ЭКОНОМИЧЕСКАЯ ТЕОРИЯ

Ю.В. Крылова

ПРОБЛЕМА КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ: ЭКОНОМИКО-ПРАВОВОЙ АСПЕКТ

Постановка проблемы

С середины 1990-х годов в научно-практической литературе все больше внимания уделяется вопросам преступлений в информационной сфере. Тем не менее до сих пор отсутствует общепринятый термин для их обозначения. Наиболее часто специалисты используют термин «компьютерные преступления» (*computer crimes*) и примерно соответствующие ему термины «высокотехнологичные преступления» (*high-tech crimes*) и «киберпреступления» (*cybercrimes*). Взяв за основу подходы, озвученные в докладах Министерства финансов Великобритании (2002) и Федеральной торговой комиссии США (2001),[1] в рамках настоящей статьи под компьютерными преступлениями мы понимаем противоправные деяния, совершенные с использованием информационных технологий (ИТ), в частности, сети Интернет.

Сложность проблем современного мира вызывает необходимость междисциплинарного подхода к их анализу. В данном контексте проблема компьютерных преступлений не является прерогативой правоведов и криминологов. В условиях, когда электронное предпринимательство и торговля получают все большее распространение, преступления в сфере ИТ могут стать серьезной экономической угрозой. Очевидно, использование ИТ обеспечивает сильные преимущества не только корпорациям и финансовым организациям, но и криминальным субъектам, тем самым порождая новые вызовы, которые условно можно подразделить на следующие виды:

- вызовы научно-технического характера — создание и внедрение методов защиты в области компьютерной информации;
- вызовы экономического характера — разработка инструментария оценки финансовых потерь от компьютерных преступлений и методики обоснования инвестиций в сфере информационной безопасности;

Юлия Валентиновна КРЫЛОВА — канд. экон. наук, доцент кафедры экономической теории СПбГУ. Окончила экономический факультет СПбГУ (2000) и аспирантуру (2003). С 2005 г. работает на экономическом факультете СПбГУ. Автор 12 научных работ. Сфера научных интересов — новая институциональная экономическая теория.

♦ вызовы организационного характера — координация действий различных субъектов информационных отношений в борьбе с преступностью;

♦ вызовы правового характера — устранение пробелов в законодательстве, создание системы регулирования информационных правоотношений.

Данная статья посвящена оценке темпов роста компьютерной преступности в сфере экономики и сопряженных финансовых потерь, а также проблемам и перспективам регулирования правоотношений в сети Интернет.

Динамика компьютерных преступлений в сфере экономики

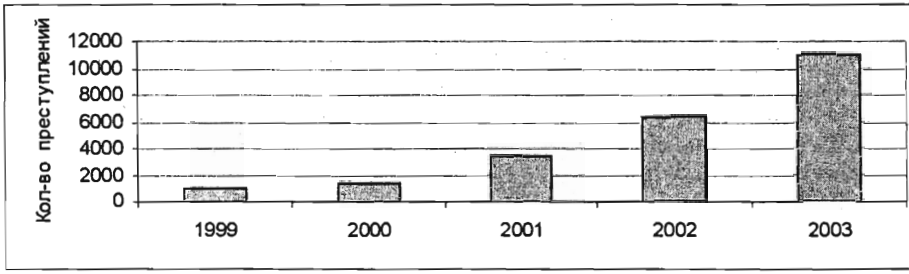
Наиболее полные данные о количестве компьютерных преступлений накоплены в организованном под эгидой ФБР Центре жалоб на мошенничество в Интернете (*Internet Crime Complaint Center, I3C*), в который «стекаются» заявления жертв киберпреступности[2] со всего мира (табл. 1).

Таблица 1

Динамика киберпреступности в экономической сфере в 2001–2004 гг.

