На правах рукописи
УДК 519.816 (043)

СЕРЕДА СЕРГЕЙ АЛЕКСАНДРОВИЧ

Анализ рисков и минимизация потерь от нелегального распространения программных продуктов

Специальность: 08.00.13 – «Математические и инструментальные методы экономики»

АВТОРЕФЕРАТ

диссертации на соискание учёной степени
кандидата экономических наук

Москва 2005

Работа выполнена на кафедре Математического обеспечения и технологий программирования Московского государственного университета экономики, статистики и информатики (МЭСИ).

Научный руководитель:	кандидат экономических наук, доцент Благодатских Виктор Алексеевич
Официальные оппоненты:	доктор экономических наук, профессор Уринцов Аркадий Ильич
	кандидат экономических наук, доцент Егоров Михаил Иванович
Ведущая организация:	АО «Информационные технологии управления – ВНИИТ»

Защита диссертации состоится *24 февраля 2005 года в 14 часов* на заседании Диссертационного совета К 212.151.01 в Московском государственном университете экономики, статистики и информатики по адресу: 119501, Москва, ул. Нежинская, дом 7.

С диссертацией можно ознакомиться в библиотеке Московского государственного университета экономики, статистики и информатики.

Автореферат разослан *21 января 2005 года*

Ученый секретарь
диссертационного совета,
кандидат экономических наук, доцент Г.Е. Голкина

Общая характеристика работы

Актуальность темы. В последнее время необходимость сокращения теневого оборота программного обеспечения (ПО) становится всё более насущной. Рынок программных продуктов, как в России, так и во всём мире вышел на одно из первых мест по прибыльности и скорости роста, что обусловлено развитием информационных и коммуникационных технологий, а также наличием в мире мощного парка стандартизированных персональных компьютеров. Ввиду значительного влияния рынка ПО на экономику индустриально развитых стран последствия нелегального оборота программных продуктов (ППр) уже нельзя рассматривать как нанесение ущерба только производителям ПО. Указанный ущерб отражается на государственных доходах, оказывает общее негативное влияние на «высокотехнологичный» сектор экономики. По результатам отчёта «Business Software Alliance» и «IDC», опубликованного в июле 2004 года, совокупные мировые потери от «компьютерного пиратства» за 2003 год составили 28,794 млрд долл. Российская Федерация за этот же период потеряла 1,104 млрд долл., при этом на российском теневом рынке программных продуктов реализуется 87% от общего объёма продаж программных продуктов. В США «уровень пиратства» снижен до 23%, но считается, что и такой объём теневого оборота ПО неприемлемо высок. Согласно другому отчёту «IDC», снижение мирового теневого оборота ПО на 10% в ближайшие четыре года позволило бы создать в мировой экономике более миллиона новых рабочих мест и достигнуть её роста в размере 400 миллиардов долларов США.

Систематические исследования вопросов, связанных с несанкционированным распространением ПО, начались в конце 80-х годов XX столетия после осознания их важности и масштабов. В то же время существующие исследования предметной области не позволяют получить целостную картину исследуемого феномена, что затрудняет согласование научных результатов, полученных специалистами в различных областях. В частности, исследования, посвящённые техническим и технологическим аспектам «компьютерного пиратства», никак не учитывают существование других сторон рассматриваемого вопроса. Так же построены и работы, в которых рассматриваются правовые, психологические и экономические стороны теневого оборота ППр. Кроме того, авторы большей части публикаций предлагают бороться с теневым рынком программных продуктов, в основном используя меры и средства, основанные на принуждении, при помощи технических и правовых ограничений, без учёта экономических причин происходящего.

Таким образом, сегодня существует объективная необходимость комплексного экономического исследования причин возникновения и механизмов функционирования теневого рынка программного обеспечения для определения эффективных стратегий сокращения связанных с «компьютерным пиратством» рисков, как на частном, так и на общегосударственном уровне.

Цель и задачи исследования. Цель работы состоит в формировании экономико-математического инструментария, обеспечивающего принятие решений по противодействию теневому обороту программных продуктов.

После постановки цели были сформулированы основные задачи исследования:

- реализовать комплексный подход к исследованию теневого рынка программного обеспечения, систематизировать и расширить существующий опыт;
- построить целостное описание теневого рынка программного обеспечения с учётом его экономических, правовых, психологических и технических аспектов;
- проанализировать методики и решения из смежных дисциплин и разработать аналогичные, применительно к предметной области;
- провести экономический анализ нелегального распространения ПО на макро- и микроэкономическом уровне и построить соответствующие модели;
- разработать методики решения основных задач, связанных с противодействием нелегальному распространению программных продуктов.

Объект и предмет исследования. Объектом данного исследования являются меры, принимаемые участниками рынка и государством по борьбе с нелегальным оборотом программного обеспечения. В качестве предмета исследования рассматриваются экономические средства противодействия теневому рынку программного обеспечения.

Методика исследования. Диссертационное исследование базируется на научных результатах, полученных ведущими российскими и зарубежными специалистами в области экономики, правовой охраны интеллектуальной собственности, программно-технической защиты программного обеспечения, исследования операций и математического моделирования экономических процессов. Среди них следует отметить работы Гроувера Д., Ватолина В.С., Ляшева С.Г., Касперски К., Тимохиной И.Т., Немчиковой Р.Т., Расторгуева С.П., Дмитриевского Н.Н., Долгина А.Е., Потанина М.Ю., Семьянова П.В., Зегжды Д.П., Щербакова А., Юдкевич М., Ревинского О.В., Devanbu P.T., Stubblebine S., Drakos N., Moore R., Katz A., Samuelson P., Scotchmer S., Shy O., Thisse J.F., Poddar S., Takalo T., Warren-Boulton F.R., Baseman K.C., Woroch G.A. В работе были использованы такие общенаучные методы, как: экспериментальный; методы анализа и синтеза; индукции и дедукции; метод аналогий. Применялись также методы анализа алгоритмов, правового анализа, экономической криминалистики, анализа и управления рисками, экономического и математического моделирования.

Научная новизна. В рамках исследования получены обладающие научной новизной результаты:

- анализ теневого рынка ПО на макроэкономическом уровне, обеспечивший базу для оценки существующих и выработки новых государственных стратегий сокращения теневого оборота ПО;
- анализ теневого рынка ПО на микроэкономическом уровне, данные которого позволяют принимать управленческие решения, обеспечивающие эффективную защиту интересов производителя ПО;
- экономическая модель государственного регулирования рынка ПО, дающая возможность оценивать применяемые и планируемые меры противодействия нелегальному обороту компьютерных программ;
- математические модели экономического поведения производителя ПО, пользователя ПО и злоумышленника, на базе которых возможно оценивать

поведение агентов рынка ПО, а также прогнозировать результаты применения тех или иных мер и средств защиты ПО от теневого распространения;
- методики решения тактических и стратегических задач противодействия нелегальному распространению программных продуктов на государственном и частном уровне.

