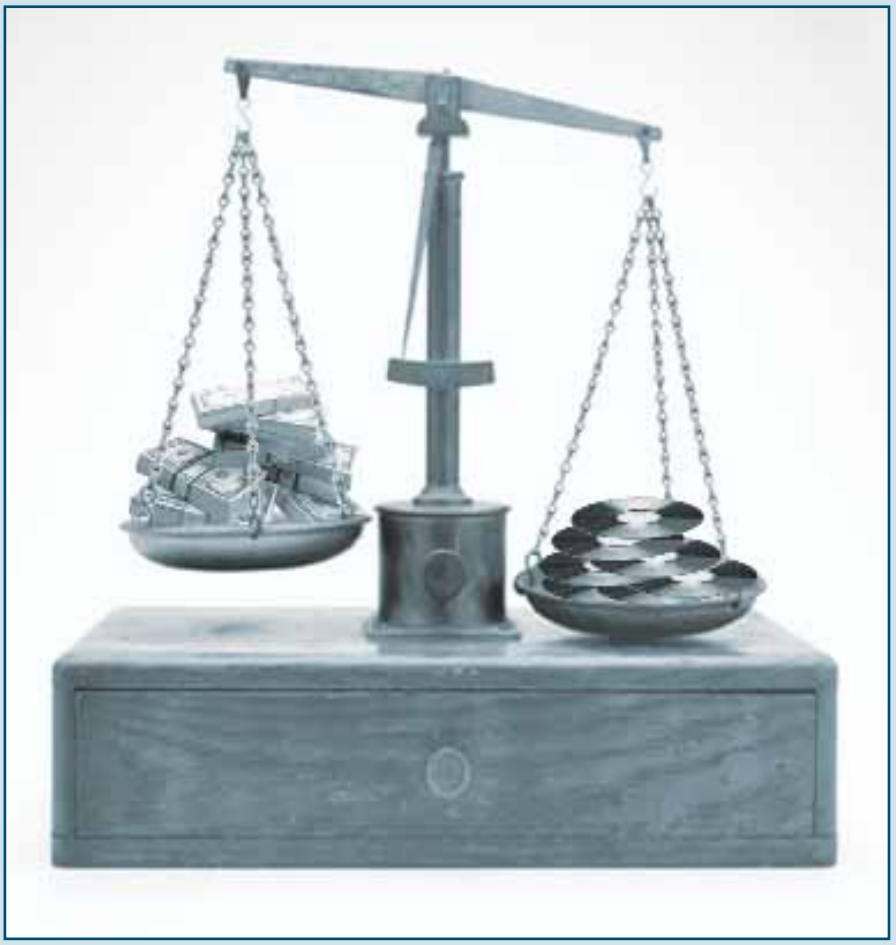
Экономический анализ поведения участников рынка программного обеспечения

Середа С.А., аспирант Экономической академии Молдовы,
кафедра кибернетики и экономической информатики
E-mail: serge_sereda@hotmail.com

В статье рассмотрен подход к изучению экономических механизмов легального и нелегального распространения программного обеспечения (ПО), а также связанных с этим критериев поведения участников рынка. Предложены модели экономического поведения покупателя ПО, злоумышленника, а так же производителя ПО. Проводится анализ предложенных моделей и возможностей их практического применения.



С развитием рынка информационных и коммуникационных технологий актуальной стала проблема несанкционированного распространения программных продуктов (попросту, "пиратство"). Указанная проблема появилась почти одновременно с появлением класса персональных ЭВМ (ПЭВМ, ПК) в 80-х годах XX века, во многом благодаря особенностям данного класса компьютеров. Для больших и малых ЭВМ проблема пиратства практически не актуальна по ряду причин: во-первых, львиная доля программного обеспечения входит в стоимость самой ЭВМ, т.е. "бесплатна", во-вторых, количество пользователей ЭВМ указанных классов ограничено, кроме того, практически всё это - корпоративные пользователи, в-третьих, реальный доступ к ПО в таких вычислительных системах есть лишь у администратора, доступ же рядовых пользователей к прикладному ПО контролируется средствами контроля и разграничения доступа, встроенными в операционную систему.

