ЕВРОПЕЙСКАЯ ЭКОНОМИЧЕСКАЯ КОМИССИЯ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ

ПРАВОВЫЕ АСПЕКТЫ ПОЛИТИКИ В ОБЛАСТИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ *В ЦЕНТРАЛЬНОЙ АЗИИ*

Руководство для разработки политики в области ИКТ

ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ
Нью-Йорк и Женева, 2007 год

ПРИМЕЧАНИЕ

Употребляемые обозначения и изложение материалов в настоящем издании не означают выражения со стороны Секретариата Организации Объединенных Наций какого бы то ни было мнения относительно правового статуса той или иной страны, территории, города или района, или их властей, или относительно делимитации границ.

ECE/CECI/1

Отпечатано в Организации Объединенных Наций, Женева (Швейцария)

ИЗДАНИЕ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ

***В продаже под №* 07.II.E.21**

ISBN: 978-92-1-416036-6

ПРЕДИСЛОВИЕ

Развитие информационно-коммуникационных технологий (ИКТ) открывает для предприятий и людей возможность общаться и заключать сделки с другими сторонами с использованием электронных средств моментально и в глобальном масштабе. Это создает для разработчиков политики ряд вопросов, связанных с нормативно-правовой базой, - от действительности электронных методов заключения контрактов и рисков для безопасности, связанных с ними, до проблем киберпреступности и возможности защиты прав интеллектуальной собственности в электронных сетях. Разработчики политики ИКТ постоянно наталкиваются на необходимость решения этих вопросов. Продвижение согласованных правовых реформ, которые могли бы способствовать надежному развитию электронной торговли и связанной с нею деятельности, обеспечивая надлежащую защиту граждан от злонамеренных действий, - путь решения этих вопросов.

Это Руководство было подготовлено по просьбе Проектной рабочей группы по ИКТ в целях развития, созданной в декабре 2005 года в рамках Специальной программы Организации Объединенных Наций для экономик Центральной Азии (СПЕКА). СПЕКА была создана в 1998 году для укрепления субрегионального сотрудничества в Центральной Азии и ее интеграции в мировую экономику. Европейская экономическая комиссия Организации Объединенных Наций (ЕЭК ООН) и Экономическая и социальная комиссия Организации Объединенных Наций для Азии и Тихого океана (ЭСКАТО) оказывают техническое содействие осуществлению проектов, согласованных ее участниками. Страны - участницы СПЕКА: Азербайджан, Афганистан, Казахстан, Кыргызстан, Таджикистан, Туркменистан и Узбекистан. Руководство предназначено для использования в качестве справочного материала для директивных органов по ИКТ в странах с переходной экономикой. Его содержание призвано соответствовать задачам стран - участниц СПЕКА, учитывая замечания, полученные в ходе ряда мероприятий по формированию потенциала, проведенных в 2006-2007 годах.

ЕЭК ООН всячески привержена цели проведения деятельности по формированию потенциала в странах с переходной экономикой, включая проекты, нацеленные на директивные органы по ИКТ, чтобы эти страны могли реализовать весь потенциал инноваций в областях, связанных с ИКТ, как средства поддержки их экономического развития, основанного на знаниях. Мы надеемся, что эта публикация внесет вклад в достижение этой цели.

Марек Белька
Исполнительный секретарь
Европейской экономической комиссии
Организации Объединенных Наций

ВЫРАЖЕНИЕ ПРИЗНАТЕЛЬНОСТИ

Это издание - один из итогов проекта технического сотрудничества ЕЭК ООН "Укрепление потенциала в целях разработки политики в сфере ИКТ", нацеленного на укрепление потенциала директивных органов по ИКТ в Центральной Азии, осуществляемого Отделом по экономическому сотрудничеству и интеграции. Работа над этим изданием велась под руководством Мичико Эномото. Проект Руководства подготовили профессор Ян Уолден (консультант) и Лора Эдгар, сотрудник Института компьютерно-коммуникационного права Центра исследований торгового права колледжа Королевы Марии Лондонского университета. Замечания существенного характера были получены от Андрея Васильева, Румена Добрински, Мичико Эномото, Джефри Хамильтона и Ханса Ханселя. Общую поддержку и форматирование обеспечивали Татьяна Апатенко и Виктория Гудева, обложка подготовлена Ивом Клоптом, текст редактировала Алисон Манжан.

Большая признательность за финансовую поддержку со стороны Счета развития Организации Объединенных Наций.

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ

ВВИО	Всемирная встреча на высшем уровне по вопросам информационного общества
ВОИС	Всемирная организация интеллектуальной собственности
ВТО	Всемирная торговая организация
ГАТС	Генеральное соглашение о торговле услугами
ГСИП	голосовая связь Интернет по протоколу
ЕБРР	Европейский банк реконструкции и развития
ЕС	Европейский союз
ИКАНН	Международная корпорация по присвоению доменных имен
ИКТ	информационно-коммуникационные технологии
ИНН	индивидуальный идентификационный номер
ИТ	информационные технологии
ОЭСР	Организация экономического сотрудничества и развития
ПВИС	платформа выбора Интернет-содержания
ПИС	права интеллектуальной собственности
ПИУ	провайдер Интернет-устуг
ПО	программное обеспечение
ПРООН	Программа развития Организации Объединенных Наций
РСС	Региональное содружество в области связи
СНГ	Содружество Независимых Государств
СПЕКА	Специальная программа ООН для экономик Центральной Азии
ЭОД	электронный обмен данными
ЮНСИТРАЛ	Комиссия ООН по праву международной торговли

РЕЗЮМЕ

Развитие информационно-коммуникационных технологий (ИКТ) позволяет предприятиям и людям поддерживать связь и совершать операции с другими сторонами с использованием электронных средств, мгновенно и в международном масштабе. Это создает для разработчиков политики ряд связанных с нормативно-правовой базой вопросов, от действительности электронных методов заключения контрактов и рисков для безопасности, связанных с ними, до проблем киберпреступности и возможности защиты прав интеллектуальной собственности в электронных сетях.

Это Руководство состоит из пяти разделов, в которых рассмотрены правовые вопросы, связанные с ИКТ:

- **Правовая инфраструктура**, где рассматриваются некоторые ключевые юридические и регулятивные средства содействия электронной торговле - от принятия принципов правовой реформы, таких, как "нейтральность по технологии", до регулятивных структур и рыночной либерализации.

- **Правовая определенность**, где рассматривается юридический статус электронных сообщений и форм заключения контрактов, прежде всего необходимость **прямого** признания действительности, обеспеченности правовой санкцией и допустимости электронных средств совершения юридических актов.

- **Правовая безопасность**, где рассматриваются риски безопасности, неотъемлемо присущие электронной среде, и рассматриваются методы, используемые для их **преодоления**, в частности использование цифровой подписи и услуг сертификации.

- **Правовая защита**, где рассматриваются права **интеллектуальной** собственности и то, как такое нематериальное имущество защищается в интерактивной среде, а также проблемы защиты прав потребителей, которые возникают в связи с Интернетом.

- **Правовое сдерживание**, где рассматривается развитие феномена киберпреступности и проанализированы методы преследования в законодательстве такого **злонамеренного** поведения и обеспечения того, чтобы правоохранительные органы могли проводить расследования и привлекать к ответственности правонарушителей.

В Руководстве рассматриваются юридические вопросы, возникающие в каждой из этих областей, и выделяются соответствующие новые моменты и инициативы, связанные с передовым опытом, на международном уровне, такие, как Конвенция 2005 года и типовые законы ЮНСИТРАЛ, а также на региональном уровне, в частности в Европейском союзе и в странах - участницах СПЕКА: Азербайджане, Афганистане, Казахстане, Кыргызстане, Таджикистане, Туркменистане и в Узбекистане.

В заключение в Руководстве представлены рекомендации для стран - участниц СПЕКА о возможных путях содействия процессу правовой реформы в вопросах ИКТ.

I. ПРАВОВАЯ ИНФРАСТРУКТУРА ИКТ

Хорошо известно, что экономическое развитие зависит от обеспеченности страной соответствующей инфраструктурой содействия такому развитию. Следует также признать, что нормативно-правовая база данной страны представляет собой элемент такой инфраструктуры. В этом разделе кратко рассмотрены эти области, в которых будут выделены новые моменты международного масштаба.

A. Правовые принципы

Реализация политической цели в дееспособных законах и подзаконных актах, разумеется, может быть сложной задачей в любой области деятельности человека. Однако технология создает для законодателя вызовы особого рода, что главным образом обусловлено темпами перемен в самой регулируемой области, в частности программном обеспечении, вычислительной технике и сетях, а также в характере использования такой технологии. Пределы нашего воображения самым очевидным образом проявляются не только в нашем незнании того, где происходит развитие науки и техники, но и в том, какие их достижения найдут практическое применение. Многое было написано о характере регулирования в среде, составляемой информацией, компьютерами и сетями.

В ответ на эти вызовы разработчики политики пытаются определить принципы, способные направлять нормотворческие инициативы в этой области. Главный и самый известный принцип регулирования - "нейтральность по технологии". Разработчики политики часто обращаются к концепции "нейтрального по технологии" регулирования, исходя из той посылки, что среда изменяется слишком быстро для того, чтобы попытаться связать юридические нормы с конкретной моделью технологии или рынка. Этот принцип во всех его вариантах используется в двух основных значениях: то, что регулируется в неинтерактивной среде, должно регулироваться в интерактивной среде; разные же технологии должны считаться сходными в той мере, в какой они вызывают те же последствия[1]. Однако продолжаются споры о том, как должен применяться этот принцип, когда речь идет о реформе материального и процессуального права.

Этот принцип также не помогает там, где при разработке политики необходимо делать выбор между различными моделями регулирования. Так, Интернет дает замечательный пример явления сближения, когда информационное наполнение разных форм передается по соединенным друг с другом сетям с использованием единого протокола. Однако вопрос о том, должна ли модель регулирования, ориентированная на ИТ/системы связи или системы вещания, передаваться в отношении передаваемого содержания - это по-прежнему щекотливый вопрос для директивных и регулирующих органов.

Помимо технологической нейтральности, Всемирная встреча на высшем уровне по вопросам информационного общества (ВВИО) призвала к тому, чтобы системы политики и регулирования "поощряли конкуренцию", государственное вмешательство ограничивалось явно необходимыми целями. В рамках процесса ВВИО конкуренция на рынке признается

[1] См. Koops, B-J., "Should ICT regulation be technology-neutral?", в Koops, B-J., *Starting Points for ICT Regulation*, Cambridge, 2006.

главным регулятором участников рынка, в функционирование которого государство вмешивается только в случаях его сбоя или необходимости поддержания добросовестной конкуренции.

Предлагался и ряд других принципов, которые, однако, в разной степени были восприняты официальными органами и общественностью. Так, для некоторых программное обеспечение с открытым исходным кодом - это не только альтернатива имеющимся на рынке пакетам программного обеспечения крупных фирм, но и элемент более широкого движения против использования законов об авторском праве как средства ограничения свободного обмена информацией. Необходимость поощрения "находящейся в общей собственности" информации воспринимается как важнейший инструмент, более пригодный для генерирования в будущем результатов творческого труда, чем среда, создаваемая подходом в духе традиционного авторского права - "все права защищены"[2]. Переформатирование интеллектуальной собственности в среде информационной экономики в терминах открытых систем и открытого кода считается особенно полезным для развивающихся стран, у которых нет средств для создания режимов интеллектуальной собственности наподобие тех, которые созданы в развитых странах, а также для контроля над ними.