Кроме этого, в процессе исследования были осуществлены:
- исследование зарубежных и отечественных инструментальных средств программно-технической защиты ПО, на базе которого создана и представлена расширенная классификация средств защиты ПО, которая позволяет наглядно проводить оценку устойчивости защищённых программных продуктов, прогнозировать недостатки и уязвимости разрабатываемых систем защиты, а также облегчает принятие решений о применении того или иного типа средств защиты;
- анализ зарубежных и отечественных инструментальных средств исследования и модификации объектного кода компьютерных программ, на основе которого создана и впервые представлена классификация средств преодоления систем защиты ПО, впервые сформулирована обобщённая процедура преодоления произвольной системы защиты, что позволяет выполнять оценку времени безопасного использования средств защиты ПО и связанных с этим рисков;
- формулирование и классификация угроз для средств программно-технической защиты ПО, а также описание процедуры анализа и управления рисками при выводе защищённого программного продукта на рынок;

Диссертационное исследование соответствует пунктам 1.2-1.4, 2.5, 2.6 паспорта специальности 08.00.13 – «Математические и инструментальные методы экономики».

Практическая значимость, апробация и внедрение результатов. Основные положения и выводы исследования могут использоваться:
- для разработки и оценки программ государственного регулирования рынка программного обеспечения, направленных на сокращение теневого оборота ПО и связанных с ним экономических потерь;
- производителями программного обеспечения для оценки рисков при выводе своих продуктов на рынок и выбора действенных мер по снижению указанных рисков;
- производителями ПО при решении технических вопросов, связанных с программной защитой их продуктов от несанкционированного использования.

Результаты диссертационного исследования были представлены на конференции аспирантов при Молдавской экономической академии «Reformele economice în Moldova la sfârşit de mileniu» (23-25 сентября 1999 г.), Международной конференции «Информационно-психологическая безопасность и Интернет-технологии - IPSIT'99» (Кишинёв, 15 октября 1999 г.), Международной конференции «Bioetică, filisofie, medicină practică: Securitatea informaţională; sinergetică şi economia în asigurarea dezvoltării feritâ de primejde a societăţii» (Кишинёв, 19-20 апреля 2000 г., 24-25 апреля 2001 г.), Международной конференции «BiT+: INFORMATION TECHNOLOGIES – 2003» (Кишинёв, 7-11 апреля 2003 г.), Международной

конференции «Trends in the Development of the Information and Communication Technologies in Education and Management» (Кишинёв, 20-21 марта 2003 г.), Всероссийской научно–практической конференции «Правовая охрана интеллектуальной собственности в современных технологиях» (Москва, Зеленоград, 2 июня 2003 г., 7 июня 2004 г.), Коллегиальных Чтениях патентных поверенных «Интеллектуальная собственность: история и современность» (Санкт-Петербург, 25-26 июня 2003 г.), Международной конференции «Проблемы противодействия компьютерной преступности» (Запорожье, 26-27 мая 2004 г.).

Результаты исследования были внедрены и используются в коммерческой и научно-практической деятельности фирмами ООО «Декарт» (г. Кишинёв, Республика Молдова) и ООО «Оптимум» (г. Одесса, Республика Украина), а также Департаментом информационных технологий (ГП «Registru») Республики Молдова.

Публикации. По теме диссертационного исследования опубликовано 7 работ, общим объёмом 3,5 печатных листа.

Структура работы. Диссертация состоит из введения, трёх глав, заключения, списка литературы, рисунков, таблиц и приложений. Количество страниц – 210, в том числе приложений - 64 страницы.

Основное содержание работы

1. Современное состояние исследований в области «компьютерного пиратства»

Активный рост рынка программного обеспечения в последнее десятилетие (по данным «BSA» мировой объём продаж программных продуктов вырос с 12,85 млрд долл. США в 1994 г. почти до 25 млрд долл. США в 2003 г.) стимулировал обострение ряда негативных явлений и противоречий, которые не были столь заметны при небольшом объёме рынка в более раннем периоде. Среди них необходимо выделить следующие:

- несанкционированное распространение программного обеспечения, создающее для производителей ПО ситуацию упущенной выгоды и формирующее теневой рынок ППр, наносящий ущерб легальному рынку и государству;
- неопределённость вопросов ценообразования в области реализации программного обеспечения, вызывающая значительные отклонения рыночных цен на ПО от себестоимости их разработки;
- отсутствие ценовой дифференциации при продаже программных продуктов в странах с различными уровнями жизни, приводящее к сокращению платёжеспособного спроса на ПО в странах с низким уровнем достатка;
- неоднозначность правового подхода к защите прав на ПО, ставящая пользователей в неравное положение по отношению к его производителям;
- развитие аппаратных средств и глобальных компьютерных сетей, создающее максимально благоприятные условия для нелегального распространения программного обеспечения.

К настоящему времени проведён ряд исследований, охвативших отдельные задачи, связанные с разработкой и распространением коммерческих программных

продуктов и их защитой от несанкционированного использования. Литературные источники по рассматриваемой проблематике можно подразделить на «технические» и «нетехнические». В «технических» источниках защита ПО от несанкционированного использования рассматривается как чисто техническая задача, решать которую необходимо при помощи средств программно-технической защиты ПО. «Нетехнические» исследования посвящены проблемам правового обеспечения борьбы с «компьютерным пиратством», экономическому анализу отдельных аспектов теневого рынка программных продуктов, а также психологическим аспектам. Но, к сожалению, в описанных выше публикациях отсутствует единый систематизированный подход к анализу процессов производства и реализации ПО. Проведённый нами анализ показал, что несогласованное применение полученных в них результатов не позволяет получить адекватную информацию о причинах происходящих явлений, что подтверждается и реальным уровнем «компьютерного пиратства». Следует также отметить явно недостаточное внимание, уделяемое экономической стороне теневого оборота программных продуктов. В частности, лишь в нескольких публикациях «компьютерное пиратство» анализируется на микроэкономическом уровне, очень незначительная часть нетехнических исследований посвящена экономическим аспектам правовой и технической защиты ПО, и, наконец, совсем отсутствуют работы , посвящённые возможностям влияния на теневой рынок ППр на макроэкономическом уровне. Негативным моментом является также твёрдое убеждение авторов в верности и действенности запретительного подхода к защите программных продуктов от несанкционированного использования. Подобная позиция не учитывает техническую невозможность создания абсолютно устойчивой системы программно-технической защиты и практическую невозможность реализации эффективной правоприменительной практики по отношению к физическим лицам и малым предприятиям – основным потребителям на теневом рынке ПО.

Таким образом, в существующих в настоящее время исследованиях предметной области отсутствует комплексность, недооценивается экономический аспект «компьютерного пиратства» и преобладает запретительный подход к решению задачи снижения объёмов теневого оборота программных продуктов.

Анализ публикаций и результаты собственных исследований дали возможность разбить проблему теневого распространения программных продуктов на ряд взаимосвязанных аспектов, отдельно рассмотренных в работах специалистов из разных областей науки. На основе предложенной в работе классификации публикаций по проблематике теневого рынка ПО выделены следующие аспекты предметной области: экономический, правовой, морально-психологический, технический и технологический, которые находятся в тесной взаимозависимости.

Систематизация и дальнейшее уточнение указанных аспектов исследуемой области позволили выполнить аналитическую работу в рамках исследования с учётом поставленной цели. Учёт же взаимосвязей между рассматриваемыми разрезами объекта исследования, а также между подходами, принятыми к их изучению в различных дисциплинах, позволил осуществить синтез полученных знаний. Кроме этого, для обеспечения комплексности исследования указанные выше аспекты

рассмотрены как на макроэкономическом (государства, общего рынка ПО), так и на микроэкономическом уровнях (агентов рынка ПО).