В случае же персональных ЭВМ ситуация совершенно иная. Персональные компьютеры чрезвычайно широко распространены, при этом значительная их доля принадлежит частным владельцам. ЭВМ этого класса находятся под полным контролем пользователя, а так же под защитой законов о частной собственности. Таким образом, организация контроля над индивидуальными владельцами ЭВМ не представляется практически возможной. При этом системное и прикладное ПО для ПЭВМ продаётся за отдельную плату (за исключением предустановленного), кроме того, существует очень широкая номенклатура и ассортимент ПО для ПЭВМ. Разумеется, существует очень большой спрос на указанное программное обеспечение, и не всегда пользователей волнует легаль-

ность приобретаемых копий программных продуктов. Не менее важным является тот факт, что стоимость ПО не только приблизилась, но, в некоторых областях, даже обогнала стоимость аппаратного обеспечения. Таким образом, нередки ситуации, когда пользователь, нуждающийся по роду своей деятельности в программном обеспечении определённого типа, принципиально не в состоянии приобрести легальную версию программного продукта. Всё вышеуказанное, наряду с упоминавшимся ранее ростом рынка, создаёт множество предпосылок для компьютерного пиратства.

В последнее время всё более очевидной становится необходимость анализа экономической составляющей процесса распространения программного обеспечения. До недавних пор основной акцент в исследованиях, посвящённых проблемам защиты ПО, делался на программно-технические методы защиты программ [2, 9, 10, 11, 115]. На второе место ставился юридический аспект защиты авторских прав на ПО [12, 13, 14].

В то же время, экономический аспект анализа отношений между производителем, покупателем ПО и злоумышленником практически не исследовался. Таким образом, рассматривались лишь внешние, технические, проявления соперничества "производитель-злоумышленник" в отрыве от исследования внутренних механизмов этого взаимодействия, важной частью которых являются экономические отношения на рынке ПО.

С другой стороны, экономический анализ поведения (потенциального) злоумышленника уже достаточно давно является стандартным этапом процедуры анализа рисков, проводимой в ходе проектирования и сопровождения систем защиты информации [1].

Более того, уже свыше двадцати лет существует экономическая криминалистика, использующая методы экономического анализа для исследования различных типов нарушений закона [4, 5, 6, 7, 8]. В рамках данной дисциплины преступник рассматривается как "рационально мыслящий экономический агент", принимающий решение о совершении преступления или отказе от него, руководствуясь экономической оценкой затрат на совершение преступления, выгоды от его совершения и риска быть пойманным органами правопорядка. В то время как применимость анализа экономического поведения сразу ко всем видам правонарушений может подвергаться сомнениям [8], экономическая сущность компьютерного пиратства говорит в пользу перспективности подобного подхода к изучению причин и выработке мер противодействия нарушениям на рынке ПО.

Одна из первых попыток анализа экономических мотивов поведения потенциального нарушителя авторских прав была сделана в работе Премкумара Деванбю и Стюарта Стаблбайна [3]. В разделе "Adversary Economics" (Экономика злоумышленника) авторами формулируется приближённая экономическая оценка "выгодности" преодоления системы программно-технической защиты ПО и последующего его нелегального распространения. Выглядит она следующим образом:

$$n C_b >> C_h + n C_c + P_{11}(n) C_{11}(n)$$

где:

C_b - цена одной легальной копии ПО;

C_h - объём затрат на "взлом" системы защиты;

n - количество распространённых нелегальных копий;

C_c - цена одной нелегальной копии ПО;

P_{11} - риск (вероятность) поимки;

C_{11} - объём штрафа при поимке,

при этом оговаривается, что последние два фактора (P_{11} и C_{11}) могут меняться в зависимости от количества распространённых нелегальных копий (n). Таким образом, видно, что, как правило, затраты на нарушение авторских прав на ПО, даже с учётом возможного наказания, значительно ниже стоимости легального приобретения ПО.

В настоящей работе предлагается свой взгляд на вышеописанную проблему, выраженный в трёх моделях, приведённых ниже.

