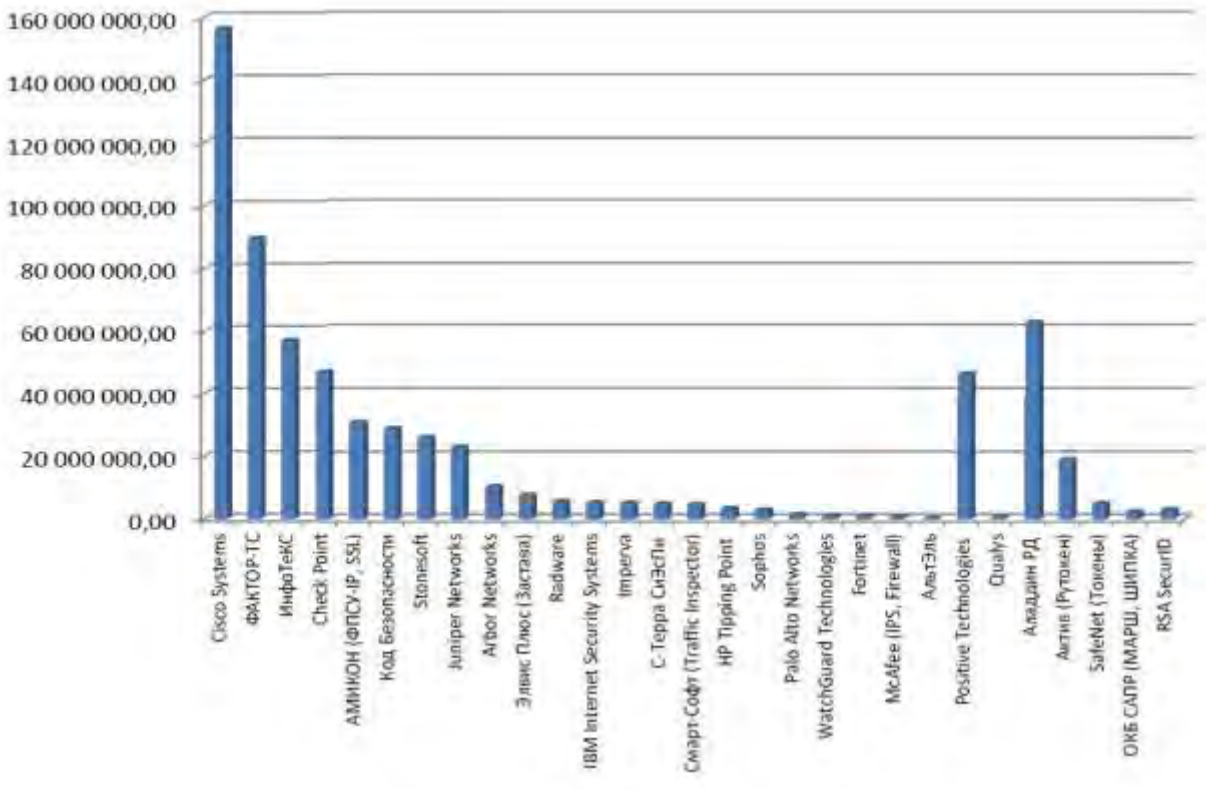

Рис. 3.10. Объемы продаж производителей (долл.) на российском рынке сетевой безопасности

На российском рынке средств обеспечения безопасности сети, как и на мировом, лидирующее положение занимает компания Cisco Systems. Практически в каждой организации стоит ее сетевое оборудование, при этом компания уделяет большое внимание вопросам сертификации по российским стандартам, что влияет на выбор потребителей. Кроме того, большое количество российских производителей показывают значительные объемы продаж в России. В основном это производители VPN-решений или различных токенов[52] для государственных структур, где требуется сертификат ФСБ России на средства криптографической защиты информации. Остальные позиции рынка практически полностью заняты зарубежными производителями.

Вплотную к рынку средств обеспечения сетевой безопасности примыкает рынок инструментальных средств анализа защищенности (сканеры уязвимости). Эти средства позволяют автоматизировать сканирование сети на проникновение и оценить состояние защищенности сетевых сервисов, осуществляют поиск уязвимостей системы и контроль соответствия стандартам безопасности, обеспечивают автоматический аудит безопасности и формирование отчетов. Лидирующее положение на этом рынке в России занимает российская компания Positive Technologies (XSpider и MaxPatrol), небольшую конкуренцию ей составляет только зарубежные компании Qualys (Qualys Guard Suite) и Outpost (OUTSCAN). Российский рынок инструментальных средств анализа защищенности сейчас оценивается примерно в 47 млн. долл.

В последние три года значительно вырос спрос на средства контентной фильтрации, обеспечивающие интеллектуальный процесс анализа Интернет трафика. Этот сегмент рынка тесно переплетается с другими

[52] Токен - электронное USB-устройство, которое служит для авторизации пользователя, для подписи документов (ЭП), для хранения закрытых ключей и сертификатов (технология PKI).

направлениями компьютерной безопасности. Как правило, функции контентной фильтрации на корпоративном уровне могут обеспечивать межсетевые экраны, системы обнаружения и предотвращения вторжений, маршрутизаторы, антивирусные программы. Реализация различных функций в одном устройстве или программном продукте может снизить затраты компаний на систему защиты, но функциональность таких систем может оказаться ограниченной. Существуют специализированные средства, разработанные непосредственно для контроля безопасности Интернет-соединений: системы мониторинга электронной почты, средства контроля Интернет-трафика, фильтры антиспам, антишпионские программы, защита от фишинговых атак и др.

Объем рынка средств контентной фильтрации возрастает в геометрической прогрессии с ростом спроса на безопасность по всему миру и к 2017 году может достигнуть отметки в 3 млрд. долл. (рис. 3.11).

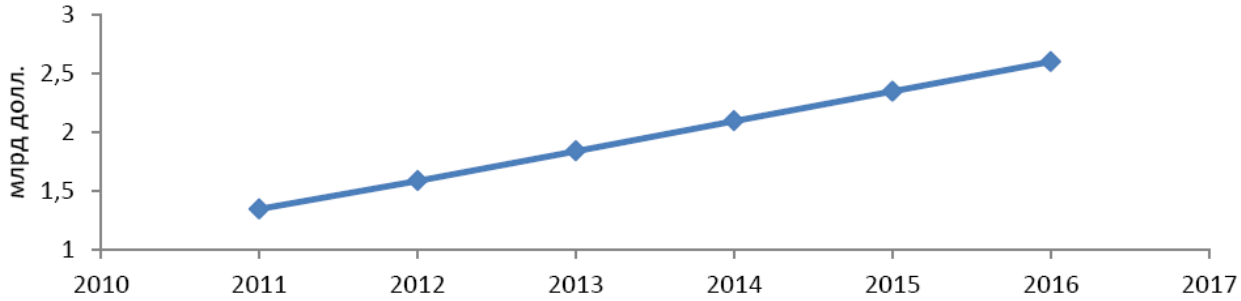

Рис. 3.11. Прогноз мирового рынка средств контентной фильтрации (The Radicati Group, Inc.)

Ведущими игроками на мировом рынке фильтрации веб-контента являются компании Barracuda Networks, Blue Coat Systems, Cisco IronPort, Clearswift, M86 Security, McAfee, SafeNet, Symantec, Trend Micro, Webroot, Websense, Zscaler, и другие.

Ведущими игроками на российском рынке средств контентной фильтрации являются американские компании: BlueCoat Systems, Websense, SafeNet, McAfee (рис. 3.12).

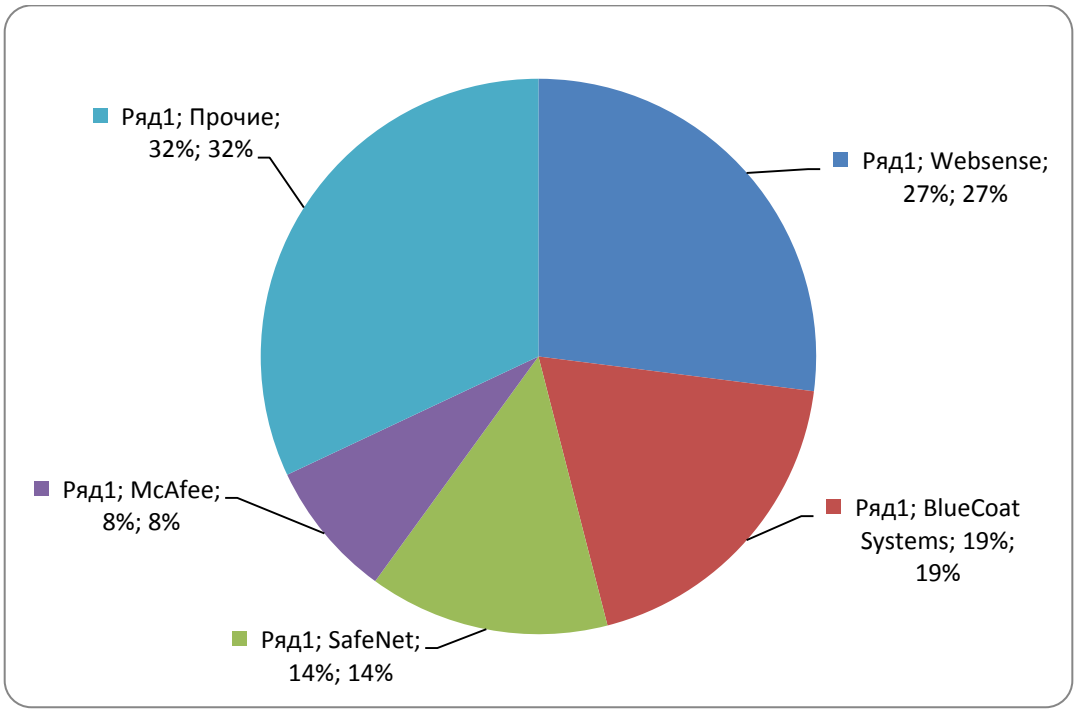

Рис. 3.12. Распределение долей рынка России по производителям

Законодательные инициативы Правительства РФ в 2012 году увеличили рынок фильтрации Интернет-ресурсов. Во-первых, Федеральный закон РФ от 28 июля 2012 г. N 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации» , обязавший учебные заведения фильтровать нежелательные Интернет-ресурсы. Во-вторых, в Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации» были внесены поправки в части ограничению операторами связи доступа к запрещенным ресурсам. Все это привело к возрастанию спроса на системы контентной фильтрации и появлению новых отечественных продуктов (МФИ софт, NetPolice Solutions).

В Российской Федерации разработка, производство, распространение средств криптографической защиты информации (СКЗИ) подлежит обязательному лицензированию[53] . Эти средства обеспечивают защиту конфиденциальности и целостности информации за счет криптографического преобразования информации. Надежность реализации криптографических (шифровальных) алгоритмов подтверждается сертификатами соответствия, выдаваемыми специальными государственными органами. Основными направлениями применения криптографических методов является шифрование конфиденциальной информации при ее хранении, обработке и передаче по каналам связи, а также использование электронной подписи для установления подлинности передаваемой информации.

Средства криптографической защиты могут функционировать самостоятельно или в составе других систем. Все большая интеграция технологий криптографии с другими технологиями безопасности затрудняет оценку этого рынка как отдельного сегмента. Значительную долю российского рынка криптографических средств занимает так называемая инфраструктура открытых ключей (PKI - Public Key Infrastructure). Инфраструктура открытых ключей использует цифровые сертификаты в качестве механизма проверки подлинности, надежной идентификации пользователя или компьютера. Основным компонентом PKI является система удостоверяющих центров для защиты взаимодействия пользователей между собой. Сертификаты PKI применяются для электронных торгов, при электронном обмене данными, в электронных формах и документах с электронной подписью, для защиты электронной почты, платежей и др.

В России насчитывается около 200 компаний, оказывающих услуги удостоверяющих центров. Значительная часть рынка приходится на не-

[53] Федеральный закон от 4 мая 2011 года № 99-ФЗ «О лицензировании отдельных видов деятельности»

сколько крупных производителей сертифицированных средств криптографической защиты, используемых в удостоверяющих центрах: ООО «Крипто-Про» (СКЗИ «КриптоПро»), ОАО «Инфотекс» (СКЗИ «ViPNet CUSTOM»), ЗАО «Сигнал-Ком» (СКЗИ «Крипто-КОМ»), ЗАО «МО ПНИЭИ» (СКЗИ «Верба») (рис. 3.13). Лидирующие позиции на этом рынке занимает компания «Крипто-Про».

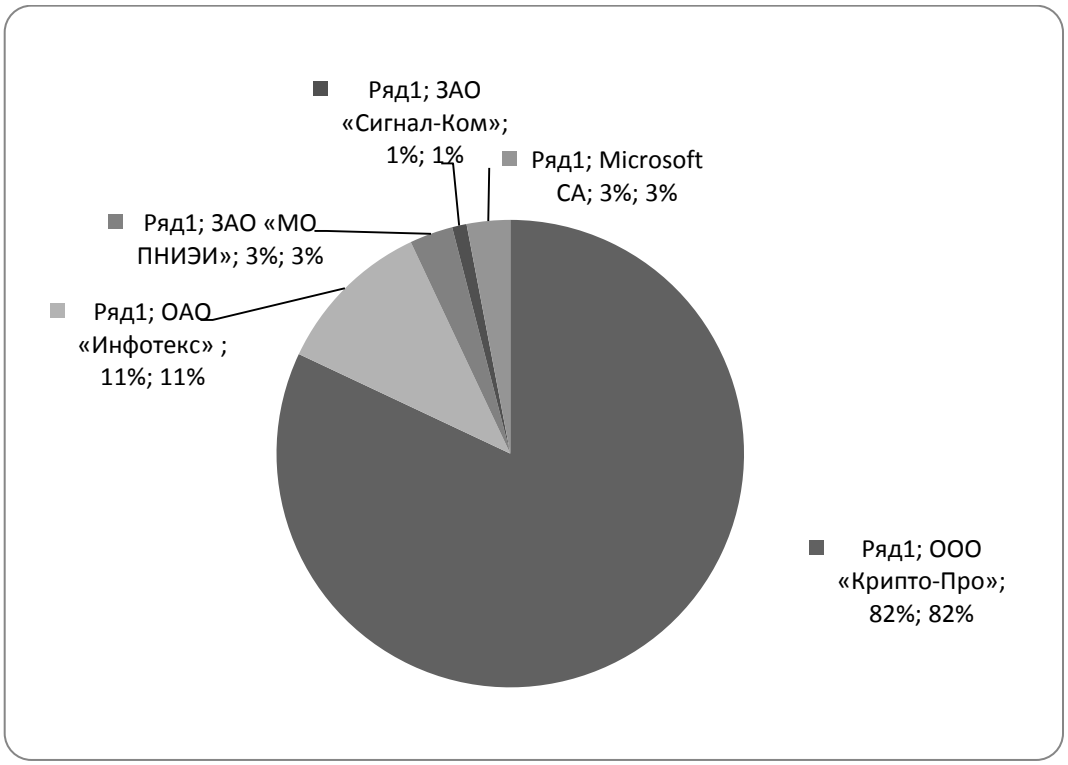

Рис. 3.13. Рынок PKI в России

Основные потребители услуг удостоверяющих центров являются организации, использующие электронную подпись в своей деятельности. На рынок ЭП главным образом влияет законодательство, регламентирующее все более широкое применение электронной подписи. Рост российского рынка ЭП за последние годы и прогноз его развития показан на рис. 3.14.

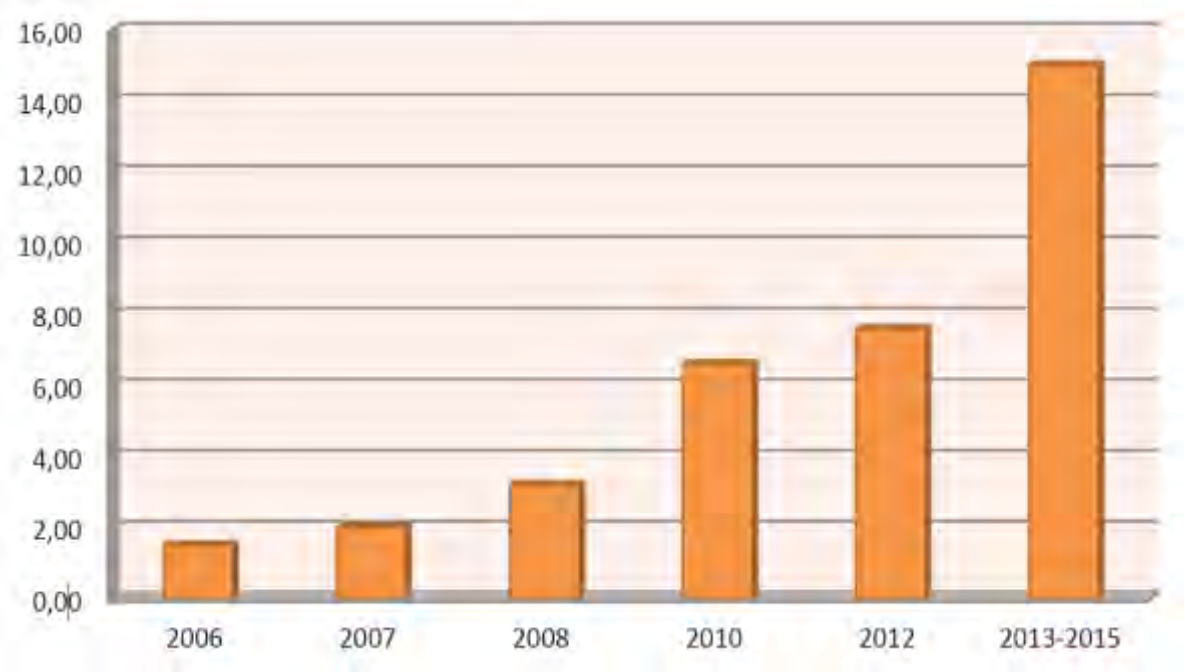

Рис. 3.14. Рост рынка ЭП в России, млрд руб.

Рынок PKI и ЭП динамично развивается, все большее количество организаций используют в своей деятельности электронный документооборот, что влечет и увеличение использования электронной подписи. Следующей сферой применения ЭП может стать использование электронной подписи физическими лицами при доступе к порталу госуслуг и проведении электронных платежей.

Любая информационная система генерирует большое количество сообщения в журналах событий, которые затруднительно просматривать и обрабатывать вручную. Системы сбора и анализа событий (SIEM - Security Information and Event Management) представляют собой набор инструментов, используемых менеджерами по безопасности и системными администраторами, для управления системами защиты, автоматического обнаружения инцидентов и своевременного реагирования на них. Данные системы осуществляют сбор и хранение информации, поступающей от других компонентов ИТ-инфраструктуры, мониторинг, анализ и выявление корреляции событий на основе накопленной статистики (рис.3.15). В связи с

ограниченностью ресурсов, выделяемых в большинстве организаций на безопасность информационных систем, одним из главных факторов при выборе системы сбора и анализа событий является простота внедрения и поддержки.

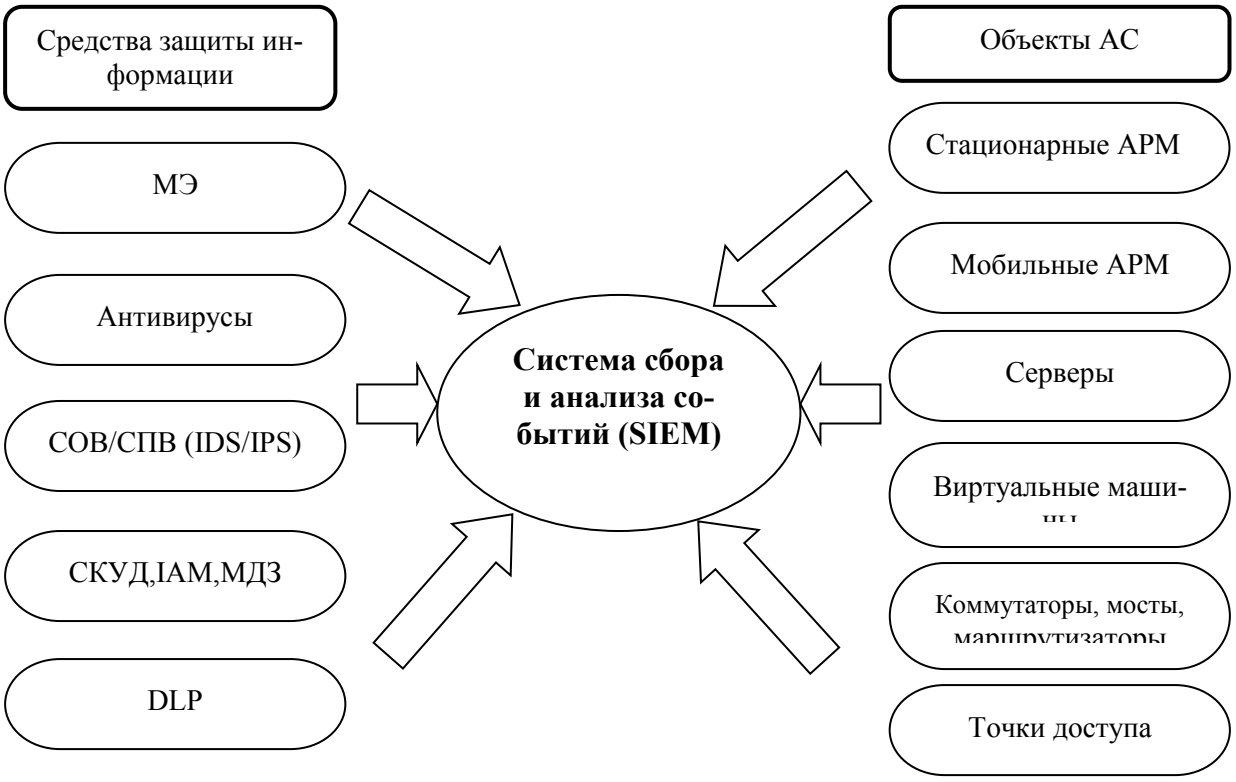

Рис. 3.15. Система сбора и анализа событий от компонентов ИТ-инфраструктуры

Мировой рынок программных SIEM решений вырос в 2012 году на 27,5% и достиг 976,4 млн. долл. Тогда как рынок аппаратных SIEM решений вырос только на 11,9% и достиг 384,1 млн. долл. По прогнозам аналитического агентства Frost&Sullivan мировой рынок SIEM к 2015 году достигнет 1,3 млрд. долларов (рис. 3.16).

