Глава 3. Правовые аспекты распространения сетевых технологий

Вопросы, рассматриваемые в главе:

3.1. Проблемы защиты права собственности в пространстве Сети.
3.2. Правовое регулирование виртуальной экономики.

3.1. Проблемы защиты права собственности в пространстве Сети

Анализ правовых аспектов, возникающих в связи с распространением сетевых технологий, мы начнем с постановки вопроса о защите права собственности в Сети, поскольку для экономиста правовая защита собственности представляет особый интерес и важность.

Права собственности в экономической теории понимаются как некие поведенческие отношения между людьми, возникающие в связи с присвоением благ, иначе говоря, это «правила игры», которые приняты в обществе. Известный «перечень Оноре» дает нам целостный набор правомочий, определяет понимание прав собственности в полном их объеме и включает 11 элементов:[1]

1) право владения (физический контроль);
2) право использования (применение полезных свойств блага);
3) право управления (право принимать решения о том, кто использует благо);
4) право на доход;
5) право суверена (право на отчуждение, изменение, уничтожение блага);
6) право на безопасность (право на защиту от внешнего вреда);
7) право на передачу благ в наследство;
8) право на бессрочность обладания благом;
9) запрет вредного использования (запрет использования способом, наносящим вред другим);

[1] А.Оноре – английский юрист, предложивший свой «пучок прав» в 1961 г.

10) право на ответственность в виде взыскания (возможность взыскания блага в уплату долга);

11) право на остаточный характер (существование институтов, обеспечивающих восстановление правомочий).

Очень важно среди прочих видов прав собственности четко выделить право интеллектуальной собственности и возможные способы его защиты. Это новый аспект деятельности государства в условиях информационного общества.

Развитие информационных технологий, появление Интернета создало определенные проблемы в этом смысле. Право собственности на информацию – предмет широких дискуссий специалистов, занимающихся вопросами информационного законодательства. Может ли информация быть объектом вещного права, в какой степени эта идея должна быть зафиксирована в вещественном виде, чтобы на нее распространялось авторское право, какова должна быть форма фиксации (для защиты в суде зафиксированными признаются интерактивные работы, появление информации в памяти компьютера во время получения электронной почты), - эти и другие вопросы требуют детальной проработки как на национальном, так и на международном уровне.

Международной основой законодательства об интеллектуальной собственности и авторском праве являются:

- Всеобщая конвенция по авторским правам;
- Многосторонняя конвенция по избежанию двойного налогообложения и выплат авторского вознаграждения;
- директивы Совета Европы: о правовой защите компьютерных программ, о правах ренты и лизинга и некоторых правах, относящихся к авторскому праву в области интеллектуальной собственности, о правовой защите баз данных и т.п.
- В рамках Всемирной организации по охране интеллектуальной собственности принят Договор об авторском праве.

Но основная часть этих и других документов была создана в «доинформационную» эпоху, поэтому сейчас возникает вопрос об их пересмотре или модификации с учетом произошедших изменений.

Идеи перемещаются в Интернете свободно, мир Интернета против закрытости: дело не в том, сколько патентов имеет тот или иной субъект, а в том, кто быстрее сумеет применить решения и инновации в действии. Логично возникает вопрос: есть ли вообще смысл бороться за защиту права интеллектуальной собственности так, как это делалось раньше?

Чтобы подойти к ответу на этот вопрос, рассмотрим модель поведения экономических субъектов при приобретении информационного продукта, например, программного обеспечения.

Прежде всего сделаем несколько замечаний.

1. Как известно, для потребителей в отношении информационного продукта возникают сетевые внешние эффекты, которые мы рассматривали в главе 1;
2. Если программное обеспечение защищено производителем, то часть потребителей будет склонно приобретать его легально, а часть потребителей будет стараться получить его нелегальным образом;
3. Потребители, которые легально приобрели программное обеспечение, тем не менее заинтересованы в его нелегальном распространении, что вытекает из пункта 1;
4. Производители также заинтересованы в распространении своего продукта, так как увеличение числа пользователей, что само по себе – благоприятное явление для производителя, к тому же в силу действия сетевых внешних эффектов увеличивает полезность продукта, который производитель реализует на рынке.