2. Анализ теневого рынка программных продуктов на макроэкономическом уровне

На макроэкономическом уровне были выделены следующие механизмы регулирования рынка программного обеспечения:

1. Правовое регулирование (законодательное обеспечение и судебная практика).
2. Стандартизация (ГОСТы по качеству, производительности и безопасности ПО).
3. Лицензирование (лицензии на производство и торговлю ПО).
4. Сертификация (сертификация безопасности, качества и происхождения ППр).
5. Ценовое регулирование (верхний порог цен).
6. Налоговое и акцизное регулирование.
7. Информационное регулирование (пропаганда).

Применение указанных механизмов зависит от таких факторов, как государственные интересы в области оборота ПО, экономические интересы крупнейших агентов рынка, технические возможности по осуществлению контроля в предметной области, морально-психологическое восприятие проблемы, технологические аспекты производства ПО, принятый правовой подход, а также внешнеэкономические факторы.

В контексте регулирования отношений на рынке программного обеспечения очень важную роль играет правовой подход к охране интеллектуальной собственности, заложенной в компьютерные программы и базы данных, так как именно законодательная база определяет объём и характер имущественных и неимущественных прав, которые принадлежат авторам, создающим программные продукты.

Проведённое исследование даёт основания утверждать, что существующий в настоящее время правовой подход к защите прав авторства на программные продукты (на базе механизма авторских прав) негативно влияет как на отдельных производителей ПО (за исключением монополистов), так и на развитие отрасли в целом.

По нашему мнению, переход от правовой охраны ППр как произведений литературы к патентной охране способов обработки данных, заложенных в программные продукты, с учётом их специфики позволит в значительной мере сократить как существующие негативные стороны индустрии ПО, так и объём теневого рынка программных продуктов.

В качестве результатов такого перехода можно указать:

- уменьшение ассортимента ППр на рынке до минимально необходимого, что позволит освободить значительные объемы людских и машинных ресурсов;
- уменьшение числа версий и подверсий продаваемых ППр, что значительно облегчит контроль ППр, а также процесс потребительского выбора;
- значительное повышение качества ППр и его надежности, что приведет к повышению эффективности использования программ;

– развитие отрасли в соответствии с законами развития технических систем, что позволит избежать затрат на развитие «тупиковых» направлений;
– повышение информированности пользователей ПО, что положительно скажется на обеспечении потребительских прав на рынке ИТ;
– лишение рынка ППр сверхприбыльности, что снизит темпы его монополизации и повысит уровень компетентности производителей программ;
– падение объёмов теневого распространения ПО, как результат указанных выше изменений.

Влияние государственных стандартов на теневой рынок программного обеспечения может осуществляться двумя путями: через обеспечение требований стандартов по безопасности, надёжности, качеству и полноте документации путём сертификации программного обеспечения и через доведение этих требований до потребителей в рамках государственной информационной политики. Таким образом, если при покупке программного продукта потребитель будет требовать у продавца предъявления сертификата качества и происхождения продукта, а также проверять комплектность документации и гарантийные обязательства (как это принято в настоящее время при приобретении, например, бытовой техники), должна будет появиться тенденция к снижению объёмов теневого оборота программных продуктов.

В настоящий момент законодательно оговорена лишь обязательная сертификация безопасности программных средств, относящихся к области защиты информации (криптографической или иной), сетям передачи данных или спец. связи. Справедливо предположить, что, с учётом всё большего уклона в сторону распределённых сетевых технологий (даже в условиях «домашних» компьютеров), требования к безопасности и конфиденциальности хранимой и передаваемой информации распространятся практически на все типы программного обеспечения.

Переход к государственной сертификации безопасности, качества и происхождения всех видов ПО может оказать следующий эффект на рынок ПО:
– исключение распространения «самодельных» дистрибутивов ППр, которые очень часто содержат модифицированные (cracked/hacked) или некондиционные (alpha/beta) экземпляры ППр.
– исключение незаконной торговли ППр в рамках розничной торговой сети;
– сокращение незаконной торговли ППр в местах рыночной торговли;
– повышение безопасности, качества и надёжности ПО;
– сокращение плагиата исходного программного кода.

Ещё одним средством осуществления государственного контроля над различными рынками (сферами деятельности) является система государственного лицензирования. По нашему мнению, необходимость государственного лицензирования в области производства и торговли ПО обусловлена двумя группами факторов: неудовлетворительным уровнем безопасности и качества производимого в настоящее время ПО и растущей тенденцией перехода к информационному обществу. Первая группа факторов свидетельствует о недостаточном контроле уровня подготовки специалистов, производящих ПО, несоблюдении ими стандартных

требований по безопасности и качеству производимых продуктов, отсутствии навыков и (или) средств тестирования ПО и др. Вторая группа факторов свидетельствует о растущей для государства роли информационных технологий и программного обеспечения как их составляющей.

Воздействие государственного лицензирования на легальный и теневой рынки ПО дополнит влияние государственной стандартизации и сертификации на сферу производства и реализации ППр следующими результатами:

- сокращение количества производителей ПО до минимально необходимого для отрасли уровня;
- упорядочение розничной торговли программными продуктами;
- обеспечение защиты прав потребителей в сфере ПО;
- появление эффективного инструмента борьбы с монополизацией рынка ПО;
- законодательное ограничение «лоточной» торговли оптическими дисками;
- возможность косвенного государственного стимулирования отдельных направлений развития ИТ;
- возможность сбора статистики продаж ППр.

Ценовое и налоговое регулирование рынков товаров и услуг является стандартным видом управляющего вмешательства государства в экономику. Осуществляя ценовое регулирование, государство устанавливает верхние или нижние границы цен в целях стимулирования увеличения или уменьшения объёма предложения на рынке, в рамках антидемпинговой политики, для борьбы со спекулятивными ценами.

В настоящее время рынок программного обеспечения не подвергается ни ценовому, ни налоговому регулированию, что приводит к серьёзному завышению рыночных цен на программные продукты, а также к превалированию на внутренних рынках многих стран (в том числе СНГ) продукции иностранного производства.

Информационное же регулирование преследует цель создания у агентов рынка желаемого отношения к теневому распространению программных продуктов. В настоящее время указанный вид регулирования только начинает использоваться на рынке ПО, поэтому доводы относительно вреда теневого распространения программных продуктов, высказываемые представителями государства, практически ничем не отличаются от доводов крупных производителей ПО. Скорее всего, этот факт обусловлен активным лоббированием интересов крупных производителей ПО, происходящим в последнее время.

По нашему мнению, рациональное использование указанных выше видов регулирования рынка может оказать положительный эффект на рынок ПО в целом, а также улучшить положение дел в области снижения объёмов теневого оборота программных продуктов.

Выполненный анализ влияния рычагов макроэкономического регулирования на «компьютерное пиратство» сформировал основу для оценки существующих и выработки новых государственных стратегий сокращения теневого оборота ПО, что обеспечило возможность построения модели государственного воздействия на теневой рынок ПО.

3. Анализ теневого рынка программных продуктов на микроэкономическом уровне

При осуществлении анализа на микроэкономическом уровне были рассмотрены факторы, влияющие на принятие решений агентами рынка ПО.

С точки зрения воздействия производителя ПО на других агентов рынка были выделены следующие механизмы: применение технических средств защиты; судебное преследование; ценообразование; управление жизненным циклом продукта; пропаганда; организационные меры при реализации ПО.