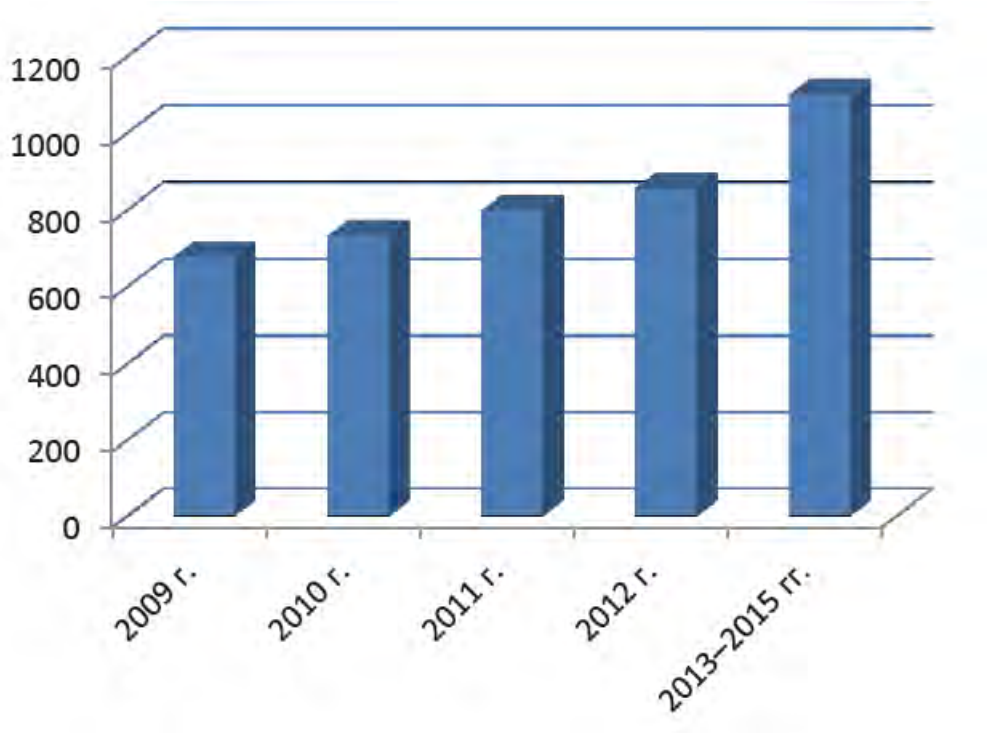

Рис. 3.16. Мировой рынок SIEM, млн. долл.

Основные игроки мирового рынка в этом секторе безопасности представлены на «магических квадрантах» компании Gartner (рис. 3.17) . Самым высоким рейтингом по мнению аналитиков Gartner обладает компания IBM Q1 Labs. Конкуренцию ее составляют производители McAfee Nitro, Splunk, LogRhythm и RSA.

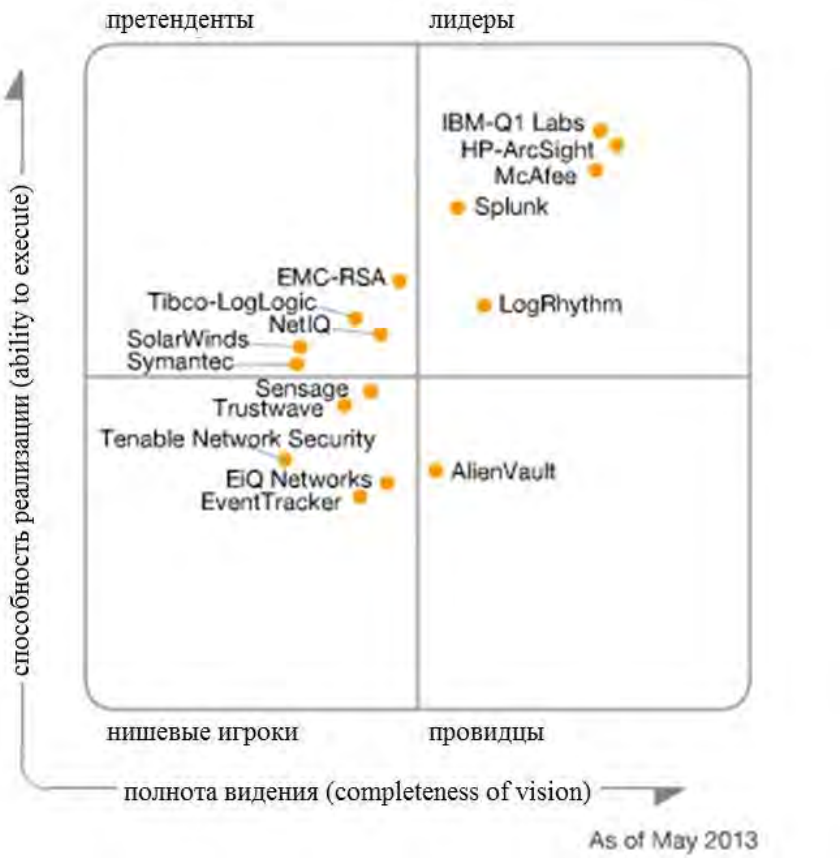

Рис. 3.17. Магический квадрант Gartner игроков рынка SIEM-решений по состоянию на май 2013 года

На российском рынке системы сбора и анализа событий распространяются медленнее, чем на мировом рынке, тем не менее, потребитель может выбирать из нескольких десятков различных SIEM-решений (рис. 3.18). Однако ведущие позиции занимают всего несколько крупных компаний: HP ArcSight, IBM Q1 Labs, Symantec SIM, RSA Envision, McAfee Nitro, Splunk и Tibco Loglogic. Лидирует на нашем рынке с максимальным количеством проектов компания HP ArcSight. Эта компания одной из первых появилась в России и по своему функционалу и интеграции с российскими популярными продуктами развивается быстрее других.

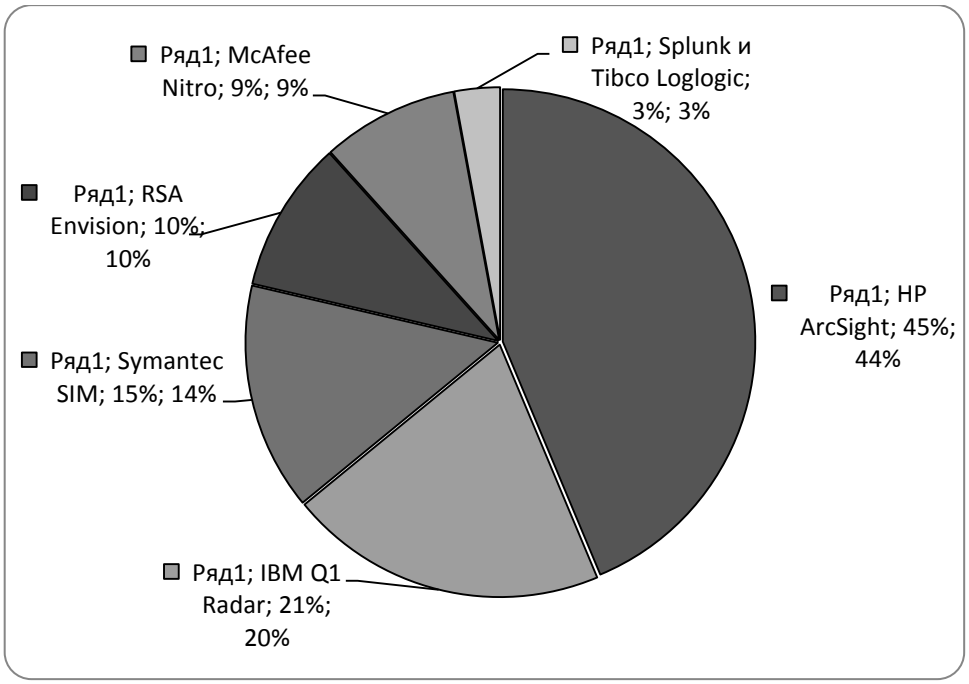

Рис. 3.18. Рынок SIEM-решений в России

К минусам SIEM-решений можно отнести дороговизну продукта, потому основными потребителями таких систем на данный момент являются банки и крупные предприятия, имеющие распределенные информационные системы.

Рынок систем сбора и анализа событий растет быстрыми темпами (рис. 3.19). Большинство российских компаний уже внедрили корпоративные системы безопасности и приходят к пониманию необходимости контроля над этими системами и мониторинга событий.

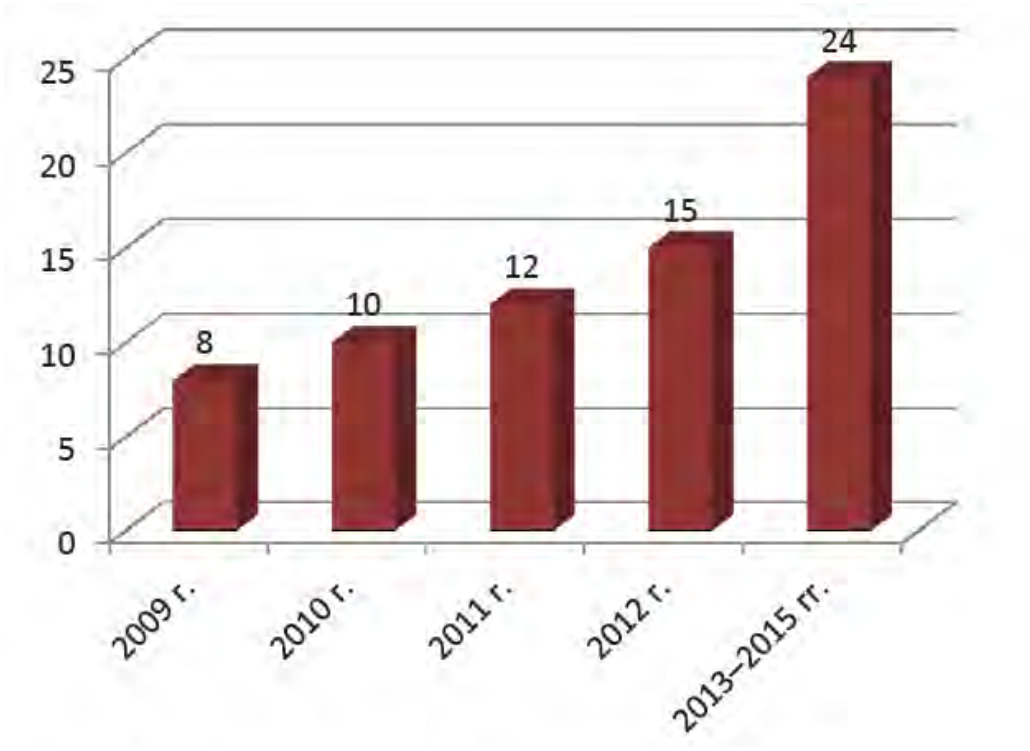

Рис. 3.19. Российский рынок SIEM, млн. долл.

Первой линией обороны системы защиты являются средства идентификации[54], аутентификации[55] и контроля доступа к сетевым, вычислительным и информационным ресурсам предприятия (IDM, Identity management; IAM, Identity and access management). Выделение этих средств в отдельную систему отражает потребность пользователей в объединении управления и синхронизации всех этих функций. Необходимость в таких системах возникает в крупных организациях с развитой информационной инфраструктурой, поскольку управление учетными записями и правами доступа вручную приводит к высоким расходам и ошибкам. Автоматизация единого управления учетными записями всех подключаемых систем позволяет контролировать права доступа и действия пользователей в соот-

[54] Идентификация - присвоение субъектам и объектам доступа идентификатора (уникальный признак субъекта или объекта доступа) и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов

[55] Аутентификация или подтверждение подлинности - процедура проверки принадлежности субъекту доступа предъявленного им идентификатора.

ветствии с ролевой моделью на протяжении всего жизненного цикла пользователя в системе.

Доступ пользователя в систему может производиться по обычному паролю, пин-коду или с использованием дополнительных аппаратных средств, таких как USB-токены, смарт-карты, сканеры отпечатков пальцев. Получают распространение и методы аутентификации, использующие мобильные устройства для генерации одноразовых паролей и технологии распознавание лиц и голоса. Нередко используются комбинация методов аутентификации из разных классов, например, двухфакторная аутентификация по смарт-карте и пин-коду.

Мировой рынок IAM – решений, несмотря на продолжающую рецессию, продолжает оставаться надежным и устойчивым. IAM является важнейшим компонентом стратегии обеспечения безопасности любого предприятия и, следовательно, получает более высокий приоритет. По оценкам экспертов многие крупные компании готовы потратить на эти решения около 8 процентов от общего бюджета на безопасность. Продукты IAM продолжают привлекать внимание и инвестиции, поскольку они позволяет предприятиям совершенствовать и автоматизировать важнейшие процессы управления доступом. Объем мирового рынка систем идентификации, аутентификации и контроля доступа в 2012 году ориентировочно составил около 10–11 миллиардов долларов. Предполагается, что этот рынок будет продолжать расти.

По материалам аналитической компании Gartner 80% крупных компаний, более половины средних компаний и 10—20% компаний малого бизнеса по всему миру уже внедрили у себя ту или иную форму IAM-решения. Основные игроки мирового рынка в этом секторе безопасности представлены на «магических квадрантах» компании Gartner (рис. 3.20) . Среди лидеров оказались как хорошо известны продукты традиционных

игроков – Oracle, CA Technologies, так и производители, специализирующиеся исключительно на IAM – SailPoint, Courion и компания Aveksa, которая в настоящий момент приобретена компанией EMS(RSA).

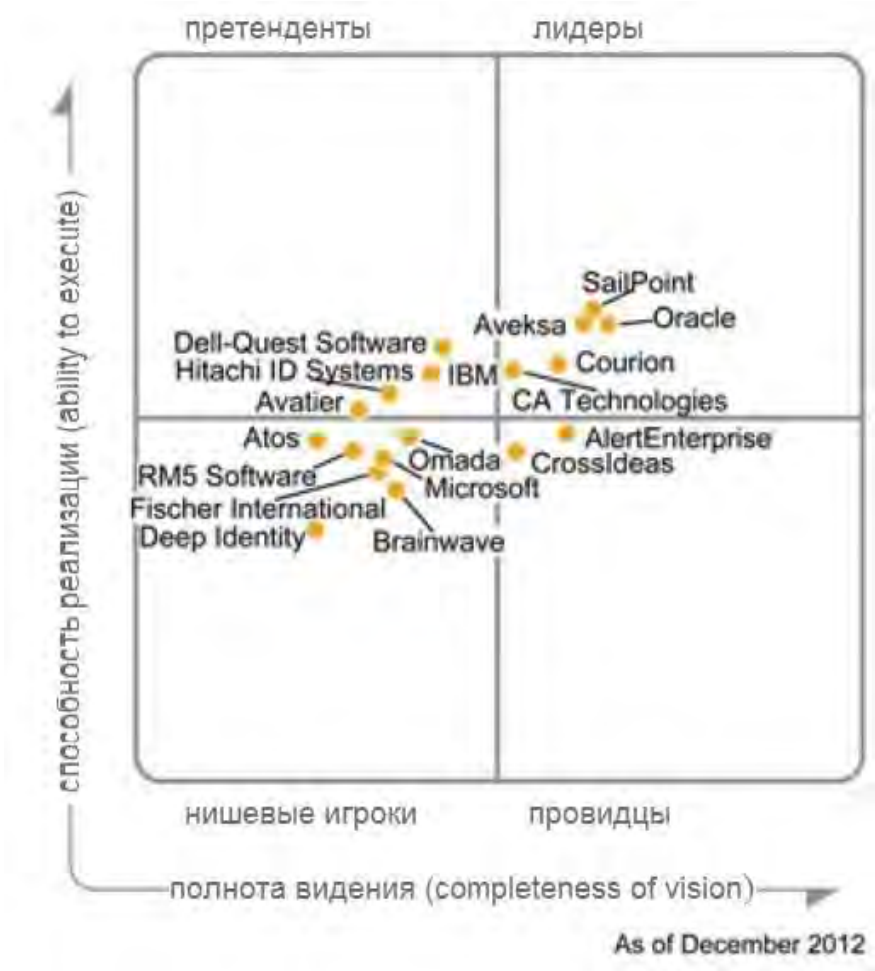

Рис. 3.20. Магический квадрант Gartner игроков рынка IAM-решений по состоянию на декабрь 2012 года

Российский рынок систем идентификации, аутентификации и контроля доступа только формируется. Эти решения используют менее 20% крупных компаний. Для огромного количества средних и малых российских компаний цена этих систем очень высока. Дело в том, что на российском рынке широко представлены только крупнейшие западные производители систем данного класса, такие как Oracle, IBM, Microsoft, Sun Microsystems, HP, ценовая политика которых рассчитана на крупный биз-

нес. Вторая проблема – это технологические сложности при внедрении, связанные с трудоемким организационным процессом построения полной ролевой модели компании. Еще одной причиной низкого внедрения IAM-систем является отсутствие требований регулирующих органов на наличие данных решений. Тем не менее, аналитики прогнозируют увеличение данного сегмента российского рынка к 2017 году до 10 раз по сравнению с 2012годом.

Законодательно все информационные системы, работающие со сведениями, составляющих государственную тайну, с персональными данными или конфиденциальной информацией, должны быть оборудованы современными программными или программно-аппаратными средствами для защиты данных от несанкционированного доступа (НСД). Под несанкционированным доступом к информации понимается любой доступ, нарушающий правила, установленные владельцем ресурса. Владелец должен защищать конфиденциальную и персональную информацию независимо от того, где она находится, на персональном компьютере, мобильном устройстве, в корпоративной сети или центре обработки данных. Обеспечение защиты такой информации должно проводиться с применением соответствующих мер, чтобы предотвратить несанкционированный доступ, изменение, раскрытие или уничтожение данных, их случайную потерю или уничтожение. Системы защиты от несанкционированного доступа могут применять современные технологии идентификации и аутентификации пользователей, контроль утечек конфиденциальной информации, разграничение доступа и управлением учетными записями пользователей информационных систем, также обычно применяется шифрование информации.

Рынок систем защиты от несанкционированного доступа в России достаточно широк, в продаже имеются продукты десятков фирм. Все сред-

ства защиты персональных или конфиденциальных данных от несанкционированного доступа должны быть сертифицированы ФСТЭК Россиипо требованиям руководящих документов (РД) и на отсутствие недекларированных возможностей. Поэтому основными игроками на этом рынке являются российские компании. На рисунке 3.21 и в таблице 3.1 представлены компании - участники рынка средств защиты информации от НСД и доля их участия в этом рынке.

Таблица 3.1.

Участники рынка средств защиты информации от НСД.