Рассмотрим экономические критерии поведения покупателя программных продуктов.

ЭКОНОМИЧЕСКАЯ МОДЕЛЬ ПОВЕДЕНИЯ ПОКУПАТЕЛЯ ПО

Введём следующие переменные:

L ($l_1, l_2, \ldots l_L$) - множество легальных продуктов производителей ПО;

U ($u_1, u_2, \ldots u_U$) - множество нелегальных продуктов ($U \subseteq L$);

IP (infringement penalty) - сумма убытка при уличении в нелегальном использовании ПО;

PL (program loses) - сумма убытка от некачественного ПО (с дефектами производства);

P - вероятность уличения в нелегальном использовании ($P(l_i)=0$, $P(u_j) \in [0;1]$);

Q^i_L - вероятность ущерба от некачественного ПО (с дефектами производства);

S - сумма, которую потребитель согласен затратить на автоматизацию;

C^i_L - цена лицензионной копии i-го программного продукта;

C^j_U - цена "пиратской" копии i-го программного продукта;

N^i_L - накладные расходы на i-й программный продукт (настройка, доводка);

I - доход (прямой или косвенный), который потребитель рассчитывает получить от автоматизации предметной области

Модель будет иметь следующий вид:

Критерий первичного отбора программных продуктов:

$$[\min\{C^i_L, (C^j_U + P^j_U * IP)\} + N^i_L + Q^i_L * PL] \le S$$

Критерий поведения потребителя:

$$B = I - (\min\{C^i_L, [C^j_U + P^j_U * IP]\} + N^i_L + Q^i_L * PL) \rightarrow \max$$

Условие приобретения легальных продуктов:

$$C^i_L \le C^j_U + P^j_U * IP$$

Необходимо отметить, что приведенная модель не основывается на теории предельной полезности, так как процесс выбора ПО довольно специфичен и не вполне совпадает с процессом выбора обычных товаров и услуг. В частности, процесс выбора ПО четко ориентирован на определенный тип программ, чаще всего приобретается единичный продукт, а не "набор благ". Кроме того, в силу тиражируемости ПО, покупка дополнительного количества продукта приносит нулевую пользу, т.е. не следует закону убывания предельной полезности.

Так как приведенная модель экономического выбора потребителя должна соответствовать реальной ситуации на рынке, в ее рамках рассматриваются чисто экономические причины, способные побудить пользователя купить легальную либо нелегальную версию программного продукта, в то же время делается допущение о том, что у пользователя есть более или менее полная информация о легальных продуктах и связанных с ними издержках, а так же информация о существовании рынка нелегального ПО. Впрочем, модель охватывает и случаи отсутствия нелегальных версий определенного ПО. Кроме того, в модели явно не указано множество бесплатных программных продуктов (ППр), но оно неявно включено в множество легального ПО [L(l_1, l_2, ... l_L)], просто при рассмотрении конкретного случая потребительского выбора цена продукта будет нулевой.

Процесс выбора в указанной модели является многоступенчатым: на первом этапе потребителем отбирается множество перспективных ППр, суммарные издержки от которых не превышают суммы, которую потребитель готов потратить на автоматизацию. На втором этапе, рассматривается как таковая функция потребительского равновесия, представляющая собой разницу между ожидаемым доходом от автоматизации и затратами на приобретение ПО. В процессе максимизации этой функции и производится оптимальный выбор потребителя на рынке ПО.

В результате первичного анализа приведенной модели можно прийти к следующим выводам:

- Критерием, определяющим, выберет ли потребитель легальный продукт, является разница в стоимостях легальной и нелегальной версий с учетом ожидания штрафа. То есть критерий выбора легальной копии представлен неравенством: $C^i_L \le C^j_U + P^j_U * IP$. Таким образом, потребитель выберет легальную копию только при условии, что издержки на ее приобретение не превысят издержек на приобретение нелегальной копии с учетом возможного наказания.

