**Правительство Российской Федерации**

**Федеральное государственное автономное образовательное**

**учреждение высшего профессионального образования**

**«Национальный исследовательский университет**

**"Высшая школа экономики"»**

**Санкт-Петербургский филиал федерального государственного**

**автономного образовательного учреждения высшего профессионального образования**

**«Национальный исследовательский университет "Высшая школа экономики"»**

**Факультет экономики**

**Кафедра** финансовых рынков и финансового менеджмента

**БАКАЛАВРСКАЯ РАБОТА**

На тему: «Экономическое обоснование модели противодействия пиратам на рынке программного обеспечения»

Направление: 080100.62 «Экономика»

Студент группы № 141 Тарасова В.Д.

Научный руководитель Котляров И.Д. к.э.н., доцент

Санкт-Петербург

2014 г.

Оглавление

[Введение 3](#_Toc389055988)

[1.Теоретические аспекты защиты от пиратства 6](#_Toc389055989)

[1.1 Пути защиты от пиратства 6](#_Toc389055990)

[1.1.1.Защита государства 6](#_Toc389055991)

[1.1.2.Организации по защите от пиратства 9](#_Toc389055992)

[1.1.3.Защита компании-производителя ПО 12](#_Toc389055993)

[1.2.Применение методов противодействия пиратству с учетом стадий жизни продукта и внешних условий 17](#_Toc389055994)

[2.Практический анализ защиты от пиратства 34](#_Toc389055995)

[2.1. Модель 34](#_Toc389055996)

[2.2. Анализ стратегий компаний-примеров 46](#_Toc389055997)

[2.2.1. Adobe Systems 46](#_Toc389055998)

[2.2.2. ABBYY 52](#_Toc389055999)

[Заключение 58](#_Toc389056000)

[Источники 61](#_Toc389056001)

# Введение

В настоящее время интеллектуальная собственность и информационные технологии стали неотъемлемой частью жизни, проникнув во все ее сферы. Развитие инновационных технологий является одним из ключевых факторов позволяющих отдельной фирме или государству в целом быть конкурентоспособными на международном рынке.

Производство программного обеспечения (далее ПО) позволяет обеспечивать работоспособность, как информационных новшеств, так и обычных офисов и школ. Разработчики программ совершенствуют свои продукты, с каждым годом выводя их на новый уровень. Несомненно, исследования и создание ПО требуют немалых затрат, покрытие которых обеспечивается продажами готового товара. Этот процесс длится уже десятилетия, однако его скорость замедляется в связи с существованием пиратства. «Пиратство» - это обобщенное название нарушения авторского права, применяемое чаще всего к таким объектам интеллектуальной собственности как фильмы, музыка, книги и ПО. Суть понятия заключается в следующем: пиратство – это деятельность, нарушающая установленные законодательством права автора на распоряжение продуктом интеллектуальной деятельности, и заключающаяся в копировании, распространении и потреблении его нелегальных копий [1].

С развитием сети Интернет пиратство ПО перешло на новый уровень, практически отказавшись от вещественных носителей и продажи нелегальных версий «с рук». Это значительно усложнило задачу производителя и государства, так как прежде прекращение пиратской деятельности являлось более осуществимой задачей. С переходом на распространение нелицензионных копий через сеть, пропал как таковой «виновный», поскольку виртуальное пространство обеспечивает пользователям анонимность. Более того, границы деятельности пиратов практически исчезли, в связи с тем, что ПО, созданное и продаваемое в одной стране, становится доступной пользователю в любой другой. Эти причины побудили предпринимателей, занимающихся производством ПО, создать новые способы защиты от пиратства и ужесточить старые. Большинство из них требуют значительных дополнительных затрат, которые далеко не всегда себя оправдывают.

Многие исследователи, изучающие вопрос пиратства, пытались оправдать полезность этого явления и убедить разработчиков снизить их защиту[10, 38]. Несмотря на правдивость подобных предположений, такие стратегии работают не для любых типов компаний и не в любых условиях. Развивая и дополняя эту идею, другие авторы рассматривали уровень пиратства, который фирма может вынести без чрезмерного ущерба для своей деятельности [3,50]. Помимо этого существует группа исследований, посвященная конкретным методам защиты и их эффективности [39, 27,18].

Если рассматривать общий объем работ, посвященных пиратству, то авторы приходят к противоречивым и разрозненным выводам. Во многом это связано с тем, что большая часть исследований акцентируется на какой-то одной стороне вопроса и старается учесть как можно больше деталей именно касательно нее. Научная новизна данной работы заключатся в поиске доказательства экономической целесообразности применения защиты при учете всех наиболее частых видов и методов борьбы с пиратством. Также мы постараемся определить пути влияния производителя на выбор пользователей.

**Целью** нашего исследования является обоснование эффективности применение тех или иных методов защиты с точки зрения фирмы. Иными словами, мы планируем определить может ли и каким образом противодействие пиратам положительно воздействовать на экономический результат фирмы-производителя ПО.

Для осуществления поставленной цели, требуется решить следующие задачи:

1. Определить типы (методы) защиты, которые может применять разработчик против пиратства. Выделить их суть и проклассифицировать.
2. Смоделировать игру потребитель-производитель, позволяющую определить ситуации, в которых может оказаться производитель, применяя ту или иную стратегию.
3. Определить по построенной модели, какие рычаги воздействия имеет разработчик на решение пользователя.
4. Рассмотреть пример реальной компании производителя ПО и оценить применимость модели.

**Объектом** исследования является рынок программного обеспечения, на котором разворачиваются сделки между игроками. Отношения производителя и потребителя на рынке ПО являются непосредственно **предметом** исследования, поскольку именно выбор одним из игроков той или иной стратегии приводит к различным исходам, которые мы рассматриваем.

**Методология**. Как уже было отмечено, достижение цели предполагается путем моделирования институциональной игры и вывода зависимости поведения потребителя от стратегии производителя.

Работа состоит из двух частей:

* Теоретическая часть будет разделена в свою очередь на две главы. Первая должна включать себя анализ методик противодействия пиратам и внешней защиты, поступающей не от разработчика. Во второй будет присутствовать теоретическое обоснование применения различных методов во времени.
* Практическая часть будет включать в себя две главы: в первой, будет описана модель игры и ее обоснование; во второй - проанализированы стратегии реально существующих фирм при помощи построенной модели.

# 1.Теоретические аспекты защиты от пиратства

## 1.1 Пути защиты от пиратства

Вопросы борьбы с пиратством являются одним из ключевых элементов управления компанией, которая занимается распространением любого интеллектуального продукта, в том числе и программного обеспечения. Для того чтобы сократить свои убытки, связанные с нелегальным копированием и распространением продукции, компании могут пытаться предупредить пиратскую деятельность или прекратить ее в последующем (то есть когда она уже была осуществлена).

Все те методы, которыми компания вправе воспользоваться, можно разделать на группы. Во-первых, по своей сути они, как уже было сказано, делятся на два типа превентивные и карательные. Это общие группы, которые могу применяться относительно пользователей ПО на разной стадии жизни продукта.

Говоря общим языком, борьба с пиратством ведется «методом кнута и пряника». Поскольку просто невозможно наказать каждого, кто хотя бы раз скачал нелицензированный продукт, правообладатели всячески стараются привлечь интерес потребителей к легальному ПО, то есть вернуть себе потенциальных покупателей «пряниками». В то же время, необходимость в защите ПО не пропадает, и для этого компании обращаются к методам, подразумевающим ограничения и наказания, то есть к «кнуту».

### 1.1.1.Защита государства

Изначально любая компания занимающаяся созданием того или иного продукта интеллектуальной деятельности может полагаться как минимум на защиту государства. Законодательство в данной сфере постоянно развивается и расширяет рамки деяний, которые могут попасть под букву закона. Тем не менее, степень защищенности интеллектуальной собственности авторов зависит от того, в какой стране они живут. Известно, что степень наказуемости материального и интернет пиратства варьируется от предупреждений и малых штрафов вплоть до уголовного ареста.

Поскольку рассматривать все возможные варианты законодательств в данной сфере нецелесообразно, их необходимо объединить в группы по строгости наказания.

В большинстве развивающихся стран данная сфера законодательства не являются ключевой для развития, поскольку она в меньшей степени может повлиять на развитие государства. Это естественно, что там, где прожиточный минимум крайне мал по сравнению с США или странами Евросоюза, потребители пользуются исключительно пиратской продукцией. В связи с этим, практически вся деятельность, связанная с передачей, распространением и использованием нелегальной продукции рассматривается правительством как сделки на уровне неформального обмена. Отсюда можно выделить первую условную группу: страны с законами, которые практически не защищают права авторов или вообще отсутствуют.

Борьба с пиратством на законодательном уровне в определенный момент столкнулась с тем, что материальное пиратство стало меньшей проблемой, чем цифровое. С началом распространения контента по сети возникла проблема того, что законодательство одной конкретной страны не может быть распространено на весь Интернет. В распространении контента по сети участвуют две стороны: те, кто выкладывают его в сеть и те, кто скачивают и пользуются. И те, и другие совершают правонарушение, поскольку первые нарушают лицензионный договор (если они в свою очередь приобрели первоначально лицензионный вариант, который впоследствии и распространяют), а вторые «воруют» контент, поскольку если они и платят за то, чтобы скачать интересующий их файл, то не правообладателю.

Для того чтобы окончательно пресечь и остановить цифровое пиратство необходимо удалить его источник, то есть закрыть сайт распространитель. Однако проблема заключается в том, что создатель данного сайта может быть жителем другой страны, и на него законодательство не будет распространяться. Тем не менее, правительства все же пытаются прекратить деятельность вредоносных сайтов, по возможности закрывая их и наказывая создателей. Стоит отметить, что далеко не всегда подобные действия имеют длительный характер: чаще всего закрытые источники пиратского контента через некоторое время возобновляют свою работу собственными силами. В связи с этим, большинство стран с развитой защитой прав интеллектуальной собственности направляют в основном свои действия на других участников этого нелегального процесса - потребителей.

Не так много стран применяют тюремное заключение в качестве наказания за цифровое пиратство, в частности, одни из самых строгих мер применяются в США. В Штатах распространители пиратской продукции могут попасть в заключение на срок до пяти лет [22]. Подобные меры будут относиться к группе самых строгих, то есть в тех странах, где они применяются, защита находится на высоком уровне.

Большинство европейских стран ограничиваются лишь штрафами и не прибегают к уголовному наказанию[58]. Система действует следующим образом: если было обнаружено, что пользователь загружает или распространяет нелегальный контент, ему высылаются предупреждения (как правило, от одного до трех) с просьбой удалить весь нелицензированные файлы. В случае если требования не выполняются, «пирату» присылают повестку в суд. Результатом такого дела может стать штраф и ограничение доступа в интернет. Поскольку самого наказания можно вовремя избежать, страны с подобными законами будут отнесены к средней группе.

Таким образом, правовая защита на уровне государства делится на три вида:

* Отсутствие правовой защиты или ее чрезмерно низкий уровень;
* Государственная защита среднего уровня строгости;
* Государственная защита высокого уровня строгости.

Правовая защита, по сути, относится к карательным мерам, поскольку невозможно кого-либо наказать до того, как совершено преступление. Однако страх быть наказанным может также оказывать превентивное действия на пользователей, особенно в тех странах, где подобное правонарушение строго наказуемо. В тоже время, защиту на уровне государства можно отнести к методу «кнута», поскольку она в любом случае подразумевает собой угрозу для нелегальных пользователей ПО.

### 1.1.2.Организации по защите от пиратства

Следующий уровень защиты, доступный для компании – это вступление в члены какой-либо ассоциации, занимающейся проблемой пиратства. Это Могут быть как международные организации, так и внутри одной страны. Как правило, большинство подобных учреждений ведут свою деятельность на некоммерческой основе, и ее владельцами являются сами компании-участники. Те услуги, которые они предлагают, во многом сходятся и имеют общую направленность. В качестве примеров можно привести следующие организации:

* + 1. SIIA - Software & Information Industry Association.
       1. Распространение информации об интересах индустрии ПО и опасностях пиратства;
       2. Распространение информации о трендах в сфере ПО и технологий;
       3. Выступает правозащитником для компаний правообладателей;
       4. Обеспечивает отслеживание пиратского контента среди пользователей и в Интернете [76].
    2. ESA-Entertainment software association.
       1. Представление интересов правообладателей, обеспечение правовой защиты;
       2. Мониторинг сети Интернет на предмет неправомерных действий относительно компаний-членов ассоциации;
       3. Обеспечение защиты в сети в США и на некоторых других иностранных рынках путем агрессивного судебного преследования, будь то уголовное расследование или гражданские споры[72].
    3. BSA-Business Software Alliance.
       1. Обеспечивает распространение информации об авторском праве среди пользователей;
       2. Предоставляет средство для аудита ПО;
       3. Осуществляет борьбу с нелегальными пользователями в сотрудничестве с правоохранительными органами[69].
    4. FAST- Federation against software theft.
       1. Предоставляет аудит ПО и лицензирование ПО;
       2. Предлагает программу по возврату убытков;
       3. Осуществляет борьбу с нелегальными пользователями в сотрудничестве с правоохранительными органами[73].