Еще один слой, лежащий выше принципов, появившихся в связи с правовой реформой в секторе информационно-коммуникационной технологии (ИКТ), - принципы общего рода, традиционно служащие основой для оценки законов, прежде всего в области уголовного права. Например, юридическая прозрачность требует, чтобы те, на которых распространяется закон, знали или имели возможность знать о нормах, касающихся конкретного вида деятельности. В соответствии с европейским правом в области прав человека прозрачность - это один из элементов того требования, чтобы ограничения прав человека "соответствовали закону".

В нашей все более глобальной экономике один из важнейших факторов, определяющих, в частности, уровень прямых иностранных инвестиций в данном секторе, - оценка степени определенности ныне действующей нормативно-правовой базы. Чем больше степень нестабильности нормативно-правовой базы, как реальная, так и субъективно оцениваемая, тем больше правовая неопределенность, а следовательно, и отрицательные стимулы для инвестиций. Область, в которой необходима юридическая определенность распространяется область от процессов законотворчества до правоприменения. Инвесторы будут испытывать особую озабоченность по поводу какого-либо процесса принятия решений по усмотрению министерств, регулирующих органов и судов. Определенная свобода действий - неизбежная черта всех правовых систем, однако она требует определенных мер контроля и ограничений.

С юридической определенностью тесно связано требование состоятельности законов. В состоятельности можно выделять два ключевых аспекта. Во-первых, период времени, в течение которого комплекс юридических норм остается дееспособным в плане достижения общих целей в тех условиях, в которых он применяется. Во-вторых, возможность обеспечения соблюдения норм, т.е. пресечение запрещенного поведения. Хотя в любой

[2] http://www.creativecommons.org.

области права цель неукоснительного соблюдения остается недостижимой, в частности в киберпространстве множественных и вступающих в противоречие юрисдикций, массовая неспособность обеспечить соблюдение закона подрывает ценность любого комплекса правовых норм.

B. Структура и субъекты регулирования ИКТ

Роль государства заключается в том, чтобы управлять и в общем плане принимать законы и подзаконные акты, предназначенные для регулирования определенных форм деятельности. При этом широко признается, что деятельность государства по регулированию выходит за рамки системы государственных органов, охватывая широкий круг учреждений и механизмов контроля. Например, как показывает международный передовой опыт, в некоторых секторах, таких, как связь, лучше всего создавать независимый регулирующий орган для контроля за конкурентной либерализацией отрасли и магистральной инфраструктуры и создания предпосылок для развития электронной торговли.

Дееспособные регулирующие институты нуждаются в соответствующих кадрах и ресурсах, которых, возможно, трудно найти развивающимся странам. Для устранения таких препятствий в большинстве программ развития предусматривается укрепление потенциала в области регулирования, включая программы подготовки кадров и обменов с регулирующими учреждениями развитых государств.

Однако такие официальные учреждения могут также получать поддержку со стороны структур негосударственного сектора, как предпринимательских, так и гражданского общества, действующих в качестве органов регулирования, будь то прямого или косвенного. Например, саморегулирование или совместное регулирование предусматривает выработку в отрасли правил для ее предприятий и контроль за их соблюдением.

Хотя мы традиционно воспринимаем регулирование в плане законов и регламентаций, мы не должны забывать и о других процессах, происходящих на национальном и международном уровне, которые реально регулируют то, каким образом общество воспринимает проявления информационной экономики. Так, стандарты и протокол, лежащие в основе функционирования Интернета и его различных услуг, от электронной почты до голосовой связи по Интернет-протоколу (ГСИП), содействуют или ограничивают наше взаимодействие с такими технологиями либо в результате намеренного желания разработчика, либо случайно или по ошибке. Характер нашего использования Интернета определяется конъюнктурой рынка: например, телефонные тарифы ограничивают пользование им в случае повременной оплаты. Нормы культуры также определяют то, как люди пользуются и злоупотребляют Интернетом как средством связи и экономической деятельности.

Один из методов развития и координации деятельности государства в области экономики ИКТ - создание новых институциональных структур, которым конкретно поручено решать такие вопросы. Как развитые, так и развивающиеся государства используют такой метод. В некоторых случаях необходимо законодательное закрепление таких учреждений, как

Казахстанское агентство по информатизации и связи[3], для повышения прозрачности и обеспечения независимости от существующих государственных ведомств и органов государственной власти, что способно повысить статус и авторитетность такого учреждения.

Однако при всей важности самостоятельности необходимо также обеспечить надлежащее сотрудничество и координацию между различными государственными органами, к которым обычно относятся основные министерства, отвечающие за вопросы финансов, доходов и торговли. Однако ключевым фактором часто будет являться, помимо прочего, политическая поддержка, прежде всего в свете разнообразных политических приоритетов, которые могут потребовать, чтобы такое учреждение было связано с ключевыми политическими действующими лицами в данной стране.

Инициатива по раскрытию возможностей в цифровой сфере[4], государственно-частное партнерство фирмы "Аксенчур", фонда Мерклов и Программы развития Организации Объединенных Наций (ПРООН), в своем докладе "Формирование динамики развития" признает важное значение участия в реализации стратегии развития ИКТ всех заинтересованных сторон, представляющих государственный и частный сектор, гражданское общество и международные организации, которое они называют "стратегическими договорами" как на этапе разработки, так и на этапе осуществления.

С функционированием конкуренции как принципа регулирования связана идея саморегулирования, когда поставщики товаров и услуг в секторе ИКТ вправе сами регулировать свое поведение или по крайней мере совместно регулировать его на основе партнерства с государством и отраслевыми ассоциациями. Растущая готовность государства опираться на саморегулирование на общем уровне обусловлена рядом движущих сил - от признания непомерной сложности современной торговли до желания снизить нагрузку на государственные финансы. В секторе ИКТ такие движущие силы дополняются общим признанием того, что Интернет и связанные с ним услуги развились до своего нынешнего состояния в условиях относительного отсутствия существенного вмешательства со стороны государственных органов.

Один из элементов саморегулирования - роль стандартов во всех аспектах функционирования Интернета. Помимо стандартов, связанных с технологическими элементами систем электронной торговли, были также разработаны отраслевые стандарты, касающиеся передаваемого содержания. Например, спецификация платформы выбора Интернет-содержания (ПВИС)[5] была разработана для того, чтобы создать возможность присвоения определенного ярлыка данному виду Интернет-содержания. Первоначально она была предназначена для того, чтобы родители могли закрыть доступ их детей к содержанию, которое они считают неприемлемым. В областях защиты прав потребителя и защиты частной жизни были разработаны системы маркировки электронной торговли для того, чтобы дать пользователям наглядные указатели соблюдения некоторых минимальных стандартов защиты. Такие системы могут включать процедуры разрешения споров, предназначенные для усиления защиты прав частных граждан.

---

[3] Создано в 2003 году; к нему перешли функции и полномочия, ранее осуществлявшиеся министерством транспорта и связи.

[4] http://www.opt-init.org/

[5] http://www.w3.org/PICS/

Что касается защиты прав, то были созданы финансируемые отраслью органы для контроля и представления информации о связанной с Интернетом деятельности, затрагивающей определенные виды незаконного информационного содержания, от материалов, нарушающих права интеллектуальной собственности, которые, как правило, защищаются в гражданско-правовом порядке, до детской порнографии, преследуемой в уголовном порядке (см., например, о Фонде по наблюдению за Интернетом)[6].

Однако саморегулирование вызывает некоторые вопросы, касающиеся легитимности. Можно считать, что, приняв системы саморегулирования, законодатель устранился от исполнения функций, которыми он наделен в результате демократического процесса. Необходимо также обеспечить ответственность и контроль для предотвращения того, чтобы со временем цели политики, лежащие в основе систем регулирования, не казались оттеснены на второй план противоречащими им коммерческими интересами.

Какой бы государства ни приняли метод регулирования в вопросах ИКТ - самостоятельного или саморегулирования/совместного регулирования, - расходы на него, безусловно, будут решающим фактором, когда создание специального органа потребует чрезмерных затрат во многих развивающихся странах, которые не смогут получить для этого содействия со стороны организаций по вопросам развития. Хотя метод саморегулирования или совместного регулирования может показаться интересным в плане сведения к минимуму государственных расходов на регулирование, его успех зависит от наличия достаточно мощного и активного частного сектора, желающего и готового финансировать деятельность по регулированию. Для уменьшения связанных с этим издержек такая структура могла бы координировать другие приносящие доход виды деятельности, связанные с электронной торговлей. Например, управление системой присвоения доменных имен странового уровня дает потенциальный источник лицензионных поступлений.

C. Либерализация сектора

С точки зрения регулирования либерализация предполагает открытие сектора для сил конкуренции. Если Интернет воспринимается как в высшей степени конкурентная среда экономической активности, средства, с помощью которых граждане получают доступ к Интернету, могут быть значительно менее конкурентными. В частности, рынок телекоммуникаций - ключевой фактор, делающий возможным рост и развитие электронной торговли.

На международном уровне усилия по либерализации сектора телекоммуникаций направляются главным образом в рамках Всемирной торговой организации (ВТО) под эгидой Генерального соглашения о торговле услугами (ГАТС), приложения по

[6] http://www.iwf.org.uk

телекоммуникациям и справочного документа[7]. Из числа стран-участниц Специальной программы Организации Объединенных Наций для экономик Центральной Азии (СПЕКА) только Кыргызстан является членом ВТО и официально принял обещание провести полную либерализацию своего сектора телекоммуникаций[8].

Однако другие страны-участницы СПЕКА продемонстрировали существенный прогресс в этом секторе, опираясь на содействие со стороны структур по финансированию развития, в частности Европейского банка реконструкции и развития (ЕБРР), предоставившего финансирование инициатив по реформе законодательства, а также более традиционное финансирование, признавая то, что современные системы регулирования способствуют привлечению частных инвестиций в этот сектор[9]. Закон Казахстана "О связи"[10] - пример такой либерализации сектора.

В ГАТС затрагивается четыре способа оказания услуг: a) с одной территории на другую, т.е. международная поставка, b) оказание услуг иностранным потребителям на территории поставщика услуг, т.е. потребление за границей, c) присутствие юридического лица в другом государстве и d) присутствие физического лица в другом государстве[11].

В соответствии с ГАТС конкретные обязательства государств-участников затрагивают роль "внутреннего регулирования" (статья VI). Во-первых, имеется то общее требование, что все меры должны осуществляться "разумным, объективным и беспристрастным образом". Во-вторых, в нем требуется, чтобы были созданы "судебные, арбитражные или административные органы" и процедуры для предоставления поставщикам услуг возможности обжалования решений, сказывающихся на торговле услугами. В-третьих, разрешительные процедуры, которые должны быть пройдены структурой до начала оговоренной деятельности, должны быть завершены "без чрезмерного промедления". В-четвертых, признается роль технических стандартов в регулировании деятельности, а государства-участники обязуются не принимать стандартов, более обременительных, чем это необходимо, непрозрачных и субъективных по своему характеру.