Группировка заявлений о мошенничестве в Интернете	Количество заявлений			
	2001 г.	2002 г.	2003 г.	2004 г.
1. Интернет-аукционы	7 180	22 244	38 623	88 650
2. Непоставка оплаченных товаров	3 405	15 103	13 233	19 672
3. Мошенничество с пластиковыми картами	1 577	5 597	4 369	6 723
4. Мошенничество с чеками	117	241	1 076	1 619
5. Мошенничество в сфере бизнеса	235	627	760	н/д
6. Мошенничество с использованием информации о документах, удостоверяющих личность	218	483	760	374
7. Мошенничество в сфере инвестиций	285	724	633	747
8. Мошенничество путем злоупотребления доверием	520	531	570	498
9. Мошенничество в финансовой сфере	н/д	н/д	н/д	125
10. Мошенничество посредством рассылки электронных писем	2 600	193	190	249
11. Другие	638	2 509	3 102	5 852
ИТОГО:	16 775	48 252	63 316	124 509

Рассчитано по: IFCC 2001 Internet Fraud Report. NW3C. 2002. P. 5; IFCC 2002 Internet Fraud Report. NW3C. 2003. P. 6; IC3 2003 Internet Fraud Report. NW3C. 2004. P. 6; IC3 2004 Internet Fraud Report. NW3C. 2005. P. 6.



Источник: Главный информационный центр МВД (www.cyberpool.ru).

Рис. 1. Количество зарегистрированных и расследованных компьютерных преступлений в РФ в 1999–2003 гг.

Как видно из табл. 1, наиболее динамично развивающиеся категории экономической компьютерной преступности — Интернет-аукционы, непоставка оплаченных товаров, мошенничество с чеками. Их среднегодовые темпы роста за 2001–2004 гг. составили соответственно 138, 127 и 168%. Общие темпы роста киберпреступности в 2002 г. по сравнению с предыдущим годом равнялись 188%, в 2003 г. — 31, в 2004 г. — 97%.

Интересно отметить, что в десятку стран, лидирующих по количеству компьютерных преступлений в 2003 г., помимо промышленно развитых вошли те, которые в соответствии с мировыми рейтингами характеризуются низким уровнем развития информационного сектора (Нигерия, Румыния, Южная Африка).[3] Это соотносится с результатами социологических исследований, согласно которым темпы роста компьютерной преступности определяются не столько уровнем развития ИТ той или иной страны, сколько социокультурным типом информатизации и интенсивностью процессов институционализации киберпреступников.[4] Помимо этого, одним из важных факторов, стимулирующих противоправную активность в компьютерном пространстве, является неразвитость национального законодательства, регулирующего информационные отношения.

Так как отличительным свойством компьютерных преступлений выступает трансграничность, то жертвами преступников из слаборазвитых стран, как правило, становятся граждане более благополучных государств. Так, в 2001 г. в ряде развитых стран был зарегистрирован бум электронных писем от мошенников, главным образом из стран Западной Африки (см. строку 10 табл. 1). Подобные письма получили название «нигерийских» (*Nigerian letters*).[5] Их примерное содержание сводится к предложению участия в переводе денег за пределы некоего государства в Африке в обмен на проценты от сделки.

В России статистический учет компьютерных преступлений осуществляется с 1997 г., когда была введена уголовная ответственность в этой сфере. В 1998 г. было создано специализированное подразделение «Р» МВД РФ по борьбе с преступностью в сфере высоких технологий. В настоящее время его функции выполняет управление «К» МВД РФ по борьбе с компьютерными преступлениями. За период 1999–2003 гг. среднегодовые темпы роста компьютерной преступности в России составили 88% (рис.1).

Анализируя статистические данные, следует иметь в виду высокую латентность компьютерной преступности. Значительное количество неучтенных преступлений объясняется, во-первых, тем, что субъекты информационных отношений могут не знать о том, что их ресурсы несанкционированно используются преступниками. Во-вторых, корпорации и финансовые компании, на базы данных которых часто совершаются атаки, не спешат сообщать об этом правоохранительным органам и широкой общественности, в связи с возможной потерей репутации и снижением стоимости акций на фондовом рынке.

Частные и общественные издержки компьютерных преступлений

С учетом высокой латентности компьютерных преступлений возникают существенные трудности в процессе оценки сопряженных финансовых потерь. Это усугубляется отсутствием унифицированной методики расчета ущерба и применением субъективных оценок издержек отдельных видов преступлений, особенно связанных с незаконным использованием конфиденциальной информации. Некоторые оценки материального ущерба приведены в табл. 2.