Игроки рынка СЗИ от НСД	Продукт	Степень охвата рынка
«Код Безопасности» (Группа компаний «Информзащита»)	ПАК «Secret Net» и электронный замок «Соболь»	52%
ОКБ САПР	ПАК «Аккорд» и «Аккорд-АМДЗ»	25,8%
ООО «Анкад»	ПАК «Криптон»	10,7%
Центр защиты информации «Конфидент»	ПК «Dallas Lock»	5,8%
Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН)	ПК «Аура»	3,4%
ЗАО НПП «ИТБ»	ПК «Панцирь»	2,3%
ООО «ТСС»	ПАК «Diamand ACS»	0,2%

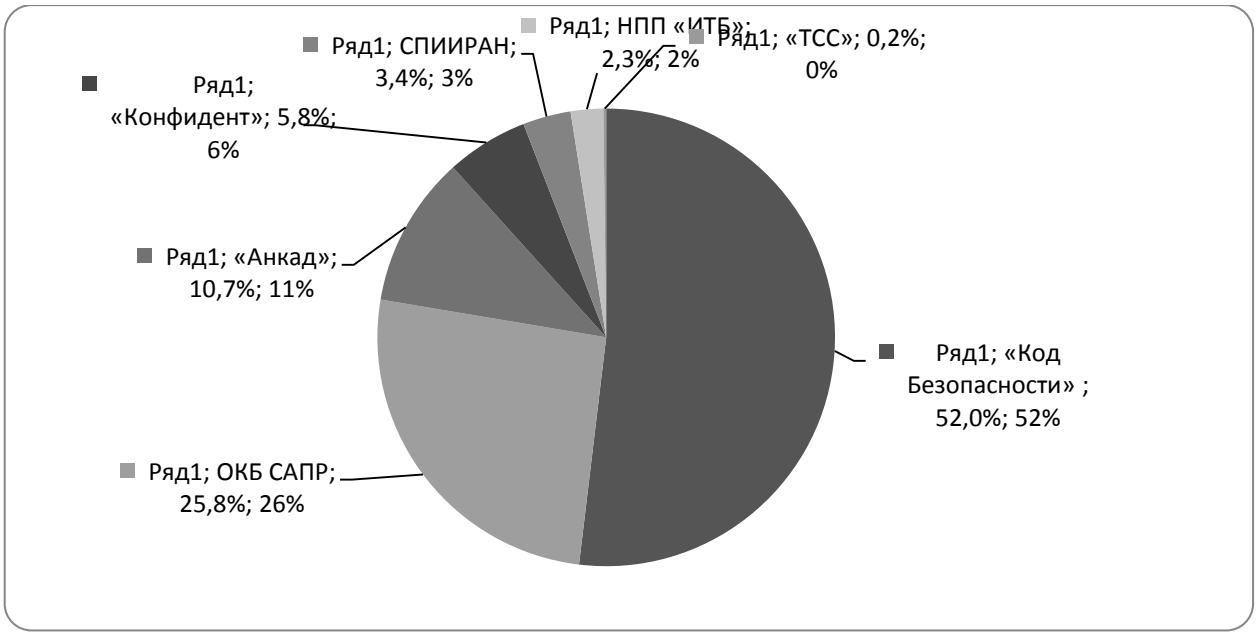

Рис. 3.21. Степень охвата рынка производителями систем защиты информации от несанкционированного доступа

Общий объем продаж средств защиты информации от несанкционированного доступа растет с каждым годом и достиг к 2012 году в России 1 млрд. рублей (рис. 3.22).

Рис. 3.22. Динамика роста рынка систем защиты от НСД

На выбор потребителя влияет совместимость системы защиты от несанкционированного доступа с операционной системой, класс защищенности, цена изделия, временные характеристики, простота установки и эксплуатации.

Обнаружить или блокировать несанкционированную передачу конфиденциальной информации из информационной системы по какому-либо каналу коммуникации помогают средства контроля утечек данных (DLP, Data Loss Prevention). Важные и конфиденциальные данные могут включать в себя, например, интеллектуальную собственность компании, финансовые документы, документы стратегического планирования, информацию о сотрудниках, данные о клиентах. Каждый сотрудник и каждое устройство, которое хранит информацию о компании, является потенциальной угрозой утечки данных. К утечке данных может привести и недостаточная осведомленность сотрудников, они могут не обращать внимания на тот факт, что их поведение или действия небезопасны. Очень часто воспринимается как должное, что все сотрудники знают о мерах безопасности и предосторожности для защиты конфиденциальных корпоративных данных. Конфиденциальные данные могут быть скопированы и вынесены за пределы организации с помощью периферийных устройств, таких как USB-устройства, мобильные устройства, подключаемые к компьютеру беспроводным способом, фото- и видеокамеры, или переданы по сетевым каналам через электронную почту, программы-мессенджеры и Интернет.

По мере того как возрастает количество подключенных к Интернету устройств, предотвращения утечки данных становится все более важной задачей для любой компании. Технологии предотвращения утечки данных выполняют проверку содержимого в состоянии покоя или движения и мо-

гут использоваться как для простого уведомления о нарушении, так и для активной блокировки. Продукты DLP поддерживают сложные методы обнаружения контента, которые выходят за рамки простого поиска по ключевым словам и регулярным выражениям.

Мировой рынок DLP-систем по оценке аналитиков Gartner в течение последних семи лет проявляет устойчивые тенденции стабильного роста. Объем этого сектора мирового рынка составил в 2012 году - 535 млн. долл., в 2013 году - около 670 млн. долл. (рис. 3.23) .

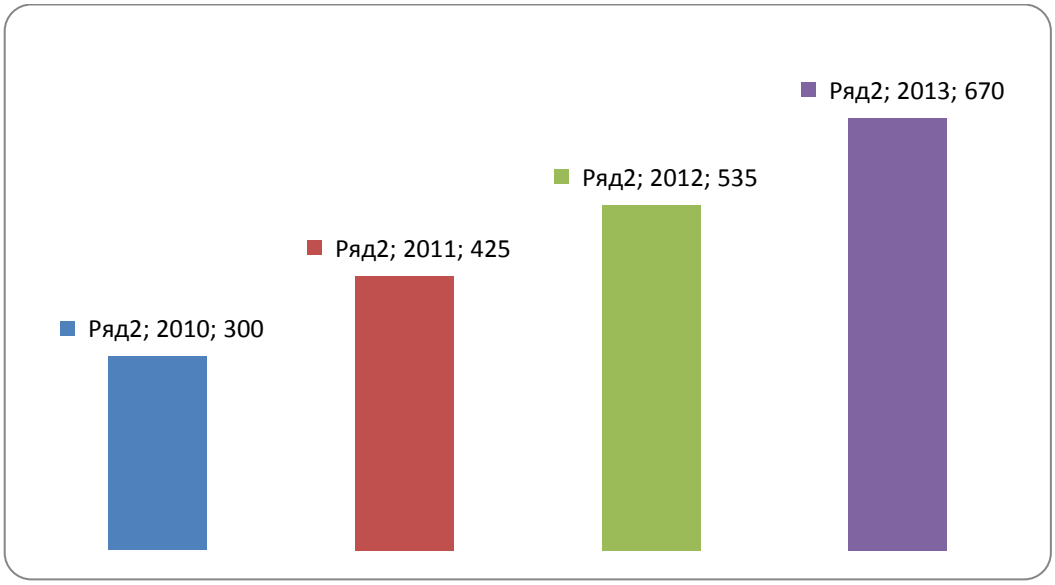

Рис. 3.23. Динамика мирового рынка систем предотвращения утечек данных (млн. долл.)

Основные игроки мирового рынка в секторе безопасности DLP-систем представлены на «магических квадрантах» компании Gartner (рис. 3.24) . Лидирующие положение на рынке поставщиков, предлагающих системы контроля утечек данных, занимают компании, которые широко известны другими своими продуктами для обеспечения безопасности информации в организациях. Это, прежде всего, Symantec, Websense, RSA, McAfee, CA Technologies и Verdasys.

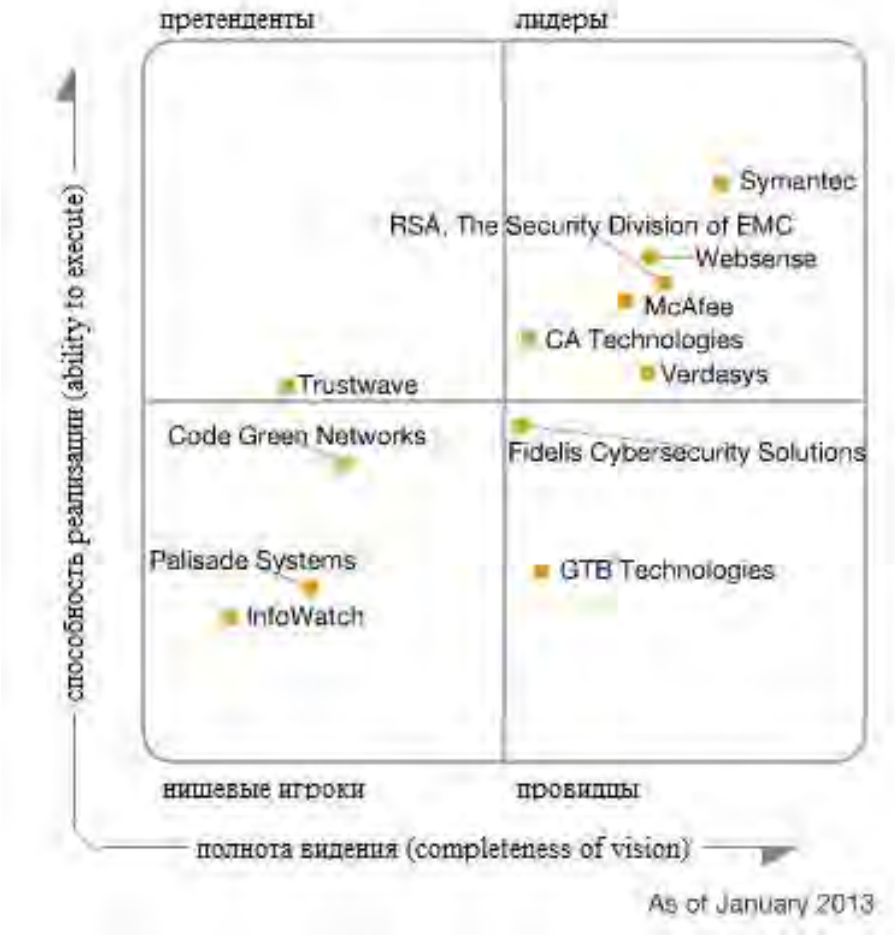

Рис. 3.24. Магический квадрант Gartner игроков рынка DLP-систем по состоянию на январь 2013 года

Российский рынок DLP-решений также растет, но остается небольшим по объему по сравнению с другими секторами рынка средств защиты информации. В большинстве случаев потребители пока не видят большой угрозы в своих собственных сотрудниках. Противодействовать инсайдерам можно и с помощью IAM-решений за счет правильного распределения ролей пользователей, дополнительно можно использовать функции контентной фильтрации Интернет - трафика. Кроме того в другие средства защиты, такие как многофункциональные UTM-устройства, системы электронного документооборота, производители часто встраивают лицензированные DLP-модули. Российское законодательство также никак не регулирует

применение систем защиты от утечек конфиденциальных данных, но в то-же время это обеспечивает высокую конкурентную составляющую, заставляя производителей повышать функциональность и качество своих решений.

Пик роста в России рынка чистых DLP-решений приходится на последние три года, когда он превысил 40% (рис. 3.25). И темпы роста продолжают сохраняться. К концу 2013 года DLP-рынок в России достиг объема в 76-78 млн. долл.

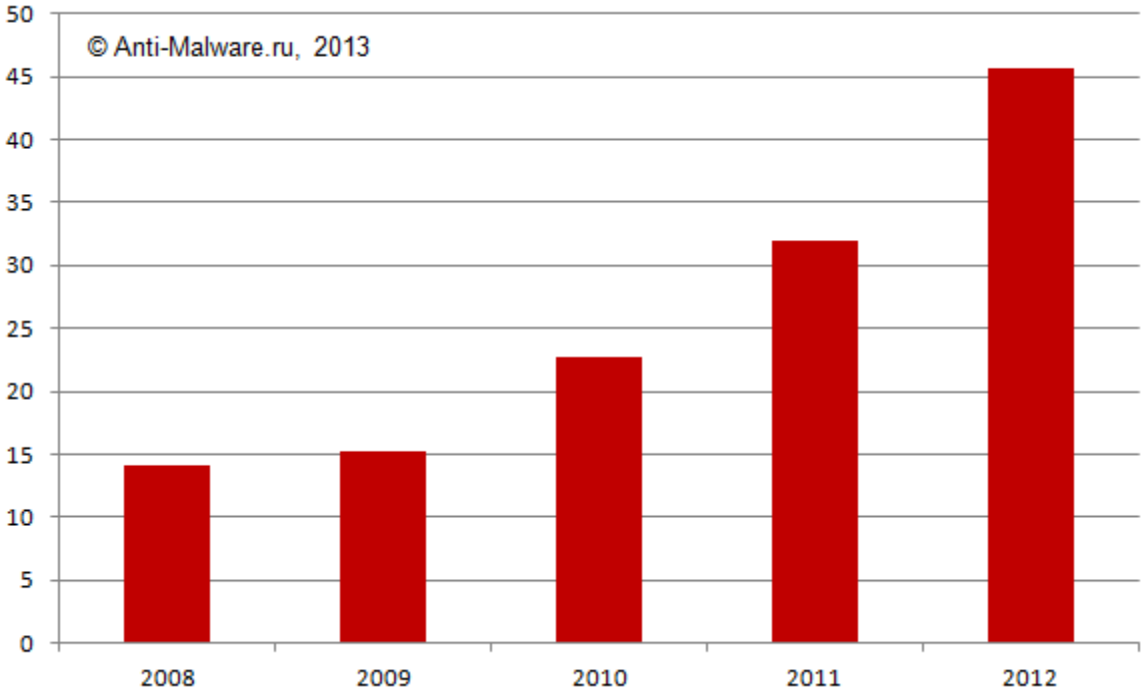

Рис. 3.25. Динамика объема рынка DLP в России 2008-2012 (млн. долл.)

На российском рынке лидируют по объему продаж российские компании InfoWatch ($20,4 млн.), «Инфосистемы Джет» ($11,8 млн.) и Zecurion ($9,5 млн.). За ними следуют зарубежные производители Websense (5,2 млн.) и Symantec ($2,6 млн.) (рис. 3.26).

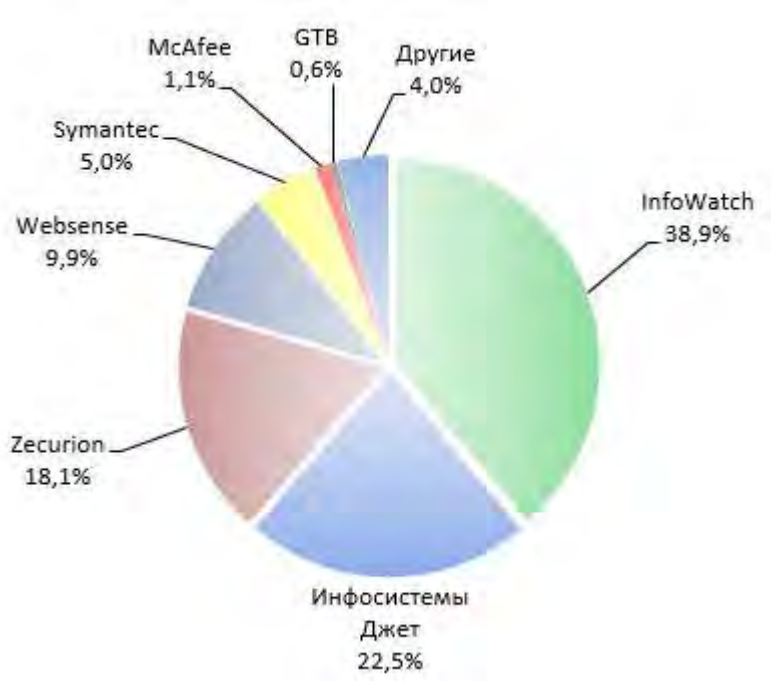

Рис. 3.26. Доли рынка ключевых игроков DLP-систем в России за 2012 год

Заказчиками DLP-решений в России в основном являются крупные компании и госструктуры. Средний и малый бизнес пока практически не использует эти системы ввиду высокой стоимости услуг по внедрению DLP-решений. В перспективе этот сектор рынка будет расширен за счет «облегченных» версий (DLP – Lite), которые используют менее сложные методы обнаружения и поддерживают ограниченное число протоколов.

Кроме рынка технологий развивается и рынок услуг, который включает в себя проектирование систем защиты, аудит, услуги по сертификации продукции по требованиям информационной безопасности, образовательные услуги и консультирование по вопросам информационной безопасности.

Объемы продаж для каждого сегмента российского рынка средств защиты информации в 2013 году показаны на рис.3.27.

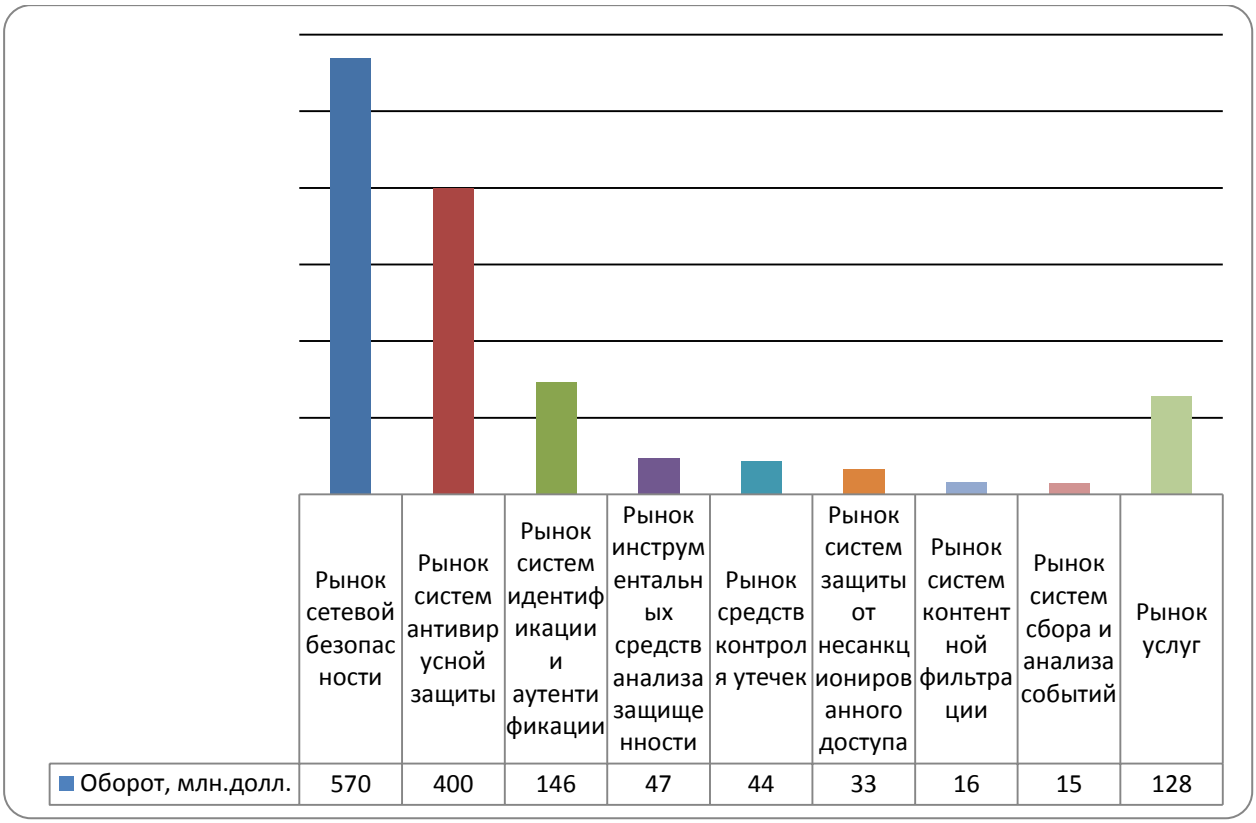

Рис. 3.27. Интегральная оценка российского рынка средств защиты информации (2012 г.)

Российский рынок средств защиты, как это следует из его анализа, более консервативен и менее прозрачен, чем западный, слабо используются стандарты безопасности, некоторые международные тенденции. Очень немногие отечественные решения безопасности находятся в числе продуктов, являющимися лидерами на мировом рынке.

Из анализа рынка можно сделать вывод, что в тех областях безопасности, который жестко регламентируется законодателями, например, таких как рынок систем защиты от несанкционированного доступа или средств криптографической защиты информации, он является рынком несовершенной конкуренции. Средства и механизм защиты информации, представленные на рынке, необходимо рассматривать не только как технические устройства, а как специфические интеллектуальные продукты челове-

ческой деятельности и особого рода конкурентные товары во взаимоотношениях хозяйственных субъектов и государственных органов.