Одна из составляющих процесса либерализации сектора телекоммуникаций - выдача разрешений и лицензирования. Чем сложнее и дольше процесс получения государственной лицензии, предоставляющей право оказания услуг, строительства производственного объекта или экологичной деятельности, тем больше препятствий для доступа на рынок для конкурентов как внутри страны, так и из-за рубежа.

Однако сектор телекоммуникаций - не единственный, где возникают вопросы выдачи разрешений и лицензий. В некоторых странах право ввоза, реализации, подключения и эксплуатации различных категорий оборудования ИКТ может предоставляться в порядке разрешительных процедур и лицензирования, которые могут представлять собой по сути нетарифные ограничения торговли. Хотя обоснования такого рода режима могут быть вполне убедительными в плане предотвращения того или иного ущерба, например

---

7 Подробнее см. http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm

8 С 1 января 2003 года.

9 См. EBRD Report, Telecommunications, Informatics and Media, January 2000.

10 От 5 июля 2004 года.

11 ГАТС, статья I, пункт 2.

безопасности граждан и другим неэкономическим интересам общества, в силу характера практического использования такого рода систем могут возникать препятствия для развития ИКТ, такие, как сроки или издержки получения соответствующих разрешений и лицензий. ВТО приняла декларацию о торговле продукцией информационной технологии[12], к которой присоединился Кыргызстан; однако в ней предусматриваются только строгие обязательства в отношении снижения тарифов, а не нетарифных ограничений.

D. Сближение законодательства в сфере ИКТ

В нашей глобальной информационной экономике правовые реформы, которые во многом не стыкуются с процессом в других странах, могут серьезно препятствовать экономическому развитию. Поэтому государство часто заинтересовано в том, чтобы отразить в ходе правовой реформы региональный или международный передовой опыт. С конца 1990-х годов разработано несколько типовых законов, которые могут послужить полезным ориентиром для любой страны, переходящей на новую систему регулирования, в целях содействия электронной торговле. В этом разделе представлен краткий разбор этих типовых законов и директив, которые будут более подробно рассмотрены в других разделах доклада.

1. Типовые законы и Конвенция ЮНСИТРАЛ об электронных сообщениях

Комиссия Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ)[13] - ведущий форум для инициатив по унификации законодательства, призванных содействовать электронной торговле. Хотя в настоящее время страны-участницы СПЕКА не являются членами, меры ЮНСИТРАЛ оказали воздействие на инициативы по реформе законодательства в этой области. Еще в 1985 году ЮНСИТРАЛ рекомендовала государствам-членам рассмотреть правовые нормы, затрагивающие использование записей на ЭВМ в качестве доказательства требования формы и допустимости представления документов в электронной форме для государственных органов[14]. 12 июня 1996 года был принят Типовой закон ЮНСИТРАЛ об электронных подписях (Типовой закон 1996 года). Цель типового закона заключалась в содействии использованию электронных средств связи и хранения информации. Закон предусматривает комплекс международно приемлемых норм, цель которых - создание стабильной и безопасной среды для электронной торговли путем устранения имеющихся юридических препятствий. В законе рассмотрены функции различных требований к форме и предусматривается функциональный эквивалент в электронных сетях таких связанных с бумажными носителями концепций, как письменная форма, подпись и оригинал.

Представив типовые нормы, такой закон может служить для стран руководством к использованию при разработке своего законодательства. В типовой закон могут вноситься изменения с учетом особенностей данной правовой системы; кроме того, может быть взят не весь типовой закон целиком, а, в зависимости от необходимости, его конкретные положения.

---

[12] Вступила в силу 1 июля 1997 года. Общие сведения см. http://www.wto.int/english/tratop_e/inftec_e/inftec_e.htm.

[13] Общие сведения см. http://www.uncitral.org.

[14] ЮНСИТРАЛ, "Рекомендации в отношении юридической ценности записей ЭВМ", 1985 год.

Типовой закон сопровождается руководством, в котором содержатся общие сведения о типовом законе, а также дается пояснительная информация по положениям закона.

В 1996 году, когда был подготовлен Типовой закон, хотя в нескольких странах были приняты законодательные нормы, призванные учесть электронные способы заключения контрактов, ни в одной из стран еще не было создано нормативно-правовой базы, регламентирующей электронную торговлю как таковую. Десятилетие спустя ситуация стала совсем иной. Например, сам типовой закон послужил основой законодательства об электронном заключении контрактов в самых разных странах, включая Австралию, Бахрейн, Бермудские Острова, Гонконг, Доминиканскую Республику, Дубай, Ирландию, Канаду, Колумбию, Мексику, Сингапур, Словению, Соединенное Королевство, Соединенные Штаты, Филиппины и Францию.

В 2001 году ЮНСИТРАЛ также был принят Типовой закон об электронных подписях, в котором дополняется положение об электронных подписях в статье 7 Типового закона 1996 года. Этот типовой закон посвящен ключевым функциям подписей - удостоверение подлинности и целостности - для обеспечения равного режима технологий подписи. В нем зафиксированы определенные требования, которым должна удовлетворять подпись, чтобы считаться юридически действительной, а также предусматривается ответственность поставщиков услуг подписи.

Хотя типовые законы оказались исключительно полезными для многих стран, разрабатывавших свое законодательство, в качестве основы или справочного материала, они не имеют какого-либо официального статуса в качестве нормативных актов. Поэтому для того, чтобы содействовать дальнейшей реформе и унификации в области электронной торговли, ЮНСИТРАЛ поручил своей Рабочей группе по электронной торговле разработать проект Конвенции об использовании электронных сообщений в международных договорах (Конвенция 2005 года), которая была принята Генеральной Ассамблеей Организации Объединенных Наций в ноябре 2005 года и открыта для подписания в январе 2006 года.

Цель Конвенции - повысить правовую определенность в случаях использования электронных сообщений в связи с международными договорами. В Конвенции устанавливаются положения о заключении и исполнении договоров с использованием электронных сообщений в связи с международными договорами. Поэтому Конвенция не охватывает все вопросы, затронутые в Типовом законе 1996 года, например в ней исключаются вопросы, касающиеся доказательственной ценности электронных сообщений. В ней также не затрагиваются определенные виды договоров, такие, как договоры по личным или семейным вопросам и некоторые виды финансовых соглашений, такие, как межбанковские платежные системы.

2. Европейские директивы по ИКТ

Кроме того, имеется ряд новых документов регионального уровня, которые могут оказаться полезным подспорьем для стран - участниц СПЕКА, в частности документов Европейского союза.

Европейский союз (ЕС) подготовил соответствующие директивы об электронной торговле, электронных подписях, защите данных и о дистанционных продажах[15]. Это - директива 1999/93/ЕС о порядке использования электронных подписей в сообществе (директива об электронных подписях) и директива 2000/31/ЕС об определенных правовых аспектах сферы информационных услуг, в частности электронной торговле на внутреннем рынке (директива об электронной торговле), директива 1995/46/ЕС о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных (директива о защите данных) и директива (97/7/ЕС) о защите потребителей в связи с дистанционными договорами.

Эти директивы отличаются от типовых законов, поскольку государства - члены ЕС несут правовую обязанность в конкретно установленный срок ввести в действие нормы, содержащиеся в данной директиве, в свое законодательство. Директивы не устанавливают конкретных формулировок, которые должны использоваться при принятии норм, будучи направлены на достижение цели внесения таких поправок в законодательство.

3. Региональное содружество в области связи

Региональное содружество в области связи (РСС)[16] было создано в декабре 1991 года представителями Содружества Независимых Государств (СНГ). Оно официально признано в качестве межгосударственного органа по координации деятельности в области почтовой и электросвязи, включая инициативы по реформе законодательства:

> "Совершенствование и гармонизация нормативной, технической и нормативной правовой базы в области связи и информатизации стран - участников РСС, включая разработку модельных законодательных актов в сотрудничестве с Парламентской ассамблеей государств - участников СНГ с учетом норм международного права"[17].

Межпарламентская ассамблея государств СНГ разработала типовой закон "Об электронной торговле", который дорабатывается для представления парламентам государств-членов в октябре 2007 года.

---

15 Общие сведения см. http://europa.eu/scadplus/leg/en/s21012.htm#ECOMMERCE.

16 См. общие сведения в http://www.rcc.org.ru/en/index.htm.

17 РСС, "Стратегические направления деятельности Регионального содружества в области связи" решение № 36/2 от 12 декабря 2006 года, пункт 5.

E. Заключение

Решение нормативно-правовых вопросов ИКТ затрагивает некоторые общие вопросы политики, которые должны быть рассмотрены данной страной, а также специфические вопросы данной темы, такие, как заключение контрактов в электронной форме или киберпреступность. Бессистемная реформа законодательства может создать больше проблем и препятствий, чем устранить, чем и объясняется необходимость комплексного и последовательного подхода в более общем контексте стратегии развития ИКТ данной страны. Такой подход должен основываться на некоторых принципах, в сопоставлении с которыми можно оценивать инициативы по правовой реформе. Кроме того, следует рассмотреть вопрос о каких-либо регулирующих структурах, необходимых для поддержки, контроля и обеспечения соблюдения любых обязательств, возлагаемых на государственные или частные структуры. Наконец, региональная и международная правовая унификация в эпоху, в которую доминирует Интернет, часто является жизненно важным элементом достижения целей правовой реформы, помогая избежать появления структур, занимающихся регулятивным арбитражем между государствами.

II. ЮРИДИЧЕСКАЯ ОПРЕДЕЛЕННОСТЬ

В этом разделе руководства рассмотрены вопросы юридической действительности, правового обеспечения и допустимости электронных сообщений, способные затруднить внедрение и использование электронной торговли.

Во многих странах имеются потенциальные ограничения на использование электронных средств связи, поскольку в нормативных актах предусматриваются определенные требования формы, такие, как письменная форма, подпись и подлинник. Эти требования формы в законодательстве стран вызывают некоторую степень неопределенности в том, что касается юридической действительности использования электронных сообщений для определенных целей, таких, как заключение договоров, выставление счетов или представление электронных подтверждающих документов. Проблемы могут возникать не только в национальном масштабе: такого рода юридическая неопределенность может также серьезно мешать международной торговле. Поскольку электронные сообщения становятся исключительно важной частью многих сообщений и операций, во всем мире ощущается растущая необходимость обеспечения того, чтобы нормативно-правовая база была изменена, обеспечив их юридическую действительность.

Некоторые страны - участницы СПЕКА уже приняли меры по решению вопросов юридической определенности. В Казахстане в 2003 году был принят закон "Об электронном документе и электронной цифровой подписи"[18]; в 2002 году в Таджикистане принят закон "Об электронном документе"[19]; а в Туркменистане в 2000 году был принят закон "Об электронном документе"[20].

Этот раздел призван обрисовать некоторые вопросы, которые возникают при использовании электронных сообщений, и дать анализ соответствующих международных тенденций в этой области. В нем будут рассмотрены следующие вопросы:

- юридическое признание электронных сообщений
- требования формы применительно к письменному виду, подписи и подлиннику документа
- сохранение сообщений, содержащих данные
- признание иностранных электронных документов и подписей
- допустимость электронных свидетельств
- заключение и действительность контрактов

---

[18] От 7 января 2003 года. Текст на русском языке имеется по адресу: http://www.cis-legal-reform.org/document.asp?id=8048.