Прямой ущерб, нанесенный обществу в результате совершения таких преступлений, как электронный вандализм, можно рассматривать как чистые общественные потери (*dead-weight loss*). Кражи и мошенничество в Интернете не ведут напрямую к сокращению благосостояния граждан, а только к его перераспределению. Другими словами, потери жертвы компенсируются приростом дохода преступника. Однако из этого не следует, что общественные издержки подобного рода правонарушений равны нулю, что еще в 1960-е годы отмечали Г. Таллок и Г. Беккер в отношении традиционных преступлений против имущества.[6]

Таблица 2

Финансовые потери от компьютерных преступлений

Источник	Основные виды компьютерных преступлений	Год	Потери, млн долл.
Federal Trade Commission; FTC (USA) Анализ 205 568 заявлений потребителей	Мошенничество в сфере электронной торговли	2004	265,38
Computer Security Institute, CSI (USA) Опрос 269 организаций	Все виды экономических компьютерных преступлений	2004	141,50
Association for Payment Clearing Services, APACS (UK) Обзор данных финансовых институтов	Мошенничество с платежными картами в сети Интернет	2004	61,60
Internet Crime Coplaint Center, 13 C Анализ 63 316 инцидентов	Мошенничество в сети Интернет	2003	125,60
National Hi-Tech Crime Unit, NHTCU (UK) Опрос 167 организаций	Все виды экономических компьютерных преступлений	2003	102,71

Составлено по: Card Fraud: The Facts. APACS. 2005. P. 20; *Gordon L., Loeb M., Lucyshyn W., Richardson R.* 2004 CSI/FBI Computer Crime and Security Survey. CSI. 2005. P. 10 ; High-Tech Crime: The Impact on UK Business. NOP World. NHTCU. 2004. P. 17; IC3 2003 Internet Fraud Report. NW3C. 2004. P. 3; www.ftc.gov/sentinel.

Во-первых, совершение преступлений подразумевает отвлечение ресурсов из производственной в перераспределительную сферу, в качестве которой в данном случае выступает криминальная. Во-вторых, рост преступности способствует увеличению расходов на защиту прав собственности, которые составляют косвенные издержки противоправной деятельности. В отношении компьютерных преступлений к ним относятся: расходы на системы обнаружения сетевого вторжения, антивирусное программное обеспечение, резервирование компьютерных систем, биометрические опознавательные устройства, технический аудит, содержание служб информационной безопасности (ИБ), содержание и обучение сотрудников специализированных подразделений правоохранительных органов и т. д. Это означает отвлечение ресурсов из традиционных сфер инвестирования. Иначе говоря, рост трансакционных издержек защиты прав собственности ведет к дополнительным общественным потерям.

С учетом необходимости оценки косвенных издержек преступлений, в 2004 г. эксперты Института компьютерной безопасности США (*Computer Security Institute, CSI*) провели специальное обследование, в ходе которого было опрошено 494 организаций частного и общественного секторов. Обследование показало, что на долю затрат на ИБ приходится значительная доля бюджета информационно-технологических подразделений. В частности, организации с ежегодным уровнем продаж ниже 10 млн долл. расходуют на компьютерную безопасность в среднем 500 долл. в расчете на одного сотрудника (операционные расходы — 334 долл., капитальные вложения — 163 долл.). Фирмы с ежегодными объемами продаж свыше 1 млрд долл. тратят в этих целях в среднем около 110 долл. в расчете на одного сотрудника (операционные расходы — 82 долл., капитальные вложения — 30 долл.).[7]

Несмотря на рост затрат на ИБ, до настоящего времени не до конца проработаны вопросы экономического обоснования инвестиционных решений в данной сфере. Анализ зарубежной литературы показывает, что только в последние два года начались разработки в области теории инвестирования применительно к ИБ.[8] Необходимость этого направления объясняется операционными трудностями, с которыми сталкиваются специалисты, работающие в информационной сфере. Основные проблемы связаны с измерением рисков и потерь от компьютерных преступлений, методикой расчета эффективности инвестиций в системы безопасности и обоснования бюджетов соответствующих подразделений организации.