- Исходя из вышесказанного, можно сделать вывод, что на "сознательность" потребительского выбора можно повлиять тремя путями: снижением цены на легальную копию ППр, усилением наказания за использование нелегальной копии и повышением вероятности уличения в использовании нелегальной копии. Проанализируем стратегии различных производителей ПО в части борьбы с пиратством.

1. Корпорация Sun Microsystems с недавних пор реализует свою операционную систему Solaris бесплатно (через Интернет) или по стоимости носителя информации, осуществляя ее платное сопровождение и предлагая платное ПО для данной ОС. То же самое касается и продукта StarOffice этой же фирмы. Данный офисный пакет (один из самых сильных конкурентов офисного пакета Microsoft) распространяется бесплатно в виде исходных текстов OpenOffice (при этом пользователь, как правило, должен сам собирать пакет из исходных текстов) или за символическую плату (менее 50 USD) в виде как такового пакета с соответствующим сопровождением.

2. Корпорация Microsoft повышает стоимость своих продуктов и стоимость их сопровождения и т.п., параллельно лоббируя законы, ужесточающие наказание за использование и распространение нелегальных версий ППр. Параллельно этой же корпорацией внедряется институт платных информаторов, сообщающих корпорации о фактах нелегального использования ее продуктов, доносы неплохо оплачиваются. Аналогично поступают и другие корпорации-участники Альянса Делового ПО (Business Software Alliance - BSA): Adobe, Apple и др.

Что касается Российской Федерации и стран СНГ, здесь более перспективен первый подход - удешевление ПО. Причинами тому являются: более низкий, чем западный, уровень оплаты труда, относительная экономическая и политическая независимость от западных стран, отсутствие радикально ориентированных законов в области ИТ и, наконец, возможность официального приобретения (с получением копии чека и т.п.) нелегальных копий ПО в торговой сети. То есть, второй подход - ужесточение наказания - в существующих условиях практически неприменим к частным лицам, приобретающим львиную долю нелегального ПО и слабо применим к юридическим лицам. Для успешного же его применения необходим переход к "полицейскому государству", что, вроде бы, несовместимо с принципами демократии.

Исходя из вышесказанного, можно предположить возможность использования приведённой модели для анализа реального поведения покупателей тех или иных программных продуктов, реализуемых на рынке ПО.

Обратимся теперь к экономическим мотивам действий злоумышленника (пирата).

ЭКОНОМИЧЕСКАЯ МОДЕЛЬ ПОВЕДЕНИЯ ЗЛОУМЫШЛЕННИКА

Введём следующие переменные:

L (l_1, l_2, . . . l_L) - множество легальных продуктов производителей ПО;

C^i_L - цена лицензионной копии *i*-того программного продукта;

CI ({C_P, P_P, PP}$_1$, {C_P, P_P, PP}$_2$, . . . {C_P, P_P, PP}$_{cl}$) [copyright infringements] - множество видов нарушений;

Указанное множество состоит из триплетов, каждый из которых содержит следующие элементы:

C_P (piracy cost) - затраты на *i*-й вид нарушений;

P_P (probability of piracy disclosure) - вероятность уличения в *i*-м виде нарушений;

PP (piracy penalty) - денежное выражение наказания за *i*-й вид нарушений;

В настоящий момент это множество содержит следующие триплеты:

C_I (infringement cost) - затраты на нелегальное использование ПО (цена пиратской копии)

P_I - вероятность уличения в нелегальном использовании ПО

IP (infringement penalty) - сумма убытка при уличении в нелегальном использовании ПО

C_W (warez cost) - затраты на нелегальное распространение ПО (часто включает C^i_L)

P_W - вероятность уличения в нелегальном распространении ПО

WP (warez penalty) - сумма убытка при уличении в нелегальном распространении ПО

C_C (crack cost) - затраты на нелегальную модификацию ПО

P_C - вероятность уличения в нелегальной модификации ПО

CP (crack penalty) - сумма убытка при уличении в нелегальной модификации ПО

C_V (virus cost) - затраты на написание и внедрение ПЗ

P_V - вероятность уличения в написании и внедрении ПЗ

VP (virus penalty) - сумма убытка при уличении в написании и внедрении ПЗ

C_{CC} (credit card cost) - затраты на мошенничество с кредитными картами

P_{CC} - вероятность уличения в мошенничестве с кредитными картами

CCP (credit card penalty) - сумма убытка при уличении в мошенничестве

N - накладные расходы на деятельность злоумышленника (ПК, ПО, чел.-часы и т.п.)