Таким образом, у производителя есть основания для уменьшения степени защиты продукта. Продемонстрируем это с помощью примера. Для простоты рассмотрим сначала случай производителя – монополиста. Цифры для нашего примера используем условные.

Итак, предположим, что у производителя X, являющегося монополистом, есть всего 4 потребителя, которым он реализует свою продукцию, причем двое из них – это законопослушные потребители, легально приобретающие продукт, а двое готовы приобретать продукт исключительно нелегальным образом, а в случае отсутствия такой возможности просто воздерживаются от потребления продукта. Распространение сетевых внешних эффектов показано в таблице 3.1.

Таблица 3.1.

Оценка отдельным потребителем полезности продукта по мере увеличения количества потребителей

Количество потребителей	**1**	**2**	**3**	**4**
Готовность платить, условные единицы	**100**	**150**	**200**	**250**

Обозначим через $N_Л$ пользователей, которые будут легально приобретать продукт, а через $N_Н$ пользователей, которые будут пользоваться продуктом только нелегально, то есть копируя его. N – общее количество пользователей, $N = N_Л + N_Н$.

Тогда, если монополия защищает продукт, то:

$N_Л = 2$

$N_Н = 0$

$N = 2$

А поскольку максимальная цена при двух покупателях составляет 150, общая выручка монополии: TR = P x Q = 150 x 2 = 300.

Если монополия не защищает продукт, то:

$N_Л = 2$

$N_Н = 2$

$N = 4$

А поскольку максимальная цена при четырех участниках составляет 250, общая выручка монополии: TR = P x Q = 250 x 2 = 500.

Итак, мы видим, что в данном случае монополии гораздо выгоднее отказаться от защиты своего продукта.

Предположим, что теперь у нас не один, а два производителя одного продукта: X и Y, причем один законопослушный потребитель покупает только продукт X, а второй – только продукт Y. Сетевые внешние эффекты распространяются в случае двоих производителей так, как это показано в таблице 20.

Если оба производителя защищают свой продукт, то каждая каждый из них продает по одной единице своему потребителю и получает валовой доход: TR = P x Q = 100 x 1 = 100.

Если производитель A защищает свой продукт, а производитель B не защищает свой продукт, то A продает одну единицу своему потребителю и по-прежнему получает доход : TR_B = P x Q = 100 x 1 = 100. Производитель B продает одному потребителю единицу своего продукта, но уже по цене 200, так как его продукт потребляют уже три потребителя (один легальный и два нелегальных), и его доход равен: TR = P x Q = 200 x 1 = 200.

Итак, в случае, когда все фирмы защищают свой продукт, одна фирма отказывается от защиты, именно эта фирма может увеличить прибыль за счет действия сетевых внешних эффектов.

Можно посмотреть на вопрос защиты и несколько иначе. Как известно, свойства сетевых благ неразрывно связаны друг с другом, и, анализируя сетевое благо, для полного понимания его особенностей необходимо рассматривать свойства этого блага в комплексе. Так, например, в условиях наличия сетевых внешних эффектов производители сетевых благ могут получать больше прибыли, если производимые ими блага являются совместимыми, что позволяет им более полно использовать сетевые внешние эффекты, а совместимость, в свою очередь, предполагает меньшую степень защищенности в том смысле, что она требует устранения технических барьеров использования блага в сети.

Исходя из вышеизложенного, мы приходим к следующему выводу. Степень необходимой защиты своего продукта фирма может определить, зная следующие четыре показателя:

1. Скорость распространения сетевых внешних эффектов;
2. Степень монополизации отрасли;
3. Первоначальную оценку блага законопослушным потребителем;
4. Соотношение между законопослушными и прочими потребителями, то есть потенциальную готовность платить за благо.