[19] От 10 мая 2002 года. Текст на русском языке имеется по адресу: http://www.cis-legal-reform.org/document.asp?id=6037.

[20] От 19 декабря 2000 года. Текст на русском языке имеется по адресу: http://www.cis-legal-reform.org/document.asp?id=4979.

- признание контрагентами сообщений, содержащих данные.

A. Юридическое признание электронных сообщений

Электронная торговля ведется путем обмена электронными сообщениями или информационными сообщениями. Обеспечение того, чтобы сообщения не считались незаконными или недействительными лишь на основании их электронной формы крайне важно для развития электронной торговли. Поэтому, возможно, потребуются меры для того, чтобы в законодательстве страны не проводилось дискриминации, генерирования, хранения или передачи информации в электронной форме.

Этой цели служит Типовой закон ЮНСИТРАЛ 1996 года, где в статье 5 содержится следующее положение:

> *Информация не может быть лишена юридической силы, действительности или исковой силы на том лишь основании, что она составлена в форме сообщения данных.*

Вместо того, чтобы подходить к вопросу о подтверждении информационных сообщений бессистемным образом, цель Типового закона 1996 года заключается в том, чтобы дать общее положение, которое охватывает все формы электронных сообщений и предоставления электронной информации. Цель этого положения заключается в том, чтобы обеспечить, чтобы дискриминация не могла возникать только на основании электронного характера сообщения.

Что касается сферы охвата типовых законов, то оба они предусматривают широкие определения используемых терминов. Термин "сообщение данных" используется для обозначения как информации, содержащейся в данных, так и сообщения, содержащего данные, тем самым это положение будет охватывать как электронные сообщения - оферты и акцепты, которые составляют электронный договор, - так и информационные сообщения, которые просто передают информацию, такие, как электронный счет или сообщение, уведомляющее о сроке прибытия судна. Цель этого - охватить все виды ситуаций, в которых генерируется, хранится или передается информация, независимо от используемого средства.

B. Требования формы

Многие нормативные акты предусматривают требование составления документов в письменном виде или подписания договора. В этой связи нет определенности в том, что касается действительности или правовой обеспеченности электронных сообщений или подписей. Поэтому для содействия электронной торговле, возможно, потребуется внести поправки в положения законодательства, устраняющие юридические препятствия для электронных сообщений, либо путем снятия требования о письменной форме, подписях и подлиннике вообще, либо путем введения альтернативной действительной формы, которая может использоваться для электронных сообщений.

Бумажные документы служат нескольким возможным функциям, включая обеспечение того, чтобы содержание документа оставалось неизменным с течением времени, а также того, чтобы информация представлялась в форме, которая могла бы быть допустимой для судов и государственных органов. В частности, при сделках на большие суммы возможность

представить документ в подтверждение того, что данная сделка имела место, считается необходимой мерой защиты от мошенничества. Устранение мошенничества - не единственная причина, обусловливающая такое требование. Требования формы могут также служить напоминанием сторонам сделки о значении их обязательств. Таким образом, по-прежнему существует законная причина сохранения таких требований формы.

Поэтому электронный эквивалент требования бумажного документа или подписи должен отвечать той цели, которой обусловлены требования письменной формы, подписания и подлинника, давая возможность выполнения этих функций электронными средствами.

1. Письменная форма

В большинстве правовых систем имеется множество нормативных актов, предусматривающих, что некоторые договоры должны заключаться в виде письменного документа или в той или иной конкретной форме. Такие требования могут быть предусмотрены в общих нормативных актах по вопросам толкования или в положениях самих нормативных актов по конкретным вопросам. Такие положения могут исключать договоры, которые, например, заключаются с использованием электронных средств, или по крайней мере могут вызвать вопрос о том, был ли договор заключен юридически действительным образом.

Одно из средств расширения требования формы можно найти в пункте 1 статьи 9 Конвенции 2005 года:

> *Ничто в настоящей Конвенции не требует, чтобы сообщение или договор составлялись или подтверждались в какой-либо конкретной форме.*

Далее в пункте 2 статьи 9 указывается:

> *В случаях, когда законодательство требует, чтобы сообщение или договор были представлены в письменной форме, или предусматривают наступление определенных последствий в случае отсутствия письменной формы, это требование считается выполненным путем представления электронного сообщения, если содержащаяся в нем информация является доступной для ее последующего использования.*

В этих положениях выделена цель требования письменной формы - чтобы информация была доступна и считываема в будущем - и соответственно предусматривая, что электронные сообщения способны выполнить это требование, если они направляются в такой форме, которая позволяет получать доступ к ним при необходимости. В Европе директива об электронной торговле следует сходному подходу, требуя в пункте 1 статьи 9, чтобы государства-члены "*обеспечили, чтобы их правовая система допускала заключение контрактов с использованием электронных средств*".

Общий подход, подтверждающий действительность использования электронных сообщений и документов, открывает дорогу для формирования более благоприятных условий развития электронной торговли, чем несистематический подход, предусматривающий внесение по мере необходимости поправок в те или иные нормативные

акты. Такой несистематический подход чреват той опасностью, что не будут внесены изменения в некоторые важные законы, а также тем, что затормозится развитие электронной торговли, если применяемое законодательство будет толковаться столь узким образом, что оно будет ограничивать использование новых научно-технических достижений и средств связи.

Может потребоваться предусмотреть отступления от этого принципа в отношении некоторых видов договоров. В пункте 3 статьи 6 Типового закона 1996 года предусматривается основание формулирования исключений государствами, принимающими этот закон:

"Положения настоящей статьи не применяются в следующих случаях…"

В то время как Конвенция 2005 года в статье 3 устанавливает:

Стороны могут исключать применение настоящей Конвенции или отступать от любого из ее положений или изменять ее действие.

2. Подписи

Кроме того, в некоторых случаях нормы законодательства устанавливают требование подписания письменного документа, например в некоторых странах договор купли-продажи на сумму свыше определенного уровня должен быть подписан, иначе он не имеет правового обеспечения. Даже, если в законодательстве не дается определения подписи, в котором прямо говорится о ручке и чернилах, может иметься определенная расплывчатость в том, что касается действительности электронной подписи и ее обеспеченности правовой санкцией в данной стране.

Подпись выполняет несколько функций, включая идентификацию лица или установление связи между лицом и содержанием документа. В зависимости от характера документа подпись может также служить подтверждением намерения подписавшегося быть связанным содержанием договора или удостоверением того, что данное лицо присутствовало в данном месте в данное время. Поэтому подпись может служить нескольким разным целям в зависимости от вида документа, снабженного ею. Некоторые юридические акты, например завещание, должны быть подписаны в присутствии свидетелей, что обеспечивает еще большую надежность.

Поскольку подписи выполняют разные функции в зависимости от того, засвидетельствованы ли они, с ними связаны разные уровни надежности. Один из вариантов внесения поправок в нормы законодательства - предусмотреть электронный эквивалент всех различных видов и уровней требований к подписи. Однако даже если разные уровни электронной подписи могут служить воспроизведению различных целей традиционных подписей, положение, необходимое для реализации таких функций, может оказаться чересчур технически сложным. Это может оказаться нежелательным по ряду соображений. Такого рода нормы могут не вполне годиться для того, чтобы учесть новые научно-технические достижения, а также могут быть чересчур тесно связаны с какой-либо конкретной технологией, не получившей распространения в коммерческой области.

Поэтому формулировка таких норм может связывать нормативные акты с конкретным периодом развития технологии, вместо того, чтобы создавать юридическую структуру, основанную на базовых правовых принципах.

Поэтому в этих типовых законах основное внимание в целом уделяется двум главным функциям подписей - идентификации автора документа и указанию того, что автор согласен с содержанием документа.

Конвенция 2005 года в пункте 3 статьи 9 устанавливает следующее:

"В случаях, когда законодательство требует, чтобы сообщение или договор были подписаны стороной, или предусматривает наступление определенных последствий в случае отсутствия подписи, это требование считается выполненным в отношении электронного сообщения, если:

a) использован какой-либо способ для идентификации этой стороны и указания намерения этой стороны в отношении информации, содержащейся в электронном сообщении;

b) этот способ:

i) либо является настолько надежным, насколько это соответствует цели, для которой электронное сообщение было подготовлено или передано с учетом всех обстоятельств, включая любые соответствующие договоренности;

ii) либо, как это фактически продемонстрировано на основании самого способа или с помощью дополнительных доказательств, позволил выполнить функции, описанные в подпункте a) выше.

При таком подходе определяются функции, обеспечиваемые подписью, и не устанавливается форма, которую должна иметь электронная подпись. Цитированная норма предусматривает, что для того, чтобы быть действительной, электронная подпись должна давать возможность идентифицировать сторону и подтвердить целостность содержания сообщения.

В общем плане в типовых законах также используется формулировка, что метод должен быть "настолько надежным, насколько это соответствует цели", для которой создано или передано информационное сообщение. Это позволило обойтись в указанной норме от установления технических требований, не препятствуя тому, чтобы электронные подписи использовались и для других функций. При определении пригодности данного метода, можно было бы учесть различные юридические, технические и коммерческие факторы. Пригодность используемого метода будет также зависеть от характера коммерческой деятельности, суммы и размеров сделки и связей между контрагентами, цели подписи, принятия таких методов в данной отрасли и от любых положений о механизмах обеспечения.

Типовой закон 1996 года ставит цели установить, что функциональный эквивалент подписи сам по себе будет обеспечивать юридическую действительность; поэтому в нем вопрос юридической действительности оставлен на усмотрение законодательства стран. Как Типовой закон 1996 года, так и Конвенция 1995 года устанавливают, что электронные подписи должны соответствовать требованиям, установленным в законе. Поэтому в них принят подход обеспечения минимальных требований к подписям. Вопросы электронных подписей рассматриваются подробнее в разделе III.C ниже.

3. Подлинник

Когда посылается электронное сообщение, получатель получает не то же самое сообщение, которое было напечатано отправителем, а его точную копию. Всякий раз, когда это сообщение записывается, считывается или передается, с него делается копия. Сама эта копия может пройти через несколько стадий обработки в ходе пересылки или хранения, таких, как уплотнение, разуплотнение, шифрование или форматирование тем или иным образом. Этим оно отличается от бумажной копии, когда получатель письма в большинстве случаев получает не копию письма, а его подлинник.

Юридические требования изготовления подлинного документа в первую очередь касаются документов, удостоверяющих право собственности и оборотных документов. Цель требований изготовления подлинника документа обычно заключается в том, чтобы обеспечить сохранность содержания документа и его неизменность после его первоначального составления или пересылки. Электронный эквивалент должен ставить задачу обеспечения тех же мер защиты целостности.

Поэтому требования законодательства к составлению "подлинника" документа вряд ли будут выполнены применительно к представлению электронных документов, если только в характер этих положений не будут внесены некоторые изменения.