Среди факторов, влияющих на принятие решения агентами рынка, выделены: экономический (разница в стоимости легальных и нелегальных экземпляров ПО, их соответствие уровню жизни); правовой (уровень юридической защиты авторских прав на ПО); психологический (отношение к охране авторского права, платному распространению ПО и контролю над его распространением); технологический (наличие технологий надёжной защиты ПО от копирования); технический (стойкость средств защиты и доступность средств их преодоления).

С точки зрения организационного подхода мы выделили меры и средства защиты программного обеспечения. При этом под мерами защиты ПО понимается определенный образ действий по достижению необходимой цели, а под средствами защиты – инструментарий для осуществления указанных действий.

Предложена следующая классификация мер по защите ПО:

1. Экономические: повышение качества ПО, снижение цен, предоставление денежного вознаграждения за информацию о «пиратах», предоставление легальным пользователям скидок при приобретении новых версий продукта, проведение маркетинговых мероприятий, предоставление гарантий на ППр.
2. Организационные: индивидуальное распространение ПО («из рук в руки»), борьба с источниками распространения средств «взлома» ПО и «пиратских» копий ППр, оперативное распространение обновленных версий с улучшенными средствами защиты, выявление недобросовестных пользователей, предоставление высококачественной документации и сервиса.
3. Юридические: привлечение нарушителей к ответственности, борьба за более полное использование законодательства, разработка и лоббирование новых законодательных актов.
4. Психологические: запугивание потенциальных нарушителей, создание мифов о «неломаемости» систем программной защиты ПО, воззвания к совести, обман, замена денежной формы оплаты косвенной в виде обязательного просмотра рекламы, пропаганда аморальности исследования и декомпиляции ПО и «пиратства».
5. Технические: применение технических средств защиты ПО, разработка специализированных замкнутых аппаратных или программных платформ, для которых в дальнейшем будет создаваться ПО, создание программно-аппаратных комплексов, сдача ПО в аренду (ASP).

6. Карательные: «охота» на конкретных «взломщиков» или группы «взломщиков», закрытие «хакерских» сайтов Интернет, подача в суд направленных исков, составление в защищаемых продуктах «черных списков» с именами взломщиков.

Средства защиты программ по функциональной направленности были разделены на следующие категории:

1. Средства криптографического закрытия информации. Применяются для шифрования критической информации, а также дистрибутивных пакетов ПО.
2. Средства разделения доступа и мониторинга в локальных вычислительных сетях. Используются для предотвращения и выявления несанкционированного использования ПО в корпоративных сетях.
3. Средства программной (алгоритмической) защиты ПО. Осуществляют динамическую защиту ПО во время его функционирования.
4. Средства комплектования и защиты дистрибутивов. Позволяют производителю создать автоматический дистрибутив, облегчают установку ППр для пользователя и затрудняют его копирование и использование для злоумышленника.
5. Средства глобального сетевого поиска и мониторинга. Необходимы для обнаружения украденных копий ППр, информации о «взломе», источников распространения копий и средств «взлома».
6. Средства информационной защиты сервера глобальной сети. Защищают информационную систему производителя или распространителя ПО от сетевых атак, преследующих цель незаконного завладения ППр.
7. Средства учета и контроля пользователей. Позволяют оперативно реагировать на запросы легальных пользователей, а также отслеживать недобросовестных пользователей и злоумышленников.
8. Средства оперативного распространения ПО. Дают возможность быстро обновлять дистрибутивы при внесении изменений в продукт, а также при смене системы его программной защиты.

Для решения задачи эффективного выбора мер и средств защиты ПО на уровне его производителей предложено проводить анализ рисков, связанных с возможностью теневого распространения выводимых на рынок программных продуктов, и осуществлять управление этими рисками. Анализ рисков включает: определение множества возможных угроз; выделение из него подмножества вероятных угроз; определение потенциального ущерба по каждой угрозе; выработка контрмер; разработка общей стратегии поведения в условиях риска.

Угрозы, согласно нашей классификации, делятся на технические и нетехнические. К техническим угрозам относятся как угрозы, обычные для задач защиты информации («маскарад», перехват или подбор пароля, повторное использование объектов и др.), так и угрозы, специфичные для ПО (дизассемблирование, декомпиляция, анализ алгоритмов защиты, модификация кода, «раздевание», «отвязка», плагиат). К нетехническим угрозам относятся: распространение копий ППр легальными пользователями, нелегальное завладение копиями ППр со стороны третьих лиц, приобретение ППр злоумышленниками

«в складчину», приобретение ППр злоумышленниками по украденной/фальшивой кредитной карте.

При этом жизненный цикл программного продукта в данном контексте был разбит на три этапа: а) период «безопасной торговли»: злоумышленники ещё не успели реализовать ни одну из угроз; б) период «рискованной торговли»: есть отличная от нуля вероятность того, что определённые угрозы реализованы; в) период конкуренции с «пиратами»: существуют достоверные данные о появлении экземпляров программного продукта на теневом рынке. Целью предложенной процедуры управления рисками является максимизация первых двух обозначенных периодов жизненного цикла программного продукта.

По нашему мнению, важным является и вопрос восприятия «компьютерного пиратства». Факторы, оказывающие влияние на выбор между легальным и нелегальным приобретением ППр, представлены ниже (табл. 1).

Таблица 1

Причины приобретения легального и «пиратского» ПО

Причины, по которым пользователи легально приобретают программные продукты (по степени важности)	Причины, по которым пользователи приобретают программные продукты на теневом рынке (по степени важности)
Необходимость использовать продукт для учёбы или работы.	Дороговизна программного обеспечения.
Длительное использование программного продукта.	Желание попробовать программный продукт.
Наличие «бумажной» документации.	Слишком низкие доходы, чтобы легально купить ПО.
Соблюдение законов.	Краткосрочное использование программного продукта.
Возможность получения технической поддержки.	Лёгкость копирования программного обеспечения.
Политика учебного заведения или фирмы.	Ожидание новой версии продукта.
Невозможность найти продукт у знакомых.	Низкая вероятность изобличения.
Гарантия от вирусов.	Использование «пиратских» программ большинством знакомых.
Наличие информации об обновлениях.	Неприемлемо жёсткие ограничения «лицензии» легального продукта.
Престиж от владения легальной копией.	

Таким образом, можно заключить, что использование лишь запретительных мер и правового преследования нарушителей авторских прав является стратегией, не вполне адекватной реально существующей ситуации.

Предложенная классификация инструментальных средств программно-технической защиты программных продуктов заменила целый ряд неофициальных классификаций подобного рода и позволила сформулировать критерии оценки эффективности и применимости указанных инструментальных средств, которые легли в основу предложенной процедуры выбора (разработки) производителем адекватной системы защиты программного продукта.

Разработанная классификация угроз, связанных с риском теневого распространения программных продуктов, дала возможность разработать процедуру оценки и управления рисками на стадии рыночной реализации ПО, что позволило сформулировать задачу принятия решений по максимизации периода «безопасной торговли» программными продуктами.

Исследование психологического восприятия теневого рынка программных продуктов позволило выявить основные факторы, влияющие на принятие пользователями решения о легальном или нелегальном приобретении программного продукта, что послужило основой для создания моделей поведения агентов рынка ПО.

5. Моделирование государственного воздействия на легальный и теневой рынки программного обеспечения

Обобщив материал, связанный с государственными рычагами влияния на рынок программных продуктов, можно наглядно представить процесс регулирования рынка при помощи графической модели (рис. 1).