В России явно просматривается тенденция к снижению степени защиты информационного продукта. Что касается первого пункта, то для ответа на этот вопрос можно использовать вычисления на основе закона Меткалфе (см. главу 1, параграф 1.2), и совершенно очевидно, что высокая скорость распространения сетевых внешних эффектов действует против усиления защиты. Ответить на второй вопрос достаточно сложно, но легкая воспроизводимость продукта посредством копирования снижает входные барьеры в отрасль и соответственно понижает тенденцию к защите продукта. Что касается третьего пункта, то в России этот показатель скорее всего будет невысоким из-за низкого платежеспособного спроса в целом. И, наконец, совершенно очевидно, что процент незаконопослушных потребителей высок в общем количестве потребителей. Все это приводит нас к выводу о том, что, скорее всего, в России достаточно сильны доводы против защиты информационного продукта.

Аналогичные доводы против защиты действуют и в других странах. И хотя в странах с более отработанным законодательством в области интеллектуальной собственности эти доводы в какой-то степени скомпенсированы юридическими традициями, тем не менее не учитывать мы их не можем. Уже в начале 1980-х гг., несмотря на стремительное развитие компьютерной индустрии, американские фирмы – производители программного обеспечения начали постепенно снижать степень защиты от копирования своих продуктов. Исследования продаж в информационном

секторе свидетельствуют о том, что в Великобритании за период с 1987 г. по 1992 г. на каждого легального покупателя приходилось шесть нелегальных пользователей, но в то же самое время рост продаж легальным потребителям рос по мере увеличения числа нелегальных пользователей.[2] Таким образом, нелегальные пользователи могут оказывать существенное влияние на решение потенциальных легальных пользователей приобрести информационный продукт, а потому целесообразность эффективной защиты такого продукта ставится под сомнение.

При современной низкой стоимости копирования и развитии коммуникаций нельзя действовать старыми методами; невозможно, используя патентное право, остановить развитие технологий. Никто не станет жертвовать свободой информационного пространства ради защиты прав собственности на какие-либо виды информации. Содержание *per se* становится почти бесплатным для потребителей. Очевидно, самое простое, что можно сделать с таким легко копируемым содержанием, - это продать его, но не как копию, а как капитал, то есть со всем набором правомочий на капитал: правами показывать, изменять его и извлекать из него прибыль. Именно на продажу содержания как капитала, а соответственно, на выработку методов продажи такого интеллектуального ресурса, обращают внимание многие зарубежные исследователи, занимающиеся проблемами защиты права интеллектуальной собственности.[3]

Тем не менее, нельзя полностью игнорировать вопрос о защите прав интеллектуальной собственности и прав собственности вообще в связи с возникновением Интернета. Отсюда возникает целый комплекс проблем.

Первая проблема связана с защитой от явления, получившего название *киберсквоттинга*, к рассмотрению которого мы переходим.

---

[2] Shy O. The Economics of Network Industries / O. Shy. – Campridge, UK; New York, USA: Cambridge University Press, 2001. – P.75.

[3] См., например: Dyson, E. A Design for Living in the Digital Age / E. Dyson. - New York: Broadway Books, 1998. - 370 p.

Сеть породила новый нематериальный актив - *доменное имя*, то есть обозначение, состоящее из нескольких частей, которое дает возможность пользователям Интернетом применять в качестве адреса имя, имеющее смысловое значение и созданное по правилам определенной иерархии. Доменное имя имеет много общего с товарными знаками и фирменными наименованиями, но, в отличие от них, доменное имя не привязывает заявителя к роду товара или услуги, и в принципе можно превратить в брэнд любое сочетание знаков. С другой стороны, такая доступность и открытость доменов превратила их в предмет недобросовестной конкуренции.

Регистрацией и продажей доменов занимаются две категории посредников: *торговцы доменными именами (domain name traders)* - те, кто старается зарегистрировать общеупотребимые слова, термины, сочетания слов и терминов, и *киберсквоттеры (cybersquotters*) – те, кто регистрирует имена, напоминающие или даже полностью копирующие известные торговые марки, товарные знаки и т.п., ведь для привлечения аудитории на свои сайты большое значение имеет наличие определенного брэнда. Деятельность последних и получила название киберсквоттинга.