В опросе Института компьютерной безопасности организациям предложили указать, какой показатель они используют в процессе обоснования расходов на ИБ. В ходе обследования выяснилось, что только 54% респондентов применяют процедуру оценки эффективности соответствующих инвестиционных расходов. При этом 55% респондентов отдают предпочтение показателю рентабельности инвестиций (*ROI*). Между тем любое инвестиционное решение должно приниматься с учетом фактора времени, поэтому более предпочтительным является использование показателей чистой текущей стоимости (*NPV*) и внутренней нормы доходности (*IRR*), их используют только 25 и 28% опрошенных соответственно.[9]

В России комплексное исследование проблем ИБ проводилось в 2004 г. компанией *InfoWatch* путем опроса представителей 387 государственных и

коммерческих структур. Обследование показало, что в большинстве российских организаций отсутствует система учета издержек и рисков компьютерных преступлений. Так, 67% опрошенных организаций не могут точно определить масштабы компьютерных угроз. При этом 99% респондентов, в организациях которых были зафиксированы противоправные деяния в области компьютерной информации, затруднились оценить нанесенный ущерб в финансовых показателях.[10]

Одним из важных аспектов проблемы компьютерных преступлений является управление рисками. Обследование 200 государственных и коммерческих организаций в Великобритании, организованное Национальным департаментом по борьбе с высокотехнологичными преступлениями в 2004 г., показало, что больше трети респондентов не имеют формальной процедуры оценки соответствующих рисков.[11] Организации, которые внедрили у себя подобную процедуру, представлены в основном финансовыми институтами и телекоммуникационными компаниями. При этом первые отдают предпочтение специализированной процедуре оценки рисков в области ИБ, а вторые интегрируют ее в общую систему управления организационными рисками.

В настоящее время все большее распространение получают различные схемы страхования от высокотехнологичных преступлений. Так, в США их применяют 28% организаций.[12] В России еще в 1997 г. компания «Ингосстрах» предложила услугу по комплексному страхованию от компьютерных преступлений, которая предусматривает возмещение финансовых потерь от вредоносных программ, а также мошенничества и несанкционированных действий третьих лиц, совершенных с помощью ИТ.[13] Однако этой услугой воспользовались немногочисленные организации, главным образом финансового сектора. Сдерживающим фактором является сложность оценки рисков и убытков при наступлении страхового случая.

Процедура оценки специфических рисков также важна при расчете эффективности инвестиций в ИБ, связанных с применением радикально новых технологий. В настоящее время наблюдается возрастающий интерес к сфере биометрических технологий, причем не только в США, но и в Европе. Так, в 2003 г. Европейская Комиссия инициировала в рамках программы «Технологии информационного общества» проект комплексного исследования проблем и перспектив внедрения биометрических технологий в европейских государствах.[14] В частности, данный проект предполагает широкомасштабное использование биометрических систем в финансовом секторе для усиления безопасности электронных расчетов. По нашему мнению, одним из недостатков проекта является чрезмерное увлечение качественными методами обоснования инвестиций и оценки рисков новых технологий в ущерб количественным. В этой связи представляется необходимой разработка модели обоснования отдельных инвестиционных проектов в сфере ИБ.

Если рассматривать проблему ИБ в целом, то частные издержки защиты от преступлений могут не иметь социальной значимости. Безусловно, установка системы безопасности в отдельно взятой организации имеет частную выгоду для инвестора, который стремится обеспечить сохранность своего имущества. Это получило название эффекта частного сдерживания (*private deterrence effect*). Однако здесь возникает отрицательная экстерналия, связанная с эффектом пе-

перераспределения преступления (*redistributing crime effect*),[15] который заключается в том, что, столкнувшись с препятствием, преступник выберет в качестве жертвы организацию, которая хуже защищена.[16]

Исходя из этого, более предпочтительным является стимулирование (прежде всего на государственном уровне) тех инвестиций, которые направлены не на перераспределение ущерба, а на снижение темпов роста преступности. В данном контексте необходимо рассмотреть проблемы и перспективы регулирования общественных отношений, связанных с использованием ИТ.

Регулирование информационных отношений в сети Интернет

К основным формам регулирования сети Интернет относятся: государственное регулирование, саморегулирование и сорегулирование.

Государственное регулирование сети Интернет. Основная проблема в данной сфере связана с неопределенностью правового статуса сети. Интернет не является единой организацией, не обладает признаком юридического лица, никому не принадлежит, хотя все, что используется в сети (каналы связи, компьютерное оборудование, информация), имеет своих владельцев. Нечеткая спецификация прав собственности в Интернете ведет к конфликтам в процессе эксплуатации сети пользователями, собственниками ресурсов и провайдерами.