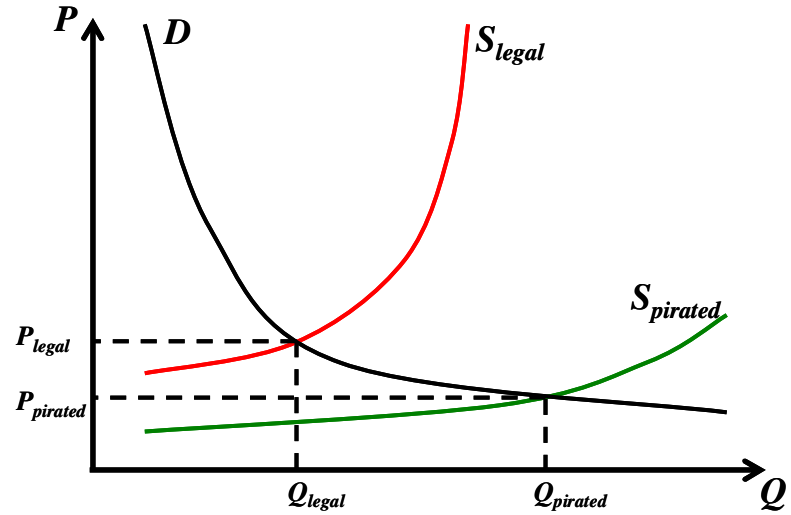


Рис. 1. Графическая модель рынка ПО с учётом нелегального предложения

Отличием предлагаемой модели является присутствие на рынке ПО двух источников удовлетворения спроса: официальных поставщиков ППр и «пиратов», что отражено наличием двух кривых предложения. Кривая предложения официальных поставщиков S_{legal} имеет стандартный для подобных моделей вид, в то время как кривая теневого предложения $S_{pirated}$ является более пологой, что отражает низкую цену «пиратских» экземпляров ПО, а также низкую эластичность теневого предложения по цене.

Вследствие существования двух кривых предложения есть и две точки пересечения кривой спроса D с кривыми предложения, а следовательно, две точки рыночного равновесия: точка равновесия на рынке легальных программных продуктов Q_{legal} и точка равновесия на теневом рынке $Q_{pirated}$. Таким образом, общий объём продаж на рынке ПО определяется значением $Q_{pirated}$, объём легальных продаж – Q_{legal}, а объём теневого рынка определяется разницей ($Q_{pirated} - Q_{legal}$). Объём же потерь от теневого распространения ПО определяется произведением количества

реализованных «пиратских» экземпляров на цену одного экземпляра. Указанный объём соответствует площади фигуры, ограниченной слева и справа вертикальными перпендикулярами из точек Q_{legal} и $Q_{pirated}$, а сверху – кривой спроса на программные продукты, что можно записать как $\int_{P_{pirated}}^{P_{legal}} \boldsymbol{D}(\boldsymbol{P})\boldsymbol{dP} + P_{pirated} \times (Q_{pirated} - Q_{legal})$, где P_{legal} и $P_{pirated}$ – соответственно равновесные цены на легальном и нелегальном рынках программных продуктов.

Отобразим при помощи графической модели три возможных пути сокращения теневого рынка ПО:

1. Сдвиг кривой $S_{pirated}$ вверх, что приведёт к сдвигу точки $Q_{pirated}$ влево. Этот путь реализуется при помощи ужесточения законодательства об охране авторских прав, использования программно-технической защиты ПО и создания систем «доверительных вычислений».
2. Сдвиг кривой S_{legal} вниз, что приведёт к сдвигу точки Q_{legal} вправо, что также вызовет сокращение суммарных потерь. Указанного эффекта можно добиться, стимулируя снижение цен на программные продукты до уровня, близкого к себестоимости (фиксация верхнего порога цен, налоговая политика).
3. Изменение конфигурации кривой D, что соответствует стимулированию снижения спроса на теневые экземпляры программных продуктов. Такое изменение также приведёт к сдвигу точки $Q_{pirated}$ влево. В рамках регулирования рынка данный эффект достигается при помощи внедрения систем стандартизации, сертификации и лицензирования в области производства и коммерческой реализации программных продуктов.

Необходимо отметить, что из указанных трёх подходов, фактически, используется лишь первый, подразумевающий силовое давление на теневой рынок ПО. Учитывая показанную ранее низкую результативность указанного подхода, мы считаем, что для эффективной нейтрализации теневого распространения программных продуктов необходимо использование и остальных двух.

Построенная экономико-математическая модель государственного регулирования рынка программных продуктов позволила описать влияние государственных рычагов управления на объёмы теневого распространения программных продуктов, что дало возможность сформулировать и решить в общем виде стратегическую задачу определения набора мер по борьбе с «компьютерным пиратством» на макроэкономическом уровне.

6. Моделирование экономического поведения агентов рынка программного обеспечения

Для обеспечения комплексности исследования было проведено моделирование экономического поведения всех агентов рынка ПО: пользователя, злоумышленника и производителя.

Рассмотрены экономические критерии поведения пользователя программных продуктов. Введено множество легальных продуктов на рынке ПО – L (l_1, l_2, ... l_i, ... l_m).

При формулировании ограничения, согласно которому пользователь отбирает из всего множества программных продуктов, доступных на рынке, набор потенциально привлекательных, было сделано предположение, что пользователь отбросит те продукты, суммарные издержки на которые превышают бюджетное ограничение. При этом было учтено, что, реально у пользователя есть выбор между приобретением легального экземпляра ППр по высокой цене и приобретением «пиратского» экземпляра с риском быть уличённым в нелегальном использовании ПО. Таким образом, «пиратская копия» ППр с высокой легальной ценой может успешно конкурировать с недорогим легальным экземпляром ППр. Это ограничение записывается в следующем виде:

$$\min_i \{ C_i^L, (C_i^U + P_i^U \times IP) \} + N_i + Q_i \times PL \le S, \; i = \overline{(1,m)},$$

где C_i^L – цена лицензионной копии i-го программного продукта; C_i^U – цена «пиратской» копии i-го программного продукта; P_i^U – вероятность уличения в нелегальном использовании ($P_i^U \in [0;1]$); IP (‘infringement penalty’) – сумма убытка (штрафа) при уличении пользователя в нелегальном использовании ПО; N_i – накладные расходы на i-й программный продукт (настройка, доводка); Q_i – вероятность ущерба от некачественного ПО (с дефектами производства); PL (‘program loses’) – сумма убытка от ПО ненадлежащего качества; S – сумма, которую пользователь согласен затратить на покупку ПО.

Аналогичным образом был сформулирован критерий поведения пользователя, которым он пользуется при выборе среди оставшихся после первого этапа альтернативных вариантов. По нашему мнению, таким критерием служит разница между ожидаемым доходом от использования программного продукта и суммарными издержками на его приобретение:

$$Ch = I - (\min_i \{ C_i^L, [C_i^U + P_i^U \times IP] \} + N_i + Q_i \times PL) \to \max, \; i = \overline{(1,m)},$$

где Ch (‘choice’) – потребительский выбор в денежном выражении; I – доход (прямой или косвенный), который пользователь рассчитывает получить от использования программного продукта.

Проанализированы экономические мотивы действий злоумышленника.