Данные организации являются примерами одних из крупнейших и наиболее развитых вариантов ассоциаций по борьбе с пиратством. Как можно заметить, их деятельность имеет общие черты и в целом имеет некоторую «образовательную» направленность. Иными словами, подобные организации в первую очередь ставят цель показать компаниям производителям ПО, как они сами могут защитить свои продукты от посягательств пиратов. Если объединять их услуги в более общие группы, то к ним можно отнести:

* Повышение информационной осведомленности пользователей и правообладателей;
* Представление интересов правообладателей в суде;
* Предоставление программ, позволяющих обеспечивать контроль над пиратской продукцией в интернете.

Основной плюс вступления в подобные ассоциации заключается в том, что у компании больше шансов отсудить себе хотя бы часть нанесенного пиратами ущерба. Самостоятельно подобными судебными делами заниматься может далеко не каждый производитель ПО, более того, если пытаться подавать иск в суд на каждого, кто использовал пиратский вариант ПО, то даже в случае выигрыша большинства дел, затраты на их проведение скорее всего окажутся еще выше.

Еще одно преимущество членов данных организаций – это уже готовый программный продукт для контроля над нелегальным распространением копий в Интернете. Использование средств, разработанных ассоциацией, может позволить сократить издержки на создание собственных технических способов защиты в данной сфере.

Говоря о том, к каким типам защиты обращаются организации по защите от пиратства, можно отметить, что, несмотря, на образовательные программы, которые, несомненно, относятся к превентивным методам, довольно большая ставка делается на карательные меры – судебные разбирательства, рейды, возврат ущерба и т.п.

Альтернативой большим международным организациям являются коммерческие компании, предоставляющие примерно те же самые услуги, но уже на платной основе. Можно предположить, что для не столь крупных компаний данный вариант более приемлем, поскольку в международные организации, как правило, вступают гиганты индустрии. Коммерческие организации также обещают помощь менеджменту компании, с целью переквалифицировать пользователей пиратской продукции в покупателей оригиналов. Вероятно, собственная коммерческая заинтересованность в возврате потерь правообладателей, может приводить к даже лучшим результатам, чем деятельность крупной международной ассоциации.

### 1.1.3.Защита компании-производителя ПО

Последний уровень защиты, к которому может прибегнуть производитель ПО - это собственная защита от пиратов. На данной стадии, у правообладателя больше свободы в выборе стратегии защиты. Так, существует возможность комбинирования разных тактик, как превентивных, так и карательных.

Большинство авторов, исследовавших методы защиты от пиратства, к которым может прибегнуть сама фирма, в основном выделяли группы, имеющие общие черты [48]. Так можно выделить следующие категории:

**Методы взаимосвязи.** Многие компании предоставляют возможность пользователям самим доложить о пиратской продукции. Подобные жалобы в некоторых случаях даже поощряются денежными вознаграждениями. Так в 2010 году 16 из 157 человек, сообщивших об использовании пиратского ПО получили вознаграждение общей суммой $57,500 от SIIA [77]. Таким образом, компании призывают потребителей принять хотя бы пассивное участие в борьбе с пиратством. Кампании описывают на сайтах в разделе «пиратство» все возможные последствия использования нелегальной продукции, как для самих пользователей, так и для компании и индустрии. Таким образом, производители стараются повлиять на решение приобретать лицензионный продукт или нет, действуя на совесть потребителя. С целью убедить покупателя во вреде пиратства компании проводят собственные исследования и предоставляют их результаты всем желающим. Этот способ побуждения потребителей приобретать лицензионный товар относят к «методам пряника» и называют коммуникационным [19]. Следует отметить, что подобные меры вполне могут действовать в странах, где большая часть населения имеет активную гражданскую позицию, как то США, Канада и некоторые страны Европы. Тем не менее, те, кто не боится сообщать о подобных нарушениях, рискуют потерять свою работу. Из вышеупомянутых 157 человек, доложивших о нарушениях в своей компании, более 59% были уволены. В Великобритании больше половины офисных работников закрывают глаза на противозаконные действия компании в данной сфере: 13% участвовавших в опросе the Federation Against Software Theft связали это со страхом потерять работу, 22% не захотели оказаться изобличителями, 46% просто было все равно.

Помимо информации о потенциальных угрозах для индустрии, производители также стараются убедить потребителей в том, что лицензионный продукт обладает множеством преимуществ по сравнению с нелегальными копиями. Некоторые компании, осуществляют всяческого рода «благотворительную» деятельность, результаты который могут освещаться на сайте компании или в СМИ. Это позволяет компаниям улучшить отношение пользователей к себе, и, опять, же, воздействуя на моральные качества потенциальных покупателей побудить их приобретать лицензионный товар, поскольку тем самым они могут помочь «несчастным».

Эти и другие способы призыва потребителей к легальным действиям, основанные исключительно на доверительном общении и повышении пользовательской информированности о данной проблеме, относятся к методам взаимосвязи или коммуникационным методам защиты.

Преимуществом коммуникационных методов является то, что они практически не требуют затрат и доступны любой, даже самому маленькому производителю. Информация, которая стоит за данными методами, может быть указана на сайте, в рекламной компании, на пресс релизах и так далее.

**Правовые методы.** Поскольку не все компании способны вступить в крупные международные ассоциации, которые осуществляют посильную поддержку правообладателей в суде, они могут заниматься данным вопросом самостоятельно. К данным методам можно отнести как патентирование и лицензирование, так и ведение судебных тяжб с особо злостными нарушителями [19]. Использование подобных методов защиты, особенно судебных разбирательств, может быть затруднительно для производителя ПО, который не является крупным участником рынка. Это, в первую очередь, связано с тем, что прежде чем пытаться получить компенсацию за пиратство, необходимо обнаружить нелегальных пользователей, а для этого применить технические методы защиты. Таким образом, правовые методы защиты зависят от эффективности других. Также стоит отметить, что правовые методы защиты требуют определенных затрат, которые могут варьироваться в течение времени.

Однако, правовое вмешательство может быть достаточно эффективным способом борьбы с пиратством, особенно в странах, где обеспечен высокий или хотя бы средний уровень защиты прав автора на уровне законодательства. Преимуществом правовых методов является тот факт, что только их применение может принести возмещение ущерба, а не только затраты связанные с их осуществлением.

**Техническая защита.** Некоторые исследователи не выделяют данные способы как отдельный вид, присоединяя их к более обширной группе - защите непосредственно через продукт. В данной работе, они все же будут стоять отдельной строкой, поскольку под ними подразумевается не только добавление особых свойств самому контенту, но и использование специальных ПО для мониторинга ситуации в интернете. Онлайн пиратство является одной из наибольших опасностей для ПО, поскольку его сложно контролировать и еще сложнее остановить. Как уже упоминалось, ассоциации по защите прав производителей и авторов ПО предлагают свои силы для мониторинга сети или готовые средства для этого. Помимо или вместо этого фирма может сама разработать или купить готовые программы. Подобное ПО, предназначенное за отслеживанием и удалением пиратских копий, предоставляется такими сервисами как Attributor, Covington & Burling и BayTSP [79] . Особенно технические методы важны для компаний, которые не являются членами каких-либо организаций по борьбе с пиратством и хотят помимо прочего пользоваться правовыми методами.

Таким образом, технические способы защиты – это те средства, которые не являются частью продукта, но подразумевают необходимость каких-либо технических средств.

**Защита через продукт*.*** Данный метод борьбы с пиратством состоит из двух частей: первая – привлечение интереса потребителей за счет усовершенствования продукта; вторая - защита от пиратства посредством добавления особых свойств продукту.

Многие крупные производители ПО проводят периодические обновления продукта, с целью исправить недочеты, дополнить функции и т.п. Во много основанная на обратной связи система позволяет разработчикам улучшать продукт и понимать чего хотела бы потенциальная аудитория от программы в будущем. Помимо периодических мелких дополнений, которые доступны, по сути, только лицензионному варианту ПО, существуют крупные обновления. Которые могут производиться реже, но вносить большие изменения в продукт. Это может приводить даже к тому, что те файл, которые были созданы в новой версии, то есть обновленной, не смогут полноценно работать со старой программой. Также производитель может со временем предлагать полноценные дополнения к уже имеющемуся продукту. Оно может также стать жертвой пиратов, однако существует некоторый временной лаг, между моментом выпуска дополнения и появлением копий в сети. В зависимости от того, насколько он большой зависит ценность продукта. Если те, кто до этого пользовался нелицензионной копией, не могут долгое время обновить ее, а им уже необходимо работать с файлами, которые были созданы в дополненной лицензионной, это нанесёт им ущерб. Хотя подобные способы влияние на желание потребителей пользоваться легальной версией продукта скорее можно отнести к мягким и предупредительным, для пиратов и пользователей их копий они вполне могут оказаться и карательными.

Иные способы защиты с помощью продукта подразумевают включение в ПО каких-либо технических особенностей, которые позволят отслеживать нелегальные версии продукта или нарушения соглашения. Примером может служить лицензионный ключ, который необходим для установки и регистрации продукта. Некоторые программы закрепляются за одним компьютером и не могут быть установлены на каком-либо другом. То есть большая часть данных методов направлена на то, чтобы ограничить распространение ПО даже в пределах одного домохозяйства. Те, кто нарушают лицензионное соглашение, могут быть привлечены к суду.

Особенность данных методов заключается в том, что они являются частью самого продукта, а не дополнительным средством борьбы. Естественно, они требуют затрат на разработку, но они же и позволяют производителю получить дополнительную прибыль при выпуске обновлений.

**Ценовые методы*.*** Самая «финансовая» стратегия – это изменение цены. Данные методы могут выражаться в скидках на более старые версии, выгодных ценах пакетов ПО и т.п. Поскольку одна из наиболее упоминаемых причин, по которой пользователи предпочитают нелицензионные копии, это завышенные цены, то уместно предположить, что влияние на стоимость продукта может отразиться на готовности потребителей покупать оригинальный продукт [14]. В настоящее время во многих домах/семьях во владении находится не один ПК, а несколько, если не у каждого члена семьи. Особенно это касается тех домохозяйств, где есть дети, которые учатся в школе или университете. В связи с этим создается потребность не только в операционной системе для каждого ПК, но и в частичном или полном пакете программ типа Office . Приобретение такого количества лицензионных ПО, с учетом того, что оно может быть установлено только на один компьютер, в большинстве случаев не по карману.

Компания Microsoft предлагает выход из такой ситуации: комплект операционной системы и пакета office для 5 компьютеров, с ежемесячной или ежегодной оплатой. Хотя «абонентская плата» в 700 долларов [74] ежегодно по-прежнему достаточно велика для ряда пользователей, подобные действия передают смысл ценовых методов.

Несмотря на то, что снижение цены может повлечь серьезные потери для компании, данные методы могут оказаться одними из самых действенных. Это связано с тем, что в случае если цена достаточно низкая для того, чтобы потребитель предпочел ее поиску пиратской продукции и связанными с ней рисками, компания имеет возможность расширить круг клиентов.

Ценовые методы защиты относятся к мягким, поскольку направлены на привлечение потребителей и предоставление им лучших условий.

## 1.2.Применение методов противодействия пиратству с учетом стадий жизни продукта и внешних условий

Мы предполагаем, что стратегия компании при взаимодействии и борьбе с пиратством должна включать в себя почти все формы защиты, однако степень их внедрения будет зависеть от ряда факторов. Все типы защиты имеют разное предназначение и разный по силе и свойству эффект, более того некоторые из них взаимосвязаны. В связи с этим, будет предложена стратегия, включающая разные методы защиты, основывающаяся на их свойствах и необходимости в тот или иной момент.

Так как рассматривается рынок программного обеспечения, товар который может подвергнуться пиратскому воздействию – это, соответственно, некоторая программа. Именно для такого типа продукта будет строиться стратегия противодействия пиратству. Как и другие блага, ПО имеет свой срок жизни. Как правило, это 3-5 лет, до момента, когда продукт устаревает окончательно и становится невостребованным.