Проблем, связанных с киберсквоттингом, не могут избежать даже известные во всем мире компании. Так, например, международная платежная ассоциация American Express зарегистрировала свое доменное имя в 19 странах, но в то же самое время в 11 странах оно принадлежит другим владельцам. Спекуляция доменными именами становится весьма прибыльным делом. В США регистрация доменного имени стоит в среднем 50 долларов, а чтобы выкупить его у киберсквоттера, требуется уже от 10 000 долл. до 3 млн.долл.[4]

Обезопасить доменное имя очень сложно. Возникающие судебные процессы в связи с захватом доменных имен демонстрируют неготовность к подобному разбирательству как самих сторон, так и судебной системы. В России прошли судебные процессы в связи с захватом доменных имен:

[4] Афонина С.В. Электронные деньги / С.В. Афонина. – СПб: Питер, 2001. - С.14.

известные дела «Мосфильма», «Quelle», «Кодака».[5] В первых двух случаях недобросовестность захватчиков доменных имен была быстро доказана, а в последнем случае пришлось обращаться в Высший арбитражный суд. Хотя ход всех трех разбирательств свидетельствует о неурегулированности судебных процессов в этой области, сам факт судебных разбирательств свидетельствует о положительных тенденциях.

Есть и другие способы урегулирования процессов, связанных с использованием доменных имен. На мировом уровне единая политика по разрешению споров в отношении доменных имен была принята в августе 1999 г. международной организацией ICANN. Эта политика называется UDRP (United Dispute Resolution Policy) – Единая политика по урегулированию споров в области названий доменов. Нормы UDRP включаются в текст договора при осуществлении регистрации домена и становятся обязательными для владельцев доменов.

Не менее важную проблему составляет на сегодняшний день *торговля базами данных*, причем в данном случае речь идет как об информации коммерческого характера, так и об информации личного свойства. Во многих странах, несмотря на различный подход к этому вопросу, часть информации закрыта для публичного распространения, тем не менее чрезвычайно часто закрытая информация продается теми лицами, которые имеют к ней доступ.

Необходим разумный и приемлемый баланс между более широким участием индивидов в информационном пространстве и соблюдением личных свобод и прав граждан, присутствующих в Сети. По мере того, как к Сети подсоединяется все большее количество компьютеров, все больше информации личного характера попадает в общее информационное пространство. Цифровые данные практически не могут регулироваться, так как они не подпадают под какие-либо нормы, применяемые к обычным благам. Традиционно регулирующие нормы применяются к почтовым службам, к печати, телевидению и радиовещанию, но сигналы в цифровой среде не могут быть

[5] Подробнее см. Наумов В.Б. Право и Интернет: Очерки теории и практики / В.Б. Наумов. – М.: Книжный дом

дифференцированы среди голосовых, видео или печатных сигналов. Потенциальные возможности недобросовестного использования информации оказываются очень велики, причем они возрастают в результате принятия административных решений или осуществления коммерческих трансакций. Так, например, в США растет беспокойство в связи с широким использованием номеров социального страхования для широкого спектра деятельности: налоговыми органами, при выдаче водительских прав и т.д., поскольку существует опасность утечки информации и ее недобросовестного использования. Совершенно очевидно, что по мере распространения все более совершенных способов коммуникации такая опасность возрастает.

Учитывая вышеизложенное, необходимо принимать меры, позволяющие, если не полностью исключить, то хотя бы минимизировать эту опасность. В Канаде под руководством Комиссара по защите частных прав (Privacy Commissioner) был выпущен перечень пунктов, относящихся к частной жизни граждан, включая:

- открытость/прозрачность – в случае, когда происходит сбор новой информации, права граждан не должны нарушаться;
- информированность – граждане должны быть информированы относительно любых видов обнародования информации персонального содержания;
- доступ – граждане должны иметь возможность изменить информацию относительно их статуса, если такое изменение происходит;
- ограниченность – системы, которые предназначены для пользования ограниченным количеством участников, должны быть закрыты для доступа со стороны других участников;
- достоверность – должна быть организована эффективная защита от недобросовестного использования информации в отношении граждан;

«Университет», 2002. – С. 170-174, приложение 3.