Для упрощения модели введено множество видов нарушений CI ($\{C_1^P, P_1^P, PP_1\}$, $\{C_2^P, P_2^P, PP_2\}$, ... $\{C_j^P, P_j^P, PP_j\}$, ... $\{C_n^P, P_n^P, PP_n\}$), где C_j^P (‘piracy cost’) – затраты на j -й вид нарушений, P_j^P (‘probability of piracy disclosure’) – вероятность

уличения в нарушении, PP_j (‘piracy penalty’) – денежное выражение наказания за j -й вид нарушений, $j=\overline{(1,n)}$.

Процесс выбора стратегии злоумышленником состоит из двух этапов. На первом злоумышленник осуществляет выбор программного продукта для атаки. На втором – выбирает один или несколько видов нарушений, которые будут применены к отобранному продукту. Поскольку всех злоумышленников можно условно подразделить на «взломщиков» и «пиратов», были сформулированы два различных критерия первичного отбора программных продуктов.

- Критерий отбора программных продуктов «взломщиком»: $C_C + P_C \times PP_C \le C_i^L$ (для $C_i^L \ge 50$ у.е.), где C_C (‘crack cost’) – затраты на нелегальную модификацию i-того программного продукта; P_C (‘probability of crack disclosure’) – вероятность уличения в нелегальной модификации; PP_C (‘piracy penalty for crack’) – денежное выражение наказания за нелегальную модификацию ПО.
- Критерий отбора программных продуктов «пиратом»: $\sum_{j=1}^{n}(C_j^P + P_j^P \times PP_j) + N_P \le S_P$, $j=\overline{(1,n)}$, где N_P – накладные расходы на деятельность злоумышленника; S_P – сумма, которую злоумышленник согласен потратить на нарушение.

То есть «взломщик» при отборе ППр сравнивает затраты на преодоление системы защиты с рыночной ценой легального экземпляра этого продукта, а «пират» сравнивает сумму общих издержек на нарушение с суммой, которую он готов затратить.

Был сформулирован и обобщенный критерий поведения злоумышленника, определяемый разницей между планируемым доходом от нарушения и общими затратами на него: $IS = I_P - (\sum_{j=1}^{n}(C_j^P + P_j^P \times PP_j) + N_P) \to \max$, $j=\overline{(1,n)}$, где IS (‘infringer strategy’) - стратегия злоумышленника в денежном выражении; I_P – доход (польза), который злоумышленник рассчитывает получить от нарушения (если польза носит нематериальный характер, используется ее денежное выражение).

Исследовано экономическое поведение производителя программных продуктов. При выборе конкретных стратегий противодействия «пиратам» производитель ПО в первую очередь отбрасывает те из них, затраты на которые сопоставимы с затратами на разработку самого программного продукта либо превышают суммы существующих потерь от распространения продукта на теневом рынке: $C_{AP} \le {}^1/_2 C_{SD}$; $L_P \ge C_{AP}$, где C_{AP} (‘anti piracy measure cost’) – затраты на «антипиратскую» меру; C_{SD} (‘software development cost’) – затраты на разработку ПО; L_P (‘piracy loses’) – величина убытков от «пиратства».

Введено множество «антипиратских» мер $MS(\{C_1^{AP}, E_1^{AP}\}, \{C_2^{AP}, E_2^{AP}\},...\{C_i^{AP}, E_i^{AP}\},...\{C_m^{AP}, E_m^{AP}\})$, которые может принять производитель ПО, где C_i^{AP} (‘anti piracy measure cost’) – затраты на i -ю «антипиратскую» меру, E_i^{AP} (‘anti piracy measure effect’) – эффект от i -й «антипиратской» меры.

В дальнейшем производитель выбирает стратегию по критерию «стоимость-эффективность»: $\min_i \{E_i^{AP} - C_i^{AP}\}$, $i = \overline{(1,m)}$. Обобщённый критерий поведения производителя ПО представлен следующим образом**:**

$$VS = I_{PRG} - (C_{SD} + [E_i^{AP} - C_i^{AP}]) \to \max,\ i = \overline{(1,m)},$$

где VS ('vendor strategy') – стратегия производителя ПО в денежном выражении; I_{PRG} ('programmed income') – запланированный объём прибыли.

В рамках приведённой модели производитель ПО может предпринять следующее: установить программно-техническую защиту ПО (увеличить затраты на «пиратство»); стимулировать повышение раскрываемости (увеличить риск уличения); стимулировать ужесточение законодательства (ужесточить наказание); использовать организационные меры (увеличить затраты на пиратство); не предпринимать «антипиратских» мер, положившись на свою розничную сеть и используя «пиратов» как средство захвата рынка у конкурентов.

Построенные модели поведения агентов рынка программных продуктов дали возможность сформулировать задачи максимизации экономического эффекта от «антипиратских мер» и минимизации суммарных затрат на борьбу с «пиратством», стратегическую задачу определения набора мер борьбы с «компьютерным пиратством» на уровне производителя программных продуктов.

7. Задачи принятия решений, связанные с противодействием нелегальному распространению программных продуктов

С учётом описанной ранее процедуры управления жизненным циклом программного продукта была сформулирована задача принятия решения по максимизации периода «безопасной торговли» программным продуктом (т.е. периода отсутствия экземпляров продукта на теневом рынке).

Мы выделили факторы, которые, по нашему мнению, оказывают ключевое влияние на продолжительность временного интервала между выпуском продукта на рынок и его появлением на теневом рынке.

К ним относятся:

- тип программного продукта (специализированный или общего пользования);
- популярность;
- информационная политика производителя (есть ли ограничения на аудиторию, до которой доводится информация о выпуске новой версии продукта);
- используемый режим продаж (продажи через Интернет, розничная продажа либо адресная рассылка оптических дисков);
- язык программирования и платформа реализации программного продукта;
- тип системы программно-технической защиты продукта;
- использование мер противодействия теневому распространению продукта в компьютерных сетях.

Лицо, принимающее решения, может влиять лишь на следующие из перечисленных факторов:

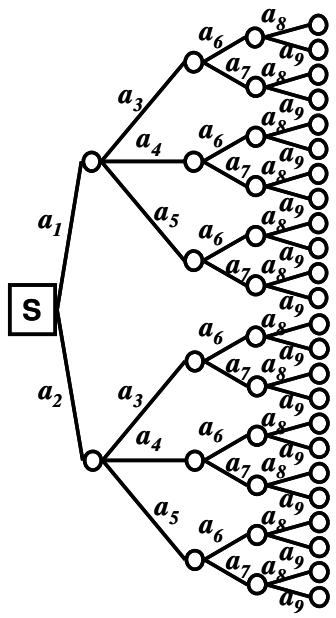
- информационная политика производителя;
- используемый режим продаж;
- тип системы программно-технической защиты продукта;
- использование мер противодействия теневому распространению продукта в компьютерных сетях.

При этом период «безопасной торговли» можно дополнительно разделить на три интервала:

- интервал между началом продаж продукта и появлением свободно доступной информации об этом;
- интервал между появлением информации о выпуске продукта и появлением экземпляра продукта в распоряжении злоумышленников;
- интервал между появлением у злоумышленников экземпляра программного продукта и началом его теневых продаж.

Соответственно, длительность первого интервала зависит от информационной политики производителя, второго – от используемого режима продаж, а третьего – от типа системы защиты и мер противодействия сетевому распространению «пиратских копий» продукта.