Для построения стратегии, срок жизни ПО будет условно разделен на три стадии. Для удобства они отображены на рисунке:

Период запуска

Период развития

Период окончания

Рис. 1. Периоды жизни ПО

1. Период запуска продукта, когда он только входит на рынок. На данной стадии предполагается, что у потребителей должен появиться интересе к продукту за счет его новизны и более высокий спрос, в особенности если присутствовал момент ожидания выпуска ПО (то есть потребители ждали дату релиза, делали предварительные заказы и т.п.).
2. Период развития или поддержания продукта. Подразумевается, что через некоторое время, повышенный интерес спадет, пользователи смогут самостоятельно оценить продукт, что отразится на общей готовности его приобретать. На этом этапе, компании, как правило, начинают внедрять дополнения и обновления программы. Этим действиям часто сопутствует снижение цены или «специальные предложения», когда дополненная версия стоит дешевле первоначального варианта. Это позволяет продолжить отношения с уже имеющимися потребителями и привлечь новых.
3. Период окончания жизненного цикла ПО. С течением времени появляются (если их не было ранее) или развиваются (если они были) продукты конкурентов. Все те пользователи, которые были готовы приобрести ПО производителя, это уже сделали. Сам разработчик уже переключается на другой новый продукт, который разрабатывался в течение первых двух стадий. Естественно, ПО не пропадает из обихода, но вероятность того, что компания сможет получить серьезную прибыль от него крайне мала. Зачастую, в конце жизни устаревшее ПО становится предметом свободного пользования, распространяемым самой компанией-производителем.

В зависимости от ПО и его успешности длительность того или иного периода может различаться. В общем случае, предполагается, что первая стадия наиболее короткая, поскольку эффект новизны и ажиотаж вокруг продукта длится лишь некоторое время: до того момента, как о нем начнет складываться более или менее общее мнение потребителей. Период развития - это более длительная стадия: от того насколько «качественным» окажется ПО зависит количество исправлений вносимых разработчиком и, соответственно, то сколько времени компания способна будет поддерживать интерес к своему продукту. Можно сказать, что стадия конца жизни продукта наиболее длительная. Хотя его жизненный цикл заканчивается, и продукт перестает быть стратегически важным для компании, остается некоторая доля потребителей, которая продолжает им пользоваться или которая все еще хочет его опробовать. Таким образом, применения разных методов защиты будет распределяться по этим стадиям.

Уже оговаривался тот факт, что для любого производителя ПО задача защиты своей интеллектуальной собственности может быть облегчена внешними условиями, такими как государственная защита и вхождение в организации занимающиеся противодействием пиратству. В случае если эти факторы на высоком уровне, общие усилия и затраты на некоторые виды защиты могут быть ниже.

Мы выделили три типа государств с разным уровнем защиты: низкая - Gl, средняя - Gm, высокая - Gh. Также компания может вступить в некоммерческую организацию по защите от пиратства (Af) или воспользоваться услугами коммерческой(Ap). Мы постараемся рассмотреть различные условия, в которых может оказаться компания, поскольку, как и любые другие интеллектуальные блага ПО распространяется не только на территории одного государства, но по всему миру. Иными словами, компания сможет ориентироваться на внешние условия и, исходя из них, применять соответствующую стратегию.

Также одним из изначальных условий является общее количество потенциальной аудитории, которое будет определяться как 100% или 1. На рынке есть доля потребителей, которая использует только лицензионную продукцию – n; часть тех, кто вообще не заинтересован в приобретении данного ПО - α; те, кто предпочитает пиратские копии – (1–n-α). Количество разных пользователей может меняться на протяжении жизни продукта, от чего также будет зависеть необходимость применения защиты.

Поскольку нас интересует экономическая сторона вопроса и взгляд производителя на проблему, то логика построения стратегий будет отталкиваться от минимизации издержек на защиту. Каждый способ будет рассмотрен в отдельности на трех стадиях жизни продукта при разных внешних условиях, и затем они будут собраны воедино.

Прежде чем описывать их по отдельности, необходимо установить общее ограничение для затрат на защиту, которое должно выполняться для всех вариантов.

Первый ключевой параметр – это уровень пиратства относительно продукта. Данная величина подразумевает потери от неправомерного использования потребителями копий продукта и зависит от их количества и цены, так как чем выше стоимость продукта, тем больше пользователей готовы переключиться на пиратскую копию [29]. Очевидно, что данный фактор не единственный, влияющий на желание потребителей использовать «бесплатную» копию, но для нашего исследования он наиболее значим. Иными словами ущерб от пиратства – это функция от количества нелегальных копий и цены на оригинал – Piracy(1–n-α). Однако, исходя из того, что мы учитываем характеристики страны, в которой ПО будет распространяться, то более логично будет отталкиваться от уровня пиратства в конкретном государстве. Это может быть некий коэффициент, полученный из статистических данных организации по защите интеллектуальной собственности (например, BSA). Либо, если разработчик уже относительно долгое время находится на рынке, то он может собрать собственные данные по этому вопросу, которые более точно могут отразить угрозу для ПО того типа, что он производит.

На рынке ПО распространение пиратских копий несколько отличается от того, как это происходит с фильмами или музыкой. Для того чтобы пираты смогли «произвести» свой вариант продукта, должно пройти некоторое время, поскольку необходимо пройти ту защиту, которая включена в сам продукт. Более того, если прокат фильмов начинается в разное время в разных странах и нелегальные копии могут начать распространять еще до официального его выхода, то в случае ПО выпуск происходит практически одновременно для всех государств. Таким образом, в первый период жизни продукта, уровень пиратства мал и близок к нулю в связи с временным лагом, вызванным необходимостью «взлома» защиты».

Когда наступает вторая стадия развития продукта, количество пиратской продукции уже почти невозможно сдерживать, так как те, кто приобрел лицензионный продукт, начинают его распространять в сети, тем самым увеличивая общее число пользователей копий. На этой стадии уровень пиратства резко возрастает до тех пор, пока он не достигнет своего пика. В этот период происходит насыщение продуктом, то есть все те, кто хотел опробовать или приобрести продукт уже это сделали и интерес к нему начинает падать. Количество «раздающий» контент сокращается так же, как и количество желающих его скачать. Процесс изменения уровня пиратства отражен на Рисунке 2., где вертикальная ось –это уровень, а горизонтальная – время (данные координаты остаются неизменными и для последующих графиков).

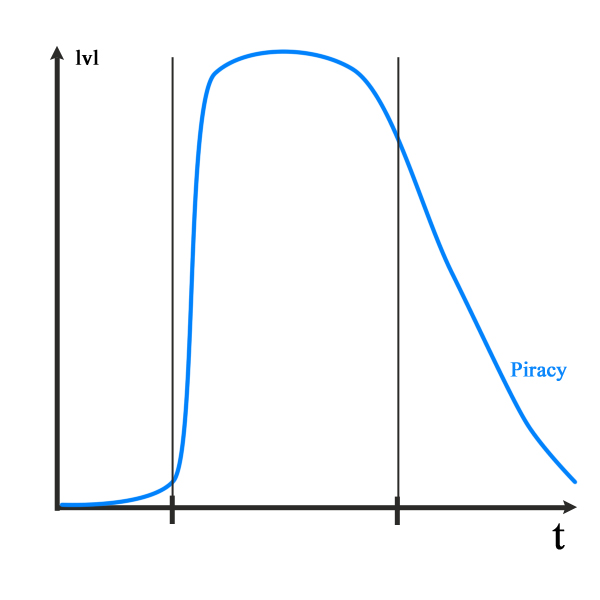


Рис. 2. График изменения уровня пиратства в течение жизни продукта

Для того чтобы ограничивать потом пиратской продукции на рынок (в данном случае, по большому счету, это сеть) компании применяют различные методы противодействия.

Первый наиболее очевидный – это ценовой. Особенность данного метода в том, что он не может основываться исключительно на необходимости искоренить пиратство. Первичная цель ценовой политики компании – это обеспечить прибыль, привлечь пользователей и увеличить продажи. Ценовой метод не может быть выраженным в затратах, поскольку это противоречит его сути. Исходя из этого, данный параметр будет отражать прибыльность продукта. Однако, его направленность, как способа противодействия пиратам основана на привлечении потребителей, исходя из этого, мы предполагаем, что он зависит от количества желающих использовать лицензионное ПО, то есть Price+(n).

В общем случае, предполагается, что изначальная цена, которая устанавливается на первой стадии, максимальна. В период, когда все только хотят познакомиться с ПО и не могут сопоставить его содержание и цену, производитель может получить максимальный доход. В период развития тактика меняется в сторону снижения стоимости, так как наступает необходимость расширить круг пользователей, которые отказывались от приобретения оригинального продукта по высокой цене [35]. Специальные предложения и скидки на ПО также позволят лицензионной версии соревноваться с пиратской. Полезность от нее будет выше, чем от пиратской, и, что более того, цена станет ниже изначальной. На стадии конца жизни продукта компании, как правило, максимально сбрасывают цену и в некоторых случаях переходят на бесплатное распространение, поскольку происходит запуск нового ПО, которое обеспечит больший доход, а свободное пользование ПО позволит повысить репутацию компании [4].

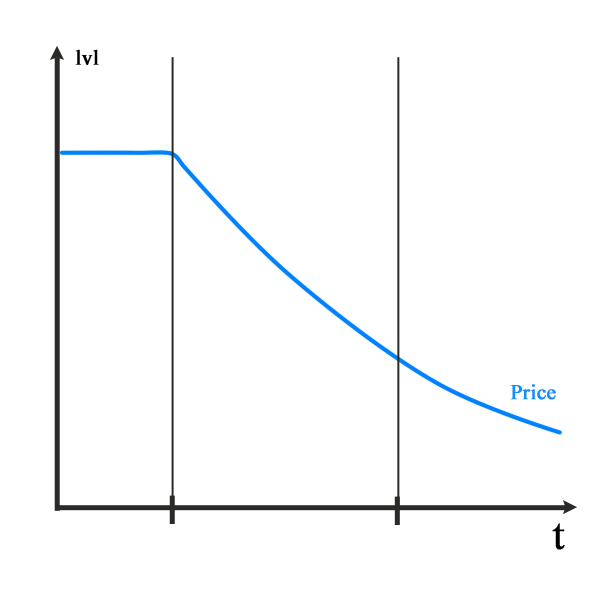


Рис. 3. График изменения цены в течение жизни продукта

Следующий метод защиты – это правовой. Как уже упоминалось ему присущ тот факт, что помимо затрат, который он требует для осуществления защиты интересов разработчика, его результаты могут выражаться в денежной компенсации. В связи с этим, мы разделим данный параметр на две части: затраты на правовую защиту(L-) и компенсации полученные благодаря правовой защите (L+). Степень того, сколько компании необходимо потратить на правовую защиту своего продукта зависит от трех факторов. Во-первых, от типа государства, поскольку в тех странах, где законодательство охраняет права автором интеллектуальной собственности, легче добиться правосудия в вопросах пиратства. Во-вторых, от того состоит ли разработчик в каком либо альянсе по борьбе с пиратством, так как подобные организации обеспечивают посильную помощь в защите на судебном уровне. И в-третьих, непосредственно от количества пользователей нелицензионных копий: если не с кем бороться, то и тратиться не надо. В итоге, уровень правовой защиты – это функция, зависящая от типа государства, членства в ассоциации и количества пользователей пиратских копий - L(G, A, 1–n-α).

Технологическая защита, представляет собой стороннее ПО, которое необходимо для мониторинга сети на распространение и использование нелегальных копий. У разработчика есть возможность создать подобные методы защиты самому или же приобрести их у другой компании специализирующейся на них. Применение технических способов защиты упрощается, если производитель состоит в организации по защите прав создателей интеллектуальной собственности. Там компания может не только получить соответствующие программы, но и пройти обучение. Таким образом, уровень затрат, которые сама фирма должна понести для осуществления защиты на техническом уровне зависит опять же от того, состоит ли она членом ассоциации. Так как данный метод подразумевает исключительно защиту и сокращение пиратского контента, уровень его реализации зависит от необходимости в нем, то есть от количества пиратских копий. Уровень технической защиты может быть представлен как соответствующая функция – T(A, 1–n-α).

Защита через продукт относится к побудительным методам и ориентирована на привлечение новых пользователей и поддержание интереса уже существующих. Она выражается как в технических особенностях ПО, направленных на ограничение распространения и нелегального копирования, так и в разработке дополнений и обновлений для уже существующей программы. Техническая сторона данного метода осуществляется еще до его непосредственного запуска, поэтому мы учитываем ее на протяжении жизни продукта на уровне отличном от нуля. Более того, затраты на ее осуществление входят в производственные и не получают развитие в дальнейшем. По-другому дело обстоит с обновлением продукта. Предположительно, необходимость в нем зависит от изначального качества программы, выпущенной разработчиком и, соответственно, количества ошибок и неисправностей в ней. В действительности же, выпуск дополнений также привязан еще к количеству потребителей, которые приобрели продукт на первой стадии его жизни. Это основная масса пользователей, с которой в дальнейшем работает производитель. Затраты на усовершенствование программы должны оправдываться тем, что на них будет однозначный спрос хотя бы в пределах этого круга потребителей. Если ПО не было востребовано на стадии запуска, когда о его возможном плохом качестве никто не знал, то в будущем оно вряд ли станет более желаемым даже в улучшенном варианте. Таким образом, мы предполагаем, что уровень защиты через продукт выражается через функцию от количества пользователей оригинальной версии – P(n).