Среди юристов нет единого мнения в отношении правовых основ Интернета. В соответствии с одним подходом сеть Интернет, как совершенно новое явление, находится вне юрисдикции какого-либо государства и правовых норм. Следовательно, необходимо разработать принципиально новые нормативные акты. Согласно другому подходу Интернет не создает новых проблем, соответственно, к нему с определенными корректировками может применяться действующее законодательство.

В странах, где процессы информатизации характеризуются высокой интенсивностью, законодатели, как правило, руководствуются первым подходом. При этом особое значение придается международному сотрудничеству. Это обусловлено тем, что Интернет представляет собой открытое транснациональное пространство, в рамках которого взаимодействуют миллионы пользователей. Помимо этого, в сети не предусмотрено внутренней полиции, ориентированной на защиту жертв преступлений. Отсутствие системы инфорсмента (*enforcement*) внутри сети, а также пробелы в законодательстве только стимулируют распространение общественно опасной деятельности.

В сфере экономики приоритетного внимания заслуживают вопросы электронной коммерции, налогообложения электронных сделок, проведения электронных расчетов, защиты прав потребителей и объектов интеллектуальной собственности в сети Интернет. В настоящее время существенным достижением в сфере государственного регулирования является принятие специальных норм в области несанкционированной сетевой рекламы. Так, в Австрии, Италии, Норвегии, США, Финляндии были приняты законы, направленные на ограничение или запрещение не запрашиваемой массовой рассылки информации коммерческого и некоммерческого содержания (спама).[17]

Активно развивается область государственного регулирования электронной коммерции. В большинстве стран приняты специальные законы об электронной торговле. К важнейшим международным документам в данной сфере отно-

сятся: директива Европейского парламента и Совета «Об электронной торговле» (2000),[18] «Руководство по защите потребителей в контексте электронной коммерции» ОЭСР (2000),[19] типовой закон «Об электронной торговле» (1998) и проект «Конвенции об электронной торговле» (2005) ЮНСИТРАЛ.[20]

Российское законодательство в сфере Интернет-регулирования находится в зачаточном состоянии. Отсутствуют юридические определения базовых понятий — Интернет, вэб-сайт, доменное имя, электронная торговля, электронная коммерция, электронная сделка, электронный документ и др. Соответственно, нет и специального законодательства, регулирующего такие важные области, как электронная торговля и реклама, новые объекты промышленной собственности. Все конфликты, возникающие в Интернете, решаются в рамках действующего законодательства. Например, споры вокруг регистрации доменного имени рассматриваются на основании законодательства о товарных знаках.[21] Действующих законов и норм в гражданском и уголовном законодательстве, регулирующих информационные отношения, явно недостаточно.

Однако следует отметить, что в данном направлении наблюдается определенная активизация российских законодателей. Так, начиная с 2000 г. было разработано несколько законопроектов: «О государственной политике РФ по развитию и использованию сети Интернет», «О предоставлении электронных финансовых услуг», «О сделках, совершаемых при помощи электронных средств». Особенно следует выделить проект Закона «Об электронной торговле», работа над которым ведется уже пять лет. Основной целью этого Закона является создание благоприятных правовых условий и обеспечение защиты прав участников электронной торговли. Предполагается, что принятие данного Закона станет базой для современной системы регулирования экономических отношений в Интернете.

Саморегулирование. Регулирование сети Интернет может осуществляться и без вмешательства государственных органов, самими субъектами информационных отношений. Тогда мы можем говорить о *саморегулировании* (*self-regulation*), которое в широком смысле означает формирование и исполнение правил и норм поведения без внешнего принуждения. В таком случае непосредственно заинтересованные в выполнении данных норм и правил агенты самостоятельно определяют санкции за их нарушение, а также механизмы разрешения индивидуальных и организационных конфликтов. Для решения этой задачи создаются специальные *организации саморегулирования,* которым делегируются определенные полномочия контроля деятельности субъектов, входящих в сферу их юрисдикции.[22]

В США наиболее активное участие в процессах саморегулирования принимают организации по защите прав потребителей в сети Интернет. Так, американская организация саморегулирования *Better Business Bureau* разработала кодекс практики онлайн-бизнеса (*Code of Online Business Practices*), в рамках которого сформулированы основные требования к защите частной информации.