В Конвенции 2005 года такое признание электронных документов достигается с помощью следующих положений пунктов 4 и 5 статьи 9:

> *4. В случаях, когда законодательство требует, чтобы сообщение или договор предоставлялись или сохранялись в их подлинной форме, или предусматривает наступление определенных последствий в случае отсутствия подлинной формы, это требование считается выполненным в отношении электронного сообщения, если:*
>
> *a) имеются надежные доказательства целостности содержащейся в нем информации с момента, когда оно было впервые подготовлено в его окончательной форме в виде электронного сообщения или в каком-либо ином виде; и*
>
> *b) при необходимости предоставления содержащейся в нем информации, эта информация может быть продемонстрирована лицу, которому она должна быть предоставлена.*
>
> *5. Для целей пункта 4 a):*

a) критерием оценки целостности является сохранение информации в полном и неизмененном виде, без учета добавления любых индоссаментов и любых изменений, происходящих в обычном процессе передачи, хранения и демонстрации; и

b) требуемая степень надежности оценивается с учетом цели, для которой информация была подготовлена, и всех соответствующих обстоятельств.

В этом положении Конвенции 2005 года основное внимание уделяется функции обеспечения целостности документа; оно позволяет электронным документам выполнить это требование в случае наличия надежного средства обеспечения неизменности содержания. То, что форматирование документа было изменено при обработке электронного документа или что в конце сообщения было помещено электронное подтверждение его подлинности, не будет считаться достаточным основанием признания недействительности документа. Критерии надежности будут зависеть от соответствующих обстоятельств. Это положение также устанавливает требование доступа к информации для любого, кто имеет право видеть ее.

C. Сохранение информационных сообщений

Хранение данных имеет огромное значение во многих сферах коммерческой практики. Сохранение документов в электронном виде может обеспечивать эффективный и экономящий площади способ сохранения больших количеств данных. Такая форма хранения документов также имеет преимущество простоты поиска. Многие нормативные акты требуют хранения письменных документов на протяжении определенного периода времени для таких целей, как бухгалтерский учет, налоговые проверки или ревизии. Могут также храниться документы, призванные подтвердить наличие контракта или владения определенными правами интеллектуальной собственности.

Поэтому требования хранения документов необходимо изменить, чтобы обеспечить юридическую действительность хранения документов в электронном формате.

Типовой закон 1996 года предусматривает сохранение информационных сообщений в своей статье 10:

1) Если законодательство требует сохранения определенных документов, записей или информации, это требование выполняется путем сохранения сообщений данных при соблюдении следующих условий:

a) информация, содержащаяся в сообщении данных, является доступной для ее последующего использования; и

b) сообщение данных сохраняется в том формате, в котором оно было подготовлено, отправлено или получено, либо в таком формате, в котором можно показать, что подготовленная, отправленная или полученная информация представлена точно; и

c) сохраняется такая информация, если таковая существует, которая позволяет установить происхождение и назначение сообщения. данных, а также дату и время его отправления или получения.

2) Обязательство сохранять документы, записи или информацию в соответствии с пунктом 1 не распространяется на любую информацию, единственная цель которой состоит в том, чтобы сделать возможным отправление или получение данного сообщения.

Это положение дает возможность удовлетворения сообщениями требования сохранения, даже если сообщение подвергается изменениям, например при форматировании, если информация, содержащаяся в сообщениях, точно отражает информационное сообщение в его первоначально посланном виде. Хотя может быть важно сохранить некоторую информацию о передаче сообщения, например, содержащуюся в блоке данных, когда он был создан или сохранен, или подтверждение получения сообщения, эти положения не устанавливают какого-либо обязательства сохранить дополнительную информацию о передаче, которая не имеет отношения к информации, содержащейся в сообщении. Тем самым, учитывается то обстоятельство, что информационные сообщения подвергаются разнообразным изменениям, которые фактически не влияют на информацию, содержащуюся в нем, однако необходимы для передачи и хранения блоков данных. К ним относятся методы уплотнения, разуплотнения, шифрования или преобразования данных для целей их хранения.

D. Признание иностранных электронных документов и подписей

Международная торговля очевидным образом требует юридического признания не только электронных документов и подписей в масштабах одной страны, но и, равным образом, иностранных документов. При внесении такого рода изменений следует обдумать вопрос о том, должно ли такое признание быть предоставлено на в точности тех же условиях, что и признание документов данной страны. Должны ли исходные посылки в чем-то различаться? Если государство ставит цель содействия международной электронной торговле, то необходимо будет предусмотреть равное признание иностранных документов и подписей.

E. Допустимость электронных доказательств

Там, где встает вопрос о действительности электронных сообщений, также может возникнуть различие во мнениях относительно допустимости электронных доказательств. Рассматривая спор, суд может потребовать доказательства данного факта. Необходимо определить, выполнят ли электронные сообщения и документы доказательственные требования суда. Хотя в некоторых странах имеются широкие доказательственные нормы, часто все же требуется выполнение формальностей применительно к некоторым видам документов, таких как завещание. В других странах действуют весьма строгие процедуры и нормы, которые должны быть соблюдены как условие принятия судом доказательств в качестве таковых.

Цель представления доказательств - в том, чтобы суд мог в большей или меньшей степени опираться на них при вынесении решения по данному делу. Поэтому для того, чтобы доказательство могло быть представлено в суде, требуется определенная степень его надежности. Во многих правовых системах имеются нормы, касающиеся как допустимости документов, так и доказательной силы этих документов. Некоторые правовые системы предусматривают строгие формальные требования в том, что касается представления документов, например нотариальная форма, в то время как в других устанавливается обязательство стороны, представляющей доказательство, обосновать возможность его использования в качестве такового, например, удостоверив надлежащее функционирование компьютерной системы, из которой выведен электронный документ. Такое обязательство доказывания может быть достаточно обременительным, поскольку для этого может оказаться необходимым привлечь нескольких экспертов, которые могут удостоверить надлежащее функционирование компьютерной системы в данное время. После того, как доказательство признано допустимым, суд переходит к стадии изучения доказательства для определения той доказательной силы, которую ему следует придать, используя такие разнообразные факторы, как вид примененной технологии.

Один из способов повышения надежности электронного документа - показать, что система, из которой он выведен, функционировала должным образом.

Статья 9 Типового закона 1996 года предусматривает допустимость электронных сообщений, устанавливая следующее:

1) При любых процессуальных действиях никакие положения норм доказательственного права не применяются таким образом, чтобы отрицать допустимость сообщения данных в качестве доказательства:

a) на том лишь основании, что оно представляет собой сообщение данных; или

b) если оно является наилучшим доказательством, которое, как этого можно разумно ожидать, может быть получено представляющим его лицом, на том основании, что оно не представлено в его подлинной форме.

2) Информации в форме сообщения данных придается надлежащая доказательственная сила. При оценке доказательственной силы сообщения данных учитывается надежность способа, с помощью которого подготавливалось, хранилось или передавалось это сообщение данных, надежность способа, с помощью которого обеспечивалась целостность информации, способа, при помощи которого идентифицировался его составитель, и любой другой соответствующий фактор.

Тем самым эта норма исключает отведение доказательства только на том основании, что оно представляется в электронной форме. В подпункте b) пункта 1 уточняется, что, если применяется принцип "наилучшего доказательства", в соответствии с которым сторона обязана представить доказательство в наилучшей из имеющихся форм, например, подлинник документа вместо копии, то тогда электронное доказательство не может быть отведено лишь на том основании, что оно не является документом в его подлинной форме.

Что касается доказательной силы, устанавливаемой для представляемых электронных сообщений и документов, то в этом положении предусмотрено несколько факторов, которые могут использоваться при определении надлежащего уровня устанавливаемой доказательной силы.

F. Заключение и действительность электронных контрактов

До начала коммерческого использования Интернета электронное заключение контрактов уже существовало в практике отношений между предприятиями с использованием электронного обмена данными (ЭОД). От связи с помощью сайтов в Интернете или электронных сообщений ЭОД отличается тем, что при ЭОД сообщения, пересылаемые между компьютерами, основываются на стандарте или коде, согласованном контрагентами. Как в национальном, так и в международном масштабе принят ряд стандартов ЭОД, а в последнее время были разработаны типовые соглашения между торговыми партнерами.

Хотя ЭОД по-прежнему используется предприятиями, Интернет открыл новые возможности ведения дел, позволяя участникам торговли, которые ранее не имели торговых связей, легко и быстро заключать сделки, даже если они находятся в разных странах. При всех своих преимуществах, это означает, что контрагенты заключают контракты не на основе взаимного соглашения. Поэтому это может вызвать некоторые юридические неясности относительно правовой обеспеченности и режима электронных контрактов.

Законодательство страны о заключении договоров может быть адекватно для урегулирования многих аспектов электронного заключения контрактов, однако некоторые моменты, такие, как место и время заключения контракта и шаги, необходимые для включения в него типовых условий, могут вызвать проблемы. Процедура, которая должна использоваться для исправления ошибок в вводе информации, - это также новая проблема, которая возникает в результате заключения контрактов с помощью сети. Возросшие возможности розничных продаж также вызывают многочисленные вопросы защиты прав потребителей.

Возможно, потребуется ввести в законодательство стран новые нормы, призванные обеспечить большую степень определенности относительно заключения договора электронными средствами.

1. Заключение и действительность контракта

Конвенция 2005 года и Типовой закон 1996 года содержат различные положения, касающиеся процесса заключения договора. Они обеспечивают юридическую определенность, связанную с использованием электронных сообщений при заключении договора, и обеспечивают то, что договор не считается не имеющим правового обеспечения лишь из-за того, что он был заключен с помощью электронных средств. Эти положения не устанавливают, как должен заключаться договор, или же шагов, которые должны быть предприняты для заключения договора, а вместо этого лишь обеспечивают возможность заключения юридически действительного договора с использованием электронных средств при условии, что выполнены все необходимые требования. Поэтому эти нормы не заменяют

традиционных норм заключения договоров, а лишь дополняют их, предусматривая возможность связи в электронной форме. Эти положения также не возлагают на контрагентов какого-либо обязательства принимать электронные средства заключения контрактов или связи, если они не захотят этого.

Признавая возможность электронного заключения контрактов, Типовой закон 1996 года в своей статье 11 устанавливает:

> *В контексте заключения контрактов, если стороны не договорились об ином, оферта и акцепт оферты могут производиться с помощью сообщений данных. В случае, когда при заключении контракта используется сообщение данных, этот контракт не может быть лишен действительности или исковой силы на том лишь основании, что для этой цели использовалось сообщение данных.*

Формулировка, использованная в этом положении, прямо устанавливает, что контракт не может быть лишен действительности или исковой силы только из-за того, что он заключается с использованием электронных средств связи, однако может быть лишен действительности на других основаниях.