Широкий спектр аппаратных и программных средств обеспечения безопасности информации, представленный на рынке, затрудняет потребителям их выбор. При выборе средств защиты информации сотрудникам информационных служб таможенных органов рекомендуется ориентироваться на выполнение требований ФСБ Россиии ФСТЭК, цену продукта, простоту его использования, совместимость с операционной системой и аппаратной платформой. Также предлагается отслеживать аналитические материалы и тесты известных мировых независимых испытательных лабораторий, в первую очередь это консалтинговые компании Gartner, Frost & Sullivan и anti-malware.ru. Лидерами их рейтингов являются ведущие производители с точки зрения возможностей продукта, анализа рынка, опыта заказчиков в работе с решениями производителя и стратегического видения.

3.2. Управление рисками и инвестициям в обеспечение безопасности информации

3.2.1. Возможные угрозы безопасности в автоматизированных информационных системах таможенных органов

Внедрение новых информационных технологий должно идти вместе с развитием систем защиты. Если на первых этапах жизненного цикла информационных систем не уделить должного внимания проблеме информационной безопасности, то в дальнейшем возрастает риск столкнуться с проблемой незащищенности всей системы перед угрозами неправомерного доступа, копирования и изменения информации, представленной в электронном виде. Угрозы безопасности информации реализуются их источниками, которые могут воздействовать на объекты информационных систем

таможенных органов. Если угроза реализована, то информация теряет часть или все свойства безопасности.

В Концепции обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года сформулированы основные угрозы обеспечения информационной безопасности таможенных органов Российской Федерации . По своей общей направленности угрозы информационной безопасности таможенных органов подразделяются на следующие виды:

угрозы конституционным правам и свободам человека и гражданина в информационной сфере деятельности таможенных органов;

угрозы информационному обеспечению государственной политики в области таможенного дела;

угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей таможенных органов в ее продукции, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов в области таможенного дела;

угрозы безопасности информационных и телекоммуникационных средств и систем таможенных органов.

Угрозами безопасности информационных и телекоммуникационных средств и систем таможенных органов могут являться:

нарушения технологии обработки информации ограниченного доступа, обрабатываемой в таможенных органах;

нарушение законных ограничений на распространение информации ограниченного доступа, обрабатываемой в таможенных органах;

противоправные сбор и использование информации ограниченного доступа, обрабатываемой в таможенных органах;

компрометация ключей и средств криптографической защиты информации;

перехват, дешифрование или подмена информации в ведомственной интегрированной телекоммуникационной сети ЕАИС таможенных органов или передаваемой при информационном взаимодействии ФТС России с таможенными администрациями иностранных государств, международными организациями, федеральными органами исполнительной власти Российской Федерации, организациями банковской сферы и участниками внешнеэкономической деятельности;

несанкционированный доступ к информации, находящейся в базах данных таможенных органов;

неправомерное использование должностными лицами и работниками таможенных органов Российской Федерации информации, к которой им предоставлен доступ, для исполнения должностных обязанностей;

разработка и распространение программ (компьютерных вирусов), нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения таможенных органов;

уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

использование при разработке и модернизации автоматизированных информационных систем таможенных органов Российской Федерации несертифицированных по требованиям безопасности информационных технологий, средств вычислительной техники, телекоммуникации и связи, программного обеспечения и средств защиты информации;

утечка информации ограниченного доступа, обрабатываемой на объектах информатизации таможенных органов Российской Федерации, по техническим каналам.

Данный список угроз в полной мере относится в целом к информационной сфере таможенных органов, как к документированной информации и средствам ее обработки, так и к информации, представленной в электронном виде, и техническим средствам обработки такой информации.

Конкретные вопросы защиты информации в деятельности таможенных органов Российской Федерации относятся к ведению Федеральной таможенной службы. На основе Концепции обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года приняты конкретные приказы, определяющие конкретные меры по обеспечению компьютерной безопасности.

Среди угроз субъектам таможенной деятельности в информационной сфере наиболее критичных по своим последствиям следует выделить угрозы нарушения таких свойств информации, как целостность, конфиденциальность и доступность. Данные типы угроз могут быть реализованы вследствие таких событий[56], как:

[56] Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). - М: Гостехкомиссия России, 2001.

несанкционированное ознакомление, кодирование или хищение (утечка);

несанкционированная модификация, либо уничтожение;

несанкционированное блокирование доступа к информации.

Основными источниками угроз информационной безопасности являются:

неблагоприятные события природного, техногенного и социального характера;

последствия ошибок проектирования и реализации информационных систем;

сбои, отказы, разрушения/повреждения программных и технических средств;

ошибки эксплуатации пользователей или операторов;

работники таможенных органов, реализующие угрозы информационной безопасности с использованием легально предоставленных им прав и полномочий (внутренние нарушители);

работники таможенных органов, реализующие угрозы информационной безопасности вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками таможенных органов, но осуществляющие попытки несанкционированного доступа (внешние нарушители).

Современные угрозы носят комплексный характер. На фоне уже обычных вирусных и сетевых атак достаточно регулярно возникают целенаправленные устойчивые комплексные атаки, о которых появляются сообщения в прессе. Общими чертами этих атак является использование методов социальной инженерии и осведомленность о наличии уязвимостей в информационной системе компании. Методами эффективного противодействия угрозам является наличие у организации не только технологий

защиты, но и методик процессов реагирования на угрозы, в том числе построение модели угроз, модели нарушителя и оценка рисков.

Модель угроз строится для конкретной информационно-вычислительной системы и содержит описание защищаемых информационных ресурсов, источников и методов реализации угроз безопасности информации, уязвимостей, используемых источниками угроз; типов и масштабов возможных потерь. Выявление всех угроз в ЕАИС ТО и построение реальной модели угроз позволяет выявить существующие источники угроз безопасности информации, разработать эффективные меры противодействия и оптимизировать затраты на защиту информации.

Структурируя защищаемые информационные ресурсы, можно построить обобщенную структуру модели угроз безопасности информации в АИС в виде таблицы соответствия (матрицы): информационный ресурс – угроза (рис. 3.28). В тех ячейках таблицы, где угроза актуальна для защищаемого объекта, ставится значение вероятности реализации угрозы в отношении данного ресурса, в противном случае вероятность равна нулю. Таким образом, мы получаем возможность наглядно оценить опасность определенных угроз, и уровень уязвимости ресурсов защищаемого объекта.

	Угроза 1	Угроза 2	Угроза 3	Угроза 4
Ресурс 1	P11	P12	P13	P14
Ресурс 2	P21	P22	P23	P24
Ресурс 3	P31	P32	P33	P34

Рис. 3.28. Пример модели угроз

Вероятность реализации угрозы в отношении каждого информационного ресурса может определятся экспертным методом в соответствии с таблицей 3.2.

Таблица 3.2.

Шкала значений вероятности реализации угрозы

Вероятность реализации угрозы	Описание уровня
Нереализуемая	Используемые средства защиты и методы их использования гарантируют защиту по отношению к данному типу угроз в пределах заданной уязвимости (используются сертифицированные средства защиты)
Минимальная	У источника угрозы недостаточно мотиваций или возможностей, либо существующие средства контроля способны предотвратить или, по крайней мере, значительно помешать использованию уязвимости
Средняя	Источник угрозы мотивирован и обладает возможностями, но существующие средства контроля могут препятствовать успешному использованию уязвимости
Высокая	Источник угрозы имеет высокие мотивации и достаточные возможности, а методы контроля для предотвращения проявления уязвимости не гарантируют защиту.
Критическая	Уровень мотивации, технические и организационные возможности источника угроз превышают соответствующие параметры защиты

Большинство современных методик построения модели угроз базируются либо на статистических методах, либо на экспертном оценивании. Прогнозировать угрозы можно исходя из собственной статистики нарушений безопасности или чужих статистических отчетов. При отсутствии статистической информации оценка угроз может быть проведена экспертным путем. Эксперты ранжируют угрозы по их значимости и вероятности реализации, исходя из своего опыта и знаний анализируемой системы.

При построении модели угроз необходимо использовать список угроз, содержащийся в стандартах информационной безопасности и доку-

ментах ФСТЭК Россиии ФСБ России. Модели угроз составляются на основе постоянно изменяющихся данных, с течением времени на защищаемом объекте могут проявиться новые уязвимости, а соответственно возникнуть новые угрозы. Поэтому модель угроз должна быть динамичной и периодически пересматриваться и обновляться на основе анализа статистических данных о нарушениях информационной безопасности, результатов исследований и опыта эксплуатации автоматизированных систем. Построенная модель угроз является исходными данными для оценки рисков информационной безопасности.

3.2.2. Оценка рисков информационной безопасности в таможенных информационных системах

Решение задачи построения системы безопасности должна начинаться с формулирования требований к разрабатываемой системе. В таможенных органах должна быть разработана методика определения ценности информации или ее критичности, идентифицированы угрозы безопасности в отношении сформированного перечня информационных активов и оценены риски реализации этих угроз. Анализ рисков проводится для оценки реальных угроз нарушения информационной безопасности и разработки мер, выполнение которых позволит минимизировать эти угрозы. При анализе рисков осуществляется:

классификация информационных активов;

идентификация и анализ угроз и уязвимостей;

формирование перечня источников угроз;

оценка рисков информационной системы.

В процессе анализа рисков проводится оценка критичности идентифицированных уязвимых мест и возможности их использования потенциальным злоумышленником для осуществления несанкционированных действий.

Оценка критичности (или ценности) каждого информационного продукта определяется собственником, владельцем или пользователем данного продукта. Ценность информационного продукта таможенных органов рассмотрена в подпараграфе 1.4.3.

Проведя выборку информации по ее ценности, мы получаем перечень информационных ресурсов, требующих защиты. Основываясь на уровне ценности информации необходимо разбить всю защищаемую информацию по степени ценности на несколько уровней, и в дальнейшем, при организации защиты, отталкиваться от этой схемы. Этим, в перспективе, достигается снижение затрат на систему защиты информации, и в определенной степени упрощается схема документооборота в таможенном органе. Кроме того, надо учесть, что необходимость защиты той или иной информации зависит и от длительности ее существования. С течением времени, как правило, информация перестает быть актуальной и необходимость в ее защите отпадает.

После того как защищаемые ресурсы конкретизированы, необходимо идентифицировать угрозы информационной безопасности в отношении сформированного перечня информационных ресурсов.

Построенная модель угроз является исходными данными для оценки рисков информационной безопасности. Оценка рисков информационной безопасности производится на основании оценивания:

– вероятности реализации угроз выявленными или предполагаемыми источниками угроз, зафиксированными в моделях угроз;

– цены ущерба от нарушений безопасности для рассматриваемых информационных ресурсов.

Большинство современных методик анализа рисков базируются либо на вероятностно-статистических методах, либо на экспертном оценивании. Риски могут оцениваться качественно и количественно. Качественная

оценка рисков направлена на выявление существующих рисков и их ранжирование по значимости и вероятности реализации экспертным путем. Количественная оценка уточняет качественные результаты и помимо оценки вероятности возникновения включает еще оценку величины ущерба.

Какой метод оценки рисков выбрать, зависит от того, насколько точно можно рассчитать стоимость информационных активов, оценить вероятность реализации угрозы и степень уязвимости информационной системы к данной угрозе.

К сожалению, статистические данные угроз редко доступны. На практике, оценка рисков часто основана на субъективной и качественной оценке экспертами по безопасности рисков ущерба для информационных ресурсов и уменьшения этих рисков за счет внедрения контрмер.

Рассмотрим механизм качественного оценивания рисков на основе нечеткой логики[57]. Он требует формирования оценок ключевых параметров и представления их в виде нечетких переменных. Этот метод базируется на экспертных оценках. К экспертной оценке рисков информационной безопасности привлекаются сотрудники таможенных органов, обладающие необходимыми знаниями, образованием и опытом работы.

Нечеткие описания при анализе риска появляются в связи с неуверенностью эксперта, что возникает в ходе различного рода классификаций. Тогда применение нечетких описаний означает следующее:

1. Эксперт строит лингвистическую переменную со своей шкалой значений. Например, переменная «Угрозы информационной безопасности» может обладать шкалой вероятности событий: «Нереализуемая; Минимальная; Средняя; Высокая; Критическая» (табл. 2.1)

[57] Заде Л. Понятие лингвистической переменной и ее применение к принятию приближенных решений, М.: Мир, 1976.

2. Чтобы конструктивно описать лингвистическую переменную, эксперт выбирает соответствующий ей количественный признак — например, сконструированный специальным образом показатель уровня угрозы, который принимает значения от нуля до единицы.

3. Далее эксперт каждому значению лингвистической переменной сопоставляет функцию принадлежности уровня угроз тому или иному нечеткому подмножеству. Общеупотребительными функциями в этом случае являются трапециевидные функции принадлежности (Рис. 3.28). Верхнее основание трапеции соответствует полной уверенности эксперта в правильности своей классификации, а нижнее — уверенности в том. что никакие другие значения интервала (0,1) не попадают в выбранное нечеткое подмножество.

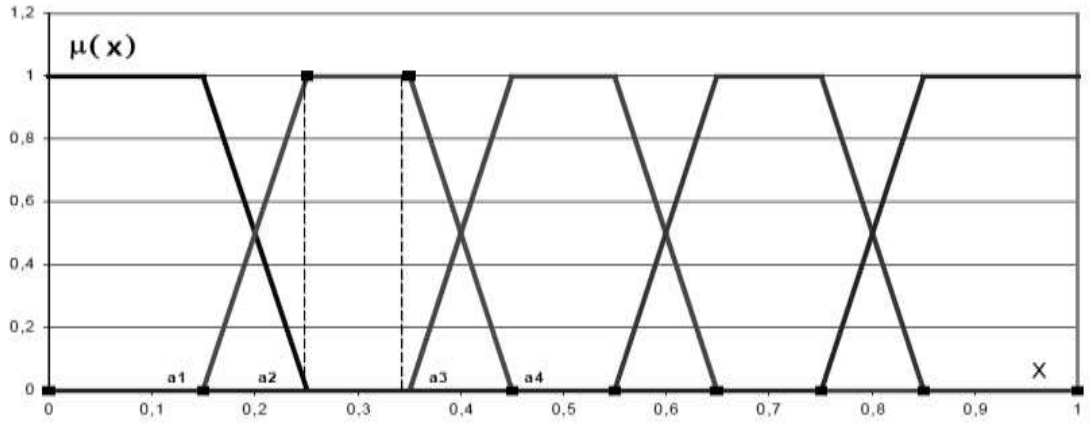

Рис. 3.28. Трапециевидные функции принадлежности

Для целей компактного описания трапециевидные функции принадлежности μ(x) удобно описывать трапециевидными числами вида

β(a1, a2, a3, a4),

где a1 и a4 - абсциссы нижнего основания, а a2 и a3 - абсциссы верхнего основания трапеции, задающей μ(x) в области с ненулевой принадлежностью носителя x соответствующему нечеткому подмножеству.

Теперь описание лингвистической переменной завершено, и аналитик может употреблять его как математический объект в соответствующих операциях и методах.

Для лингвистической переменной «Ущерб от реализации угроз информационной безопасности» можно предложить следующую качественную шкалу степеней: «Минимальный; Средний; Высокий; Критический» (табл. 3.3). А для оценки рисков информационной безопасности шкалу: «Допустимый; Недопустимый» (табл. 3.4). Данная шкала может быть расширена за счет добавления новых делений, например, «Высокий, Средний, Низкий» или 1-10.

Таблица 3.3

Степени воздействия (ущерб) угроз на безопасность системы

Степень воздействия	Описание воздействия Проявление уязвимости может:
Критический	Нанести значительный урон государству или участнику ВЭД и их интересам
Высокий	Привести к потерям материальных активов или ресурсов. Нанести урон репутации таможенных органов или участников ВЭД и их интересам
Средний	Привести к потерям некоторых материальных активов или ресурсов;
Минимальный	Потери материальных средств ресурсов быстро восполняются. Влияние на репутацию ничтожно мало.

Таблица 3.4

Шкала рисков

Уровень риска	Описание риска и необходимые действия
Допустимый	Если сведения расцениваются как допустимый риск, необходимо определить необходимость корректирующих воздействий или возможность принять риск.

Недопустимый	Уровень риска имеет критическое значение для основных ресурсов системы. Необходимо незамедлительно принять меры по уменьшению риска.

Механизм получения оценок риска формализуется с помощью продукционных правил вида «ЕСЛИ, …, ТО» Например:

ЕСЛИ Вероятность «Высокая» И Ущерб «Высокий», ТО
Риск = «Недопустимый»;

ЕСЛИ Вероятность «Высокая» И Ущерб «Минимальный», ТО
Риск = «Допустимый» и т. д.

В результате заполняется таблица («тепловая карта») допустимых / недопустимых рисков информационной безопасности (табл. 3.5).

Таблица 3.5.

Допустимые/недопустимые риски информационной безопасности

Вероятность угрозы	Ущерб от реализации угроз			
	минимальный	средний	высокий	критический
нереализуемая	допустимый	допустимый	допустимый	допустимый
минимальная	допустимый	допустимый	допустимый	недопустимый
средняя	допустимый	допустимый	недопустимый	недопустимый
высокая	допустимый	недопустимый	недопустимый	недопустимый
критическая	недопустимый	недопустимый	недопустимый	недопустимый

После получения качественной оценки риски информационной безопасности могут быть переведены в количественную форму с использованием формулы: Риск = Вероятность угрозы × Ущерб.

Суммарная количественная оценка риска информационной безопасности вычисляется как сумма количественных оценок по всем отдельным рискам информационной безопасности.

При этом для оценки дохода каждого возможного проекта безопасности необходимо использовать один и тот же определенный набор показателей. Так же, как и с приносящей доход деятельности, стоимость проек-

та безопасности должна быть меньше выгоды, которую он приносит. При этом руководители организации заинтересованы в минимизации расходов на обеспечение безопасности, при сохранении максимального уровня защиты.

На основании информации, полученной в ходе обследования информационной системы, и результатов анализа рисков разрабатываются меры по совершенствованию системы защиты, применение которых позволит минимизировать риски.

Анализ рисков — это не просто этап, а постоянно выполняемая задача. Модернизируются таможенные технологические процессы и, соответственно, поддерживающая их информационная инфраструктура, любое изменение которой ведет к изменению значений рисков.

3.2.3. Экономическая оценка затрат на защиту информации таможенных органов

Оценка альтернативных проектов защиты информации и обоснование затрат на обеспечение безопасности является постоянной проблемой для руководителей служб информационной безопасности. Часто это обоснование происходит качественно, и основано на риске публичного раскрытия информации, на соблюдении нормативных требований или на давлении - идти в ногу с конкурентами. Это не означает, что они не являются необходимыми, но трудно оценить их полезность и сравнить альтернативные предложения друг с другом. Именно поэтому перед финансовыми службами и подразделениями обеспечения информационной безопасности таможенных органов встает проблема количественного расчета для финансового обоснования инвестиций в системы защиты информации.

Для того, чтобы точно оценить затраты на инвестиционные проекты и экономическую прибыль, которую они способны принести, существуют различные методики. Те же самые подходы могут быть применены и для

определения финансовых возможностей затрат на безопасность. Разница в том, что проекты информационной безопасности никогда не дают доход, а скорее они предотвращают потерю средств, которые в противном случае будут потрачены на восстановление информационных ресурсов.

Стоимость проекта выражается в сумме денег, которые он «спас» для организации с точки зрения предотвращения потерь. Так же, как с приносящей доход деятельности, стоимость проекта безопасности должно быть меньше стоимости самих защищаемых активов.

Прибыль проекта выражается в сумме денег, спасенных для организации, с точки зрения предотвращения убытков, за счет ожидаемого улучшения после внедрения средства защиты, например, 50-процентное сокращение числа нарушений за счет использования межсетевого экрана. В контексте безопасности, улучшение характеризуется не как конкретные выгоды, а как снижение риска. Убытки могут быть, например, из-за следующих видов потерь.[58] :

- Потери производительности. Сколько человек будет не в состоянии работать из-за нарушения безопасности, и как долго? Как много времени будет потрачено персоналом подразделений таможенных органов на ремонт повреждений, вызванных нарушением?

- Потеря доходов от простоев. Например, сотрудники не могут работать через ведомственную сеть. Сколько дохода теряется в минуту, в час или в день в этом сценарии? Что делать, если потеряно подключение к Интернету?

- Потеря данных, временная или постоянная. Восстановление из резервной копии может быть дорогостоящим. Если, например, внутренний

[58] Allen Julia Making the Business Case for Information Security: Selling to Senior Management// Carnegie Mellon University at InfoSec World – 2003. - March 10

нарушитель (инсайдер) уничтожил резервную копию, а затем удалил данные, это может иметь катастрофические последствия.

- Компрометация данных из-за раскрытия или модификации. Например, стратегические планы или конфиденциальная финансовая информация.

- Затраты на ремонт. Например, возможно, необходимо купить новое оборудование или использовать диск восстановления.