В России система саморегулирования менее развита. Выделим несколько организаций и сообществ, деятельность которых оказывает существенное воздействие на формирование социальных норм регулирования сети Интернет: Открытый Форум Интернет-Сервис-Провайдеров (ОФИСП), Региональный об-

щественный центр Интернет-технологий (РОЦИТ), Российское общество по мультимедиа и цифровым сетям (РОМС), Национальная ассоциация участников электронной торговли (НАУЭТ).

К основным российским инициативам саморегулирования относятся «Нормы пользования сетью» и «Рекомендации по организации деятельности лиц в сфере Интернет-коммерции в Российской Федерации». «Нормы пользования сетью», разработанные ОФИСП в 1999 г., предусматривают запрет спама, несанкционированного доступа и сетевых атак, недопустимость фальсификации, идентифицирующих пользователя сведений. «Рекомендации по организации деятельности лиц в сфере Интернет-коммерции в Российской Федерации» являются первым проектом Закона «Об электронной торговле», который был представлен на слушаниях в Государственной Думе в 2000 г.[23] В дальнейших разработках данного Закона активное участие принимает НАУЭТ.

Сорегулирование. В первом приближении сорегулирование (*co-regulation*) можно определить как регулирование общественных отношений с помощью правовых и социальных норм. Структура сорегулирования предполагает включение, помимо формальных институтов, общественного и частного регулирования. Сорегулирование является наиболее предпочтительным с той точки зрения, что принятие новых законов или инициатив саморегулирования в одностороннем порядке — не самый эффективный путь решения сетевых проблем. Исходя из этого, можно говорить о неизбежности создания многоуровневой системы регулирования компьютерного пространства.

Многоуровневый подход предполагает выделение основных групп агентов, которые *совместно* занимаются разработкой формальных и неформальных правил социальной практики. В отношении сети Интернет традиционно выделяют пять регулирующих групп: Интернет-пользователи, Интернет-провайдеры, отделы безопасности корпораций, государственные структуры и общественные организации.[24] Однако с учетом множества стейкхолдеров, которые воздействуют и испытывают на себе воздействие от деятельности в Интернет-пространстве, эту систему можно расширить, включив дополнительные элементы (рис. 2).

На рис. 2 выделено три уровня системы Интернет-регулирования. Базисный уровень представлен основными субъектами информационных отношений: провайдерами, собственниками информационных ресурсов, пользователями. Второй уровень — это бизнес-среда, к которой относятся как отдельные корпорации и финансовые институты, так и организации саморегулирования (бизнес-ассоциации, ассоциации участников электронной торговли). И наконец, третий уровень включает в себя общественные организации, СМИ, государственные и наднациональные структуры.

Заметим, что каждый уровень в системе сорегулирования не является автономным. Ключевой чертой многоуровневого подхода является взаимосвязанность всех элементов системы. Таким образом, основное преимущество совместного регулирования заключается в том, что если отдельные субъекты и бизнес-ассоциации мотивируются прежде всего получением частных и коллективных благ, то система сорегулирования ориентирована на производство общественных благ на основе обеспечения баланса интересов различных стейкхолдеров.

Подводя итог, отметим, что с учетом высоких темпов роста компьютерной преступности, а также сопряженных с ней прямых и косвенных издержек оче-

Рис.2. Схема многоуровневой системы Интернет-регулирования.

видна необходимость разработки превентивных и проактивных мер пресечения злоупотреблений в киберпространстве. В связи с этим приоритетными задачами являются дальнейшие разработки инструментария оценки рисков и финансовых потерь от компьютерных преступлений, методики обоснования инвестиций в области ИБ, а также создание многоуровневой системы регулирования информационных отношений.

---

[1] Statement of the Federal Trade Commission on «Internet Fraud» // *Schweitzer D.* Internet Security Made Easy. A Plain-English Guide to Protecting Yourself and Your Company Online. New York, 2002. P. 221–244; 2001–2002 Fraud Report. An analysis of reported fraud in Government Departments. HM Treasure, 2002. P. 6.

[2] В Конвенции о киберпреступности (*Convention on Cybercrime*), подписанной в 2001 г. 42 государствами, включая Россию, США, Японию и страны–члены ЕС, определение киберпреступлений аналогично рассматриваемому выше определению компьютерных преступлений. Исходя из этого, далее термины «киберпреступления» и «компьютерные преступления» используются как синонимы.