Конвенция 2005 года также содержит положения о заключении контракта с помощью электронных средств. Статья 8 устанавливает:

> *1) Сообщение или договор не могут быть лишены действительности или исковой силы на том лишь основании, что они составлены в форме электронного сообщения.*

Согласно этим нормам направление оферты или акцепта в электронной форме - это недостаточное условие признания недействительности контракта; но что насчет нажатия на кнопку для согласия с условиями контракта? Достаточно ли этого для направления оферты или акцепта оферты? Единственная модель, в которой конкретно затрагивается этот вопрос, это Типовой закон Содружества об электронных операциях. В своей статье 18 этот типовой закон предусматривает:

> *1) Если только стороны не договорились об ином, оферта, акцепт оферты или любой иной вопрос, существенный для заключения или действия договора, могут быть выражены:*
>
> *a) с помощью информации в электронной форме или*
>
> *b) с помощью акта, призванного иметь своим результатом электронное сообщение, такого, как щелчок или нажатие на соответствующую икону или другое место на экране компьютера, либо голосовая команда.*

Единственная оговорка относительно включения такого условия в законодательство - то, что оно может оказаться чересчур ограничительным, не охватывая будущее развитие технологий. Хотя щелчок по иконе сегодня может быть распространенным методом заключения контрактов в сети, будет ли он использоваться и далее, или же на смену ему

придет новый метод, - это еще не ясно. Положения, которые ставят целью сделать возможной электронную торговлю и заключение электронных контрактов с использованием электронных средств, должны по возможности пытаться оставаться нейтральными по отношению к методу, используемому для достижения этой цели.

При всей очевидной полезности электронных форм связи их использование не должно обязательно навязываться контрагентом. Например, в Конвенции Организации Объединенных Наций 2005 года в статье 8 предусматривается:

> *2. Ничто в настоящей Конвенции не требует от какой-либо стороны использовать или принимать электронные сообщения, однако ее согласие на это может быть выведено из поведения этой стороны.*

В пункте 2 статьи 8 устанавливается, что ни один из контрагентов не обязан принимать электронные сообщения, если только он положительно выраженным образом или косвенным образом своими действиями не решает принять их. Разумеется, если оферта сделана с использованием электронных средств, оферент не вправе отказаться признать акцепт, выставленный в той же форме.

Государства также могут принимать решение ограничить заключение некоторых видов соглашений с использованием электронных средств.

2. Использование автоматизированных систем обмена сообщениями

Развитие технологии и программного обеспечения позволило компьютерным программам автоматически выставлять и получать электронные заказы без какого-либо участия человека. Способность электронных хозяйствующих субъектов независимо заключать контракты может создавать вопросы, касающиеся юридической действительности таких контрактов, в частности в странах, в которых требуется волеизъявление сторон.

Конвенция 2005 года предусматривает действительность использования автоматизированных систем обмена сообщениями для заключения контрактов в своей статье 12, где устанавливается следующее:

> *Договор, заключенный в результате взаимодействия автоматизированной системы сообщений и какого-либо физического лица или в результате взаимодействия автоматизированных систем сообщений, не может быть лишен действительности или исковой силы на том лишь основании, что никакое физическое лицо не осуществляло просмотра или вмешательства в отношении каждой отдельной операции, выполненной автоматизированными системами сообщений, или заключенного в результате договора.*

Эта норма предусматривает, что в тех случаях, когда электронные сообщения об оферте и акцепте создаются без участия человека, этого недостаточно для признания договора лишенным исковой силы.

3. Инкорпорация отсылкой

Условия договора обычно устанавливаются в соглашении между сторонами - либо положительно выраженным образом в тексте соглашения, либо косвенным образом в законе, обычае или практике, либо выводятся из действий сторон. Однако в некоторых случаях постоянных связей между контрагентами такие условия часто даются с отсылкой к отдельному документу, не будучи непосредственным образом зафиксированы в контракте. Такая инкорпорация отсылкой - это признанная коммерческая практика. Для того чтобы обеспечить юридическую действительность такой инкорпорации в электронной среде, в Типовом законе 1996 года в статье 5-бис предусматривается:

> *Информация не может быть лишена юридической силы, действительности или исковой силы на том лишь основании, что она не содержится в сообщении данных, обусловливающем наличие такой юридической силы, а лишь упоминается в таком сообщении данных.*

4. Запрос оферты

Вопрос о том, направляет ли сайт в Интернете, продающий определенный товар, оферту на покупку данного товара или просто-напросто запрос оферты, вызвал продолжительные споры. Если структура сайта такова, что он считается направляющим оферту на продажу перечисленных товаров, то тогда при условии безусловного акцепта этой оферты может быть заключен юридически действительный контракт. В случае ограниченного наличия товаров для продажи владелец сайта мог бы оказаться в затруднительном положении, если заключено больше контрактов, чем имеется товаров для продажи. Поэтому обычно считается, что на сайте направляются запросы оферт. Схожий принцип может касаться и массовой почтовой рассылки.

Чтобы уточнить этот момент, Конвенция 2005 года предусматривает в статье 11 следующее:

> *Предложение заключить договор, сделанное посредством одного или нескольких электронных сообщений, которое адресовано не одной или нескольким конкретным сторонам, а является общедоступным для сторон, использующих информационные системы, включая предложения, в которых используются интерактивные прикладные средства для размещения заказов через такие информационные системы, следует считать приглашением представлять оферты, если только в нем ясно не указывается намерение стороны, делающей предложение, считать себя связанной в случае акцепта.*

5. Инкорпорация условий контрактов

Обеспечение юридически действительной инкорпорации условий в контракте может быть связано с принятием некоторых мер, призванных обратить внимание контрагента на эти условия. Наличие условий контрактов рассматривается в статье 13 Конвенции 2005 года:

Ничто в настоящей Конвенции не затрагивает применения любой нормы права, которая может требовать от стороны, оговаривающей некоторые или все условия договора посредством обмена электронными сообщениями, предоставить каким-либо конкретным образом в распоряжение другой стороны те электронные сообщения, которые содержат условия договора, и не освобождает сторону от юридических последствий невыполнения этого требования.

Право договоров обычно требует, чтобы сторона договора могла знакомиться с условиями договора до подписания соглашения. Иначе в некоторых случаях условия не считаются включенными в договор и поэтому не являются обязательными для данной стороны.

Распространенный метод включения условий в договор - с помощью сайта в Интернете, где поставщик предлагает клиенту нажать на кнопку, если он согласен с условиями договора, прежде чем заключить договор. В противном случае поставщик может дать гиперссылку на вебстранице, где помещены условия договора. Инкорпорация условий с помощью этого метода, впрочем, не столь надежна, поскольку согласие тут предполагаемо, нежели положительно выражено. Поэтому обязательный характер условий может быть оспорен из-за недостаточной прозрачности, например, если ссылка недостаточно заметна для пользователя.

Кроме того, что условия должны быть доступны, клиент должен иметь возможность сохранить их для последующего изучения. Это предусмотрено в пункте 2 статьи 10 директивы об электронной торговле, в которой устанавливается следующее:

Коммерческие и общие условия контрактов, предоставленные получателю, должны быть предоставлены таким образом, чтобы тот мог хранить и воспроизводить их.

6. Предоставление информации о процессе заключения контрактов

Неоднозначен также вопрос о том, как и когда заключается электронный контракт. Например, когда заключается контракт - когда послано или когда получено сообщение об акцепте? И где он заключается? Там, где клиент щелкает по кнопке "Я согласен" на экране своего компьютера, или там, где находится поставщик?

Эти вопросы будут решаться нормами договорного права стран. Однако для того, чтобы снять неопределенности, в частности, в отношении контрактов с потребителями, целесообразно указать, что означает каждый шаг в процессе заключения контракта и когда и где это приведет к заключению контракта.

Директива об электронной торговле устанавливает, что клиент должен быть полностью информирован о тех шагах, которые должны быть предприняты для заключения контракта. Пункт 1 статьи 10 устанавливает:

Помимо других информационных требований, установленных в нормативных актах Сообщества, государства-члены обеспечивают, за исключением тех случаев, когда

иное согласовано сторонами, не являющимися потребителями, чтобы до размещения заказа получателем услуги поставщик услуг четко, полно и недвусмысленно предоставлял, по крайней мере, следующую информацию:

a) различные технические шаги, ведущие к заключению контракта;

b) будет ли заключенный контракт сохранен поставщиком услуг и будет ли он доступен;

c) технические средства выявления и исправления ошибок при вводе до размещения заказа;

d) предлагаемые языки контракта.

Эти требования, которые предусматривают, главным образом, предоставление информации на сайтах, не касаются обмена сообщениями по электронной почте.

7. Исправление ошибок

В процессе заключения электронных контрактов неизбежно будут допускаться ошибки. Заказ может быть по ошибке размещен дважды, или же необходимое количество товара может быть впечатано неправильно. Можно ли исправить такую ошибку? Есть на сайте возможность отменить заказ, сделанный по ошибке, или способ связаться с отправителем, чтобы объяснить ошибку?

Конвенция 2005 года в статье 14 устанавливает следующее:

1. В случаях, когда какое-либо физическое лицо допускает ошибку при вводе информации в электронное сообщение, являющееся предметом обмена с автоматизированной системой сообщений другой стороны, и эта автоматизированная система сообщений не предоставляет этому лицу возможности исправить ошибку, такое лицо или сторона, от имени которой действовало это лицо, имеет право отозвать ту часть электронного сообщения, в которой была допущена ошибка при вводе информации, если:

b) это лицо или сторона, от имени которой действовало это лицо, уведомляет другую сторону об ошибке в кратчайший возможный срок после обнаружения ошибки и указывает, что в электронном сообщении им была сделана ошибка; и

c) это лицо или сторона, от имени которой действовало это лицо, не использовали полученные от другой стороны товары или услуги, если таковые имеются, и не получали от них никакой материальной выгоды или стоимости.

Это положение касается только физических лиц и поэтому служит механизмом защиты прав потребителей, нежели нормой, применимой в случае сделок между предприятиями. Директива об электронной торговле идет дальше, требуя от поставщиков услуг предоставить

эффективные технические механизмы исправления ошибок ввода. В пункте 2 статьи 11 предусматривается:

Государства-члены обеспечивают, что, за исключением тех случаев, когда иное согласовано сторонами, не являющимися потребителями, поставщик услуг предоставляет получателю услуги, надлежащие, эффективные и доступные технические средства, позволяющие ему выявлять и исправлять ошибки ввода до размещения заказа.

8. Определение отправителя информационного сообщения

Как и в случае письменных документов, может возникать вопрос о том, действительно ли данный документ послан предполагаемым отправителем сообщения. В случае бумажного документа возможно предположение, что подпись на документе была подделана. В электронной среде можно утверждать, что лицо, фактически направившее сообщение, не имело на это разрешения.

В Типовом законе 1996 года вводится презумпция, что в некоторых случаях информационное сообщение будет считаться происходящим от отправителя, хотя эта презумпция снабжена оговоркой на тот случай, когда получатель по той или иной причине знал или должен был знать о том, что информационное сообщение на самом деле поступило не от отправителя. В нем уточняется, что автор информационного сообщения связан им, если оно было послано им. Эта презумпция также сохраняет силу в том случае, когда сообщение послано кем-либо, уполномоченным на то составителем.

Статья 13 устанавливает:

1) Сообщение данных считается сообщением данных составителя, если оно было отправлено самим составителем.

2) В отношениях между составителем и адресатом сообщение данных считается сообщением данных составителя, если оно было отправлено:

a) лицом, которое имело полномочия действовать от имени составителя в отношении этого сообщения данных; или

b) информационной системой, запрограммированной составителем или от его имени функционировать в автоматическом режиме.