- Потеря репутации. Например, косвенные расходы от нарушения для участников ВЭД?

Преимущества технологии защиты зависит от того, как часто предполагается реализация угрозы, какой ущерб может произойти и насколько эффективным является технология защиты в смягчении ущерба от нападения. Затраты на альтернативные проекты безопасности можно точно оценить с помощью инструментов финансового анализа. В отличие от этого, количественная оценка дохода основана на оценке рисков. При этом для каждого возможного проекта безопасности необходимо использовать один и тот же определенный набор показателей. Так же, как и с приносящей доход деятельности, стоимость проекта безопасности должна быть меньше выгоды, которую он приносит. При этом учитывается, что руководители таможенных органов заинтересованы в минимизации расходов на обеспечение безопасности, при сохранении максимального уровня защиты.

После получения качественной оценки, риски информационной безопасности могут быть переведены в количественную форму с использованием формулы:

Риск = Вероятность угрозы × Ущерб.

Для оценки затрат и эффективности инвестиций в безопасность наряду с традиционными методами финансового анализа инвестиционных проектов, такими как чистая приведенная стоимость, рентабельность инве-

стиций, внутренняя норма рентабельности, срок окупаемости[59], могут использоваться менее распространенные методики: совокупная стоимость владения, экономическая добавленная стоимость, рентабельность инвестиций в обеспечение безопасности.

Чистая приведенная стоимость (Net Present Value — NPV)

Чистая приведенная стоимость (NPV) проекта или инвестиций определяется как сумма стоимости ежегодных дисконтированных денежных потоков минус первоначальные инвестиции.

Ежегодные денежные потоки представляют собой чистые выгоды (доходы минус расходы), полученные от инвестиций в течение жизни проекта. Эти денежные потоки дисконтируются или корректируются, для учета изменения стоимости денег с течением времени и приведения ее к одному моменту. NPV является одним из самых надежных финансовых инструментов для оценки инвестиций.

NPV применяется не только к экономии средств в будущем. Деньги, потраченные сегодня стоят больше, чем экономия завтра. Будущие расходы дешевле, чем затраты в настоящем.

Формула расчета NPV приведена ниже:

$$NPV = \sum_{t=0}^{N} \frac{CF_t}{(1+r)^t} = -IC + \sum_{t=1}^{N} \frac{CF_t}{(1+r)^t} ,$$

где CFt - чистый денежный поток для t-го года проекта: доходы минус расходы;

IC (Invested Capital) - это инвестиции, сделанные в начале проекта;

r - ставка дисконтирования. Эффект проекта и размер капиталовложений рассчитываются с учетом их обесценивания во времени — дисконтирования;

[59] Васина А.А. Финансовая диагностика и оценка проектов / Васина А.А. СПб.: Питер, 2004. С. 389.

N - последний год жизни проекта.

Положительное значение NPV представляет прибыли, в то время как отрицательное NPV означает потери. Проект эффективен только если NPV больше или равно нулю.

При применении анализа NPV к информационной безопасности, необходимо выявить полученные денежные потоки, под которыми понимается предотвращение ущерба, экономия затрат, дополнительный доход. Если необходимо взвесить издержки и выгоды, при этом некоторые расходы являются немедленными, а выгоды будут долгосрочными, как очень часто бывает в проектах информационной безопасности, NPV может обеспечить более точное измерение является ли проект действительно стоящим. Этот метод может быть особенно полезен при сравнении инвестиций с разными сроками использования. Анализ NPV является гибким и может быть объединен с другими финансовыми инструментами.

Рентабельность инвестиций (Return On Investment, ROI)

Рентабельность или окупаемость инвестиций (ROI) является прямым финансовым инструментом, который измеряет экономическую отдачу от проекта или инвестиций. Он также известен как рентабельность инвестированного капитала.

Есть несколько вариантов расчета рентабельности инвестиций (ROI), учитывающие многочисленные толкования и применения в различных отраслях. Это отсутствие последовательности в определении ROI приводит к путанице при сравнении значения ROI нескольких проектов. Ниже приведены наиболее распространенные варианты расчета ROI:

$$ROI = \frac{чистая\ прибыль}{расходы} \times 100\%,$$

где чистая прибыль - доходы минус расходы;

расходы - первоначальные и периодические (или текущие) затраты.

Возврат от инвестиций с использование чистой приведенной стоимости учитывает изменение стоимости денег во времени:

$$ROI = \frac{NPV}{PV} \times 100\%$$,

где NPV - чистая приведенная стоимость;

PV – приведенная стоимость инвестиций.

ROI показывает относительное превышение полученной выгоды над первоначальными капиталовложениями, а NPV - абсолютное значение этой выгоды.

Все чаще рентабельность инвестиций применяется для оценки инвестиций в безопасность. ROI позволяет сравнить несколько альтернатив инвестиций в безопасность и выбрать ту, которая дает максимальный «процент» на вложенный капитал. Рентабельность инвестиций измеряет ожидаемое улучшение по сравнению с текущим состоянием. Между тем, невозможность предсказать, когда и где произойдет нарушение безопасности, приводит к тому, что снижает применимость метода ROI.

Внутренняя норма рентабельности (Internal Rate of Return, IRR)

Внутренняя норма рентабельности (IRR) определяется как ставка дисконтирования, при которой чистая приведенная стоимость (NPV) равна нулю. IRR является альтернативным методом оценки инвестиций без расчета ставки дисконтирования. Компании должны инвестировать в проект с доходностью выше, чем процентная ставка на капитал плюс премия за риск.

IRR использует уравнение NPV в качестве отправной точки:

$$NPV = 0 = -IC + \frac{CF_1}{(1+IRR)^1} + ... + \frac{CF_N}{(1+IRR)^N}$$

или

$$IC = \sum_{t=1}^{N} \frac{CF_t}{(1+IRR)^t},$$

где IC (Invested Capital) - это инвестиции, сделанные в начале проекта;

CF_t - поток денежных средств для t-го года проекта: количество денежных средств, заработанных после оплаты всех расходов и налогов;

IRR - внутренняя норма рентабельности;

N - последний год жизни проекта.

IRR – это ставка, при которой значение оттока денежных средств равно стоимости денежных поступлений. В отличие от расчета NPV, IRR показывает руководителю службы информационной безопасности норму прибыли, при какой проект будет безубыточным.

Модифицированная внутренняя норма рентабельности (Modified Internal Rate of Return, MIRR) расширяет возможности IRR и устраняет некоторые недостатки. Во-первых, IRR предполагает, что дисконтированные денежные потоки реинвестируются с одной и той же доходностью. Как правило, это нереалистичный сценарий, и более вероятно, что средства будут реинвестироваться по ставке ближе к стоимости капитала. Во-вторых, для проектов с чередующимися положительными и отрицательными денежными потоками можно найти более одного значения IRR, что приводит к путанице и неопределенности. MIRR находит только одно значение. MIRR рассчитывается следующим образом:

$$MIRR = \sqrt[N]{\frac{FV(ставка\ реинвестирования, полож.денежные\ потоки)}{-PV(финансовая\ ставка, отриц.денежные\ потоки)}} - 1$$

где N - это количество равных периодов, в конце которых происходит движение денежных средств;

PV – это текущая стоимость (на начало первого периода);

FV - это будущая стоимость (в конце последнего периода).

Формула учитывает отрицательные денежные потоки после дисконтирования их в нулевой момент времени, используя внешнюю стоимость капитала, а также положительные денежные потоки, включая доходы от реинвестирования денежных средств, и приводятся к будущей (конечной) стоимости.

Недостатком методов IRR и MIRR является относительная сложность их расчета. Вычисление IRR и MIRR, как правило, осуществляется с помощью приложения Microsoft Excel.

Срок окупаемости (Payback Period, PP)

Срок окупаемости рассчитывает время, которое потребуется, чтобы окупить первоначальные вложения средств и показать прибыль. Точкой окупаемости называется тот момент времени, в который чистый доход становится положительным. Формула расчета срока окупаемости:

$$PP = \frac{IC}{CF_{СГ}},$$

где IC (Invested Capital) – первоначальные инвестиции;

$CF_{СГ}$ – среднегодовой чистый денежный поток.

Срок окупаемости является широко используемым показателем, но при этом существуют две основные проблемы:

не учитывает изменение стоимости денег во времени;

игнорирует потоки денежных средств, которые происходят в конце жизни проекта, например, такие как ликвидационная стоимость.

Первая проблема может быть легко решена путем использования модели дисконтированного срока окупаемости (Discounted PayBack Period, DPP). В отличие от анализа NPV, который обеспечивает общую стоимость проекта, дисконтированный срок окупаемости дает число лет, необходимое для достижения уровня безубыточности от реализации первоначальных расходов.

Дисконтированный срок окупаемости не решает вторую проблему. Именно поэтому обычно предпочтение отдается другим методам оценки приемлемости инвестиций, таким как NPV, IRR. К расчёту срока окупаемости целесообразно обращаться только для получения дополнительной информации об инвестиционном проекте.

Функционально-стоимостной анализ (Activity Based Costing, ABC) - это процесс распределения затрат с использованием первичных носителей стоимости, ориентированных на производственную и/или логистическую структуру предприятия с конечным распределением затрат по основным носителям (продуктам и услугам). Данный подход позволяет весьма точно и понятно установить связь между элементами себестоимости продукции и производственными процессами.

Применимо к оценке эффективности систем защиты информации метод функционально-стоимостного анализа используется для построения моделей бизнес- процессов предприятия: «Как есть» и «Как будет». Модель «Как будет» отражает изменение технологии реализации основных бизнес-процессов при использовании выбранной системы информационной безопасности. На основе показателей стоимости, трудоемкости и производительности определяется наилучшая модель бизнес-процессов «Как будет».

Данный подход в применении к оценке систем защиты информации использует модели бизнес-процессов, описывающие состояние без использования системы безопасности и после ее внедрения. Применение функционально-стоимостного анализа в этой сфере требует предварительного описания составляющих бизнес-процессов анализируемого таможенного органа, что достаточно трудоемко в настоящий момент времени.

Совокупная стоимость владения (Total Cost of Ownership, TCO)

Совокупная стоимость владения (TCO) – это методика, предназначенная для систематической количественной оценки всех затрат, в течение всего жизненного цикла проекта. Модель совокупной стоимости владения позволяет определить показатель, который отражает общую стоимость инвестиций, включая единовременные и текущие расходы, а не только первоначальные затраты[60].

$$TCO = \frac{\sum_{t=1}^{N} единовременные\ расходы + текущие\ расходы\ (t)}{N},$$

где единовременные расходы – разовые расходы, которые могут включать обучение персонала, внедрение новых процессов или инвестиции в активы;

текущие расходы - это повторяющиеся расходы, например, непрерывный мониторинг производительности;

N – срок жизни проекта или стандартный срок, который используется для нормализации всех расчетов TCO в организации.

Очень часто TCO рассчитывается как суммы всех расходов нарастающим итогом, без деления на срок жизни проекта. Приведенное значение TCO (PV TCO) рассчитывается с учетом ставки дисконтирования.

Как правило, затраты на защиту информации подразделяются на следующие категории[61]:

А. Единовременные затраты:

затраты на формирование и поддержание звена управления системой защиты информации (организационные затраты);

[60] Philip Robinson, Bryan Stephenson TCO-aware provisioning of information security infrastructure. HP Laboratories, 2008. p. 21

[61] Петренко С.А., Симонов С.В. Управление информационными рисками: Экономически оправданная безопасность. – М.: ДМК пресс, 2004. – 381 с.

стоимость компонентов системы защиты информации и информационных активов (серверы, клиентские компьютеры, периферийные устройства, сетевые устройства);

расходы на аппаратные и программные средства защиты информации;

расходы на организацию защиты информации;

расходы на организационные меры защиты информации;

косвенные расходы на организацию информационной безопасности и обеспечение непрерывности или устойчивости деятельности.

Б. Систематические затраты:

затраты на контроль, то есть на определение и подтверждение достигнутого уровня защищенности ресурсов предприятия;

внутренние затраты на ликвидацию последствий нарушения политики информационной безопасности - затраты, понесенные организацией в результате того, что требуемый уровень защищенности не был достигнут;

внешние затраты на ликвидацию последствий нарушения политики информационной безопасности - компенсация потерь при нарушениях политики безопасности в случаях, связанных с утечкой информации, потерей имиджа компании, утратой доверия партнеров и потребителей и т. п.;

затраты на техническое обслуживание системы защиты информации и мероприятия но предотвращению нарушений политики безопасности предприятия (затраты на предупредительные мероприятия).

Затраты на контроль включают:

затраты на проверки и испытания программно-технических средств защиты информации;

затраты на проверку навыков эксплуатации средств защиты персоналом предприятия;

затраты на обеспечение работы лиц, ответственных за реализацию конкретных процедур безопасности по подразделениям;

оплату работ по контролю требований, предъявляемых к защитным средствам при разработке любых систем;

расходы на внеплановые проверки и испытания;

затраты на контроль реализации функций, обеспечивающих управление защитой конфиденциальной информации;

затраты на проведение аудита безопасности по каждой автоматизированной информационной системе, выделенной в информационной среде организации;

материально-техническое обеспечение системы контроля доступа к объектам и ресурсам организации.

затраты на контрольно-проверочные мероприятия, связанные с лицензионно-разрешительной деятельностью в сфере защиты информации.

Пересмотр политики информационной безопасности организации сопровождается следующими направлениями расходов:

затраты на идентификацию угроз безопасности;

затраты на поиск уязвимостей системы защиты информации;

оплата работы специалистов, выполняющих работы по определению возможного ущерба и переоценке степени риска;

затраты на ликвидацию последствий нарушения режима ИБ (восстановление системы безопасности до соответствия требованиям политики безопасности, приобретение технических средств взамен пришедших в негодность, затраты на утилизацию скомпрометированных ресурсов);

затраты на восстановление информационных ресурсов предприятия;

затраты на выявление причин нарушения политики безопасности (на проведение расследований нарушений политики безопасности - сбор данных о способах совершения, механизме и способах сокрытия неправомер-

ного деяния, поиск следов, орудий и предметов посягательства, выявление мотивов неправомерных действий и т. д.);

затраты на внедрение дополнительных средств защиты.

Внешние затраты на ликвидацию последствий нарушения политики безопасности содержат:

реализацию обязательств перед государством и партнерами;

затраты на юридические споры и выплаты компенсаций;

потери в результате разрыва деловых отношений с партнерами;

отказ от организационных, научно-технических или коммерческих решений, ставших неэффективными в результате утечки сведений, и затраты на разработку новых средств ведения конкурентной борьбы;

потери от снижения приоритета в научных исследованиях и невозможности патентования и продажи лицензий на научно-технические достижения.

Затраты на обслуживание системы безопасности (затраты на предупредительные мероприятия) включают:

расходы на управление системой защиты информации (планирование системы защиты информации, осуществление технической поддержки производственного персонала при внедрении средств защиты и процедур, проверка сотрудников на лояльность, выявление угроз безопасности, организация системы допуска исполнителей и сотрудников конфиденциального делопроизводства);

расходы на регламентное обслуживание средств защиты информации (обслуживание и настройка программно-технических средств защиты, операционных систем и используемого сетевого оборудования, организация сетевого взаимодействия и безопасного использования информационных систем, проведение инженерно-технических работ по установлению

сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, средств вычислительной техники и т. п.);

затраты на аудит системы безопасности (контроль изменений состояния информационной среды организации и контроль за действиями исполнителей);

затраты на обеспечение соответствия требованиям качества информационных технологий;

затраты на доставку (обмен) конфиденциальной информации;

затраты на обеспечение соответствия принятым стандартам и требованиям, достоверности информации, действенности средств защиты.

затраты на обучение персонала и повышение квалификации сотрудников организации в вопросах использования имеющихся средств защиты, выявления и предотвращения угроз безопасности.

Концепция ТСО широко используется в области информационных технологий (ИТ), где выгоды трудно оценить количественно и основное внимание уделяется минимизации затрат по проекту. Обычно используют методологию ТСО при сравнении аналогичных продуктов от различных производителей. Характеристики продуктов различных производителей не могут сильно отличаться, но качество и поддержка продукции могут привести к большой разнице в значениях совокупной стоимости владения. Элемент с низкой совокупной стоимостью владения будет выгоднее в долгосрочной перспективе.

Экономическая добавленная стоимость (Economic Value Add, EVA)

Экономическая добавленная стоимость позволяет принимать решение на основе стоимости. Идея состоит в том, что стоимость создается, когда отдача от экономического капитала больше, чем стоимость этого капитала. EVA представляет собой чистую операционную прибыль после уплаты налогов за вычетом цены капитала.

Экономическая добавленная стоимость рассчитывается по формуле[62]:

$$EVA = (r - c) \times IC = NOPAT - c \times IC ,$$

где r - возврат на вложенный капитал, определяется как $r = \frac{NOPAT}{IC}$;

NOPAT - чистая операционная прибыль после уплаты налогов;

c – средневзвешенная стоимость капитала (WACC);

IC – инвестированный капитал.

При использовании этого показателя в области информационных технологий расходы сравниваются со стоимостью получения той же услуги через внешних поставщиков по рыночной цене. После определения рыночной стоимости EVA дает количественную оценку разницы между рыночной ценой и фактической стоимостью предоставленной услуги. При оценке, например, новой системы защиты данная модель требует учета всех инвестиций, в том числе затрат на закупку, поддержку, на обучение и т. д. Все эти затраты считаются платой за предполагаемую выгоду, которая будет способствовать снижению издержек.

Преимуществом методики EVA является единый финансовый показатель, который может быть использован как компромисс между общей стоимостью инвестиций и потенциальной ценностью. Несмотря на достоинства этого метода, достаточно сложно принять решение, например, о покупке нового межсетевого экрана без проведения промежуточных расчетов. Поэтому чаще всего EVA применяется вместе с другими методологиями оценки.

Рентабельность инвестиций в обеспечение безопасности (Return On Security Investment, ROSI)

[62] Anil K. Sharma Economic Value Added (EVA) - Literature Review and Relevant Issues. International Journal of Economics and Finance, Vol 2, No 2, 2010. p.21

Рентабельность инвестиций (ROI) часто используется для сравнения альтернативных инвестиционных стратегий. Но при этом не учитываются специфические показатели безопасности (например, угрозы, уязвимости, риски). Это привело к разработке новых моделей экономических расчетов и к появлению методики ROSI. Этот подход основан на вычислении ущерба от нарушений безопасности и его сравнении с затратами на защиту информации.

Расчет ROSI включает в себя несколько этапов[63]:

Определяются и оцениваются информационные активы организации (Asset Value – AV).

Стоимость активов достаточно сложно оценить. Например, для сервера стоимость актива равна сумме стоимости замены информации, потери доступности, потери конфиденциальности и целостности данных, а также расходов на замену программного и аппаратного обеспечения и реконфигурацию. Значение стоимости активов будет варьироваться в зависимости от вида нападения. DDoS-атака[64], например, не повлечет замену оборудования, тогда как прямая кража сервера будет включать множество возможных затрат, например, связанных с утратой конфиденциальности и целостности информации.

Оценивается фактор подверженности неблагоприятному воздействию информационных активов (Exposure factor – EF). Определяется список угроз, которым могут быть подвержены информационные активы организации, затем оценивается ущерб, который может возникнуть в результате реализации выявленной угрозы. Фактор EF определяет процент акти-

[63] Sonnenreich, Wes; 'Return on Security Investment (ROSI): A Practical Quantitative Model', Journal of Research and Practice in Information Technology, vol., 38, no. 1, February 2006, Australia, 2006

[64] DDoS-атака – распределенная атака типа отказ в обслуживании. В результате атаки нарушается или полностью блокируется обслуживание законных пользователей, сетей, систем и иных ресурсов.

вов, которые были бы потеряны при возникновении определенного типа угрозы.

Определяется ожидаемый ущерб от одной угрозы (Single Loss Exposure, SLE) - затраты, связанные с одной атакой на конкретный актив. Он может быть определен как произведение общей стоимости защищаемых информационных активов (AV) на коэффициент их разрушения, при возникновении определенного типа угрозы (EF). Показатель SLE оценивает влияние одного нарушения информационной безопасности по следующей формуле:

$$SLE = AV \times EF$$

Определяется годовая частота возникновения угроз (Annual rate of occurrence - ARO). Показатель ARO представляет собой вероятность атаки в течение одного года. Чаще всего этот показатель определяется экспертно или с помощью статистических данных, публикуемых правительственными или институциональными организациями сбора информации. В то же время, статистические данные из различных источников могут оказаться противоречивыми, в этом случае лучше взять более пессимистичную оценку.