Помимо вышеуказанных способов защиты мы указывали также коммуникационные методы. Как уже говорилось, они практически не требуют затрат на осуществление и построены на доверии и лояльности пользователей. С экономической точки зрения подобные способы защиты не влияют на общие результаты производителя. Даже если учитывать тот факт, что некоторый компании (обычно большие корпорации) выплачивают вознаграждение тем, кто придал огласке особенно большие нарушения, такие случаи единичны. В связи с этим, методы взаимосвязи будут причислены к альтернативным методам защиты, не будут учитываться как часть ограничений.

В итоге получается, что компания получает доход от ценовых и правовых методов. Ценовые способы в данном случае представляют собой общий уровень дохода от продаж. Уровень затрат на каждый из остальных типов защиты – это то, сколько компании предстоит вложиться в защиту ПО. Защита от пиратства целесообразна, когда затраты на нее не превышают доходов от продаж и получаемых компенсаций, то есть:

Price(n)+L+(G, A, 1–n-α)-(P(n)+L-(G, A, 1–n-α)+T(A, 1–n-α))≥0

Помимо необходимости учитывать величину дохода, так же важно понимать, что защита имеет смысл только в том случае, когда она стоит меньше, чем убыток от пиратства, иными словами, цель должна оправдывать средства. Если это условие не будет выполняться, то разработчик ,возможно, и избавится от проблемы нелегального распространения копий, но это выльется в еще большие затраты, которые он сам себе и создаст.

P(n)+L-(G, A, 1–n-α)+T(A, 1–n-α)-Piracy(1–n-α)≤0

Таким образом, для любого периода в любых внешних условиях должны выполняться эти два свойства:

Price(n)+L+(G, A, 1–n-α)-(P(n)+L-(G, A, 1–n-α)+T(A, 1–n-α))≥0

P(n)+L-(G, A, 1–n-α)+T(A, 1–n-α)-Piracy(1–n-α)≤0

P(n)+L-(G, A, 1–n-α)+T(A, 1–n-α)≤ Price(n)+L+(G, A, 1–n-α)

P(n)+L-(G, A, 1–n-α)+T(A, 1–n-α)≤ Piracy(1–n-α)

Поскольку мы все же предполагаем, что количество легального продукта больше, чем пиратских копий (иначе все деятельность компании производителя теряет смысл), то второе условие становится главным. Теперь перейдем непосредственно к анализу отдельных способов защиты.



Рис. 4. График применения правовой защиты в течение жизни продукта, с учетом различных внешних условий защиты

Первый рассматриваемый метод - правовой. От внешних условий он зависит больше всего. В случае если в государстве нет соответствующего законодательства, которое ограничивало бы пиратскую деятельность и сдерживало желание пользователей выбирать нелегальные версии продукта, и компания не является членом какой-либо ассоциации по защите правообладателей, весь груз защиты ложится на плечи разработчика. Поскольку выиграть дела, касающиеся распространения или использования нелегальных копий крайне трудно, затраты на судебные процессы увеличатся. Без участия в них представителей защитных организаций разработчик лишается опыта в подобных делах, которым обладают ассоциации. В связи с этим уже в период запуска продукта компания вынуждена обеспечивать правовую защиту на среднем уровне, поскольку у пользователей отсутствует страх наказания, и государство не обеспечивает ограничения распространения пиратских копий. В этот период, компания ведет как бы подготовку к реальным действиям, которые начинаются уже на второй стадии жизни продукта, когда пиратство разворачивается в полную силу. Поднимая уровень правовой защиты до максимума, то есть до высокого, разработчик переходит к более решительным действиям: накопившаяся информация об особо больших источниках распространения нелегальных копий позволит ему противодействовать именно им, что в дальнейшем повысит вероятность возмещения ущерба. Предполагается, что поддержание легальной защиты на высоком уровне в течение всей стадии развития продукта позволит наиболее действенно использовать данный метод, поскольку наибольшая активность пиратской деятельности приходится именно на него.

В период конца жизни продукта, когда желающих воспользоваться пиратской копией становится все меньше, необходимость в правовой защите падает, однако не так резко, поскольку все еще есть возможность противодействовать тем, кто занимался неправомерной деятельностью относительно продукта в предыдущем периоде.

Наличие членства в платной организации требует затрат на вступление, однако его наличие позволяет компании более успешно выступать против пиратства. Поскольку в этом случае разработчик получает поддержку более опытной организации он также может рассчитывать на больший шас получения компенсации за причененный ущерб. Все это приводит к тому, что общие затраты на использование правовой защиты ПО становятся ниже, чем в случае с отсутствием членства в государстве с низким уровнем правовой защиты. Членства в бесплатной организации повзолит разработчику сохранить еще больше средств. Стоит отметить, что поскольку ассоциации работающие на некоммерческой основе обычно основаны гигантами индустрии, они обладают наибольшим опытом в подобных делах и знакомы с прецендентами.

Аналогично градируются ситуации в странах, где законодательство обеспечивает частичную защиту интересов праообладателей и полную( на высоком уровне). Крайним случаем явлется ситуация, когда разработчик распростроняет ПО в государстве с высокой степенью защиты ПО и состоит в бесплатной организации по защите прав авторов. В таких условиях затраты на данный метод минимальны и общие внешние условия наиболее благоприятны для разработчика. Более того, производитель заранее понимает, что государство осуществляет собственый контроль за ситуацией и сдерживает пиратскую деятельность по крайней мере посредством страха быть наказанным. Это предоставляет компании большую свободу для выбора собственной стратегии : например, отказываясь от правовой защиты в первом периоде разработчик может воспользоваться сетевыми эффектами.

Мы предполагаем, что промежуточные стадии совпадают по затратам. Так, правовая защита в государстве с низким уровнем защиты, но при наличии членства в некоммерческой организации обеспечивает такие же условия, как страна со средним уровнем защиты без членства в каких-либо ассоциациях. Это связано с тем, что в первом случае, несмотря на участие в разбирательствах профессионалов, часть затрат все же ложится на разработчика, а во втором затраты наборот становятся чуть меньше в связи с защитой государства.

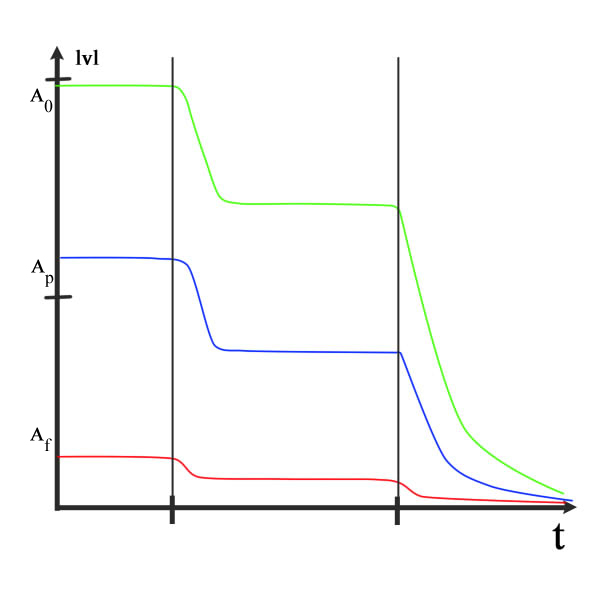


Рис. 5. График применения технической защиты в течение жизни продукта, с учетом различных внешних условий защиты

Следующий метод защиты, который зависит от внешних условий – это технический метод. Получение уже готовых программ для отслеживания пиратства заметно упростило бы задачу разработчика и снизило бы его затраты на создание или приобретение собственных аналогов. Однако, когда компания не является членом какой-либо ассоциации, а значит, не имеет доступа к подобным продуктам, осуществляется исключительно за ее собственные средства. Уровень технической защиты на первой стадии продукта должен быть максимально высок, поскольку в течение данного периода ожидается наибольшее количество продаж, а устранение пиратских копий из сети еще возможно, так как количество не так велико [44]. С наступлением следующей стадии, применение данного типа защиты теряет во многом свою целесообразность, поскольку скорость распространение нелегальных версий практически невозможно сдерживать. Тем не менее, так как предполагается, что в этот же период компания будет предоставлять пользователям дополнения или обновления, то их также необходимо защитить, поэтому технические методы могут применяться на среднем уровне.

Когда программа устаревает и наступает финальная стадия, в технической защите нет необходимости. Это связано с тем, что количество пиратских копий слишком велико и попытки сдерживать их распространение не будут оказывать такого же эффекта, как ранее, из чего следует, что компания только увеличит свои затраты. Исходя из этого, в третьем периоде, разработчик может резко снижать техническую защиту вплоть до нуля.

Наличие членства в коммерческой организации снизит затраты разработчика на обеспечение мониторинга сети, за счет того что ему не придется искать собственные средства данного типа защиты, однако это все же не снижает затраты до нуля. Оптимальный вариант – это членство в некоммерческой организации, которая предоставляет свое ПО и обучение, более того, такие ассоциации сами следят за тем, чтобы продукты участников не подвергались пиратским действиям

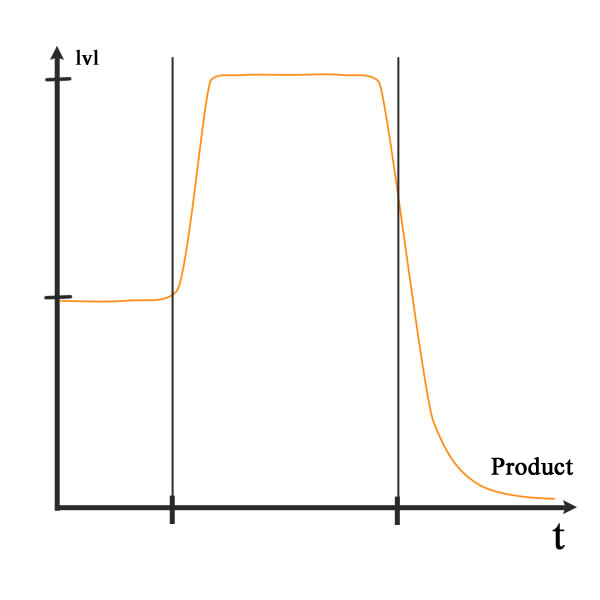


Рис. 6. График применения защиты через продукт в течение жизни продукта, с учетом различных внешних условий защиты

Защита через продукт мало зависит от внешних условий и остается практически одинаковой во всех ситуациях. Суть данного метода в том, что он согласуется с ценовым, хоть и не повторяет его траекторию. На первой стадии запуска программы, в нее как часть продукта уже заложены защитные механизмы, то есть изначально разработчик запускает товар, потратившись на обеспечение сохранения его оригинальности. Более того, как правило, программы обеспечиваются технической поддержкой сразу же, то есть уровень защиты через продукт устанавливается на средней величине. На второй стадии, когда разработчик двигается дальше и обновляет или дополняет товар, происходит резкий рост защиты через продукт. Поскольку она относится к побудительным методам защиты, то направлена на привлечение потребителей и ее использование связано с необходимостью расширить круг пользователей [28]. Помимо добавления новых особенностей программе, разработчик старается исправить все возможные недочеты, которые могли бы повлиять на решение потребителей использовать лицензионную программу или нет. На финальном этапе жизни продукта, привлечение новой аудитории не является главной целью разработчика, более того предполагается, что программа к этому моменту приобретает уже свой окончательный вид, дорабатывать который уже нет смысла, поскольку вышли или готовятся к выходу новые продукты. Это служит причиной резкому спаду уровня данного метода защиты.

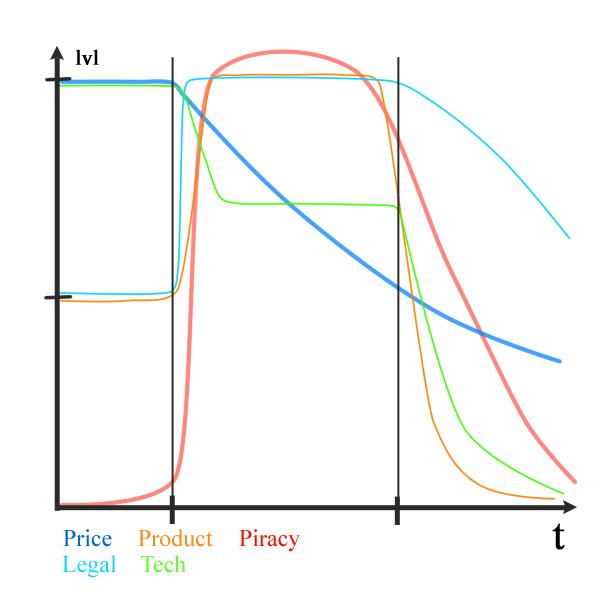


Рис. 7. Общий график методов защиты и уровня пиратства

В общем виде все виды защиты представлены на графике без учета внешних условий, для того чтобы отобразить суть стратегии.