S - сумма, которую злоумышленник согласен потратить на нарушение

I - доход (польза), который злоумышленник рассчитывает получить от нарушения (если польза носит нематериальный характер, используется ее денежное выражение)

ПЗ - программное злоупотребление (вирус, троянский конь, червь, бомба и т.п.)

Модель будет иметь следующий вид:

Критерий отбора программных продуктов "взломщиком":

$$C_C + P_C * CP \le C^i_L \quad (\text{для } C^i_L \ge 50 \text{ USD})$$

Критерий отбора программных продуктов "пиратом":

$$\sum_{i=1}^{CI} (C_P + P_P * PP) + N \le S$$

Обобщенный критерий поведения злоумышленника:

$$B = I - \left(\sum_{i=1}^{CI} (C_P + P_P * PP) + N\right) \rightarrow \max$$

Приведенная модель учитывает деление злоумышленников на "взломщиков", выполняющих дезактивацию систем защиты ПО, и "пиратов", осуществляющих более широкий круг нарушений в области прав на ПО. В то же время, в рамках модели возможно и рассмотрение многоступенчатого выбора злоумышленника, совмещающего обе "профессии".

На первом этапе злоумышленник принимает решение о дезактивации системы защиты ППр, для продуктов стоимостью более 50 USD злоумышленник сравнивает издержки на "взлом" и распространение со стоимостью легальной копии ПО. Если стоимость ПО превышает указанные издержки, принимается решение об атаке на продукт. Что касается ППр стоимостью менее 50 USD, приведенный критерий в этой области действует не всегда и нередки случаи "взлома" такого ПО из других соображений (например, принципиальных).

На втором этапе атака на ПО рассматривается более широко, с учетом различных вариантов нарушения смежных прав. В данном случае затраты на нарушение сравниваются с суммой, которую злоумышленник готов потратить на нарушение. Как видно из приведенного критерия, в нем учтены и такие варианты, как приобретение ПО при помощи похищенной кредитной карты и даже совершенно легальное приобретение ПО с целью его дальнейшего несанкционированного распространения. Здесь необходимо отметить, что в рамках модели при отсутствии какого-либо вида нарушений, вероятность уличения в этом виде нарушений становится равна нулю, как и затраты на этот вид нарушения.

Наконец, на третьем этапе рассматривается функция рыночного равновесия злоумышленника, представляющая собой разницу между ожидаемым доходом от нарушения смежных прав на ППр и затратами на реализацию нарушения с учетом возможного наказания. В процессе максимизации этой функции достигается экономическое равновесие злоумышленника на рынке ПО.

Проанализировав данную модель, можно сказать следующее:

- Принудить злоумышленника отказаться от атаки на ППр можно теми же тремя путями, что и стимулировать потребителя купить легальный продукт. В частности, критерий, аналогичный "условию сознательности потребителя" для "взломщика" имеет вид:

$C_C + P_C * CP \le C^i_L$, т.е. при первичном отборе ПО зло-

умышленник руководствуется соображениями, аналогичными таковым у рядового потребителя. Выводы по этому поводу аналогичны предшествующим, необходимо, правда, учесть гораздо большую независимость и информированность злоумышленника по сравнению с рядовым потребителем.

- Существует целый ряд практикуемых злоумышленниками видов нарушений прав на ПО, что отражено множеством CI. При реализации злоумышленником одного или нескольких видов нарушений суммируются затраты на них с учётом потерь при возможном уличении, вероятности P_P зависят от раскрываемости данных видов нарушений в стране проживания злоумышленника. При этом затраты на все остальные виды нарушений, как и вероятности уличения в них, принимают нулевые значения. Если полученная сумма превысит запланированный злоумышленником уровень затрат, высока вероятность его отказа от атаки на ПО.