Процедуру принятия решения в рамках данной задачи удобно представить при помощи дерева решений (рис. 2). Каждой дуге дерева сопоставляется время задержки появления продукта на теневом рынке, определяемое выбранным значением регулируемого фактора. Таким образом, задача сводится к отысканию самого длинного пути от корня дерева до одного из листьев.



a_1 – время задержки при распространении информации о выходе продукта;
a_2 – время задержки при отказе от распространения такой информации;
a_3 – время задержки при распространении продукта через Интернет;
a_4 – время задержки при розничном распространении продукта;
a_5 – время задержки при адресной рассылке экземпляров продукта;
a_6 – время задержки при пользовании систем программно-технической защиты;
a_7 – время задержки при отсутствии защиты;
a_8 – время задержки при противодействии сетевому распространению контрафактных экземпляров продукта;
a_9 – время задержки при отсутствии контроля над сетевым распространением «пиратских» экземпляров продукта;

Рис. 2. Дерево принятия решений по максимизации периода «безопасной торговли»

При этом существует дополнительное ограничение в виде запланированного срока окупаемости инвестиций в разработку ПО. Соблюдение же срока окупаемости зависит от используемого режима продаж.

Решение задачи, представленной на рис. 2, можно осуществить двумя способами: используя обход дерева, либо сведя её к задаче поиска максимального пути на графе. Во втором случае необходимо ввести дополнительную вершину-«сток», а также фиктивные дуги нулевой длины, соединяющие её со всеми листьями дерева (рис. 3).

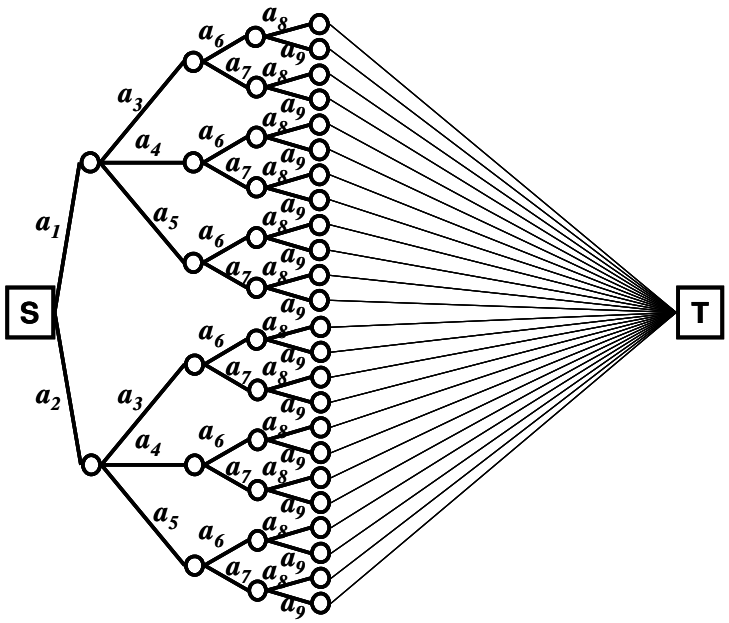


Рис. 3. Дерево принятия решений, преобразованное в сеть

В этом случае задача решается при помощи хорошо известных методов. Для решения примера на усреднённых данных нами был выбран алгоритм Форда.

Для учёта ограничения по срокам окупаемости была предложена итеративная процедура, состоящая из следующих шагов:

1. Решается исходная задача.
2. Если выбранный режим продаж удовлетворяет ограничению по срокам окупаемости, задача решена.
3. Если ограничение нарушено, найденный путь вычёркивается из графа и задача решается снова без его учёта.
4. Если выбранный режим продаж удовлетворяет ограничению по срокам окупаемости, задача решена.
5. Если ограничение нарушено, осуществляется попытка совместного использования найденных решений, с учётом их синхронизации по времени окончания периода «безопасной торговли» (т.е. чем меньше срок, который требуется злоумышленникам для вывода продукта на теневой рынок, при том или ином режиме продаж, тем позже этот режим должен применяться). Таким образом при использовании разных режимов продажи обеспечивается единовременность завершения указанного периода.
6. Если сочетание найденных решений удовлетворяет ограничению, задача решена.
7. При наличии невычеркнутых путей в графе выполнятся возврат к п.3.
8. Если возможные пути в графе исчерпаны, а ограничение не выполняется, задача в данной постановке решения не имеет.

Описанная методика позволяет находить эффективные решения по продлению периода «безопасной торговли» выводимыми на рынок программными продуктами. При этом выбор решения возможен как в условиях определённости, так и в условиях риска. В последнем случае значения интервалов времени заменяются их математическими ожиданиями.

На основе построенных моделей поведения агентов рынка была сформулирована задача максимизации производителем программных продуктов экономического эффекта от принимаемых «антипиратских» мер.

В качестве критерия оптимальности набора мер принимается суммарный экономический эффект (снижение потерь от «пиратства») от их применения. При этом выбор тех или иных сочетаний мер противодействия теневому обороту ПО ограничен бюджетом, выделенным для борьбы с «пиратством». Также, при формулировании задачи было принято, что экономический эффект от каждой меры противодействия проявляется лишь при её полной реализации, то есть каждую меру можно либо применить, либо нет – частичное применение меры не даст эффекта.

Исходя из описанных условий, была сформулирована линейная оптимизационная задача с булевыми переменными:

$$\sum_{j=1}^{n} \boldsymbol{c}_j \boldsymbol{x}_j \to \max$$

$$\begin{cases} \sum_{j=1}^{n} \boldsymbol{a}_j \boldsymbol{x}_j \le \boldsymbol{M} \\ x_j - \textit{булевы переменные}, \end{cases}$$

где c_j – экономический эффект от применения j-й меры, a_j – затраты на применение j-й меры, x_j – признак применения j-й меры, M - бюджетное ограничение.

Была сформулирована и обратная задача – минимизировать суммарные затраты на борьбу с «пиратством», обеспечив заданный экономический эффект от набора применяемых мер.

$$\sum_{j=1}^{n} \boldsymbol{a}_j \boldsymbol{x}_j \to \min$$

$$\begin{cases} \sum_{j=1}^{n} \boldsymbol{c}_j \boldsymbol{x}_j \ge \boldsymbol{D} \\ x_j - \textit{булевы переменные}, \end{cases}$$

где D – запланированный экономический эффект от «атипиратской» деятельности.

Указанные задачи относятся к задачам дискретного программирования, для решения которых существуют хорошо известные методы. Для решения примера на усреднённых данных нами был выбран метод Гомори.

На базе моделей государственного регулирования рынка ПО и поведения производителя программных продуктов была сформулирована задача выбора эффективной долгосрочной стратегии противодействия теневому распространению программных средств. По нашему мнению, этот процесс, как на уровне государственного регулирования, так и на уровне экономического агента – производителя ПО, целесообразно представить в виде игры двух лиц с нулевой суммой (стратегическая игра). При этом игроком, который выбирает стратегию первым, является «сообщество компьютерных пиратов», а игроком,

минимизирующим свой проигрыш, – сторона, противодействующая теневому обороту ПО. В такой постановке задача отыскания оптимальной стратегии игрока решается классическими методами теории игр. Задача с участием производителя программных продуктов будет отличаться от задачи государственного регулирования рынка программного обеспечения лишь стратегиями игроков и суммами выигрыша.