3) В отношениях между составителем и адресатом адресат имеет право считать, что сообщение данных является сообщением данных составителя, и действовать исходя из этого предположения, если:

a) для того чтобы установить, что сообщение данных является сообщением данных составителя, адресат надлежащим образом применил процедуру, предварительно согласованную с составителем для этой цели; или

b) сообщение данных, полученное адресатом, явилось результатом действий лица, отношения которого с составителем или любым представителем составителя дали такому лицу возможность получить доступ к способу, используемому составителем.

Если адресат получает уведомление о том, что отправитель не получал сообщение, тогда презумпция теряет силу, как это предусмотрено в пункте 4 статьи 13:

Пункт 3 не применяется:

a) с момента получения адресатом уведомления составителя о том, что сообщение данных не является сообщением данных составителя, при условии, что адресат имеет в своем распоряжении разумное время для совершения надлежащих действий; или

b) в случае, предусмотренном в пункте 3 b), в любое время, когда адресату стало известно или, если бы он проявил разумную осмотрительность или использовал любую согласованную процедуру, должно было стать известно о том, что сообщение данных было получено не от составителя.

Эта норма устанавливает, что адресат не связан информационным сообщением с того момента, когда адресат получает уведомление о том, что оно поступило не от адресата. До этого момента адресат вправе исходить из того, что данное сообщение было послано адресатом.

9. Подтверждение получения

После подтверждения заказа многие Интернет-компании направляют подтверждение о получении заказа. Это дает покупателю гарантию того, что процесс заказа был успешным и что контракт был действительно заключен. В Европе поставщик обязан подтвердить получение заказа, если он ведет дела с потребителями, а также предприятиями, если не установлено иное.

Статья 11 директивы ЕС об электронной торговле предусматривает следующее:

Поставщик услуг также должен без необоснованного промедления подтвердить с использованием электронных средств получение заказа получателя.

Этот вопрос также рассматривается в Типовом законе 1996 года, хотя Типовой закон основывается на той посылке, что отправитель может по своему выбору воспользоваться или не воспользоваться процедурой подтверждения. Эта норма лишь устанавливает время получения подтверждения, не рассматривая любых прочих юридических последствий.

Какова ситуация тогда, когда подтверждение запрошено, но не получено, а отправитель прямо не сообщил, что информационное сообщение не имеет силы до получения подтверждения? Связан ли по-прежнему отправитель сообщения юридическим обязательством по отношению к этой стороне или же он может направить оферту другой

стороне? Очевидный ответ на этот вопрос - предусмотреть срок подтверждения оферты, указав последствия неполучения подтверждения в этот срок, однако там, где такого не предусмотрено, могут возникнуть проблемы. Типовой закон 1996 года пытается урегулировать эту ситуацию, установив в пункте 4 статьи 14:

> *В случае, когда составитель не указал, что сообщение данных обусловливается получением подтверждения, и подтверждение не было получено им в течение оговоренного или согласованного срока, либо, если такой срок не был оговорен или согласован, в течение разумного срока, составитель:*
>
> *a) может направить адресату уведомление, указав в нем, что подтверждение получено не было, и установив разумный срок, к которому подтверждение должно быть получено; и*
>
> *b) если подтверждение не получено в течение срока, установленного в подпункте a), может после уведомления об этом адресата, считать сообщение данных неотправленным или осуществить любые другие права, которые он может иметь.*

В этом положении прямо указывается, что отправитель сообщения не вправе сразу же перестать брать в расчет информационное сообщение, как если бы оно не было послано, а должен представить адресату дополнительное уведомление.

10. Время и место отправки и получения

Хотя положения законодательства стран и/или контрактов будут определять те шаги, которые необходимы для заключения контракта, остаются вопросы о том, в какой момент сообщение считается отправленным и откуда. Это имеет юридическое значение в плане места и времени заключения контракта и может также иметь значение в случаях споров при определении применимого права или судебного органа в соответствии с нормами международного частного права.

Имеется несколько возможных толкований того, когда сообщение считается посланным. Должно ли информационное сообщение считаться посланным, как только оно отправлено? Что происходит, если система связи отправителя допускает сбой? Когда сообщение считается полученным адресатом? Когда адресат фактически читает сообщение или когда сообщение может быть прочитано адресатом?

В Конвенции 2005 года в статье 10 проводится прагматический подход к определению времени и места отправки и получения электронных сообщений:

> *1. Временем отправления электронного сообщения является момент, когда оно покидает информационную систему, находящуюся под контролем составителя или стороны, которая отправила его от имени составителя, или, если электронное сообщение не покинуло информационную систему, находящуюся под контролем составителя или стороны, которая отправила его от имени составителя, момент получения электронного сообщения.*

2. Временем получения электронного сообщения является момент, когда создается возможность для его извлечения адресатом по электронному адресу, указанному адресатом. Временем получения электронного сообщения по другому электронному адресу адресата является момент, когда создается возможность для его извлечения адресатом по этому адресу и адресату становится известно о том, что электронное сообщение было отправлено по этому адресу. Считается, что возможность извлечения электронного сообщения адресатом создается в тот момент, когда оно поступает на электронный адрес адресата.

Определение в Конвенции 2005 года времени, когда что-либо отправлено или получено, связано с тем, кто обладает контролем над конкретным сообщением. Сообщение считается отправленным, когда оно поступает в информационную систему за пределами контроля отправителя. Аналогичным образом подтверждение считается действительным, когда сообщение поступает в специальную информационную систему получателя. Однако если такой специальной информационной системы не имеется, сообщение не будет считаться полученным до того, как получатель фактически получает его.

Вопрос о том, откуда направлено сообщение или где оно получено, может вызвать еще большую неопределенность. Это связано с тем, что физическое местоположение сторон может быть неизвестно в данный момент времени или может меняться. Поэтому Конвенция 2005 года содержит дополнительные уточнения относительно того места, в котором считается посланным и полученным электронное сообщение.

Статья 10 гласит:

3. Электронное сообщение считается отправленным в месте нахождения коммерческого предприятия составителя и считается полученным в месте нахождения коммерческого предприятия адресата, как они определяются в соответствии со статьей 6.

4. Пункт 2 настоящей статьи применяется независимо от того, что место, в котором находится информационная система, поддерживающая электронный адрес, может отличаться от места, в котором электронное сообщение считается полученным в соответствии с пунктом 3 настоящей статьи.

Конвенция также устанавливает в статье 6 нормы определения места нахождения коммерческого предприятия сторон.

1. Для целей настоящей Конвенции коммерческим предприятием какой-либо стороны считается место, указанное этой стороной, если только другая сторона не докажет, что сторона, сделавшая такое указание, не имеет коммерческого предприятия в этом месте.

2. Если какая-либо сторона не указала коммерческого предприятия и имеет более одного коммерческого предприятия, коммерческим предприятием для целей настоящей Конвенции является то, которое с учетом обстоятельств, известных

сторонам или предполагавшихся ими в любое время до или в момент заключения договора, имеет наиболее тесную связь с этим договором.

3. Если физическое лицо не имеет коммерческого предприятия, принимается во внимание его обычное местожительство.

4. Какое-либо местонахождение не является коммерческим предприятием лишь в силу того, что в этом месте: a) находятся оборудование и технические средства, поддерживающие информационную систему, используемую какой-либо стороной в связи с заключением договора; или b) эта информационная система может быть доступна для других сторон.

В пункте 5 статьи 6 Конвенция также предусматривает, что использование доменного имени конкретной страны или конкретного электронного адреса не определяет местонахождения предприятия:

То обстоятельство, что какая-либо сторона использует доменное имя или адрес электронной почты, связанные с какой-либо конкретной страной, не создает само по себе презумпции, что ее коммерческое предприятие находится в этой стране.

G. Признание сторонами информационных сообщений

Обеспечение признания информационных сообщений, не составляющих часть контракта, однако имеющих отношение к конкретному исполнению договорных обязательств, например предложение произвести оплату или признание долга, также имеет значение. Хотя это обеспечивается принятием положения, предусматривающего недискриминацию на том основании, что сообщение является электронным, во многих типовых нормативных актах было сочтено важным также включить конкретное положение, предусматривающее признание сторонами информационных сообщений.

В статье 12 Типового закона 1996 года предусматривается:

1) В отношениях между составителем и адресатом сообщения данных волеизъявление или другое заявление не может быть лишено юридической силы, действительности или исковой силы на том лишь основании, что для этой цели использовалось сообщение данных.

H. Заключение

В этом разделе рассмотрены некоторые важные вопросы, связанные с действительностью, юридическим обеспечением и допустимостью электронных сообщений. В нем также представлены подходы, используемые на международном и региональном уровнях. Однако при определении наиболее целесообразного подхода для законодательства страны необходимо учитывать ныне действующие нормы ее законодательства, касающиеся требований формы, письменной формы и подписания, доказательственных требований, а также особенностей, связанных с заключением договоров.

Вопросы, вытекающие из этого раздела о юридической определенности, включают следующее:

- Обеспечение того, чтобы требования формы, письменной формы подписания и подлинников могли быть выполнены с использованием электронных средств
- Обеспечение юридического признания электронных средств хранения данных
- Обеспечение юридического признания иностранных электронных документов и подписей
- Возможность признания электронных свидетельств
- Обеспечение заключения и юридической действительности электронных контрактов.

I. Литература

Международная торговая палата (МТП), Общая практика для международных торговых операций, заверенных в цифровой форме, 2001 год, имеется на http://www.iccwbo.org/home/guidec/guidec.asp.

Конвенция Организации Объединенных Наций об использовании электронных сообщений в международных договорах - текст и пояснительное примечание секретариата ЮНСИТРАЛ: имеется на http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf.

III. ЮРИДИЧЕСКАЯ НАДЕЖНОСТЬ ИКТ

В этом разделе доклада рассмотрены вопросы, связанные с надежностью электронной торговли. Для обеспечения защищенной среды для предприятий, государственных органов и частных лиц необходим свой уровень надежности. Коммерческая среда не может быть динамичной без гарантии того, что электронные данные подписи и свидетельства будут юридически действительными и допустимыми при заключении договоров, как об этом говорилось в разделе II доклада. Подобным образом доверие к банковской системе не будет прочным, если клиенты не будут уверены в конфиденциальности и безопасности электронной связи. С точки зрения государственных органов, информационно-коммуникационные технологии должны обеспечивать наличие данных, когда в них возникнет необходимость, а также достаточно высокую надежность обеспечения того, что данные не были изменены.

В этом разделе будут рассмотрены вопросы целостности, подтверждения подлинности и конфиденциальности, а также методы устранения риска безопасности в интерактивной среде, в частности, использование электронных подписей.

A. Вопросы

1. Целостность и подтверждение подлинности

Документы, написанные чернилами на бумаге, трудно изменить, не оставив следов. В отличие от изменения рукописного документа изменение электронных данных не столь заметно. Из-за простоты изменения документа трудно определить, каким образом был изменен документ и когда именно. Например, электронный контракт мог быть изменен любой из сторон в некоторый момент после достижения соглашения. Для решения этой проблемы защиты были разработаны электронные подписи, обеспечивающие надлежащий уровень юридической уверенности в электронных сообщениях и при электронном заключении контракта.

2. Конфиденциальность

В традиционной среде уже давно используются методы защиты, призванные обеспечить защиту и конфиденциальность бумажных документов и досье. Меры по защите неприкосновенности документов традиционно связываются с закрытыми помещениями и шкафами и, возможно, системами сигнализации для обнаружения проникновения в служебные помещения. В зависимости от характера защищаемых документов может потребоваться разная степень защиты - от банковских сейфов для обеспечения сохранности денег или облигаций до простых шкафов для хранения дел.