Определяются ожидаемые ежегодные потери (Annual Loss Exposure ALE). ALE может использоваться в процессе составления бюджета организации, при рассмотрении инвестиций в оборудование. Ежегодные потери рассчитываются по формуле:

$$ALE = SLE \times ARO = (AV \times EF) \times ARO$$

Непосредственный эффект от внедрения средств защиты информации будет проявляться в том, что отрицательные последствия реализации каждой угрозы будут меньше, чем до внедрения мер защиты, а частота возникновения угроз уменьшится.

Оцениваются ежегодные расходы на обеспечение безопасности (Solution Cost – SC). Чтобы предотвратить ожидаемые потери, необходимо инвестировать средства в программные или аппаратные технологии безопасности, например, в межсетевые экраны, системы обнаружения вторжений, антивирусные программы. Обобщенно стоимость защиты информации будет складываться из единовременных и периодических затрат, которые можно рассчитать с помощью приведенной совокупной стоимости владения.

Рассчитывается показатель рентабельности инвестиций в обеспечение безопасности (ROSI) в процентах по следующей формуле:

$$ROSI = \frac{ALE - SC}{SC} \times 100\%$$

В соответствии с этой формулой может быть определен эффект от реализации мер защиты информации и показано, насколько оправданным являются инвестиции в те или иные средства защиты с учетом сделанных допущений и предположений. К сожалению, рентабельность инвестиций в обеспечение безопасности невозможно вычислить точно, главным образом потому, что трудно оценить вероятность возникновения инцидента.

Считается, что инвестиция в обеспечение безопасности будет выгодной, если экономический эффект от снижения рисков больше, чем ожидаемые затраты. Данная формула помогает для принятия решений об одной инвестиции, но не установлению приоритетов из нескольких альтернатив.

Все рассмотренные методы оценки инвестиций имеют определенные ограничения их использования. Поэтому применение лишь одного из методов может не дать результата вовсе, а если и дав какой-либо результат, привести к ошибочным управленческим решениям. Следовательно, очевидна необходимость использования методов в комплексе. Для более полной оценки инвестиций в весь проект системы защиты информации тамо-

женных органов можно взять комбинацию методов NPV, ROI (ROSI), TCO. Сочетание этих методов даст оценку не только затратной, но и результатной части проекта.

Если необходимо определиться лишь с выбором конкретного средства защиты, то оценить альтернативы можно с помощью одного из методов: NPV, ROI (ROSI), TCO.

Также при использовании рассмотренных методов предполагается, что можно точно предсказать вероятность события. Но прогнозирование вероятности атаки злоумышленника может быть затруднено. Часто, лучшее, что можно сделать, это произвести приблизительную оценку на основе предыдущих данных. Так как злоумышленники не хотят быть обнаружены, предыдущие данные об атаках часто является неполными и, следовательно, соответствующие прогнозы могут быть основаны на некорректных данных.

Расчет риска произвести не так просто. Для этого необходимо иметь представление о реальных угрозах, уязвимостях и вероятности воздействия. Такие данные не так легко найти. Кроме того, характер рисков будет меняться со временем. Существует очень мало фактических данных о стоимости взлома, следовательно, и прогнозирование затрат на редкие но разрушительные события чревато опасностью. Поэтому не представляется возможным точно рассчитать выгоду, которая является производной от повышения безопасности при внедрении средств защиты.

Таким образом, из всех рассмотренных финансовых методов наиболее точен в применении к информационной безопасности только метод совокупной стоимости владения (TCO), оценивающий инвестиции по общей сумме расходов с течением времени. Концепция TCO широко используется в области информационных технологий (ИТ), где выгоды трудно оценить количественно. Характеристики продуктов различных производите-

лей могут не сильно отличаться, но качество и поддержка продукции могут привести к большой разнице в значениях совокупной стоимости владения. Элемент с низкой совокупной стоимостью владения будет выгоднее в долгосрочной перспективе. В связи с тем, что выгоды не рассматриваются в ТСО, общий финансовый анализ упрощается.

3.3. Разработка моделей и методических рекомендаций по минимизации затрат на защиту информации таможенных органов российской федерации

3.3.1. Разработка объектной модели на основе декомпозиции системы защиты распределенных информационных систем на подсистемы

ЕАИС ФТС России является распределенной системой и не имеет ограниченного периметра, число ее подсистем может меняться во времени. Между подсистемами существуют каналы передачи данных, которые могут проходить по незащищенной и неконтролируемой территории. Таким образом, информационную систему таможенных органов можно рассматривать как совокупность подсистем, каждая из которых является самостоятельной защищенной системой. Вопросы ее гарантированной защиты сводятся к доказательству защищенности подсистем в условиях рассматриваемого окружения и организации защищенных каналов для взаимодействия компонент.

Для сокращения размерности задачи оптимизации и упрощения формализации политики безопасности предлагается рассматривать систему защиты в виде совокупности взаимодействующих подсистем. Декомпозиция системы защиты производится с целью распределения различных слабосвязанных функций защиты по различным подсистемам. В результате, они могут проектироваться, реализовываться и управляться в процессе эксплуатации раздельно. Число подсистем определяется, исходя из прак-

тических потребностей и минимизации затрат на проектирование и построение системы безопасности. Информационное взаимодействие подсистем осуществляется на основе аутентификации взаимодействующих сторон с установлением защищенного соединения. Подобное построение позволяет комплексно использовать различные средства и методы защиты, повысить общую эффективность системы в целом при снижении затрат на проектирование и реализацию, а также сократить размерности задачи оптимизации и упростить формализацию правил функционирования подсистем защиты. Каждая подсистема в свою очередь может делиться на вложенные подуровни защиты. Связь между подсистемами защиты осуществляется при помощи средств электронной подписи.

Все подсистемы должны иметь одинаковую степень защищенности, что позволяет эффективно распределить ресурсы системы защиты. По мере проектирования системы защиты производится поэтапная детализация и конкретизация целей, задач и структуры подсистем защиты. На этапе эксплуатации системы по мере выявления неучтенных угроз осуществляется уточнение структуры и состава подсистем безопасности. Проектирование и построение систем защиты с заданными свойствами, соответствующих необходимому уровню безопасности, достаточно трудоемкая задача, проектирование оптимальной системы также затруднено из-за множества параметров, которые надо учесть.

Рассмотрим формальную модель подсистемы защиты информационной системы. Имеется множество объектов информационной системы, подлежащих защите $O = \{O_i\}$, $i=1,...,n$. Объектом может быть активный процесс, который способен выполнять некоторые операции над другими объектами системы, получая управление, или неактивный объект – пассивная сущность информационной системы, например таможенная декларация.

Также есть множество угроз безопасности для данной системы $T = \{T_k\}$, k=1,...,l, и множество возможных механизмов защиты $M= \{M_j\}$, j=1,...,m. Система защиты представляет собой отношения между элементами этих множеств. Множество отношений угроза – механизм защиты - объект образует три непересекающихся подмножества, связанные между собой ребрами, результатом является трехдольный граф {<T, M, O>}, отображенный на рис.3.29.

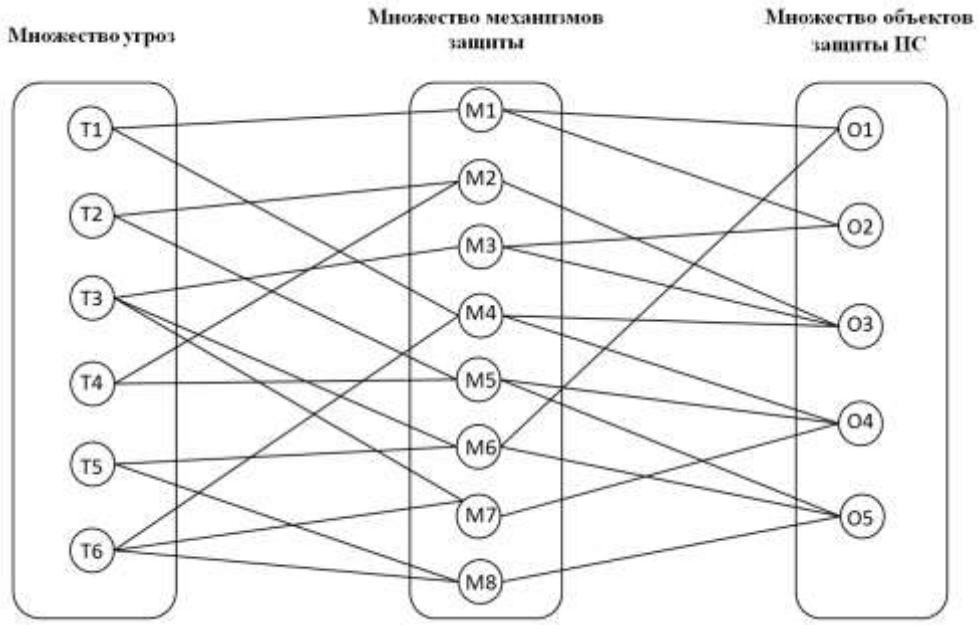

Рис. 3.29. Модель системы защиты

В этом случае каждая из частей множества объектов защиты $O = \{O_i\}$ может рассматриваться как объект атак. Очевидно, что данное представление системы обработки информации, является агрегированным, т.е. каждый из объектов защиты может делиться на элементы (в зависимости от конкретной системы). Таким образом, при построении модели СЗИ необходимо сформировать полный перечень элементов защиты. При этом для небольшой инфраструктуры допустимо рассматривать весь ее объем, однако, если размеры информационной подсистемы не позволяют сделать

всеобъемлющую оценку и выбор объектов защиты в реальные масштабы времени, то в таком случае, следует сосредоточиться на наиболее важных сервисах, заранее соглашаясь с приближенностью итоговой оценки. Уязвимым может оказаться каждый компонент информационной системы - от кабеля, который может быть разрушен, например, при проведении ремонтных работ, до базы данных, которая может быть повреждена из-за неумелых действий администратора. Однако с учётом того, что в сферу анализа невозможно включить каждый элементарный объект, нужно заранее определиться с глубиной детализации.

Для построения объектной модели необходимо описать процесс взаимодействия между объектами системы и управления информационными потоками в вычислительной среде. Существует набор операций над объектами в информационной системе. Правила доступа определяют, какие именно операции над какими объектами в сети разрешены. Реализация управления данных правил доступа позволяет получить требования к системе безопасности. При выполнении требований обеспечения информационной безопасности, предъявляемых к объектам, а также к процедурам взаимодействия с ними, информационная система будет находиться в безопасном состоянии, в рамках выполнения описанного набора операций.

3.3.2. Разработка модели рационального выбора механизмов защиты с учетом экономических показателей

Модель построения рациональной системы защиты

Выбор рациональной стратегии защиты данных – важная и сложная задача. При этом задача определения рациональных мероприятий для создания системы защиты информации, как правило, индивидуальна. Под рациональным выбором средств защиты понимается достижение требуемых значений параметров системы защиты информации, при минималь-

ном расходовании ресурсов. Эта задача в каждом конкретном случае должна решаться с учетом всех особенностей документооборота таможенного органа.

В общем случае построение рациональной системы защиты может быть реализовано в виде модели (рис. 3.30) следующим образом:

Для каждого объекта O_i составляется список угроз $\{ T_k \}$.

На основе опыта создания систем защиты информации для каждой угрозы, составляются варианты наборов задач защиты $\{ M_j \}$.

Определяются наиболее подходящие наборы средств, использованием которых могут быть решены различные задачи защиты на различных рубежах.

На основе технико-экономических оценок средств защиты определяются размеры затрат, необходимых для практического использования различных средств.

При более качественном проектировании и практической реализации механизма защиты один и тот же уровень обеспечения защиты информации может быть достигнут при меньших материальных затратах. Основной задачей данной модели является научное обеспечение процесса создания системы защиты информации за счет правильной оценки эффективности принимаемых решений и выбора рационального варианта технической реализации системы защиты информации.

Для решения задачи рационального построения структуры и выбора состава средств защиты информации необходимо иметь множество критериев, отражающих наиболее существенные аспекты создаваемого комплекса средств защиты. Для каждого средства защиты наиболее целесообразно применять следующие группы критериев:

относительные показатели эффективности (защищенности) средства защиты при воздействии каждой из угроз безопасности;

экономические, учитывающие различные виды и составляющие затрат, рассчитанные с помощью метода совокупной стоимости владения (ТСО);

дополнительные критерии (необходимый объем оперативной памяти, быстродействие, показатели простоты и удобства использования и т.д.).

Следовательно, каждое из средств защиты описывается набором параметров, интересующих заказчиков системы:

$M_j = \{ C_j , \{P_{jk}\}, W_j , V_k, ,\ldots\}$,

где C_j – затраты средства защиты по ТСО;

$\{P_{jk}\}$ – множество относительных показателей эффективности (защищенности) средства защиты для каждой из угроз безопасност;

W_j – время на осуществление элементарной операции;

V_j – необходимый объем оперативной памяти.

При необходимости проектировщики системы защиты могут добавить новые критерии для оценки механизмов защиты.

Относительный показатель эффективности средства защиты для одной из угроз безопасности P_{jk} – количественная характеристика оценки уровня обеспечиваемой информационной защиты, которой обладают средства защиты при осуществлении данной угрозы. Значение этого показателя лежит в переделах от 0 до 1. Чем он больше, тем эффективнее использование данного средства защиты для противодействия угрозе. При отсутствии перекрытия механизмом защиты M_j определенной угрозы T_k, показатель эффективности P_{jk} средства защиты для угрозы безопасности принимается равным 0. Таким образом, решением рационального проектирования системы является набор выбранных компонентов M_1, M_2 , M_3 , … , M_m, при котором соблюдаются все установленные ограничения.

Задача оптимизации по критерию стоимость/эффективность защиты многокритериальная. На практике получение точных значений приведен-

ных характеристик относительной эффективности затруднено, т. к. эти понятия угрозы, риска и «сопротивляемости» механизма защиты труднофор-мализуемы. И чаще всего для их оценивания применяются экспертные оценки и методы нечеткой логики. Поэтому в предлагаемом алгоритме построение рациональной системы защиты с учетом относительного показателя эффективности и экономических показателей разбито на два этапа.

На первом этапе определяются наиболее подходящие комплексы средств защиты по критерию эффективности (защищенности) для каждой угрозы безопасности, а также, если необходимо, по быстродействию и объему памяти и другим критериям, заданными заказчиком.

На втором этапе внутри области Парето решается задача однокритериальной оптимизации - минимизация стоимости (затрат) набора средств защиты информации.

3.3.2. Выделение области компромиссов по критерию защищенности

Выделяется область компромиссов при многокритериальной оптимизации по вектору параметров подсистемы:

$M_j = \{\{P_{jk}\}, W_j , V_j ,\ldots\}$.

Решение задачи на данном этапе, чаще всего, представляет собой некоторое подмножество приблизительно равных по качеству вариантов, называемое областью Парето (или областью компромиссов)[65]. Часто область Парето содержит довольно большое число вариантов. При этом практически все варианты из этой области равнозначны, поэтому выбор сделать крайне сложно.

В случае многокритериальной оптимизации каждому из вариантов проекта системы соответствует набор значений q или точка в m-мерном

[65] Корнеенко В. П. Методы оптимизации. М.: Высшая школа, 2007. 664 с.

пространстве. Все множество возможных вариантов проектов системы Q можно разделить на два непересекающихся подмножества:

$$Q = Q_k \cup Q_s;$$

$$Q_k \cap Q_s = Ø,$$

где Q_k – область компромиссов;

Q_s – область согласия.

Область согласия – подмножество множества вариантов возможных проектов системы, обладающее тем свойством, что любой вариант данного множества может быть улучшен либо одновременно по всем критериям, либо по одному или нескольким из них без ухудшения по остальным критериям.

Область компромиссов – подмножество решений, каждый вариант которого не может быть улучшен по одному или нескольким критериям без ухудшения по одному или более из оставшихся критериев. Еще данную область обозначают следующие термины: «область Парето», «переговорное множество», «область эффективных планов». Оптимальный вариант проекта системы может принадлежать только области компромиссов. Это следует из того, что любой вариант из области согласия может быть улучшен, и оба подмножества не пересекаются.

Выделение области компромиссов важный шаг при выборе варианта проекта системы. Область Парето инварианта к масштабу и шкале измерений локальных параметров и к их приоритету – это характеризует корректность разработанного проекта. Область компромиссов существенно сужает область поиска оптимального варианта.

Часто выделение данной области недостаточно для полного решения задачи, так как область Парето может содержать довольно большое число вариантов. Практически все варианты из этой области равнозначны (и равноправны), выбор сделать крайне сложно. Выделение варианта внутри об-

ласти компромиссов может осуществляться на основе принятой схемы компромиссов (некоторая аксиоматика). В ряде случаев целесообразно предоставить выбор варианта проекта системы внутри области компромиссов заказчику или пользователю системы, который может учесть характеристики вариантов проекта, не нашедших свое отражение в векторном критерии. Каждое решение будет различаться либо в одном, либо в нескольких параметрах, в этом случае заказчик может сформулировать: какие из параметров являются наиболее важными для него (произвести коррекцию критериев) и, исходя из этого, принимать решение о выборе.

Приведем наиболее распространенные методы поиска решений внутри области компромиссов[66].

1. *Принцип равномерности*. Пусть критерии нормализованы и имеют одинаковую важность. Считается целесообразным выбор такого варианта решения, при котором достигается некоторая равномерность показателей по всем критериям. Выделим три принципа реализации принципа равномерности: принцип равенства, квазиравентсва и принцип максимина.

Формально принцип равенства описывается следующим образом:

$q_{opt} = \{q_1 = q_2 = q_3 = \dots q_m\} \in Q_k$.

Не всегда существует такой вариант решения, при котором все критерии равны (или он не принадлежит области компромиссов). Тогда применяется метод квазиравенства.

2. При *методе квазиравенства* требуется достичь приближенного равенства, приближенность задается диапазоном, характеризующимся некоторым значением δ.

3. В *принципе максимина*, из области Парето выбираются варианты проекта с минимальными значениями локальных параметров и среди них

[66] Мину М. Математическое программирование. Теория и алгоритмы. Пер. с франц. А.И. Штерна. - М.: Наука. - 1990 г. - 486 с.

ищется вариант, имеющий максимальное значение. В этом случае происходит постепенное увеличение критерия с наименьшим уровнем, пока все значения не окажутся приблизительно равны.

4. Проектировщик должен проверить: не дает ли небольшое отклонение от равномерных критериев значительное улучшение по одному или нескольким критериям. В этом случае целесообразно применять *принцип справедливой уступки.*

При совместном анализе трех параметров, например, быстродействие - объем оперативной памяти - защищенность, на графике появляется дополнительная ось. В общем случае, мы имеем дело с n-мерным графиком, где n – число параметров многокритериальной задачи оптимизации.

Если небольшой проигрыш по одному из факторов ведет к значительному выигрышу другого параметра, то это и называется точкой справедливой уступки. Если множество Парето не содержит в себе характерных точек, то найти точку справедливой уступки крайне затруднительно.

Переход от одного варианта из области компромиссов к другому из этой же области всегда сопровождается улучшением по одному из критериев и ухудшением по другому (другим) критерию. Принцип справедливой уступки основан на оценке и сопоставлении прироста и убыли локальных факторов. Оценка может производиться по абсолютному значению прироста или убыли критериев, либо по относительному (абсолютная и относительная уступка).

а) Справедливым по *принципу абсолютной уступки* считается компромисс, при котором абсолютное значение суммы снижения одного или нескольких критериев не превосходит абсолютного значения суммы повышения других критериев. Принцип абсолютной уступки может быть выражен следующей формулой:

$$q_{\text{опт}} = \left\{ q / \sum_{j \in I^{(+)}} \Delta q_j \geq \sum_{i \in I^{(-)}} \Delta q_i \right\} \in Q^k,$$

где Q_k- область компромиссов, $I^{(+)}$ и $I^{(-)}$ – подмножество мажорируемых и минорируемых критериев, q_i и q_j - абсолютные величины приращения.

б) При применении *принципа относительной уступки* выбирается тот вариант проекта, при котором сумма относительного снижения одних критериев меньше суммы относительного повышения других.

Принцип относительной уступки:

$$q_{\text{опт}} = \left\{ q / \sum_{j \in I^{(+\}} \Delta \chi_j \geq \sum_{i \in I^{(-)}} \Delta \chi_i \right\} \in Q^k,$$

где $\chi_j = \Delta q_j / q_{j\max}$; $\chi_i = \Delta q_i / q_{i\max}$ - относительные изменения критериев.

Целесообразно выбрать тот вариант, при котором суммарный относительный уровень снижения одних критериев меньше суммарного относительного уровня повышения других критериев.

5. *Принцип выделения одного оптимизируемого критерия*. Один из критериев объявляется оптимизируемым и выбирается тот вариант решения, при котором значение данного критерия достигает экстремума. На остальные критерии накладываются ограничения.

$q_{opt} = \max q_i$,

при $q_{i \neq j} \geq q_{i\text{доп}}$ ($q_{i \neq j} \leq q_{i\text{доп}}$).