- уважение – все участники сбора информации должны понимать и уважать принципы этики частной жизни и законы.[6]

Такие или аналогичные принципы должны действовать не только в отношении просмотра личных досье в многочисленных общественных и частных организациях, но также и при использовании различных компьютерных программ по мониторингу и наблюдению (например, при мониторинге телефонной сети), а также во всех существующих областях сетевого взаимодействия, где потенциально могут возникать подобные нарушения частных свобод граждан.

В США первый закон в области защиты личных прав граждан в данной области был принят в 1974 г. (Privacy Act). Этот закон давал гражданам право контролировать записи правительственных органов, сделанные в их отношении, и вносить в них изменения; выражалось беспокойство по поводу недобросовестного использования информации, содержащейся в компьютерных системах. В 1984 г. Конгресс принял закон, запрещающий нелегальный доступ к федеральным компьютерам, а в 1986 г. это положение было распространено и на компьютерные преступления в частном секторе.

Годовой оборот российского рынка конфиденциальной информации составляет около 20-24 млн. долларов.[7] В Российской Федерации действует закон «Об информации, информатизации, защите информации» №24-ФЗ, принятый Государственной Думой Федерального Собрания Российской Федерации 25 января 1995 г. и вступивший в силу 20 февраля 1995 г., но этим законом не определен перечень сведений, к которым доступ должен быть ограниченным, нет законов о служебной тайне или о коммерческой тайне.

Таким образом, современная правовая система сталкивается сегодня с необходимостью более четкого и эффективного регулирования защиты права интеллектуальной собственности, причем как на национальном, так и на международном уровне.

---

[6] Martin W.J. The Global Information Society / W.J. Martin. – Aldershot: Aslieb Gower; Brookfield, Vt., USA: Gower, 1995. – P. 113.

[7] Ходорыч А. Расколотая база / А. Ходорыч // Коммерсантъ Деньги. - №7, 21 февраля 2001. - С.15.

3.2. Правовое регулирование виртуальной экономики

Серьезная проблема правовой защиты в условиях распространения новых технологий связана и с урегулированием вопросов вокруг электронной коммерции и вытекающих из нее обязательств сторон. Механизму и особенностям электронной коммерции будет посвящена отдельная глава, здесь же мы предполагаем остановиться главным образом на правовом аспекте этого явления.

Категория «электронная коммерция» имеет достаточно широкое толкование и охватывает вопросы, возникающие по поводу различных коммерческих отношений. В юридическом же смысле «электронная коммерция» - это заключение на международных и внутренних рынках различных договоров в электронной форме. В связи с той важной ролью, которую играют сделки, осуществляемые в рамках электронной коммерции, невозможно не затронуть вопрос об их юридическом оформлении. Среди наиболее важных юридических вопросов, требующих решения, можно выделить:

- требования по форме заключения сделок;
- вопросы налогообложения;
- защита информации и использование электронных подписей;
- охрана интеллектуальной собственности;
- охрана прав потребителей и т.п.

Существуют разные подходы к самой проблеме регулирования электронной коммерции, разное отношение к вопросу о ее регулировании. Часть представителей юридической доктрины считает необходимой выработку законодательной регламентации электронной коммерции, которая должна сочетать традиционные юридические нормы и правила с новыми правовыми процедурами и институтами. Другая точка зрения состоит в том, что законодательство в отношении электронной коммерции должно быть сведено к

минимуму, а с учетом глобального характера явления оно должно стать международным и прозрачным. Очевидно, что такой подход будет легче реализовать странам с прецедентным правом, чем странам с исключительным применением нормативных актов.