[3] См., напр., исследования Гарвардского центра международного развития (индекс сетевой готовности) и Всемирного экономического форума (индекс ИТ): *Kirkman G., Osorio C.* The Networked Readiness Index. Center for International Development at Harvard University, 2002. P. 11; www.weforum.com.

[4] Подробнее см.: *Скородумова О.Б.* Хакеры как феномен информационного пространства // СОЦИС. 2004. N 2. С. 70–79.

[5] IC3 2004 Internet Fraud Report. NW3C, 2005. P. 6.

[6] *Tullock G.* The Welfare Costs of Tariffs, Monopolies, and Theft // Western Economic Journal. 1967. N 5. P. 224–232; *Becker G.* Crime and Punishment: An Economic Approach // Journal of Political Economy. 1968. Vol. 76. N 2. P. 169–217.

[7] *Gordon L., Loeb M., Lucyshyn W., Richardson R.* 2004 CSI/FBI Computer Crime and Security Survey. CSI, 2005. P. 5.

[8] См., напр.: *Gordon L., Richardson R.* The New Economics of Information Security // Information Week. 2004. March 29. P. 53–56; *Gordon L., Loeb M.* Return on Information Security Investments: Myths vs. Reality // Strategic Finance. 2002. November. P. 26–31.

[9] *Gordon L., Loeb M., Lucyshyn W., Richardson R.* Op. cit. P. 7.

[10] Внутренние ИТ-угрозы в России 2004 (www.InfoWatch.ru).

[11] High-Tech Crime: The Impact on UK Business. NOP World, NHTCU, 2005. P. 29.

[12] *Gordon L., Loeb M., Lucyshyn W., Richardson R.* Op. cit. P. 8.

[13] Страхование от электронных и компьютерных преступлений (www.ingos.ru).

[14] *Rejman-Greene M.* BIOVISION Roadmap for Biometrics in Europe to 2010. Issue 1.1, 2003. Project IST-2001-38236.

[15] *Cooter R., Ulen T.* Law and Economics, 3rd ed. Massachusetts, 2000. P. 452–453.

[16] Очевидно, в отношении специфических компьютерных преступлений это не всегда верно. Например, в случае «цепных бомб» (*chain-bombs*) вредоносная программа посылается сначала на один компьютер, а затем автоматически передается другому и т.д. по цепочке. В подобной ситуации установка системы безопасности на одном компьютере предотвращает распространение вируса, тем самым порождая положительный внешний эффект.

[17] Подробнее о национальном законодательстве регулирования спама см.: *Наумов В.* Право и Интернет: очерки теории и практики. М., 2002. С. 96–112.

[18] Directive 2000/31/EC of the European Parliament and the Council of 08.06.2000 «On certain legal aspects of information society services, in particular electronic commerce, in Internal Market» (Directive on electronic commerce) // Official Journal of the European Communities. L 178/1-L 178/16. 17.07.2000.

[19] Guidelines for Consumer Protection in the Context of Electronic Commerce. OECD. Paris, 2000.

[20] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment with additional article 5 bis as adopted in 1998; Draft of E-commerce Convention (http://www.uncitral.org/en-index.htm).

[21] Доменные имена в Интернете представляют собой новый объект промышленной собственности, не пересекающийся с товарными знаками и фирменными наименованиями. В данном случае противоправные действия заключаются в регистрации доменных имен, состоящих из названий известных компаний, с целью их последующей перепродажи владельцам сходного средства индивидуализации или с целью привлечения клиентов. Данный вид преступлений в англоязычной литературе получил название «киберсквоттинг»/«тайпсквоттинг» (*cybersquatting/typo-squatting*).

[22] *Крючкова П.* Саморегулирование бизнеса как способ управления контрактными отношениями // Вопросы экономики. 2001. N 6. С. 132.

[23] Российские инициативы в сфере саморегулирования // *Наумов В.* Указ. соч. С. 280–290.

[24] *Wall D.* Maintaining Order and Law on the Internet // Crime and the Internet / Ed. by D.S. Wall. London, 2001. P. 171.

Статья поступила в редакцию 19 октября 2005 г.