Так как во многих практических случаях шкалы измерения критериев различны, для поиска решения в области компромиссов производится нормализация пространства критериев. После нормализации можно прово-

дить ранжирование критериев по их важности. Численно это формализуется приписыванием весов каждому из рассматриваемых критериев. Далее в качестве целевой функции выбирается линейная или степенная модель важности и производится поиск оптимального решения подобно выбора наилучшего объекта из списка предложенных.

6. *Случайное и неопределенное свертывание показателей*. Целевой функцией системы объявляется тот или иной показатель функционирования (внешний параметр). В общем случае частные показатели могут зависеть от случайных или неопределенных факторов. Допустимый вариант проекта системы также может зависеть от случайных или неопределенных факторов. Неопределенность требований к системе, некомпетентность или неуверенность разработчика и заказчика приводят к тому, что выбранная целевая функция (в частности, весовые коэффициенты) случайна.

Приведенные методы позволяют производить свертку многокритериальной задачи.

3.3.3. Выбор компонентов для реализации системы защиты

На втором этапе решается задача оптимального проектирования внутри области компромиссов. Рассмотрим математическую постановку задачи оптимального выбора состава способов и средств защиты в форме, которая позволит свести ее к стандартным задачам математического программирования.

Выбор необходимых средств M_j, из всего подобного множества доступных (сертифицированных) для построения системы защиты информации, обеспечивающих перекрытие заданных угроз и минимизацию затрат на защиту информации, сформулируем в виде задачи о наименьшем покрытии[67].

[67] Кристофидес Н. Теория графов. Алгоритмический подход. М.: Мир, 1978. 429с.

Пусть дано множество механизмов защиты информации $M=\{M_1,\ldots,M_m\}$. Совокупность его подмножеств $\{M_j\}$ называется покрытием множества М. Каждому M_j приписан вес C_j – затраты на j-е средство защиты по ТСО. Требуется найти покрытие, имеющее минимальный суммарный вес.

Введем переменные x_j, j =1,…, m. Переменная x_j =1, если механизм защиты входит в покрытие, иначе x_j=0.

Определим матрицу $A=\{a_{jk}\}$, j=1,…,m, k=1,…,l:

$$a_{jk} = \begin{cases} 1, & \text{если средство } j \text{ защищает от угрозы } i, \\ 0, & \text{иначе} \end{cases}$$

Задача состоит в нахождении вектора целочисленных варьируемых переменных $X=\{x_j\}$, j = 1,...,m, минимизирующих линейную целевую функцию:

$$F(X) = \sum_{j=1}^{m} C_j x_j \rightarrow min \qquad (3.1)$$

при ограничениях

$$\sum_{j=1}^{m} a_{jk} x_j \geq 1, \; k = \overline{1,l} \qquad (3.2)$$

$$\sum_{k=1}^{l} a_{jk} x_j \geq 0, \; j = \overline{1,m} \qquad (3.3)$$

где x_j - принимают значения 0 или 1;

m - число рассматриваемых средств защиты информации;

l - количество учитываемых угроз;

C_j – затраты по ТСО выбранного средства защиты.

Условия (3.2) выражают требования обеспечения противодействие любой угрозе с помощью хотя бы одного из используемых механизмов защиты.

Если значение x_j= 1, то это соответствует включению в проектируемую систему защиты информации соответствующего (j-го) средства защиты.

Если $x_j = 0$, то j-е средство защиты в проектируемую систему защиты информации не включается.

Часто одно средство защиты может сразу обеспечить противодействие нескольким угрозам, в таком случае, оно будет встречаться в столбце матрицы А не один раз. Если же каждое средство защиты должно противодействовать только одной угрозе, то задачу покрытия можно свести к задаче о назначениях.

Для решения оптимизационной задачи формирования комплекса средств защиты в форме задач покрытия и о назначениях можно использовать достаточно эффективные алгоритмы, известные в теории дискретного математического программирования.

На Рисунке 3.30 представлен алгоритм решения задачи построения экономически эффективной системы защиты информации таможенных органов.

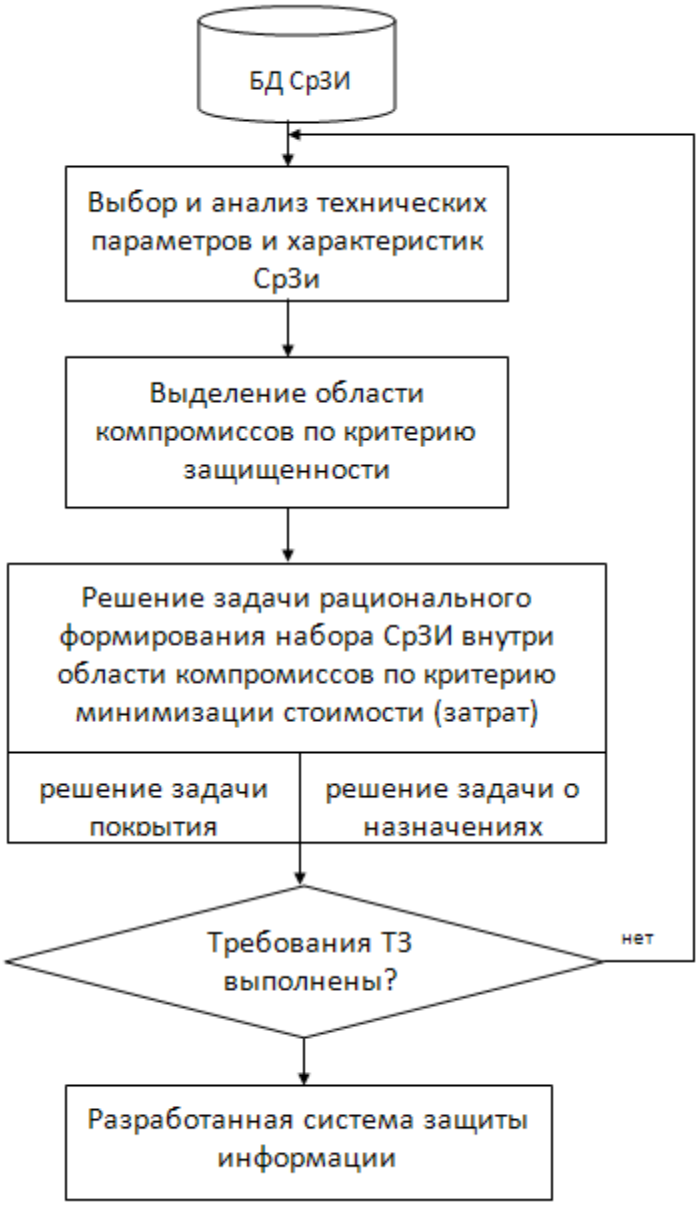

Рис. 3.30. Алгоритм решения задачи построения экономически обоснованного системы защиты информации.

Таким образом, построенная с применением данного алгоритма система защиты информации является экономически эффективной. Построение области компромиссов позволяет обоснованно выбрать те механизмы защиты, которые обеспечивают защищенность не ниже заданного уровня и соответственно возможность противостояния атакам, что находит прямое

отражение на значении убытков или ущерба от нарушений безопасности информации. Выбор же средств защиты информации по критерию минимизации затрат позволяет использовать более дешевый вариант для достижения приемлемого уровня защищенности.

Методика построения экономически эффективной системы защиты информации АИС таможенных органов РФ

Для достижения цели - построения экономически оправданной системы защиты информации таможенных органов, необходимо придерживаться определенного алгоритма проведения работ.

Исходными положениями для методики является проектируемые или модернизируемые информационные системы и информационные ресурсы ЕАИС ФТС России. Должна быть известна архитектура данной информационной системы, ее компоненты и взаимодействие между ними. Разработана политика безопасности рассматриваемой системы при обработке конфиденциальной информации таможенных органов. А также известны как программные, так и технические средства защиты информации, позволяющие эффективно противодействовать выявленным угрозам безопасности информации.

Общая схема методики построения системы защиты подсистемы ЕАИС ТО представлена на рисунке 3.31.

Рис. 3.31. Схема методики построения системы защиты ЕАИС ТО

Рассмотрим подробнее каждый из шагов.

1. Разработка вариантов декомпозиции распределенных АИС ТО .

Функционирование ЕАИС ФТС России организовано по иерархическому принципу, ее подсистемы относятся к разным уровням организационной структуры таможенных органов (центральный аппарат, региональное управление, таможня, таможенный пост). Таким образом, существующая декомпозиция ЕАИС по организационным уровням порождает множество взаимодействующих подсистем, имеющих собственную систему защиты информации. Это позволяет рассматривать систему защиты распределенной ЕАИС в виде отдельных систем защиты информационных подсистем взаимодействующих через различные защищенные соединения. В результате эти системы защиты могут проектироваться, эксплуатироваться и модернизироваться раздельно. Информационное взаимодействие подсистем должно быть защищено от перехвата, искажения или уничтожения информации при передаче по линиям связи. Каждая подсистема в свою очередь может быть подвержена дальнейшей декомпозиции на подуровни в соответствии с функциональным назначением ее компонентов.

2. Определение информационных ресурсов - объектов защиты O_i .

Информация в вычислительной системе не существует сама по себе. Она может храниться в электронном виде в файле или базе данных, она может быть расположена на сервере, персональном компьютере или на рабочей станции, подключенной к ведомственной сети или сети Интернет, информация может быть в статическом состоянии или находиться в процессе модификации и передачи по каналам связи. Информация, имеющая ценность для таможенных органов и находящаяся в распоряжении таможенных органов может быть представлена на любом материальном информационном ресурсе в форме пригодной для ее обработки, хранения или передачи.

Независимо от формы существования и средств ее хранения или распространения информация должна быть адекватно защищена. При этом обеспечение

безопасности этой информации выражается в создании необходимой защиты соответствующих ей ресурсов (объектов) информационной системы, то есть защиты технических и программных средств информатизации.

На данном этапе выявляются объекты информационной системы, состоящие из активных и пассивных компонентов системы и подлежащие защите. Сбор сведений об архитектуре информационной системы и информации, циркулирующей в ней, позволяет выявить уязвимости и оценить достаточность принятых мер защиты. В итоге формируются множество всех объектов $O = \{O_i\}$, i=1,...,n, их совокупность позволяет сформулировать требования к системе защиты.

Для сбора информации о системе могут быть использованы различные методы, в том числе изучение проектной документации, анкетирование или опрос технического и административного персонала, занимающегося разработкой или поддержкой информационных систем.

3. Оценка рисков с описанием возможных сценариев угроз.

После того как защищаемые ресурсы конкретизированы, для построения сбалансированной системы защиты на данном этапе предполагается провести определение уязвимостей, потенциальных угроз и анализ информационных рисков в отношении сформированного перечня информационных ресурсов. Выявление угроз, уязвимостей и связанного с ними риска соответствует специальным нормативным документам по обеспечению защиты информации, принятым в Российской Федерации, и соответствующим международным стандартам.[68]

Угрозы могут быть естественными, относящимися к природной среде, или быть связанными с человеком. К угрозам можно отнести любое обстоятельство или событие, которое может нанести урон информационной системе. Государственные и частные компании ведут постоянную идентификацию новых угроз безопасности информационных систем, данные списки угроз опубликованы в

[68] ISO 15408 «Информационная технология – методы защиты – критерии оценки информационной безопасности», а также стандарт ISO 17799 «Управление информационной безопасностью»

стандартах безопасности, регулирующих документах ФСБ России и ФСТЭК России, средствах массовой информации и т.д.

При использовании источников информации об известных уязвимостях и угрозах безопасности систем рекомендуется учитывать только те актуальных угрозы безопасности, которые действительно могут произойти в данной среде при конкретных условиях эксплуатации. Для выявления уязвимостей и угроз возможно также использование автоматических средств анализа защищенности (сканеров уязвимости), позволяющих провести сканирование системы на проникновение и выявить уязвимости системы.

Если АИС находится в стадии разработки, поиски угроз должны сосредоточиться на политике безопасности, на планируемых процедурах безопасности, системных требованиях, анализе безопасности средств информатизации, проведенных разработчиками или поставщиками. Если АИС находится в эксплуатации, идентификация угроз должна дополнительно включать в себя анализ характеристик безопасности информационной системы, программных, технических и организационных средств контроля, используемых для защиты системы, а также результаты аттестации (сертификации) системы.

Для построения модели угроз можно использовать оценку вероятностей реализации каждой выявленной угрозы с помощью шкалы, представленной в табл. 3.2. Построенная модель угроз является исходными данными для оценки рисков безопасности информации. Оценка рисков информационной безопасности производится на основании оценивания вероятности реализации угрозы и ущерба от нарушений безопасности для рассматриваемых информационных ресурсов (табл.3.3). Данные показатели могут быть переведены в цифровую шкалу и перемножены с последующим ранжированием полученных значений для получения количественного значения риска. Этот способ использован в методике оценки

риска NIST национального института стандартов и технологий США[69] , и в методике CRAMM, которая разработана Службой Безопасности Великобритании[70]

Экспертные оценки и анализ их с помощью механизма нечеткого вывода является основным методом при получении оценки риска. Этот метод преобразует входные данные в выходную переменную, т.е. в оценку риска. На основании анализа рисков разрабатываются или модернизируются системы защиты.

Таким образом, множеству объектов информационной системы, подлежащих защите $O = \{O_i\}$, i=1,...,n ставится в соответствие множество угроз безопасности для данной системы $T = \{T_k\}$, k=1,...,l. Множество отношений угроза – объект защиты образует граф {<T, O>}.

4. Составление для каждой угрозы списка существующих средств и механизмов обеспечения информационной защиты {M_j}.

Определение набора критериев механизмов защиты и их ограничений.

На основании модели угроз и оценки рисков выбираются технологии, которые могут эффективно противодействовать угрозам безопасности. Создаются списки доступных механизмов защиты, реализующих выбранные технологии.

Каждая угроза должна быть перекрыта одним или более механизмом обеспечения безопасности информации, представленному на рынке, и относящихся к рекомендованному оборудованию. Построенное множество механизмов защиты $M= \{M_j\}$, j=1,...,m, представляет собой набор средств защиты, противодействующих одной или более угроз безопасности объектам подсистемы. Система защиты будет представлять собой отношения между элементами множеств «угроза – механизм защиты – объект защиты» {<T, M, O>}.

Выбор технологий и средств защиты основывается на анализе параметрических показателей объектов. Определение критериев для оценки механизмов защиты выполняется путем анализа исходных данных, учитывающих особенности

[69] Risk Management Guide for Information Technology Systems. NIST, Special Publication 800-30.. - 736 с.

[70] Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность / Изд. М.: Компания АйТи; ДМК Пресс, 2004. - 384 с.

функционирования системы защиты, экономические и ресурсные ограничения, квалификацию пользователей и т. д. Формирование и выбор таких критериев, отражающие наиболее существенные аспекты создаваемой или модернизируемой системы защиты, является основой для проведения всего процесса построения рациональной системы защиты. Это, прежде всего показатели, учитывающие различные виды и составляющие затрат, отражающие надежность и уровень обеспечиваемой эффективности (защищенности) реализуемой технологии. Среди второстепенных критериев можно выделить необходимый объем оперативной памяти, быстродействие, показатели простоты и удобства использования и т.д.

Таким образом, каждое из средств защиты можно описать набором критериев, интересующих заказчиков системы:

$M_j = \{ C_j , \{P_{jk}\}, W_j , V_j, ,\ldots\}$,

где C_j – затраты j-го средства защиты по ТСО;

$\{P_{jk}\}$ – множество относительных показателей эффективности (защищенности) j-го средства защиты для k-ой угрозы безопасности;

W_j – быстродействие j-го средства защиты (начало обеспечения эффективной защиты в течении определенного промежутка времени);

V_j – объем оперативной памяти, используемый j-м средством защиты.

По мере необходимости заказчики системы защиты могут добавлять новые критерии для оценки механизмов безопасности.

Для дальнейших математических расчетов данные критерии должны быть выражены количественно. Перед проектировщиками системы защиты ставится задача, как можно точно оценить каждый механизм защиты по интересующим критериям. В случае невозможности найти значения показателей в технической документации, измерить непосредственно в результате эксперимента или вычислить аналитически с использованием накопленных статистических данных, опубликованных различными аналитическими агентствами , необходимо использо-

вать методы экспертной оценки, включающие опрос экспертов по оценке критериев и статистическая обработка полученных результатов[71] .

5. Оценка показателей эффективности (защищенности) средств защиты для каждой из угроз безопасности $\{P_{jk}\}$

Относительный показатель эффективности (защищенности) j-го средства защиты противодействовать k-ой угрозе безопасности P_{jk} – количественная характеристика оценки уровня обеспечиваемой информационной защиты, которой обладают средства защиты при осуществлении данной угрозы. Значение этого показателя представляет собой вероятность непреодоления защиты j-го средства при реализации k-й угрозы и лежит в переделах от 0 до 1. Уровень защищенности на практике не может достигать 1, так как стопроцентная защита не существует. Чем больше этот показатель, тем эффективнее использование данного средства защиты для противодействия угрозе. Тогда вероятность преодоления защиты j-го механизма при появлении k-й угрозы составит соответственно (1- P_{jk}). При отсутствии перекрытия механизмом защиты M_j определенной угрозы T_k, показатель эффективности P_{jk} средства защиты для угрозы безопасности принимается равным 0. На практике получение точных значений приведенных характеристик относительной эффективности затруднено, т. к. эти понятия угрозы, риска и «сопротивляемости» механизма защиты трудноформализуемы. И чаще всего для их оценивания применяется опрос экспертов и методы нечеткой логики или статистические методы для обработки полученных оценок.

Для решения задачи рационального построения системы защиты информационных систем таможенных органов необходимо найти наилучшее сочетание имеющихся на рынке средств и механизмов защиты, обеспечивающих минимизацию затрат при выполнение заданных ограничений и обеспечении требуемого уровня защиты. Набор средств и механизмов, отражаемый матрицей M должен

[71] Китаев Н.Н. Групповые экспертные оценки. М.: Знание. 1975 г. – 64 с.

перекрывать все множество угроз критичных для данной системы. Текущий состав комплекса средств защиты записывается следующим вектором $\overline{M}$:

$$\overline{M} = \begin{bmatrix} M_1 \\ M_2 \\ M_3 \\ \dots \\ M_m \end{bmatrix} = \begin{bmatrix} \{C_1, \{P_{1k}\}, W_1, V_1, \dots\} \\ \{C_2, \{P_{2k}\}, W_2, V_2, \dots\} \\ \{C_3, \{P_{3k}\}, W_3, V_3, \dots\} \\ \dots \\ \{C_m, \{P_{mk}\}, W_m, V_m, \dots\} \end{bmatrix}, \text{ k=1,...,l}$$

После построения матрицы всех отвечающих заданным требованиям вариантов защиты осуществляется решение задачи оптимизации по выбранным критериям. Данная задача является многокритериальной и решается на следующих шагах алгоритма.

Поэтому в предлагаемом алгоритме построение рациональной системы защиты с учетом относительного показателя эффективности и стоимости разбито на два этапа.

6. Выделение области компромиссов по заданным критериям.

На первом этапе определяются наиболее подходящие комплексы средств защиты по критерию эффективности (защищенности) для каждой угрозы безопасности, а также, если необходимо, по быстродействию и объему памяти и другим критериям, заданными заказчиком. Решение задачи на данном этапе, чаще всего, представляет собой некоторое подмножество приблизительно равных по качеству вариантов, называемое областью Парето (или областью компромиссов)[72]. Часто область Парето содержит довольно большое число вариантов. При этом практически все варианты из этой области равнозначны, поэтому выбор сделать крайне сложно.

После того как каждый параметр компонентов получил количественную оценку, формулируется задача оптимального проектирования. Когда все параметры оценены количественно, она превращается в задачу многокритериальной оп-

[72] Корнеенко В. П. Методы оптимизации. М.: Высшая школа, 2007. 664 с.

тимизации, которая может быть решена математическими методами (линейное, векторное, динамическое программирование). В ином случае могут использоваться неформальные подходы поиска оптимального решения.

7. Решение задачи покрытия, обеспечивающей перекрытие заданных угроз и минимизацию затрат на защиту информации.

На этом этапе решается задача оптимального проектирования внутри области компромиссов с помощью математической модели, описанной в подпараграфе 3.3.2. Решением рационального проектирования системы является набор выбранных компонентов M_1, M_2 , M_3 , … , M_m, при котором соблюдаются все установленные ограничения.

8. Принятие варианта подсистемы защиты происходит после перебора всех вариантов декомпозиции системы и сравнения полученных результатов с техническим заданием.

При проектировании и практической реализации механизма защиты с учетом экономических показателей один и тот же уровень обеспечения защиты информации может быть достигнут при меньших материальных затратах. Основной задачей данной методики является научное обоснование процесса выбора средств защиты в процессе разработки или модернизации систем защиты информации информационных систем таможенных органов за счет правильной оценки эффективности принимаемых решений и выбора рационального варианта технической реализации системы защиты информации.