Прежде всего, необходимо определить понятие *электронного документа*, позволяющего оформить такого рода сделки. Появление его связано с требованиями сегодняшнего дня. В последнее десятилетие XX в. в мире произошли значительные изменения в области технологий. Естественно, это не могло не отразиться и на деловой практике. Компьютерная информация стала реальностью, на основе которой во многом строится современный бизнес. Закономерно и то, что существующих возможностей для развития коммерческих отношений оказалось недостаточно, ведь деловые отношения в большей части регулируются весьма давно сложившимися правовыми средствами и методами. Не являются исключением и коммерческие отношения, связанные с использованием компьютерных технологий. Электронный документ таким образом стал одним из средств, с помощью которых право регулирует данные отношения.

Следует определить понятие электронного документа.

Электронный документ – это документ, представленный в виде данных, записанных на компьютерных носителях и обладающих определенными физическими характеристиками. Именно физические характеристики отличают электронный документ от бумажного. Если бумажный документ мы можем осязать, если на бумаге можно поставить подпись и печать, если сама бумага может быть защищена какими-либо специальными знаками, то к электронному документу все эти характеристики неприменимы. Тем не менее, все остальные требования, предъявляемые к документам, аналогичны для обоих видов документов: содержание сведений определенного характера; изложение данных в установленных порядке и форме; содержание всех необходимых данных о сторонах контракта и т.д.

С самого начала высказывались, да и сейчас слышны различные возражения против использования электронного документа как такового, либо просто сомнения в необходимости безбумажных систем документооборота: недолговечность данных на компьютерных носителях; их нестабильность, возможность внесения изменений; неосязаемость и другие. Так, например, электронный документ не может быть представлен в качестве письменного доказательства в суде, а анонимность Сети создает определенную неуверенность в том, что документооборот осуществляется уполномоченным лицом в должном порядке. Но развитие технологий, изменение экономических реалий, да и сам факт внедрения компьютерной техники во все сферы деятельности человека аннулируют высказываемые возражения и сомнения. Уже невозможно повернуть процесс вспять, да и не следует пытаться это сделать. Поэтому в настоящее время важно решать не вопрос необходимости электронного документооборота, а вопросы его эффективного правового регулирования.

Наконец, есть группа правил и законов, косвенно воздействующих на развитие электронной коммерции, способствующих ее распространению. Поскольку базы данных являются основой информационного общества, Европейский Совет принял Директиву о «Правовой защите баз данных», где определяется понятие базы данных и способы их защиты. В Германии в 1997 г. принят «Закон об информационных и коммуникационных услугах», в котором определяется статус цифровой подписи, введен ряд поправок в законы, касающиеся распространения информации. Аналогичные попытки делаются во многих странах, но, безусловно, необходимы международные договоренности в отношении дальнейшего развития глобальных компьютерных сетей.

В России пока еще сохраняется фрагментарность и неразвитость правовых норм, регулирующих отношения в сфере электронной коммерции, что является препятствием для интеграции российской электронной коммерции в глобальный информационный рынок.

В статье 158 ГК РФ регламентирует понятие «форма сделок»: «Сделки совершаются устно или в письменной форме (простой или нотариальной)».[8] Далее статья 434 ГК РФ раскрывает понятие «форма договора»: «Договор может быть заключен в любой форме, предусмотренной для совершения сделок, если законом для договоров данного вида не установлена определенная форма. Если стороны договорились заключить договор в определенной форме, он считается заключенным после придания ему условленной формы, хотя бы законом для договоров данного вида такая форма не требовалась. Договор в письменной форме может быть заключен путем составления одного документа, подписанного сторонами, а также путем обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору».[9]

Это свидетельствует о том, что законодательство Российской Федерации предусматривает возможность заключения договора посредством электронной связи, в частности, с помощью электронного документа. В этом смысле понятие электронного документа перестает быть чисто техническим и приобретает юридический смысл, поскольку электронная форма документа - разновидность письменной.