Стратегически значим первый период жизни ПО, когда оно только появляется на рынке и наиболее привлекательно для пользователей, поскольку пока еще не выявились его слабые стороны. Однако, это не значит, что все методы защиты должны применяться по максимуму. В связи с тем, что пиратские действия могут оказывать положительный эффект для разработчика в виде распространения информации о программном обеспечении и его «бесплатной» рекламе, разработчик может оставлять пользователям возможность распространить часть оригинальных копий. Это выражается в том, что лишь технологическая защита находится на высоком уровне. Поскольку ей управляет сам производитель, он в силах предотвращать массовое распространение продукта, и в то же время, может оставлять люфт для пиратов. Техническая защита особенно актуальна, потому что высокая цена, устанавливаемая в начале жизни продукта, отталкивает часть потенциальной аудитории, которая не готова приобретать незнакомый продукт за такую стоимость.

Второй стадии свойственно как наибольшая активность пиратов, так и возрастающее внимание к защите. Производитель повышает уровень побудительных и карательных мер, тем самым воздействуя и на пользователей оригинальной версии продукта, и на пиратов. Происходит также смена некоторых способов: так техническая защита, теряя свою эффективность, сменяется более активными правовыми действиями, направленными на тех, кто был отмечен как особо злостный нарушитель в ходе мониторинга сети. Не смотря на то, что цена постепенно начинает снижаться, она по-прежнему остается достаточно высокой для того, чтобы часть пользователей все же предпочитали пиратские копии. Для того чтобы повлиять на их выбор, разработчики пользуются методом защиты через продукт, повышая его до максимального уровня.

На финальном этапе, вся защита постепенно ослабляется, так как продукт уже не приносит больших объемов выгоды и его можно использовать для подержания репутации разработчика и отношений с пользователями.

# 2.Практический анализ защиты от пиратства

## 2.1. Модель

Перед производителем стоит задача максимизировать прибыль. На любом рынке, где продуктом является результат интеллектуальной собственности, существует такая помеха к достижению цели, как пиратство. Рынок ПО не исключение, более того он один из лидеров по доле нелегального контента. В предыдущей главе мы рассматривали различные виды защиты, которые разработчик может применять для защиты своего ПО от посягательств пиратов. Однако также отмечалось, что в разные периоды полезность использования методов варьируется. Изначально перед производителем стоит выбор: применять защиту или нет. Это его две основные стратегии. Необходимо отметить, что вторая стратегия не исключает того факта, что в стране, в которой происходит игра есть правительство которое может обеспечивать некоторой уровень защиты, в зависимости от строгости законов. Более того разработчик может быть членом ассоциации, которая также старается оберегать ПО участников.

В любом случае предполагается, что разработчик получает прибыль от продаж своего продукта равную:

,

где:

* *p* – цена устанавливаемая производителем в начале периода;
* *q* – количество потребителей приобретающих лицензионную версию (из общего числа пользователей заинтересованных в продукте).

Мы не учитывает затраты на производство, поскольку для любого исхода они будут одинаковыми и влияют на ситуацию с пиратством (мы не рассматриваем случай, когда производитель снижает цену за счет понижения качества продукта и сокращения затрат на его разработку).

При построении модели пиратства мы рассматриваем круг лиц, потенциальных потребителей, которые в любом случае будут использовать выпускаемый разработчиком продукт. Иными словами, не включаем ту часть населения, которая изначально не заинтересована в программе по той или иной причине (не имеет навыков работы, нет необходимости, программа нацелена на потребителей определенной профессии и так далее). Это можно объяснить тем, что нас интересует именно действенность и целесообразность методов защиты, а увеличение круга пользователей в данном случае отнесем к другой части стратегии компании, которая подразумевает рекламу и связь с общественностью. Поскольку изначальной целью всякого метода защиты является именно уменьшение или предотвращение нелегального копирования, то возможные «побочные» эффекты, влияющие на общее количество потребителей, рассматриваются отдельно.

В связи с этим, у первого участника игры – покупателя есть только две стратегии – это купить или украсть интересующее его ПО. В соответствии с определенной стратегией, мы можем определить его выигрыши. Предполагается, что в случае использование оригинальной версии ПО потребитель получает максимальную полезность от изначальной версии, поскольку пиратская копия не может быть лучше (в силу того, что для превосходства оригинала, пират должен самостоятельно понести затраты на повышение качества, из-за чего теряется весь смысл такой стратегии ). Однако общий эффект от использования продукта уменьшается на величину заплаченной за него цены. Таким образом, в случае выбора потребителем легального продукта. Положительный эффект от него равен:

,

где:

* *Ub*– полезность, получаемая от использования оригинального ПО;
* *p* – цена ПО, устанавливаемая продавцом в начале игры.

Теперь необходимо определить непосредственно выигрыши участников игры.

**Случай 1.** *Производитель защищает ПО, потребитель покупает оригинальную версию.*

В данной ситуации, производитель остается с выигрышем равным p\*q , но необходимо учесть, что к его обычным затратам добавляются затраты на защиту. Поскольку ему необходимо покрыть эту часть расходов, то он включает их в цену, тем самым повышая ее до , где с – это затраты на защиту, а – это надбавка к цене, подразумевающая что производитель распределяет свои затраты на абсолютно все лицензированные копии (то есть общее количество продуктов Q равно всему круг потенциальных потребителей, как пиратов так и честных пользователей) [47]. Исходя из новой цены и учета соответствующих расходов на противодействие пиратам, выигрыш производителя составит:

В то же время, потребитель отвечает тем, что предпочитает именно купить лицензионную версию продукта, то есть весь объем потребителей Q=q. В таком случае производитель полностью окупает свои затраты на защиту:

Выигрыш потребителя в данном случае изменяется, поскольку производитель окупает свои затраты за его счет. Пользователь вынужден платить большую цену, даже несмотря на то, что он выбирает оригинальное ПО. Вместе с тем, некоторые методы защиты могут принести дополнительную полезность потребителю (например, защита через продукт). Для того чтобы отразить эти изменения мы вводим некий коэффициент i- improvement, который находится в интервале от 0 до 1. Новая полезность от потребления легальной версии будет равна:

Такие границы для коэффициента объясняются тем, что любой метод защиты не должен уменьшать полезности от использования ПО, иначе говоря, ухудшать его качество. Равным образом улучшение продукта более чем на 100% не имеет смысла, так как в этом случае целесообразней выпустить новую версию или программу.

Принимая во внимание изменения в цене и полезности, выигрыш потребителя при стратегии 1 – покупать, в ответ на стратегию 1 производителя - защищать будет следующим:

**Случай 2.** *Производитель защищает ПО, потребитель использует пиратскую версию.*

Данная ситуация наиболее приближена к реальному положению дел. Несмотря на все усилия производителей, как правило, все равно остается доля пользователей, которые не хотят приобретать ПО у самого разработчика. В таких условиях появляются издержки связанные с пиратством – pir(piracy)- которые подразумевают прибыль, которую могу бы получить разработчик, если бы потребитель предпочел купить ПО.

Тем не менее, необходимо учесть, что защита имеет смысл тогда, когда она действенна, иными словами, должен присутствовать положительный возвратный эффект от применяемых методов защиты. Он может выражаться в количестве потребителей, которые изменят свое решение и станут покупать ПО или же, как в случае правовой защиты, материальной компенсации. Этот эффект в нашем случае отражается переменной r –return .

Цена также как и в первом случае будет повышенной в связи с необходимостью покрыть издержки на защиту. С учетом всех вышеуказанных изменений выигрыш продавца будет равен:

Потребитель в данном случае получает в первую очередь полезность от продукта, которая может и, скорее всего, отличается от той полезности, которую получают пользователи легальной версии. Чтобы отразить эту разницы, мы вводим коэффициент α 𝝐 [0;1]. Снижение качества, как правило, связано с тем, что пиратам приходится обходить защиту, которая мешает скопировать ПО таким образом, чтобы пиратская копия была абсолютно идентична, хотя это не исключено [15]. Из этого следует, что α стремится к 1, когда защита отсутствует или на низком уровне и, наоборот, близко к нулю, когда производитель на высоком уровне оберегает свой продукт. Помимо падения качества связанного с необходимостью преодолевать защиту, пиратская копия может содержать в себе вредоносные программы, вирусы или трояны [54].

Следовательно, полезность, получаемая от пиратской копии, равна =. В связи с тем, что потребитель выбирающий нелегальную версию продукта не платит соответствующую ему цену, то его выигрыш и есть полезность .

**Случай 3.** *Производитель не защищает ПО, потребитель покупает оригинальную версию.*

В подобной ситуации, производитель ничего не теряет и у него нет необходимости в дополнительных затратах на защиту от пиратства. То есть его выигрыш состоит полностью из его прибыли от продаж – .

Выигрыш потребителя в данном случае больше, чем в случае 1, поскольку пользователь не переплачивает за защиту. Тем не менее, в то же время покупатель теряет возможность увеличения полезности , получаемого за счет отдельных методов защиты ( то есть i=0). Таким образом, выигрыш пользователя -

**Случай 4.** *Производитель не защищает ПО, потребитель использует пиратскую версию.*

Отсутствие какой-либо защиты со стороны производителя приведет к тому, что производитель будет терпеть значительные издержки из-за наличия пиратства, которое присутствует на рынке в полной мере. Если, производитель не считает необходимым применять методы защиты, то отсутствуют соответствующие затраты. В таком случае выигрыш производителя составит:

С точки зрения пользователя такой исход игры достаточно благоприятен. В силу того, что потребителю нет необходимости платить за пользование ПО и отсутствует серьезная защита со стороны разработчика, он свободно получает практически идентичный или идентичный оригиналу продукт. Его выигрыш в данной ситуации равен:

|  |  |  |  |
| --- | --- | --- | --- |
|  | | **Потребитель** | |
| *Купить (1-σ)* | *Украсть (σ)* |
| **Производитель** | *Тратиться на защиту*  *(β)* |  | {; } |
| *Не тратиться на защиту*  *(1-β)* | ; | {*;}* |

Табл. 1. Выигрыши потребителя и производителя ПО

Оптимальный исход для обоих игроков это Ситуация 3 – никто не крадет, производитель не защищает. Отсутствие необходимости в защите оказывает положительный эффект для обоих игроков. Несмотря на то, что данная стратегия является равновесной, в реальности она практически невозможна и является скорее утопичной.

Хотя Ситуация 1 не является равновесием, она представляет собой то развитие событий, которое может устраивать обоих игроков. Поскольку потребитель все равно решает покупать ПО, он готов заплатить ту цену, которую на нее устанавливает производитель, даже если она выше ожидаемой. К тому же, он имеет компенсацию в виде повышения качества продукта.

Оба случая, когда потребитель предпочитает использовать нелегальную копию, являются крайне неэффективными с точки зрения производителя.

Оба игрока выбирают стратегию согласно определенной вероятности. Поскольку мы рассматриваем ситуацию с точки зрения производителя, то модно сказать, что вероятность применения защиты устанавливаем мы сами. Однако наш выигрыш и экономическая эффективность деятельности, связанной с запуском продукта, зависит от того, какую стратегию выберет потребитель. Можно сказать, что вероятность того, что пользователь предпочтет пиратскую версию – это его склонность к пиратству.

Задача производитель повлиять на потребителя так, чтобы уменьшить его склонность к использованию нелицензионных копий. Иными словами, разработчик сможет выбирать не только свою стратегию, но и в некоторой степени участвовать в принятии решения потребителем.

В связи с тем, что выигрыш потребителя зависит в первую очередь от цены на продукт, то можно предположить, что эта связь переносится и на склонность пользователя к пиратству [23]. Рассмотрим краевые точки цены. Если производитель устанавливает p=0, то есть размещает ПО в свободном доступе, то необходимость в пиратстве отпадает сама собой и σ=0. В действительности, копирование оригинального продукта, что может внести изъяны в него, становится нецелесообразным. Теперь, обратимся к случаю, когда производить пытается установить цену, которая настолько велика, что негативный эффект на благосостояние потребителя перекрывает полезность от самого ПО. В таком случае, пользователи в любом случае будут предпочитать использовать пиратскую версию, даже несмотря на ее возможные недостатки. Иначе говоря, при p→ pmax, σ=1.

Саму взаимосвязь вероятности σ и цены p можно выразить в виде следующего выражения:

,

где:

* *pmax* – это цена, при которой для нашей производственной функции;
* *Q(pmax)=*0 или, иначе выражаясь, это та цена, по которой уже никто не купит продукт.

Подставляя соответственно краевые значения, мы получаем оговоренные результаты.