Таким образом, учитывая, что большая часть переменных модели известна, данную модель можно применять для построения оценочных суждений о экономической целесообразности преодоления злоумышленником того или иного типа систем программно-технической защиты ПО (СЗПО).

Наконец, попытаемся смоделировать экономическое поведение производителя программных продуктов.

ЭКОНОМИЧЕСКАЯ МОДЕЛЬ ПОВЕДЕНИЯ ПРОИЗВОДИТЕЛЯ ПО

Введём следующие переменные:

C_{SD} (software development cost) - затраты на разработку ПО[1]

$MS(\{C_{AP},E_{AP}\}_1,\{C_{AP}, E_{AP}\}_2,...\{C_{AP}, E_{AP}\}_M)$ [measures set] - множество антипиратских мер, которые может предпринять производитель ПО;

Указанное множество состоит из пар, каждая из которых содержит следующие элементы:

C_{AP} (anti piracy measure cost) - затраты на антипиратскую меру

E_{AP} (anti piracy measure effect) - эффект от антипиратской меры

В настоящий момент это множество содержит следующие пары:

C_{SP} (software protection cost) - затраты на разработку/приобретение/смену СЗПО

E_{SP} (software protection effect) - эффект от разработки/приобретения/смены СЗПО

C_{PD} (piracy disclosure cost) - затраты на повышение раскрываемости "пиратства"

E_{PD} (piracy disclosure effect) - эффект от повышения раскрываемости "пиратства"

C_{LL} (legislation lobbying cost) - затраты на ужесточение законодательства

E_{LL} (legislation lobbying effect) - эффект от ужесточения законодательства

C_{ID} (individual distribution cost) - затраты на индивидуальное распространение ПО

E_{ID} (individual distribution effect) - эффект от индивидуального распространения ПО

C_{PA} (piracy advertising cost) - затраты на "пиратскую" рекламу ППр

E_{PA} (piracy advertising effect) - эффект от "пиратской" рекламы ППр

P_{AP} (anti piracy measures probability) - вероятность решения о борьбе с "пиратами"

L_P (piracy loses) - величина убытков от "пиратства"[2]

I_{PRG} (programmed income) - запланированный объём прибыли

---

[1] - если производитель уже использует СЗПО, её стоимость входит в затраты на разработку ПО

[2] - подразумеваются убытки именно от пиратства, а не списанные на пиратов потери

Модель будет иметь следующий вид:

<u>Вероятность принятия решения о борьбе с пиратством:</u>

$$P_{AP} \approx (L_P / I_{PRG})*2, \text{ при } (L_P / I_{PRG}) \in [0; 0,5]$$

<u>Общий критерий отбора антипиратских мер:</u>

$$C_{AP} \le 1/2C_{SD}\ ;\ L_P \ge C_{AP}$$

<u>Критерий выбора оптимальной стратегии:</u>

$$i => \min_i\{(C_{AP}/E_{AP})_1, (C_{AP}/E_{AP})_2, \dots (C_{AP}/E_{AP})_n\}$$

<u>Обобщённый критерий поведения производителя ПО:</u>

$$B = I_{PRG} - (C_S + [C_{AP} - E_{AP}]_i) \rightarrow \max$$

В рамках приведённой модели производитель ПО может предпринять следующее:

- установить программно-техническую защиту ПО (увеличить затраты на пиратство)
- стимулировать повышение раскрываемости (увеличить риск уличения)
- стимулировать ужесточение законодательства (ужесточить наказание)
- перейти на индивидуальное распространение ПО (увеличить затраты на пиратство)
- не предпринимать антипиратских мер, положившись на свою розничную сеть.

Меры (стратегии) №№ 2,3 и 5 более свойственны крупным производителям ПО и монополистам, в силу высокого уровня издержек на их реализацию.

При принятии стратегии №5 её издержками будут издержки "упущенных возможностей", т.е. $C_{PA} = L_P$.