Используя указанный подход, игру «государство – теневой рынок ПО» можно представить следующей матрицей (табл. 2):

Таблица 2

Матрица игры «государство – теневой рынок ПО»

j / i	Ужесточение законодательства	Фиксация верхнего порога цен	Стандартизация, сертификация и лицензирование	Пропаганда
Анонимность	c_{11}	c_{12}	c_{13}	c_{14}
Оперативная реакция	c_{21}	c_{22}	c_{23}	c_{24}
Международный характер деятельности	c_{31}	c_{32}	c_{33}	c_{34}
Эффективное использование глобальной сети	c_{41}	c_{42}	c_{43}	c_{44}
Общественная поддержка	c_{51}	c_{52}	c_{53}	c_{54}
Использование средств крипто- и стеганографии	c_{61}	c_{62}	c_{63}	c_{64}

Значения $[c_{ij}]$ отражают выигрыш первого игрока и проигрыш второго. В качестве элементов платёжной матрицы могут использоваться как абсолютные значения потерь, так и относительный объём теневой реализации программных продуктов. Сами же значения элементов платёжной матрицы должны определяться на основе статистических данных или (и) методом экспертных оценок.

Игру «производитель ПО – пираты» можно условно представить так (табл. 3):

Таблица 3

Матрица игры «производитель ПО – пираты»

j / i	Техническая защита	Повышение раскрываемости	Лоббирование интересов	Организационные меры	Стимулирование легального сбыта
Обход технической защиты	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}
Преодоление технической защиты	c_{21}	c_{22}	c_{23}	c_{24}	c_{25}
Копирование у легальных пользователей	c_{31}	c_{32}	c_{33}	c_{34}	c_{35}
Копирование с сервера	c_{41}	c_{42}	c_{43}	c_{44}	c_{45}
Плагиат	c_{51}	c_{52}	c_{53}	c_{54}	c_{55}
Покупка «в складчину»	c_{61}	c_{62}	c_{63}	c_{64}	c_{65}
Незаконная покупка по кредитной карте	c_{71}	c_{72}	c_{73}	c_{74}	c_{75}

В рамках данной игры с «пиратами» борется производитель программного продукта. Злоумышленники, в данном случае, реализуют стратегии, соответствующие описанным нами угрозам теневого распространения продукта.

Для решения каждой из обеих игр необходимо найти нижнюю и верхнюю цену игры. Нижняя цена игры находится по правилу «максимина»: $\boldsymbol{\alpha} = \max_i \{ \min_j \{c_{ij}\}\}$. Верхняя цена игры определяется по правилу «минимакса»: $\boldsymbol{\beta} = \min_j \{ \max_i \{c_{ij}\}\}$.

В случае равенства нижней и верхней цен игра имеет седловую точку и решение в чистых стратегиях. Тогда оптимальными считаются стратегии, соответствующие выигрышу первого игрока в размере нижней цены и проигрышу второго игрока в размере верхней цены игры.

Если седловой точки не существует ($\alpha \neq \beta$), можно найти решение игры в смешанных стратегиях. Это решение имеет смысл в условиях, когда игра повторяется многократно без изменений в игровой матрице. По нашему мнению, данные условия в целом соблюдаются для случая государственного воздействия на теневой рынок, а также при последовательной рыночной реализации производителем различных версий одного и того же программного продукта. В этом случае будут найдены смешанные стратегии ($\overline{S_1}$ и $\overline{S_2}$), позволяющие игрокам оптимизировать свои выигрыши и проигрыши в долгосрочном периоде. В нашем случае интерес представляет отыскание смешанной стратегии $\overline{S_2}$ второго игрока. $\overline{S_2} = \begin{pmatrix} B_1 & B_2 & \dots & B_n \\ q_1 & q_2 & \dots & q_n \end{pmatrix}$ будет содержать чистые стратегии и частоты (вероятности) их применения ($\sum_{j=1}^{n} q_j = 1$; $q_j \geq 0$, $j = (\overline{1,n})$), которые обеспечат второму игроку минимальный проигрыш в серии игр. Цена игры в смешанных стратегиях будет определяться как математическое ожидание выигрыша первого игрока и проигрыша второго:

$\nu = \max\limits_i \min\limits_j \sum\limits_{i=1}^{m} c_{ij} p_j = \min\limits_j \max\limits_i \sum\limits_{j=1}^{n} c_{ij} q_j$, где p_i – вероятности применения чистых стратегий первого игрока ($\sum\limits_{i=1}^{m} p_i = 1$; $p_i \geq 0$, $i = (\overline{1,m})$).

Для решения матричной игры в смешанных стратегиях формулируется задача линейного программирования:

$$\sum_{j=1}^{n} y_j = \frac{1}{\nu} \to \max, \qquad \text{где } y_j = \frac{q_j}{\nu}$$

$$\begin{cases} \sum\limits_{j=1}^{n} c_{ij} y_j \leq 1 \\ y_j \geq 0. \end{cases}$$

В результате её решения находится вектор $\overline{q_j}$, определяющий оптимальную смешанную стратегию второго игрока.

На базе проведённого исследования были сформулированы и решены в общем виде следующие задачи:

- максимизации временного лага между выпуском продукта и его появлением на теневом рынке;
- максимизации производителем ПО экономического эффекта от «антипиратских» мер;
- минимизации суммарных затрат на борьбу с «пиратством»;
- стратегическая игра «государство – теневой рынок ПО»;
- стратегическая игра «производитель ПО – пираты».

Это позволило создать методическую базу для решения задач принятия решений по противодействию теневому обороту программных продуктов, что соответствует поставленной в исследовании цели.

Основные результаты исследования изложены в следующих публикациях:

1. Середа, С.А. Оценка эффективности систем защиты программного обеспечения [Текст] / С.А. Середа // Acta Academia : сб. науч. тр. / Международная академия информатизации. – Кишинёв : Evrica, 2000. – С. 154-165. – 0,5 п.л.
2. Середа, С.А. Анализ средств преодоления систем защиты программного обеспечения [Текст] / С.А. Середа // ИНФОРМОСТ: Радиоэлектроника и Телекоммуникации. – 2002. – №4(22). – С. 11-16. – 0,66 п.л.
3. Середа, С.А. Экономический анализ поведения участников рынка программного обеспечения [Текст] / С.А. Середа // ИНФОРМОСТ: Радиоэлектроника и Телекоммуникации. – 2002. – №6(24). – С. 4-9. – 0,53 п.л.
4. Середа, С.А. Экономический анализ теневого рынка программных продуктов [Текст] / С.А. Середа : тез. конф. «Probleme teoretice şi practice ale economiei proprietăţii intelectuale». – Кишинёв: AGEPI, 2004. – С. 143-153. – 0,3 п.л.
5. Середа, С.А. Правовой подход к программному обеспечению: требуются изменения [Текст] / С.А. Середа // Патенты и лицензии. – 2004. №1. – С. 44-51. – 0,58 п.л.
6. Середа, С.А. Перспективы охраны авторских и смежных прав в условиях распространения произведений через глобальные сети передачи данных [Текст] / С.А. Середа : тез. конф. «Правовая охрана интеллектуальной собственности в современных технологиях», Москва, Зеленоград, 2004. – С. 71-75. – 0,27 п.л.
7. Середа, С.А. Процедура разработки систем программно-технической защиты программного обеспечения [Текст] / С.А. Середа // Инновации в процессе обучения: сб. науч. тр. Академического Совета МЭСИ. – М., 2004. – Вып.3. – С. 160-173. – 0,66 п.л.

Общий объём публикаций составляет: 3,5 п.л.