В то же время, на склонность потребителя к пиратству должна влиять защита, применяемая производителем, поскольку это является ее непосредственной задачей. В зависимости от уровня защиты, склонность к пиратству должна обратно пропорционально изменяться. Такая величина как уровень защищенности является функцией от затрат на методы противодействия пиратам – defence(c). В зависимости от применяемых методов и их количества и сочетания данный параметр варьируется и по своей сути уникален для каждого конкретного случая. Помимо той защиты, которая обеспечивается разработчиком надо принять во внимание участие государства и специальных организаций. Это приводит к тому, что уровень защиты становится функцией от с и с0, где с0 – это вклад внешней защиты. Таким образом, функция уровня защиты при выбранной стратегии противодействия выглядит следующим образом:

*defence(c+c0)*

Аналогично цене, данный параметр имеет свои ограничения, то есть существуют такие значения уровня защиты, при которых потребитель будет либо только покупать, либо только красть. Для этого вводим показатель defencemax - уровень защиты, при котором пиратство продукта невозможно (при выбранной стратегии противодействия).

Согласно нашим рассуждениям, можно выразить зависимость вероятности пиратства от уровня защиты:

Предположим, что знаменатель дроби стремится к нулю или равен нулю, в таком случае вероятность σ=1. Это соответствует предположению о том, что в отсутствие защиты, потребитель будет красть. И наоборот, если знаменатель стремится к максимальному значению, склонность к пиратству уменьшается.

В итоге, получается, что на стремление к пиратству производитель может повлиять через изменение цены и применение различных методов борьбы с пиратством. Прежде чем объединять эти зависимости, напомним, что выделяют такой способ противодействия нелегальному распространению копий, как ценовой. Его издержки заключается в изменении (снижении) цены, в связи со скидками и специальными предложениями, предоставляемыми официальным продавцом. Это позволяет нам внести часть изменения σ от p в ее зависимость от уровня защиты. В конечно счете, остается следующее выражение:

Зная то, как мы может повлиять на решение пользователя, необходимо понять, как наши действия будут влиять непосредственно на нашу прибыль (выигрыш). Рассмотрим Ситуацию 2, когда применяется защита и присутствует пиратство. В этом случае выигрыш производителя равен:

,

В данном выражении, часть, зависящая от склонности к пиратству – (pir). Параметр piracy может быть выражен следующим образом:

Такое заключение связано с тем, что убытки от пиратства - это та часть от общего числа потребителей (которые в любом случае заинтересованы в потреблении ПО), которые должна была купить продукт, но вместо этого решила его украсть.

Компенсация за пиратство - return - не столь однозначна, поскольку при применении некоторых видов защиты его может и не быть. Его величина зависит от того не столько от затрат на защиту, сколько от конкретного способа противодействия.

Подставив вместо показателя piracy выведенное выражение, мы получим выигрыш (π) равный:

Максимизируем прибыль по затратам на пиратство:

Зная функцию зависимости уровня защиты от затрат на нее, можно уже определить при каких значениях мы будем максимизировать прибыль. Как уже говорилось, для каждой комбинации методов она своя. С одной стороны, подобное соотношение не универсально, поскольку его нельзя применить для любого случая, но с другой стороны, оно позволяет разработчику самостоятельно варьировать те методы защиты их количество и силу. Также, как предполагается, модель учитывает тот факт, что производитель может специально снижать защиту, что получить положительный эффект рекламы.

Полученная модель согласуется с нашим предположением о том, что производитель может с помощью различных методов противодействия пиратам влиять на поведение потребителя и стараться приводить игру к тому исходу, который его интересует.

Также данные результаты применимы к нашему теоретическому представлению того, как могут применяться способы борьбы и как изменяется уровень пиратства ( в общем случае) на протяжении времени.

## 2.2. Анализ стратегий компаний-примеров

Смоделированная нами игра, благодаря которой мы определили стратегическую направленность производителя в области защиты ПО от пиратского копирования является идеализированной, однако ее отражение можно найти в практике компаний-разработчиков.

В качестве примеров производителей программного обеспечения рассмотрим производителей различного типа ПО и на разных уровнях. Это позволит показать различия в подходах разработчиков относительно методов защиты и желаемого результата.

### **2.2.1. Adobe Systems**

Первая рассматриваемая компания – это Adobe Systems. Данная компания является одним из крупнейших разработчиков программного обеспечения. Ее деятельность ведется с 1982 года и успешно развивается по сей день. Adobe Systems является создателем наиболее популярного профессионального программного обеспечения в области дизайна и мультимедиа. Также компания является создателем повсеместно используемого Adobe Flash Player и популярного формата «.pdf» создаваемого в их программе Adobe Acrobat.

Однако наибольшую популярность компания получила благодаря графическому редактору Adobe Photoshop. За время существования программы, а это уже 24 года (первая версия продукта была представлена публике в 1990 году), было выпущено 14 постоянно обновляющихся версий. Последняя сменила не только название с привычного CS (creative suite) на CC(creative cloud), но и метод распространения[64].

Политика компании относительно пиратства достаточно разнообразна. Организация предоставляет свободный доступ к ряду одних продуктов и с особой щепетильностью старается ограничить копирование других.

К числу первых относятся Adobe Shockwave Player, Adobe AIR, Adobe Flash Player, Acrobat reader и пробные версии большинства других продуктов фирмы. Первые четыре программы распространяются абсолютно свободно. Рассматривая это в рамках нашей модели, подобные меры можно представить как p=0, σ→0. Несмотря на отсутствие платы за данные продукты, пользователи исправно могут обновлять версию программы. Подобная стратегия вовсе не основана на альтруизме компании-разработчика. Например, Adobe Flash Player и Acrobat reader являются средствами чтения файлов определенного формата, которые были созданы уже в платных продуктах, таких как Adobe Flash Professional, Adobe Flash Builder и Adobe Acrobat. Отсутствие свободно распространяемых программ для чтения ограничило бы функционал и применимость данного ПО, а, следовательно, уменьшило потенциальный круг потребителей. Тем не менее, та стратегия, которая применяется относительно общедоступного ПО обеспечивает заинтересованность потребителей именно в лицензионных версиях. Более того, со временем Adobe Acrobat стало стандартом программ подобного типа, создавая эффект lock in. И, несмотря на то, что ПО все еще копируется и распространяется нелегально, оно все же предпочитается бесплатным альтернативам (freeware) [4].

Компания Adobe часто обвиняется в нерациональной ценовой стратегии. Жалобы пользователей связаны с тем, что те одни и те же продукты на американском рынке продаются чуть ли не в два раза дешевле, чем в Европе и других странах [62]. Так в 2007 г. и 2008 г. в большинстве стран Европы цены на Photoshop CS3 и Photoshop CS4 были намного выше чем в Америке: например, в Великобритании стандартный пакет приложений стоил £2,313.58, а в США £1,358 [56]. Еще более противоречивыми являются цены, устанавливаемые на ПО для жителей Австралии. Дороговизна контента всегда была камнем преткновения в вопросе ценовой политики, однако своего апогея конфликт с австралийскими пользователями достиг, когда Adobe Systems объявила прайсинг последней версии Photoshop CC: австралийский вариант предлагается по цене на $A1825 больше, чем в США[[1]](#footnote-1). Общий уровень пиратства в стране сравнительно невелик (Табл.2), но действия компании, устанавливающей цену близкой к максимальной (p→pmax), что может привести к его быстрому росту, если не будет применено более строгих методов защиты [68].

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 2011г. | 2010 г. | 2009 г. | 2008 г. | 2007 г. |
| Австралия (уровень пиратства в %) | 23% | 24% | 25% | 26% | 28% |

Табл. 2. Уровень пиратства в Австралии [52]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 2011г. | 2010 г. | 2009 г. | 2008 г. | 2007 г. |
| Индия (уровень пиратства в %) | 63% | 64% | 65% | 68% | 69% |

Несмотря на сложности с Австралией и европейскими странами, Adobe Systems применяла другую стратегию для Индии. В 2011 году, компания приняла меры по снижению цены в виду высокого уровня пиратства в стране (64% контента Adobe, используемого на территории Индии, были нелегальными). Делая продукт более доступным для населения с низким уровнем дохода, компания пытается снизить стремление потребителей использовать нелегальные версии [78].

Табл. 3. Уровень пиратства в Индии [52]

Согласно данным V.I.Labs графические редакторы, выпускаемые Adobe Systems занимают треть самых популярных среди пиратов ПО в Великобритании: Adobe Photoshop (16%) Adobe Illustrator (16%) Adobe Creative Suite (10%) [79]. Область применения Photoshop включает многие сферы жизни, не только графический дизайн и фото, но и судебное производство, наличные исследования и медицину[75]. Величина масштабов использования программных продуктов приводит к тому, что не только отдельные потребители скачивают нелегальные копии, но и целые организации устанавливают пиратские версии, тем самым экономя средства фирмы.

Рассмотрим методы защиты применяемые к Adobe Creative Suite и Adobe Photoshop. Поскольку одно включает в себя другое можно их обобщить. Для этого, постараемся распределить типы защиты компании, согласно приведенной нами ранее классификации.

1. **Техническая защита:** *Лицензионные ключи и регистрация(installation key)*. Часто используемый способ защиты, регистрирующий единицу продукта за конкретным пользователем и допускающий его к использованию программы. Серийные ключи Adobe включают порядка 28 знаков. Данный метод защиты далеко не самый действенный, поскольку нелегальному пользователю не составит большого труда найти генератор ключей (keygen) , который позволит получить действующий, но не занятый лицензионный ключ. В настоящее время регистрация товара при установке ПО проводится также в режиме онлайн и требует периодического соединения с сетью для подтверждения легальности продукта, получения обновлений и дополнительной информации.

При регистрации легального продукта пользователи предоставляют частичные данные о себе компании, и предполагается, что эта информация останется в сохранности и не будет доступна третьим лицам. Однако практически ежегодно пользователи продукции Adobe Systems становятся жертвами хакеров и вирусов, а их личные данные становятся общедоступными [71].

1. **Правовая:** *Лицензионное соглашение***.** Также привычная для любого ПО практика соглашения может пользователем и разработчиком о запрете копирования, распространения, правах участников соглашения и правилах легального пользования программным продуктом. Соглашаясь с условиями договора, пользователь в дальнейшем может быть привлечен к суду, в случае его нарушения. Следует отметить, что Adobe Systems достаточно часто прибегает именно к данному методу защиты. Так, например, в России компания назначила специалиста по защите прав на интеллектуальную собственность на должность руководителя соответствующего направления по России и СНГ [63]. Под его руководством с 2010 года, количество возбуждённых уголовных дел с каждым годом уменьшается (2011 г. – 1073 дела, 2012 г. – 895 дел). Это связывают как с ужесточением законодательства, так и с эффективностью деятельности компании против пиратства. Почти половина преступлений в сфере пиратства была совершена студиями дизайна и рекламными агентствами[66]. Существует пример того, как Adobe Systems смогли получить компенсацию от пирата. Так в 2009 году Грегори Фэа был приговорен к сроку в 41 месяц тюремного заключения и обязательству выплатить компенсацию компании в размере 743098 долларов США за незаконное распространение пиратских копий на E-bay[61].
2. **Защита через продукт:** *Техническая поддержка и обновления*. В качестве основного преимущества лицензионного продукта выступают именно возможности получить техническую поддержку и уверенность потребителя в том, что в интересы компании входит улучшение его удовлетворенности продуктом. Тем не менее, Adobe, несмотря на обещанное внимание к пользователям, не оправдывает их надежды. Часто критикуемая за низкий уровень обслуживания клиентов организация даже была вынуждена публично извиняться[68].   
   Поддержка продукта и его развитие являются одной из сильных сторон Adobe. Как правило, обновление приложений происходит примерно каждые 15 месяцев и на одну версию приходится по три-две модификации. В связи с тем, что ПО данной компании используется не только простыми потребителями, но и профессионалами, периодические нововведения являются для них особенно привлекательными.
3. **Методвзаимосвязи:***Предупреждения о возможной опасности.*Как и у многих других компаний, Adobe имеет отдельную страницу на сайте посвященную противодействию пиратству. Организация предоставляет пользователям информацию о том, как отличить нелегальную копию от оригинала, чем грозит использование пиратских версий, а также, куда и в какой форме необходимо сообщить о действиях пиратов.
4. **Ценовыеметоды:** *Специальные предложения*. Как уже отмечалось, ценовая политика компании весьма противоречива. Adobe устанавливает цены выше в странах с развивающейся экономикой, где, как известно, уровень пиратства на рынке ПО намного выше, чем в западных странах [57]. До недавнего времени, когда Adobe еще предлагал, в качестве основного продута, именно CS версии, цены устанавливались таким образом, что пользователь мог приобрести extended version той или иной программы по цене немногим большей, чем простой вариант. Вопрос заключался в том, что большая часть ПО ,входившая в расширенный набор, требовалась далеко не всем потребителям, но сравнительная дешевизна заставляла их потратить лишнее деньги именно на Extended edition.   
   Запуск нового формата ПО - CC- представляет собой подписку с ежемесячной или ежегодной оплатой, позволяющей потребителю пользоваться любыми программами, которые обычно входили в CS. При этом Adobe отказывается от продажи «коробочных» пакетов приложений. С одной стороны, подобная форма оплаты действительно дешевле для пользователей постоянно обновляющих программные продукты. С другой стороны, та доля клиентов, которая годами не меняла старую версию (в силу ненадобности) действительно пострадает [59].