Электронный документооборот, как отмечалось выше, - явление последних лет. Уже с середины 70-х гг. велись разработка и принятие нормативных актов, направленных на регулирование отношений в связи и по поводу электронных документов. В 1980 г. Государственный комитет СССР по делам изобретений и открытий Приказом № 158 (от 29.12.1980) утвердил Положение о всесоюзной магнитно-ленточной службе патентной информации. Однако, это в большей мере касалось внутриотраслевых электронных документов. 20 апреля 1981 г. Государственный комитет по науке и технике СССР утвердил «Временные общеотраслевые руководящие указания о

[8] Гражданский Кодекс Российской Федерации. Части первая и вторая // М.: Издательская группа НОРМА-ИНФРА-М, 1998. – С.101.
[9] Там же. - С.202.

придании юридическим документам, создаваемым средствами вычислительной техники.» 9 октября 1984 г. Государственным комитетом СССР по стандартам был введен ГОСТ 6.10.4 - 84 «Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники». Но в СССР электронный документооборот не получил широкого распространения.

В связи с изменением экономической и политической ситуации в стране проблема оформления электронного документа становится все более актуальной, так как речь идет не просто о внутриведомственном обмене информацией, а о построении бизнеса посредством электронных документов. И если ранее в ГК РСФСР 1964 г. было достаточно моментов, ограничивающих использование электронного документа, то новый ГК РФ устранил такое положение, разрешив использование электронных документов при заключении сделок (остались лишь некоторые исключения).

В России принят Федеральный Закон от 10.01.2002 №1-ФЗ «Об электронной цифровой подписи». Создаются правовые условия для использования электронной цифровой подписи (далее – ЭЦП) в электронных документах, при этом ЭЦП приравнивается в юридическом отношении к собственноручной подписи человека на бумажном носителе.

Законодательство об электронной подписи действует уже во многих странах, что значительно упрощает механизм юридического общения. При этом существуют три основных подхода к требованиям в отношении электронной подписи. В соответствии с первым подходом к электронной подписи выдвигаются те же самые требования, что и к обычной подписи: уникальность, допустимость верификации и подконтрольность тому лицу, которое ее использует. Второй подход, помимо вышеуказанного, говорит о необходимости признания подписи недействительной, если изменяются передаваемые данные, то есть устанавливает тесную связь подписи и данных. Согласно третьему подходу по отношению к электронной подписи предъявляются более жесткие требования, например, предусматривается

использование криптографической технологии открытого ключа, то есть осуществляется попытка обеспечить повышенную степень надежности электронной подписи. В разных странах по-разному подходят к электронной подписи. В США федеральное правительство признает законной любую электронную подпись, которая признается контрагентами по сделке. Европейские страны в основном используют второй подход при определении электронной подписи.

Электронная подпись в случае ее законодательного признания приравнивается по своей силе к подписи на юридических документах, поставленной в традиционном виде, для широкого круга юридических действий. Электронная подпись используется во многих странах даже на высоком государственном уровне и для подписания межгосударственных договоров. Например, электронная подпись была использована при подписании соглашения о цифровой торговле между США и Ирландией, а файл с текстом закона «Об электронных подписях в глобальной и национальной торговле» был подписан Б. Клинтоном с помощью фотографической копии его подписи, которую он вывел на компьютерном графическом планшете.

Электронная подпись будет способствовать развитию Интернет-сделок в сегменте B2B. С помощью электронной подписи можно будет заключать договоры между контрагентами, находящимися далеко друг от друга, передавать платежные поручения в банк, не используя защищенную линию связи «банк-клиент». Подписанный документ не может быть изменен, так как во время выработки электронной подписи с использованием закрытого ключа создается код, который при считывании с помощью открытого ключа подтверждает, что текст не менялся, что и дает гарантию подлинности документа. Кроме той пользы, которую закон об электронной подписи дает для развития сегмента B2B, он позволяет и физическим лицам использовать преимущества электронной подписи при заказе товара через Интеренет-магазин, а также при выдачи платежного поручения банку, что менее удобно,

чем использование платежной карты, зато гораздо надежнее, учитывая недостаток в средствах защиты в Интернете.