Производитель анализирует доходы от продаж, если они не соответствуют запланированным, он анализирует причины отклонений. При выявлении влияния "пиратского" рынка на свои доходы производителю необходимо принять решение о своих действиях по отношению к "пиратскому" распространению своего ПО. При этом сделано предположение о наличии пропорциональной зависимости между вероятностью того, что производитель обратит внимание на потери от "пиратства" и приступит к выработке мер противодействия, и удвоенного процента потерь от "пиратства" **($P_{AP} \approx (L_P / I_{PRG})*2$).**

Он может отказаться от каких-либо действий по двум причинам: при незначительном проценте потерь от "пиратства" либо при наличии эффекта бесплатной рекламы "пиратами" его продукта, приносящего стратегическую выгоду при тактических потерях. В противном случае производитель должен выбрать одно из оставшихся и указанных выше четырёх направлений в зависимости от экономической целесообразности каждого. При этом к потерям от "пиратства" добавляются и затраты на борьбу с ним. Возможна ситуация, при которой производителю будет выгоднее не предпринимать мер по борьбе с "пиратами", если эти меры не приносят эффекта, но ведут к дополнительным затратам.

Под экономическим эффектом той или иной антипиратской меры понимается ожидаемый производителем добавочный доход, который должен быть получен при выборе данной стратегии. Как правило, экономический эффект оценивается при помощи анализа действий других производителей ПО, а так же на основе собственного опыта.

Таким образом, при помощи приведённой модели можно проводить оценочные суждения о вероятных действиях производителя программных продуктов в случае появления их нелегальных копий на "пиратском" рынке.

Разумеется, представленные экономические модели поведения участников рынка программного обеспечения являются лишь первой попыткой моделирования в сфере производства и распространения программного обеспечения и нуждаются в дальнейшем развитии и детализации для получения более точных и подробных результатов моделирования. Тем не менее, даже в настоящем виде приведённые модели позволяют строить оценочные суждения относительно поведения экономических агентов на рынке ПО.

Представляется также вполне возможным применение приведённого в работе подхода для исследований в смежных областях, таких как безопасность информационных технологий и, в частности, электронная коммерция.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

[1] Сяо Д., Керр Д., Мэдник С. Защита ЭВМ: Пер с англ. - М., Мир, 1982.

[2] Защита программного обеспечения / Под ред. Д. Гроувера: Пер с англ. - М., Мир, 1992.

[3]Devanbu P.T., Stubblebine S. Software Engineering for Security: a Roadmap // ICSE 2000.

[4] Беккер Г. Преступление и наказание: экономический подход // Экономическая теория преступлений и наказаний. - 1999. №1.

[5] Рубин П. Экономическая теория преступности // Экономическая теория преступлений и наказаний. - 1999. №1.

[6] Эрлих А. Экономическая теория преступлений и наказаний // Экономическая теория преступлений и наказаний. - 1999. №1.

[7] Беккер Г. Экономическая теория преступности // Экономическая теория преступлений и наказаний. - 1999. №1.

[8] Камерон С. Экономическая теория сдерживания преступности: сравнение теории и доказательств // Экономическая теория преступлений и наказаний. - 1999. №1.

[9] Щербаков А. Защита от копирования. - М., ЭДЕЛЬ, 1992.

[10] Середа С.А. Оценка эффективности систем защиты программного обеспечения // КомпьЛог. - 2000. №2.

[11] Середа С.А. Анализ средств преодоления систем защиты программного обеспечения // ИНФОРМОСТ: Радиоэлектроника и Телекоммуникации. - 2002. №4(22).

[12] Середа С.А. Юридическая база Информационных Технологий в Республике Молдова // Сетевой узел движения "ПОтребитель" (http://consumer.nm.ru). - 2001.

[13] Середа С.А. Правовая защита авторства на программные продукты: Acta Academia / Международная академия информатизации - Кишинёв: Evrica, 2001. ISBN 9975-941-60-55

[14] Серго А. Ответственность нарушителей авторских прав в области программного обеспечения // Кодекс-info. - 2001. № 7.

[15] Bjones R., Hoeben S. Vulnerabilities in pure software security systems // Utimaco Software AG, 2000.

* * *