Обобщим стратегию Adobe Systems по борьбе с пиратством в рамках нашей модели. Уровень защиты в основном, держится на правовом методе, поддержки государства и ассоциаций, с которыми сотрудничает компания (BSA, SIIA): defence(c+c0)↑. Техническая защита находится на низком уровне, более того, компания не в состоянии обеспечить 100% сохранность данных пользователей - defence(c+c0)↓. Защита через продукт находится на относительно высоком уровне, но ее эффективность падает за счет плохой службы поддержки - defence(c+c0)↓. В сумме это говорит о низком уровне противодействия пиратам defence(c+c0)→0. Более весомым аргументом является неэффективность ценовой политики компании, когда p→pmax для большинства пользователей.

Это подтверждает неэффективность стратегии защиты ПО от пиратства, применяемую Adobe Systems.

### 2.2.2. ABBYY

Компания ABBYY пример иного подхода к защите от пиратства. Она не столь крупная компания, как Adobe Systems, не так популярна и более молода, более того ее рынок сбыта меньше. Политика ABBYY относительно пиратства более мягкая и нацелена на коммуникацию с пользователями.

ABBYY была создана в 1989 году и до 1997 года называлась BIT-Software. Сейчас компания развилась до уровня ведущих мировых разработчиков ПО. ABBYY занимается созданием продуктов в сфере распознавания документов, электронных словарей и лингвистики. На данный момент она работает уже не только на территории России, но и сотрудничает с Австралией, Великобританией, Германией и многими другими странами с развитой экономикой. Среди пользователей программ, создаваемых компанией жители более 150 стран (на Россию и СНГ приходится примерно 20-25% от общего потребления [54]).   
ABBYY занимается распространением своих продуктов как среди коммерческих организаций, так и в массовых масштабах.

Наиболее популярный продукт компании это система электронных словарей ABBYY Lingvo. Компания предлагает различные версии программы, включающие в себя большее или меньшее количество языков, тематических словарей и дополнительных функций. ПО работает с различными платформами и доступно в качестве приложения на планшеты/смартфоны. Данный продукт является основой нашего анализа способов защиты компании.

Компания ABBYY также как и остальные производители распространенного ПО, страдает от пиратства. Наибольший ущерб приносят российские и украинские пираты, где процент нелегального контента достигал 60-70% в 2011 году [chip]. Тем не менее, компания достаточно спокойно и оптимистически смотрит на такие показатели, считая их неотъемлемой частью рынка ПО. Рассмотрим методы защиты данной компании аналогично с Adobe.

1. **Техническая защита.** С момента перехода пиратов от вещественных носителей к раздаче копий через интернет ABBYY стала прибегать к методу отслеживания сайтов-распространителей, с целью их закрытия или удаления нелегальных копий. В 2011 году было объявлено, что фирме удалось закрыть около 2120 раздач и ссылок на пиратские копии. Тем не менее, руководители компании признают, что данный метод далеко не самый действенный, в силу своего недолгого эффекта.
2. **Правовая.** ABBYY придерживается мнения о том, что жесткие меры относительно пользователей не действенны. Компания использует лицензионный договор, но правами, закрепленными в нем, пользуется не часто. В основном правовая защиты ABBYY направлена на коммерческие организации, так как они могут причинить больший вред, чем отдельные пользователи. На первых этапах развития компания даже не пыталась получить компенсацию от пиратов, и дела заводимые фирмой были редкими случаями [67]. В настоящий момент, основной проблемой для ABBYY является высокий уровень пиратства в России и Украине. Компания вступает в сотрудничество с правоохранительными органами с целью проведения проверок с дальнейшим возбуждением дел относительно нелегальных пользователей [54]. Более того, в Украине организация также выступала инициатором создания соответствующих правовых норм.
3. **Защита через продукт.** Продукты ABBYY защищены лицензионным ключом, при активации которого компания имеет возможность следить за количеством ПК, на которые было установлено ПО и соответственно ограничивать их число. Также это позволяет разработчикам вести собственную статистику пользователей, как легальных, так и нет.При этом компании не требуется никакой персональной информации о пользователе, данных о его компьютере или установленных на нем программах.Техническая поддержка, предоставляемая компанией, полностью описывается на сайте разработчика. ABBYY предоставляет информацию о жизненном цикле продукта, услугах поддержки, часах работы и способах связи [65].
4. **Метод взаимосвязи.**Согласно словам руководителей компании именно на данном методе воздействия старается сосредоточитьсяABBYY. Противник драконовских мер, разработчики проводят разъяснительные семинары и акции, с целью побудить пользователей приобретать лицензионные версии продукта.
5. **Ценовые методы.**Устанавливая цены на свои продукты, ABBYY пытается угодить потребителю и его нуждам. Лицензии на корпоративные и домашние пакеты программ значительно отличаются по содержанию и по цене. В отличие от Adobe, где покупая расширенную версию, потребитель гонится за относительной дешевизной, созданной производителей, пользователи ABBYY имеют достаточно широкий выбор ПО, предназначенных именно для них с разной комплектацией и соответственно разной ценой. Также компания предлагает свои продукты в режиме онлайн, где оплата производится по числу обработанных единиц (например, страниц для FineReader Online [55]. Более того, компания старается привлечь внимание пиратов к более дешевым, облегченным версиям продуктов, и тем самым сделать их своими клиентами. Если говорить о ABBYY LINGVO словарях, то на сайте доступны 2 типа пробных словарей с ограниченным количеством данных (часть подгружается только при наличии сети), но без ограничений по времени.

Наибольшую эффективность для ABBYY приносит техническая защита, вписанная в продукт. Для того чтобы ее обойти пиратам требуется достаточно длительное время и далеко не всегда им удается сохранить полный функционал программы. Это заметно понижает качество копий и усложняет процесс их распространения и установки.

Если обобщить информацию о способах защиты ПО компанией ABBYY то можно сделать следующие выводы:

* Производитель проводит достаточно масштабные кампании по закрытию ресурсов, распространяющих нелегальные копии ПО - defence(c+c0)↑.
* ABBYY не является сторонником правовых методов, в связи с большими затратами на ведение судебных дел и содержания юридического аппарата - defence(c+c0)↓.
* Защита, устанавливаемая непосредственно в продукт находится на достаточно высоком уровне и отражается в понижении качества пиратской копии - α↓. Однако, количество обновлений и техническая поддержка (платная) не является средством привлечения новых клиентов из числа пиратов - defence(c+c0)↓.
* ABBYY считает своим долгом проинформировать пользователей о вреде пиратства не только для компании, но и для них самих и прилагает немало усилий, для пропаганды использования легальных продуктов - defence(c+c0) ↑.
* Ценовая политика компании достаточно щадящая, соотносимая с достатком жителей страны, в которой продукт распространяется и предполагает различные ценовые категории для коммерческих и домашних нужд. 0<p<pmax

Необходимо отметить тот факт, что область использования продуктов компании ABBYY достаточно широка от нефтегазовой промышленности до банковского дела и государственных нужд. Компания является одним из лидеров рынка подобного ПО и занимает долю примерно в 50%. В связи с этим та часть продукции, которая используется пиратам – это как правило частные лица (ПО домашнего использования) и небольшие компании.

Для ABBYY c0>0, так как компания входит в Некоммерческое Партнерство Поставщиком Программных Продуктов (НП ППП). Помимо этого в последние годы значительно ужесточилось законодательство в сфере интернет пиратства в России.

Стратегия ABBYY по противодействию пиратству не является эталонным показателем, однако ее результативность больше, чем у Adobe. Своими методами производитель лингвистического ПО понижает склонность потребителей к пиратству (не до нулевого показателя, но в достаточной степени, чтобы повлиять на решения части потенциальных потребителей). Помимо этого, техническая защита, вписанная в продукт, снижает полезность от пиратского ПО. Таким образом, рассматривая ситуацию с продуктами ABBYY относительно нашей игры, выигрыш потребителя предпочитающего пиратскую копию при наличии защиты меньше, чем от приобретения оригинала.

# Заключение

Целью нашей работы было установить экономическую целесообразность применения защиты от пиратства. Для этого мы проанализировали работы различных авторов, изучавших данную сферу, и расссмотрели наиболее часто выделяемые средства защиты. Так, мы определили, что все методы можно разделить на две общие группы: превентивные и карательные. Как наиболее развитые и часто используемые средства защиты выделяются следующие:

* *Методы взаимосвязи*, подразумевающие проведение образовательных мероприятий по убеждению пользователей во вреде нелегальных копий ПО, а также установление обратной связи с потребителями, которые готовы сообщить о факте пиратства.
* *Правовые методы,* заключающиеся в патентировании и лицензировании программных продуктов, а также дальнейшая их защита согласно договорам, заключаемым с клиентами. Была отмечена зависимость эффективности этого метода от работы других (непосредственно технических).
* *Техническая защита –* отслеживание пиратской деятельности в сети посредством дополнительно ПО и внедрение средств защиты в сам продукт.
* *Защита через продукт* являет собой все те особенности обеспечивающие уникальность оригинального продукта: качество, возможность получения обновлений, исправление ошибок производителем в ходе эксплуатации продукта клиентами, а также обеспечение технической поддержки.
* Ценовые методы – это самые популярные способы противодействия пиратам. Их суть заключается в установлении таких цен (скидок или специальных предложений), что потребители предпочтут оригинальное ПО пиратской копии.

Исследование внешних условий, осуществляющих собственное противодействие недобросовестным пользователям, мы определили, что компания-разработчик может получать дополнительную защиту в зависимости от уровня соответствующего законодательства в государстве и наличия членства в объединении против пиратства.

Для наглядности изменения эффективности различных методик противодействия, мы разделил жизненный цикл продукта на три стадии и подробно описали то, как ведет себя пират на каждом промежутке времени. Это позволило определить, как лучше применять защиту на конкретных стадиях и на каком уровне.

Модель игры между потребителем и производителем позволила нам понять в чем заключается преимущество каждого из исходов для участников. Мы определили, что реальной ситуации соответствует случай, когда разработчик защищает ПО, а пользователь «крадет». Также мы доказали на теоретическом уровне, что отсутствие защиты может привести к тому, что потребитель однозначно переключится на стратегию пирата. Определив задачу производителя как влияние на склонность пользователя к использованию нелегальных копий, мы вывели зависимость вероятности выбора этой стратегии от действий разработчика. Было обнаружено, что применение защитных механизмов (в особенности ценовых) действительно влияет на выбор клиента и на полезность от пиратского продукта (уменьшая ее при росте защиты). Отмечается, что создание какой-либо универсальной формулы стратегии против пиратства не приведет к положительным результатам, поскольку в каждом конкретном случае необходимо учитывать слишком много факторов, включение которых в модель лишь утяжелит ее.

Для подтверждения гипотезы о действенности защиты, мы рассмотрели примеры двух компаний различных областей и размеров. Как оказалось более крупный производитель ПО Adobe Systems использует менее эффективную политику против пиратства, чем ABBYY. Повышенная вероятность пиратства среди пользователей графических редакторов Photoыhop вызвана как слишком простой технической защитой, так и завышенными ценами. В теоретической части мы отмечали, что наиболее оптимальный вариант стратегии противодействия заключается в сочетании почти всех методов защиты, перевес или отказ от части из них приводит к неблагоприятным последствиям. Компания Adobe Systems является живым тому примером. Помимо издержек связанных с пиратством, разработчик теряет лояльность уже существующих потребители.

Компания ABBYY – это показатель более эффективной, но не идеальной политики борьбы с пиратством. Делая акцент на менее затратный метод взаимосвязи и технические способы, производитель лингвистического ПО несет меньшие затраты по самой защите и снижает уровень пиратства.

Таким образом, можно сделать вывод о том, что применение защиты действительно приносит положительный экономический эффект разработчику, но лишь при условии, что выбранная им стратегия оправдывает себя и является эффективной, при учете внешних условий и этапа жизни продукта.