Предложенная методика позволяет проводить оценку эффективности применения механизмов защиты информации в таможенных органах. Ее можно также применять для технико-экономического обоснования создания и модернизации системы защиты информации в информационных системах таможенных органов.

ЗАКЛЮЧЕНИЕ

Целью представленного в монографии исследования являлась разработка методологического подхода по проведению экономической оценки информационных продуктов и услуг, позволившего предложить совершенствование механизма закупок программных средств и оптимизацию затрат на защиту информации применительно к таможенным органам.

В ходе исследования:

проанализирован отечественный опыт расчета экономического эффекта и оптимизации затрат при разработке информационных систем;

выявлена роль информатизации, информационных и программных продуктов, защиты информации в обеспечении таможенной деятельности;

описаны экономические характеристики таможенных информационных услуг ;

предложена методология экономической оценки информационных продуктов и услуг;

проанализировано обеспечение деятельности таможенных органов программными средствами;

разработан научно-методический аппарат закупок программных средств для нужд таможенных органов;

даны рекомендации по совершенствованию механизма закупок программных средств;

дана общая характеристика и проанализированы проблемы защиты информации в распределенных автоматизированных информационных системах таможенных органов;

рассмотрены вопросы управления рисками и инвестициям при обеспечении безопасности информации;

разработаны модели и представлены методические рекомендации по минимизации затрат на защиту информации.

Принятие теоретических положений и методических рекомендаций монографии позволит:

методически правильно оценивать полезность информационных продуктов и услуг и затраты на их создание или приобретение;

обосновывать начальную (максимальную) цену контракта при закупке таможенными органами программных средств;

осуществлять выбор экономически эффективных стратегий защиты информации, когда при выборе из множества имеющихся средств защиты информации выбираются такие, которые обеспечивают достижение требуемых значений параметров системы при минимальном расходовании ресурсов.

Представленные в монографии результаты могут быть полезным для специалистов Главного управления информационных технологий и Центрального информационно-технического таможенного управления ФТС России, занимающимися разработкой задач для Единой автоматизированной информационной системы таможенных органов и организацией обеспечения информационной безопасности, для научных работников, преподавателей, аспирантов и студентов, обучающихся по специальности «Таможенное дело», экономическим и информационным специальностям.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

Официальные законодательные и нормативные документы

1. Доктрина информационной безопасности Российской Федерации, утверждённой Президентом Российской Федерации 9 сентября 2000 г. Режим доступа: World Wide Web. URL: http://www.consultant.ru.

2. Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи». Режим доступа: World Wide Web. URL: http://www.consultant.ru.

3. Федеральный закон Российской Федерации от 4 мая 2011 года № 99-ФЗ «О лицензировании отдельных видов деятельности». Режим доступа: World Wide Web. URL: http://www.consultant.ru.

4. Постановление Правительства Российской Федерации от 26 июля 2006 г. № 459. Режим доступа: World Wide Web. URL: http://www.consultant.ru.

5. «Гражданский кодекс Российской Федерации (часть четвертая)» от 18.12.2006 № 230-ФЗ. М.: consultant.ru, 2014. Режим доступа: World Wide Web. URL: http://www.consultant.ru.

6. Решение Совета Евразийской экономической комиссии от 16.07.2012 N 54 "Об утверждении единой Товарной номенклатуры внешнеэкономической деятельности Таможенного союза и Единого таможенного тарифа Таможенного союза".

7. Концепция обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года (утв. Приказом ФТС России от 13 декабря 2010 г. № 2401).

8. Приказ ФТС России от 17.01.2007 № 55 «Об утверждении Положения о Главном управлении информационных технологий». М.: consultant.ru, 2014. Режим доступа: World Wide Web. URL: http://www.consultant.ru.

9. Письмо ФТС России от 17.03.2006 г. №15-14/8524 «О таможенном оформлении информации, передаваемой по сети Интернет». М.: consultant.ru, 2014. Режим доступа: World Wide Web. URL: http://www.consultant.ru.

10. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

11. ГОСТ Р ИСО/МЭК 27001-2006 Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Режим доступа: World Wide Web. URL: http://www.consultant.ru.

12. Межгосударственный стандарт ГОСТ 19781-90 «Обеспечение систем обработки информации. Программное» (утв. постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 27 августа 1990 г. № 2467) . М.: consultant.ru, 2014. Режим доступа: World Wide Web. URL: http://www.consultant.ru.

13. Межгосударственный стандарт ГОСТ 28806-90 «Качество программных средств. Термины и определения» (утв. постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 25 декабря 1990 г. № 3278) . М.: consultant.ru, 2014. Режим доступа: World Wide Web. URL: http://www.consultant.ru.

14. Межгосударственный стандарт ISO 15408 «Информационная технология – методы защиты – критерии оценки информационной безопасности». Режим доступа: World Wide Web. URL: https://www.iso.org.

15. Межгосударственный стандарт ISO 17799 «Управление информационной безопасностью». Режим доступа: World Wide Web. URL: https://www.iso.org.

16. Межгосударственный стандарт ISO/IEC 20968 Software engineering - Mk II Function Point Analysis—Counting Practices Manual. Режим доступа: World Wide Web. URL: https://www.iso.org

17. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). - М: Гостехкомиссия России, 2001.

Монографии, учебные пособия, сборники, материалы конференций

18. Allen Julia Making the Business Case for Information Security: Selling to Senior Management// Carnegie Mellon University at InfoSec World – 2003. - March 10.

19. Anil K. Sharma Economic Value Added (EVA) - Literature Review and Relevant Issues. International Journal of Economics and Finance, Vol 2, No 2, 2010. p.21.

20. Philip Robinson, Bryan Stephenson TCO-aware provisioning of information security infrastructure. HP Laboratories, 2008. p. 21.

21. Risk Management Guide for Information Technology Systems. NIST, Special Publication 800-30. - 736 с.

22. Sonnenreich, Wes; 'Return on Security Investment (ROSI): A Practical Quantitative Model', Journal of Research and Practice in Information Technology, vol., 38, no. 1, February 2006, Australia, 2006.

23. Бизин С.В. Информационные продукты таможенных органов: классификация, стоимость, потребительская ценность. Вестник Российской таможенной академии № 2. М.: Изд-во Российской таможенной академии, 2010. – С. 131 – 138.

24. Васина А.А. Финансовая диагностика и оценка проектов / Васина А.А. - СПб.: Питер, 2004. – 389 с.

25. Глушков В.М. Мышление и кибернетика // Вопросы философии. 1963. №1. С. 36 - 42.

26. Гупанова, Ю. Е. Концептуальные и методологические основы оптимизационно-адаптивного управления качеством таможенных услуг в условиях неопределенности и риска: монография / Ю. Е. Гупанова; РТА. - Люберцы: Изд-во РТА, 2011. - 106 с.

27. Гусев С.Л. Совершенствование архитектуры Единой автоматизированной информационной системы ФТС России. Актуальные проблемы теории и практики таможенного дела и пути их решения: сборник материалов Международной научно – практической конференции: в 2 ч. Ч. 2. М.: Изд-во Российской таможенной академии, 2010. – С. 35 – 37.

28. Жимерин Д.Г., Мясников В.А. Автоматизированные и автоматические системы управления. – М.: «Энергия», 1975. – 680 с.

29. Заде Л. Понятие лингвистической переменной и ее применение к принятию приближенных решений, М.: Мир, 1976. – 235 с.

30. Информационные продукты таможенных органов: стоимость, потребительская ценность, конфиденциальность: монография / Э.П. Купринов, С.В. Бизин, Ю.И. Сомов. – М.: РИО РТА, 2011. – 111 с.

31. Калайда В.Т. Технико-экономическое обоснование стоимости программных систем: методическое пособие по выполнению экономической части выпускной квалификационной работы для студентов специальности 230105 «Программное обеспечение вычислительной техники и автоматизированных систем». – Томск: ТУСУР, 2009. – 50 с.

32. Китаев Н.Н. Групповые экспертные оценки. М.: Знание. 1975 г. – 64 с.

33. Корнеенко В. П. Методы оптимизации. М.: Высшая школа, 2007. – 664 с.

34. Кристофидес Н. Теория графов. Алгоритмический подход. М.: Мир, 1978. – 429 с.

35. Липатова Н.Г. Экономическая сущность таможенного контроля в в системе государственного контроля [Текст] / Н.Г. Липатова// Проблемы экономики и управления нефтегазовым комплексом. – 2014. – № 6. – С. 52 – 56.

36. Липатова Н.Г., Вялов М.А. Информационные технологии и современная таможня. Таможенная служба России на защите экономических интересов страны: Материалы докладов Всероссийской научно-практической конференции. – М.: Изд-во Российской таможенной академии, 2003. – С. 336 – 339.

37. Макрусев, В. В. Маркетинг таможенных услуг [Текст] : учебник / В. В. Макрусев, В. Ю. Дианова ; РТА. - 2-е изд., перераб. и доп. - М. : Изд-во РТА, 2010. – 298 с.

38. Мину М. Математическое программирование. Теория и алгоритмы. Пер. с франц. А.И. Штерна. - М.: Наука. - 1990 г. – 486 с.

39. Модернизация таможен. Справочное руководство / Под редакцией Люка де Вульфа и Хосе Б. Сокола. Всемирный банк реконструкции и развития. 2005. – 327с.

40. Научные аспекты инновационных исследований: материалы I Международной научно-практической конференции, г.Самара, 6–8 марта 2013г. – Самара: Изд-во ООО «Инсома-пресс», 2012.– Т.1-2. – 248 с.

41. Никитченко И.И., Павлюченков К.А., Соколов С.М. Оценка эффективности внедрения информационных технологий – приоритетная задача оптимизации деятельности таможенных органов Российской Федерации. Актуальные проблемы теории и практики таможенного дела и пути их решения: сборник материалов Международной научно – практической конференции: в 2 ч. Ч. 2. М.: Изд-во Российской таможенной академии, 2010. – С. 110 – 115.

42. Петренко С.А., Симонов С.В. Управление информационными рисками: Экономически оправданная безопасность. – М.: ДМК пресс, 2004. – 381 с.

43. Постышев Л.П. Методологические вопросы оптимального моделирования экономики на основе теории трудовой стоимости/Автореферат диссертации на соискание ученой степени кандидата экономических наук. - М.: АОН при ЦК КПСС, 1972.

44. Проблемы совершенствования правовой системы информационной безопасности таможенного дела: монография / М.И. Агабалаев, А.Н. Дюков, Н.М. Кожуханов и др. М.: Изд-во Российской таможенной академии, 2009. – 188 с.

45. С.Д. Бешелев, Ф.Г. Гурвич. Математико-статистические методы экспертных оценок. - 2-е изд., перераб. и доп. - М.: Статистика. 1980 г. - 263 с.

46. Семененко В.А. Информационная безопасность: Учебное пособие. 2-е изд., стереотип. – М.:МГИУ, 2006. – с. 277.

47. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность / Изд. М.: Компания АйТи; ДМК Пресс, 2004. - 384 с.

48. Сифоров В.И. Наука об информации и ее проблемы / В.И. Сифоров. – М.: Наука, 1992. – 289 с.

49. Федоров В.В. Информационные таможенные технологии: Учебник. – М.: РИО РТА, 2007. – 216с.

50. Экономическая модель услуги для анализа возможных инноваций в таможенной сфере / Ю.И. Сомов // Международная научно-практическая конференция Российской таможенной академии: матер. конф. – М., 2013. – С. 236 – 240.

Диссертации и авторефераты

51. Амелина О.В. Управление качеством проектов по созданию продуктовых инноваций (на примере разработки программного обеспечения): дисс. … канд. экон. наук. / Орловский государственный технический университет. – Орел, 2003 г. – 177 с.

52. Ермаков И.А. Логистическая поддержка процесса разработки интеллектуальной продукции в сфере производства программного обеспечения: дисс. … канд. эконом. наук / ГОУ ВПО ГУУ. – М., 2004. – 193 с.

53. Ляпунов А.Д. Модели и методы повышения эффективности развития системы управления сбытом программных продуктов: дисс. … канд. эконом. наук / Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики. – СПб, 2012. – 201 с.

54. Скалкин В.В. Управление внедрением программного обеспечения технологической подготовки производства на машиностроительном предприятии:

авт. дисс. … канд. экон. наук. / Государственная ордена Трудового Красного Знамени Академия Управления имени Серго Орджоникидзе. – М., 1993 г. – 19 с.

55. Степанов А.Н. Инновации в области применения программного обеспечения систем управления проектами: дисс. … канд. эконом. наук / ГОУ ВПО Государственный университет управления. – М., 2003. – 124 с.

Интернет ресурсы

56. Академия Cisco при ЯрГУ им. П.Г. Демидова. Режим доступа: World Wide Web. URL: http://www.cisco.yar.ru/links/Tekama.php

57. Альта – Софт. Заполнитель документов. Режим доступа: World Wide Web. URL: http://www.alta.ru/zapolnitel.php

58. Девятое ежегодное исследование российской индустрии экспортной разработки программного обеспечения. Режим доступа: World Wide Web. URL: http://www.russoft.ru

59. Министерство экономического развития Российской Федерации. Режим доступа: World Wide Web. URL: http://www.economy.gov.ru

60. Портал закупок. Режим доступа: World Wide Web. URL: http://zakupki.gov.ru.

61. Результаты конкурсных торгов. Центральное информационно-техническое таможенное управление. Режим доступа: World Wide Web. URL: http://edpc.customs.ru.

62. Рынок информационной безопасности Российской Федерации Режим доступа: World Wide Web. http://www.pcidss.ru/files/pub/pdf/Pervoe-expertnoe_issledovanie_rynka.IB.pdf.

Приложение 1

Моделирование экономики на основе теории трудовой стоимости

Исследователем Л.П. Постышевым[73] была проанализирована проблема оптимального моделирования необходимого и прибавочного продукта. На основе критического анализа существующих моделей и их интерпретаций, руководствуясь экономическим учением К.Маркса о необходимом и прибавочном продукте, автор предпринял попытку построения соответствующих этому учению обобщенных оптимальных статических и динамических моделей экономики.

С позиций трудовой экономической теории доцентом Л.П. Постышевым была предпринята попытка построения оптимальных статических и динамических народнохозяйственных моделей. Им была обоснована методология построения оптимальных моделей экономики. На основе критического анализа существующих моделей и руководствуясь экономическим учением К.Маркса о необходимом и прибавочном продукте, автор предпринял попытку построения в соответствии с ним оптимальных статических я динамических моделей социалистической экономики.

Относительно простая статическая модель приводится ниже. Ее автором были использованы следующие математические обозначения:

Матрицы: $A = \begin{bmatrix} A_1 \\ A_2 \\ A_3 \end{bmatrix}$ - матрица технологических коэффициентов в натуральном выражении порядка $m \times n$ состоит из трех подматриц; A_1 порядка $m_2 \times n$ – коэффициентов выпуска продукции $(a_{ij} \rangle 0)$ и материальных затрат, идущих на производство единицы (комплекса) выпускаемой продукции $(a_{ij} \le 0)$; A_3 порядка $m_3 \times n$ коэффициентов использования природных ресурсов $(a_{ij} \le 0)$; E_0 – матрица нали-

[73] Постышев Л.П. Методологические вопросы оптимального моделирования экономики на основе теории трудовой стоимости/Автореферат диссертации на соискание ученой степени кандидата экономических наук. - М.: АОН при ЦК КПСС, 1972.

чия новых производственных фондов порядка $m_2 \times \int$. В тех строках этой матрицы, которые соответствуют строкам использования новых фондов в матрицу A_2, расположены по одной +I, каждая в своем особом столбце. Все остальные элементы матрицы - нули. Количество различаемых в модели видов новых фонтов равно $\int$; A_f - матрица удельных фондоемкостей j - х технологе порядка $m_1 \times n$

Векторы-столбцы: все их компоненты неотрицательны, а размерности указаны буквой в скобках $(m_k):\alpha$ - заданный конечный продукт (m_1), $F = F_c + F_n$ – основные производственные фонды (m_2), F_c - старые, F_n - новые, произведенные в предшествующем (нулевом) периоде; Q. -природные ресурсы $(m_3):\mathrm{Z}$ – искомые оптимальные цены выпускаемой продукции $(m_1):p$ - искомые прокатные оценки действующая производственных фондов, воспроизводимых трудом $(m_2):r$ - искомые рентные оценки природных ресурсов $(m_3):v$ - прямые затраты на заработную плату в расчете на единицу (комплекс) продукции $(n):x$ искомые валовые выпуски продукции по всей j- м технологиям производства $(n):Y_0$ - искомые интенсивности выпуска новых средств производства в нулевом периоде $(\int)$. Отсюда следует: $E_0 Y_0 = F_N$ P - амортизационные отчисления с единицы каждого вида новых фондов - переносимая ими на продукт стоимость $(\int)$.

Скаляры: m^1 – норма прибавочного продукта; p^1 – норма прибыли.

Прямая задача математического программирования

$$\left.\begin{array}{l} A_1 X \geq \alpha \\ A_2 X + E_0 Y_0 \geq -F_c \\ A_3 X \geq -Q \\ \left[V^1(1+m^1) + p^1 \overline{\mathrm{Z}A_f}\right] X + P^1 Y_0 = \min \\ X; Y_0 \geq 0 \end{array}\right\} \quad (1)$$

Соответствующая ей двойственная задача:

$$\left.\begin{array}{l} A_1^{/}\mathrm{Z} + A_2^{/}p + A_3^{/}R \le V(1+m^{/}) + p^{/}A_f^{/}\overline{\mathrm{Z}} \\ E_O^{/}p \le p \\ d^1\mathrm{Z} - F_c^{/}p - Q^{/}r = \max \\ \mathrm{Z;p;r} \ge 0 \\ \mathrm{Z} = \overline{\mathrm{Z}} \end{array}\right\} II_0 \quad (2)$$

В этой модели m^1 и p^1 являются теми управляющими параметрами, с помощью которых может быть задана та или иная моделируемая концепция планового ценообразования. Возможность выбора концепции ценообразования вытекает из наличия в модели одной степени свободы - на две искомых переменных m^1 и p^1 накладывается лишь одно ограничение: $V^{/}\overline{X} = d_n^{/}\overline{\mathrm{Z}}$. Это математическое выражение экономического требования равенства выплаченной заработной платы $\left(V^{/}\overline{X}\right)$ сумме оптимальных цен товаров и услуг, предназначенных на ее покрытие $\left(d_n^{/}\overline{\mathrm{Z}}\right)$.

Если все рассмотренные концепции ценообразования позволяют исчислить систему оптимальных цен и получить соответствующий им экономический оптимум, то это еще не означает, что они равноценны в условиях социализма и приведут плановую экономику в результате развития к одинаковому итогу. Но проблема выбора концепции выходит за рамки статических моделей. Большое внимание Л.П.Постышевым было уделено попытке построения обобщенных оптимальных динамических народнохозяйственных моделей.

Чтобы обеспечить в моделях правильный выбор альтернативных технико-экономических и хозяйственных решений, с учетом предвидимых потребностей будущих периодов, выходящих за горизонт планирования, достаточно иметь информацию о предполагаемых темпах научно-технического прогресса я их влияния на экономику в отраслях материального производства. Получить такую информацию о будущем, конечно, легче, чем с равной надежностью прогнозировать все конкретные пути развития технического прогресса в отраслях, что необходимо

для получения аналогичной точности расчетов на традиционных динамических моделях.

В нынешних условиях целесообразно творчески заимствовать всё положительное в области экономико-математического моделирования, накопленное как в отечественной, так и зарубежной науке. Особенное внимание следует уделить изучению математических моделей, непосредственно связанных с проблематикой государственного регулирования экономики и цен.

Продуктовое моделирование, предметом которого является товар (группа товаров, агрегированный продукт) и учитывающее взаимное влияние цен возможно с использованием так называемых «шахматных» моделей, моделей типа «затраты - выпуск». К ним и относятся межотраслевой баланс (МОБ) и многопродуктовая модель цен (МПМ). Они иллюстрируют (имитируют) процесс формирования полных затрат труда на производство каждого продукта (или отрасли). Одновременно, они представляют картину расходования его на производство других продуктов (товаров) отраслей экономики.

Научное издание

Юрий Иванович СОМОВ
Эдуард Павлович КУПРИНОВ
Сергей Валерьевич КУРИХИН
Людмила Дмитриевна ЗАЙЦЕВА

ЭКОНОМИЧЕСКАЯ ОЦЕНКА И ОПТИМИЗАЦИЯ ЗАТРАТ НА РАЗРАБОТКУ ПРОГРАММНЫХ ПРОДУКТОВ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ТАМОЖЕННЫХ ОРГАНОВ

Монография

Издано в авторской редакции