Необходима четко регламентированная система электронных расчетов. В России есть ряд актов, которые регулируют порядок расчетов при использовании электронной коммерции: ст. 847 ГК РФ, Положение ЦБ РФ №20-II «О правилах обмена электронными документами между Банком России, кредитными организациями (филиалами) и другими клиентами Банка России при осуществлении расчетов через расчетную сеть Банка России» от 12 марта 1998 г., Письмо ЦБ РФ «О перечне договорных условий об обмене электронными документами» от 2 июня 1998 г.

Государственная техническая комиссия (ГТК) при Президенте РФ разработала руководящие документы в области защиты информации. В государственном секторе они обязательны для исполнения, для коммерческого сектора они носят рекомендательный характер. Так, например, запрещается использовать мощные шифровальные технологии без разрешения Федерального агентства правительственной связи и информации (ФАПСИ).

Деятельность Рунет регулируется постановлением Правительства РФ «О государственном регулировании глобальной информационной сети Интернет в РФ (российского сегмента сети Интернет)» от 20 января 2000 г. и от 13 января 2000 г. Возможно, что в России будет со временем разработана специальная программа по защите доменных имен, адаптированная конкретно к российским экономическим условиям.

Только полная правовая база даст возможность не просто говорить об электронной коммерции как о перспективном и важном направлении развития обмена, но как о реальном аналоге оффлайновому бизнесу (бизнес в традиционном виде) в онлайновом сегменте экономики (бизнес в Сети). Безусловно, для реализации этого необходимы финансовые средства.

Основные понятия:

Доменное имя (domain name)

Торговцы доменными именами (domain name traders)

Кибersквоттеры (cybersquqtters)

Единая политика по урегулированию споров в области названий доменов -

UDRP (United Dispute Resolution Policy)

Электронный документ (e-document)

Вопросы для самостоятельной подготовки:

1. Рассмотрите таблицу.

Оценка отдельным потребителем полезности продукта по мере увеличения количества потребителей

Количество потребителей	**1**	**2**	**3**	**4**
Готовность платить, условные единицы	**50**	**100**	**150**	**200**

Ответьте на следующие вопросы, учитывая, что у производителя А, являющегося монополистом, есть 6 потребителей, причем трое из них – законопослушные потребители, а трое готовы приобретать продукт исключительно нелегальным образом:
а). Какова будет выручка монополиста А, если он защищает свой продукт?
б). Какова будет выручка монополиста А, если он не защищает свой продукт?

2. От чего зависит степень необходимой защиты информационного продукта?

3. Что такое кибersквоттинг?

5. Что отличает электронный документ от бумажного документа?

Ситуация для анализа

Защищенные информационные системы

В январе 2002 г. председатель правления Microsoft Билл Гейтс обратился к 50 тысячам сотрудников корпорации с письмом, в котором поставил задачу создать для клиентов защищенную информационную среду, которая была бы

столь надежна, как электричество, работающее сегодня в наших домах и офисах. Программа защищенных информационных систем охватывает четыре направления: безопасность, конфиденциальность, безотказность и бизнес-этику.

Microsoft направляет значительные ресурсы на улучшение своих продуктов по каждому из этих аспектов. Кроме того, корпорация создала систему отслеживания и оценки успехов в достижении таких целей и задач в области защищенных информационных систем, как безопасность при разработке, безопасность при установке, безопасность при использовании и обмене информацией (secure by design, secure by default, secure in deployment, and communications, SD3+C).

Источник: Информационный бюллетень Microsoft. Государство в XXI веке. Выпуск 25. С.43.

Вопросы по ситуации:

1. Почему, на Ваш взгляд, бизнес-этика включается в понятие защищенности информационных систем?
2. Являются ли перечисленные четыре направления исчерпывающими понятие защищенности информационных систем?