# Источники

1. Гришаев С.П. Интеллектуальная собственность: учебное пособие// Понятие и значение авторского права/Юристъ, 2004. - 240 стр.
2. Математическое моделирование рынка программного обеспечения // Институт гуманитарного образования и информационных технологий. Москва. 2011.
3. Ahn I., Shin I. On the optimal level of protection in DRM // Inf. Econ. Policy. 2010. Т. 22. № 4. С. 341–353.
4. Attaya H. On the competition between Proprietary software Piracy and Free software ∗ // 2011. С. 1–19.
5. August T., Tunca T.I. Let the Pirates Patch ? An Economic Analysis Software Security Patch Restrictions // 2013. Т. 19. № 1. С. 48–70.
6. Baguley P., LoV., Lamoureux T. Is unlicensed software hurting your bottom line?// KPMG. 2013.
7. Banerjee D. Effect of piracy on innovation in the presence of network externalities // Econ. Model. 2013. Т. 33. С. 526–532.
8. Berg S. V. Copyright, conflict, and a theory of property rights // 2012. Т. 5. № 2. С. 71–79.
9. Braskamp C. Genuine Microsoft Products Vs . Pirated Counterparts // 2011.
10. Castro J.O. De, Balkin D.B., Shepherd D. a. Can entrepreneurial firms benefit from product piracy? // J. Bus. Ventur. 2008. Т. 23. № 1. С. 75–90.
11. Charoensukmongkol P., Elkassabgi A. The inverse U curve relationship between software piracy and technological outputs in developed nations // Manag. Res. Rev. 2011. Т. 34. № 9. С. 968–979.
12. Chen C., Chen C., Yeh C. Technological and Economic Indicators on Software Piracy in OECD Countries // 2012. Т. 9. № September. С. 73–82.
13. Chik W.B. The Google conundrum: Perpetrator or facilitator on the net? – Forging a fair copyright framework of rights, liability and responsibility in response to search engine 2.0 – Part I: The Google Images Search Engine // Comput. Law Secur. Rev. 2011. Т. 27. № 2. С. 111–132.
14. Chiou W.-B., Wan P.-H., Wan C.-S. A new look at software piracy: Soft lifting primes an inauthentic sense of self, prompting further unethical behavior // Int. J. Hum. Comput. Stud. 2012. Т. 70. № 2. С. 107–115.
15. Cho W.-Y., Ahn B.-H. Versioning of information goods under the threat of piracy // Inf. Econ. Policy. 2010. Т. 22. № 4. С. 332–340.
16. Choi P., Bae S.H., Jun J. Digital piracy and firms’ strategic interactions: The effects of public copy protection and DRM similarity // Inf. Econ. Policy. 2010. Т. 22. № 4. С. 354–364.
17. Cremer H., Pestieau P. Piracy prevention and the pricing of information goods // Inf. Econ. Policy. 2009. Т. 21. № 1. С. 34–42.
18. Djekic P., Loebbecke C. Preventing application software piracy: An empirical investigation of technical copy protections // J. Strateg. Inf. Syst. 2007. Т. 16. № 2. С. 173–186.
19. Ethics B. to Encourage Customers Software to Use Chiu // 2013. Т. 80. № 3. С. 583–595.
20. John C. SIIA Wins its First European Anti-Piracy // SIIA Anti-Piracy Division News 2011.
21. Harbi S. El, Grolleau G., Bekir I. Substituting piracy with a pay-what-you-want option: does it make sense? // Eur. J. Law Econ. 2011.
22. Hemmige N. Piracy in the Internet Age // 2013. Т. 18. № September. С. 457–464.
23. Hsu J.L., Shiue C.W. Consumers’ Willingness to Pay for Non-pirated Software // J. Bus. Ethics. 2007. Т. 81. № 4. С. 715–732.
24. Jean-Jacques Herings P., Peeters R., Yang M.S. Competition against peer-to-peer networks // Inf. Econ. Policy. 2010. Т. 22. № 4. С. 315–331.
25. Jeong B.-K., Khouja M., Zhao K. The impacts of piracy and supply chain contracts on digital music channel performance // Decis. Support Syst. 2012. Т. 52. № 3. С. 590–603.
26. Khouja M. Application of complex adaptive systems to pricing of reproducible information goods // Decis. Support Syst. 2008. Т. 44. № 3. С. 725–739.
27. Khouja M., Smith M.A. Optimal pricing for information goods with piracy and saturation effect // Eur. J. Oper. Res. 2007. Т. 176. № 1. С. 482–497.
28. Kogan K., Ozinci Y., Perlman Y. Containing piracy with product pricing, updating and protection investments // Int. J. Prod. Econ. 2013. Т. 144. № 2. С. 468–478.
29. Kogan K., Ozinci Y., Perlman Y. Int . J . Production Economics Containing piracy with product pricing , updating and protection investments // Intern. J. Prod. Econ. 2013. Т. 144. № 2. С. 468–478.
30. Kshetri N. Kaspersky Lab: from Russia with anti-virus // Emerg. Mark. Case Stud. Collect. 2011. Т. 1. № 3. С. 1–16.
31. Liu Y. Optimal software pricing in the presence of piracy and word-of-mouth effect // Decis. Support Syst. 2011. Т. 51. № 1. С. 99–107.
32. Minniti A., Vergari C. Turning Piracy into Profits: a Theoretical Investigation // Inf. Econ. Policy. 2010. Т. 22. № 4. С. 379–390.
33. Morris R.G., Higgins G.E. Criminological theory in the digital age: The case of social learning theory and digital piracy // J. Crim. Justice. 2010. Т. 38. № 4. С. 470–480.
34. Nill A., Shultz C.J. Global software piracy: Trends and strategic considerations // Bus. Horiz. 2009. Т. 52. № 3. С. 289–298.
35. Oprean C., Tănăsescu C. The Speed of Incorporating Information into Prices // Procedia Econ. Financ. 2013. Т. 6. № 13. С. 675–682.
36. Paul T., Al-rafee S., Cronan T.P. Factors That Influence the Intention to Pirate Software and Media Factors to Pirate that Influence Software the Intention and Media // 2012. Т. 78. № 4. С. 527–545.
37. Png I.P.L. On the reliability of software piracy statistics // Electron. Commer. Res. Appl. 2010. Т. 9. № 5. С. 365–373.
38. Prasad A., Mahajan V. How many pirates should a software firm tolerate ? An analysis of piracy protection on the diffusion of software // 2003. Т. 20. С. 337–353.
39. Qiu L.D. A general equilibrium analysis of software development: Implications of copyright protection and contract enforcement // Eur. Econ. Rev. 2006. Т. 50. № 7. С. 1661–1682.
40. Rasch A., Wenzel T. Journal of Economic Behavior & Organization Piracy in a two-sided software market ଝ // J. Econ. Behav. Organ. 2013. Т. 88. С. 78–89.
41. Robertson C.J. и др. An analysis of the predictors of software piracy within Latin America // J. Bus. Res. 2008. Т. 61. № 6. С. 651–656.
42. Sen R., Subramaniam C., Nelson M.L. Open source software licenses: Strong-copyleft, non-copyleft, or somewhere in between? // Decis. Support Syst. 2011. Т. 52. № 1. С. 199–206.
43. Shih R., Ku R. The Creative Destruction of Copyright : of Digital Technology and the New Economics Napster // 2012. Т. 69. № 1. С. 263–324.
44. Sudler H. Effectiveness of anti-piracy technology: Finding appropriate solutions for evolving online piracy // Bus. Horiz. 2013. Т. 56. № 2. С. 149–157.
45. Suh D., Hwang J. An analysis of the effect of software intellectual property rights on the performance of software firms in South Korea // Technovation. 2010. Т. 30. № 5-6. С. 376–385.
46. Tang G.H. Is administrative enforcement the answer? Copyright protection in the digital era // Comput. Law Secur. Rev. 2010. Т. 26. № 4. С. 406–417.
47. Vázquez F.J., Watt R. Copyright piracy as prey–predator behavior // J. Bioeconomics. 2010. Т. 13. № 1. С. 31–43.
48. Yang D., Fryxell G.E., Sie A.K.Y. Anti-piracy effectiveness and managerial confidence: Insights from multinationals in China // J. World Bus. 2008. Т. 43. № 3. С. 321–339.
49. Yoof C.S. Copyright and Public Good Economics : A Misunderstood Relation// University of Pennsylvania Law Review 2012. Т. 155. № 3. С. 635–715.
50. ESA Annual report // 2012.
51. Infringing File Sharing. Regulations – Fee Review // 2012. March.
52. Shadow market 2011 BSA global software piracy study // 2012.
53. The Surprising Risks of Counterfeit Software in Business //Microsoft. 2009. № October 2006. С. 1–18.
54. Письменный А. Генеральный директор ABBYY Россия о будущем OCR и облачных сервисах// Компьютерра-Онлайн. URL: http://old.computerra.ru/interactive/703174/ (дата обращения - 20.05.2014)
55. Комментарии:. URL: http://comments.ua/ht/289322-62-produktov-abbyy-ukraine.html (дата обращения - 20.05.2014).
56. Barker C. Adobe responds to CS4 pricing criticism// ZDNet. URL: http://www.zdnet.com/adobe-responds-to-cs4-pricing-criticism-3039497760/ (дата обращения – 17.05.2014).
57. Cosovanu C. Piracy, price discrimination, and development: The software sector in eastern europe and other emerging markets// Columbia Science and Technology Law Review. URL: http://www.stlr.org/html/volume5/cosovanu.txt (дата обращения - 24.05.2014).
58. Crookes D. Anti-piracy download laws around the world explained//BBC. URL: http://www.bbc.co.uk/newsbeat/16839637 (дата обращения - 10.03.2014) .
59. Diallo A. Adobe Answers Photoshop CC Uproar With Low Cost Bundle// Forbes. URL: http://www.forbes.com/sites/amadoudiallo/2013/09/05/adobe-answers-photoshop-cc-uproar-with-low-cost-bundle/ (дата обращения - 24.05.2014).
60. Grubb B. Adobe chief dodges questions over pricing// The Sydney morning herald. URL: http://www.smh.com.au/technology/technology-news/adobe-chief-dodges-questions-over-pricing-20130214-2eetr.html (дата обращения - 20.05.2014).
61. Hagan Cain R. Software Pirate's Gain Not Necessarily Adobe Systems' Loss// FindLaw. URL: http://blogs.findlaw.com/dc\_circuit/2012/11/software-pirates-gain-wasnt-necessarily-adobe-systems-loss.html (дата обращения - 22.05.2014).
62. Stone T. Creative Suite Pricing Varies Throughout World// Creative pro. URL: http://www.creativepro.com/article/creative-suite-pricing-varies-throughout-world (дата обращения – 17.05.2014).
63. 1csoft. URL: http://www.1csoft.ru/publications/8143/9672930/ (дата обращения - 22.05.2014).
64. 20 Years of Adobe Photoshop//Web Design. URL: http://www.webdesignerdepot.com/2010/02/20-years-of-adobe-photoshop/ (дата обращения – 15.05.2014).
65. ABBYY. URL: http://www.abbyy.ru/support/policy/ (дата обращения - 20.05.2014).
66. Adobe Anti-Piracy. URL: https://www.facebook.com/adobeantipiracy?fref=nf (дата обращения - 22.05.2014).
67. AgoNet. URL: http://www.algonet.ru/?ID=15475 (дата обращения - 20.05.2014).
68. AustralianIT. URL: http://www.theaustralian.com.au/australian-it-old/adobe-delays-anger-users/story-e6frgamo-1225765761841 (дата обращения - 22.05.2014).
69. Business Software Alliance. URL: http://ww2.bsa.org/country.aspx?sc\_lang=ru-RU (дата обращения – 25.03.2014).
70. Chip.ua. URL: http://www.chip.ua/novosti/rasprostraniteli-piratskogo-po-abperebirayutsyabb-v-onlain/ (дата обращения - 20.05.2014).
71. CNN Money. URL: http://money.cnn.com/2013/10/08/technology/security/adobe-security/ (дата обращения - 22.05.2014).
72. Entertainment software association. URL: http://www.theesa.com (дата обращения – 25.03.2014).
73. Federation against software theft. URL: http://www.fastiis.org (дата обращения – 25.03.2014).
74. Microsoft. URL: http://office.microsoft.com/en-us/store/?CTT=97(дата обращения – 23.04.2014).
75. Photoshop.com. URL: http://www.photoshop.com/products/photoshop/who(дата обращения - 22.05.2014).
76. Software & Information Industry Association. URL: http://www.siia.net (дата обращения – 25.03.2014).
77. Software association paid $57K in 2010 to piracy whistleblowers// Networkworld. URL: http://www.networkworld.com/news/2011/021111-siia-pays-software-piracy-whistleblowers.html (дата обращения – 10.04.2014).
78. The Hindu Business Line. URL: http://www.thehindubusinessline.com/industry-and-economy/info-tech/adobe-changes-pricing-strategy-in-india-to-beat-piracy/article2359209.ece (дата обращения – 17.05.2014).
79. V.I.labs. URL: http://www.vilabs.com/resource-section/stat-watch/ (дата обращения – 17.04.2014).

1. $4334- Австралия, $A2509-США [↑](#footnote-ref-1)