Как у частных лиц, так и у коммерческих предприятий есть причины желать сохранения конфиденциальности определенной информации. Предприятия часто включают положения о конфиденциальности в договоры найма своих работников, если они озабочены возможностью разглашения секретов фирмы или информационных процессов конкурентам. Некоторые профессии устанавливают требования конфиденциальности как элемент профессиональных обязанностей, например, неразглашение информации о клиентах - для

адвокатов и пациентах - для врачей. На государственные органы также будет распространяться обязанность сохранять конфиденциальность информации о частных лицах и компаниях.

Точно так же частные лица могут захотеть ограничить использование их личных данных. Защита использования, сбора и передачи личных данных признается в некоторых странах в нормативных актах о защите данных.

B. Снижение рисков для безопасности ИКТ

Признанием необходимости серьезно относиться к мерам безопасности можно считать все более широкое использование сетевых фильтров для защиты данных организации и виртуальных частных сетей для контроля за доступом к данным или сети организации.

Как отдельным лицам, так и предприятиям и государственным органам необходимо учитывать влияние электронной торговли на защищенность их личных данных, электронных данных и деловой инфраструктуры. Например, в финансовом секторе огромное значение имеет бесперебойная работа информационных систем. Невозможность войти в систему может привести к судебным искам в результате, например, финансовых потерь, вызванных несвоевременным проведением платежа.

Защита информации - это область, которая развилась очень быстро и продолжает развиваться в результате научно-технических достижений. Большая работа была проделана для определения рисков, возникающих в электронной среде, и возможных методов их снижения или ограничения. В частности, были разработаны механизмы установления того, где существуют риски, и введения стандартов или процедур, которые могут использоваться для уменьшения рисков.

Цели безопасности излагаются в кодексах практики, таких как "Кодекс практики по управлению информационной безопасностью" ИСО/МЭК 17799:20000. Они включают распределение ответственности за управление базой данных, файлами, программным обеспечением и процедурами по уменьшению числа случаев мошенничества или эксплуатации с нарушением установленных режимов путем отбора работников и использования соглашений о конфиденциальности на рабочем месте, обязательных для работников. Кодекс также предусматривает методы предотвращения несанкционированного доступа к системе и рабочим зонам, а также предусматривает обеспечение соблюдения применимого законодательства. Поэтому в таких кодексах предпринята попытка дать универсальные средства обеспечения учета коммерческой структурой всех рисков безопасности и принятия ею мер по сведению их к минимуму с максимальной эффективностью.

C. Цифровые подписи

О некоторых юридических мерах по содействию использованию электронных (или цифровых) подписей говорилось в разделе II.B.2. В этом разделе речь пойдет в основном о функциях безопасности, обеспечиваемых электронными подписями, которые должны

сделать возможным опознавание сторон операции и обеспечение целостности содержимого документа, а также о средствах регулирования этих функций.

Когда они поддерживают контакт в электронной среде, стороны осуществляемой по сети сделки должны иметь возможность обеспечить, чтобы сообщения, посылаемые ими друг другу, были получены адресатом в неизмененном виде. Им также необходимо удостовериться в том, что другая сторона сделки - именно та, каковой она себя называет. Имеются большие различия между техническими способами создания цифровых подписей, как и в степени достижения ими поставленной цели. Такая степень надежности варьируется в зависимости от используемого способа, который в некоторых случаях может быть столь простым, как помещение фамилии в конце электронного сообщения, использование личного идентификационного номера (ЛИН) или паролей к биометрическим системам, таким, как скан сетчатки или отпечатки пальцев, и криптография. Данные или подпись (например, отпечаток пальца), которые прилагаются к сообщению, указывают на источник сообщения (откуда оно поступает), выступая в качестве функционального эквивалента рукописной подписи.

В зависимости от уровня риска (финансового или нефинансового), связанного с данным видом операции, следует использовать разные уровни обеспечения безопасности, а следовательно и разные уровни защиты подписи. Отсканированная рукописная подпись не даст высокого уровня безопасности, не позволяя подтвердить личность отправителя сообщения или обеспечить его целостность. Отсканированная подпись может быть приложена к совершенно другому документу, а содержимое документа может быть изменено без каких-либо следов этого для получателя. С другой стороны, подпись, разработанная с использованием криптографии множественного доступа, дает более высокую степень безопасности, поскольку она связана с математическими алгоритмами, которые практически невозможно расшифровать, поэтому такие подписи могут использоваться как для подтверждения личности каждой из сторон операции, так и для обеспечения того, что сообщение не было изменено при пересылке.

1. Криптография множественного доступа

Криптография, по сути метод шифрования информации, в частности двухключевая криптография была разработана для обеспечения того, чтобы электронная почта достигла функции подтверждения личности подписавшей стороны и целостности сообщения.

Криптография двойного ключа позволяет двум или более сторонам сделки обмениваться информационными сообщениями даже в отсутствие у них прежних отношений и дает им способ подтверждения личности другой стороны. Как привило, эта система связана с привлечением поставщика сертификационных услуг, высылающего сертификат, который подтверждает личность данной стороны. Такая технология связана с использованием открытого ключа и закрытого ключа, который может использоваться для шифрования и расшифровки сообщений, пересылаемых между сторонами. Там, где сообщение зашифровано с использованием, например, открытого ключа А, оно затем может быть расшифровано только с использованием личного ключа А, и наоборот. Личный ключ всегда находится у А, в то время как открытый ключ, используемый в паре с этим личным ключом, может быть передан любому предполагаемому получателю сообщения. Задача

поставщика сертификационных услуг - обеспечить фактическое соответствие открытого ключа А, а также проверку личности А. Поэтому данный метод дает сторонам сделки возможность определить личность их корреспондента, а также обеспечить, что любое сообщение, отправленное от данного корреспондента, не было подвергнуто изменениям при пересылке.

2. Методы регулирования

Во многих странах принято законодательство, наделяющее юридической силой электронные подписи. Конвенция 2005 года и различные типовые законы предусматривают признание электронных подписей в том случае, когда они используются способом, считающимся достаточно надежным (см. раздел II.B.2). ЮНСИТРАЛ также разработала конкретный Типовой закон об электронных подписях. Типовой закон 2001 года дает определение электронных подписей в статье 2:

"Электронная подпись" означает данные в электронной форме, которые содержатся в сообщении данных, приложены к нему или логически ассоциируются с ним и которые могут быть использованы для идентификации подписавшего в связи с сообщением данных и указания на то, что подписавший согласен с информацией, содержащейся в сообщении данных.

Нейтральное определение используется для того, чтобы адекватно охватить новые и перспективные технологии. Типовой закон 2001 года в пункте 1 статьи 6 предусматривает использование электронных подписей:

В тех случаях, когда законодательство требует наличия подписи лица, это требование считается выполненным в отношении сообщения данных, если использована электронная подпись, которая является настолько надежной, насколько это соответствует цели, для которой сообщение данных было подготовлено или передано, с учетом всех обстоятельств, включая любые соответствующие договоренности.

Вопрос о том, что считается достаточно надежным для этой цели, дополнительно уточняется в пункте 6 статьи 3, где устанавливается следующее:

Электронная подпись считается надежной для цели удовлетворения требования, упомянутого в пункте 1, если:

a) данные для создания электронной подписи в том контексте, в котором они используются, связаны с подписавшим и ни с каким другим лицом;

b) данные для создания электронной подписи в момент подписания находились под контролем подписавшего и никакого другого лица;

c) любое изменение, внесенное в электронную подпись после момента подписания, поддается обнаружению; и

d) в тех случаях, когда одна из целей юридического требования в отношении наличия подписи заключается в гарантировании целостности информации, к которой она относится, любое изменение, внесенное в эту информацию.

Поэтому такая норма обеспечивает достижение подписью функции установления связи с подписавшей стороной, а также обеспечивает то, что подпись не подвергалась изменению. В типовом законе предпринята попытка обеспечить технологически нейтральный подход, предусмотрев в пункте 4 статьи 6, что для установления надежности электронной подписи могут быть использованы и другие способы.

Хотя шифрование с использованием открытого кода в настоящее время, возможно, дает наилучший способ достижения целей подписи от руки, в предстоящие годы это может быть уже не так. Поэтому во многих моделях законодательства основы регулирования в этой области не привязываются к этому конкретному виду технологии. Технологически нейтральный подход позволяет законодательству быть эффективным, охватывая будущее развитие без значительных изменений.

Подход ЕС в директиве об электронных подписях заключается в признании двух разных категорий подписей, подразделяемых на электронные подписи и улучшенные электронные подписи. Директива предусматривает, что "улучшенные электронные подписи", основанные на проверенном сертификате и созданные устройством по созданию безопасной подписи (определенная форма шифрования), могут считаться эквивалентом рукописной подписи и быть приняты в качестве доказательства в суде. Проверенные сертификаты - это сертификаты, которые удовлетворяют требованиям, установленным в директиве, и выданы поставщиками сертификационных услуг, удовлетворяющими определенным требованиям. Улучшенная электронная подпись - это подпись, которая удовлетворяет следующим требованиям, предусмотренным в пункте 2 статьи 2:

a) она однозначно связывается с подписавшей стороной;

b) она способна определить личность подписавшей стороны;

c) она создается с использованием средств, которые подписавшая сторона может сохранить под своим единственным контролем; а также

d) она связана с данными, с которыми она соотносится таким образом, что любое последующее изменение данных может быть обнаружено.

В соответствии с подходом ЕС электронные подписи, не удовлетворяющие этим требованиям, хотя они и не считаются равнозначными рукописной подписи, не могут быть лишены юридической силы или отклонены в качестве доказательства в суде лишь на том основании, что они имеют электронную форму. Поэтому уже суд, руководствуясь фактами и обстоятельствами дела, определяет доказательный вес данной подписи. Улучшенная электронная подпись получает больший вес в плане юридических презумпций и допустимости в силу презумпции большей безопасности, обеспечиваемой техническим методам, используемым для достижения этой цели.

Такой подход вызвал определенную дискуссию о том, лучший ли это способ содействовать использованию электронных подписей. Определенное беспокойство вызывает вопрос о том, не слишком ли он опирается на технологию, а не на юридический принцип. Поэтому эти положения могут считаться связанными с конкретными технологиями, которые в определенный момент в будущем могут оказаться устаревшими, тем самым сделав устаревшими и эти нормативные акты. Вместе с тем, как представляется, конкретное регулирование средств, используемых для электронной подписи, может быть необходимо в некоторых сферах, например в случае электронной связи с государственными и административными органами, такими, как налоговые органы. Вместе с тем следует рассмотреть вопрос о том, зафиксировать ли этот момент в общих основах законодательства, регламентирующего электронную торговлю, или же отнести его к области регулирования в данной конкретной сфере.

3. Сертификаты

Сертификаты могут использоваться для подтверждения личности лица, подписывающего сообщения в электронной форме. Поставщики услуг сертифицирования - это посредники, предоставляющие сертификаты, подтверждающие то, что устройство создания подписи принадлежит подписавшей стороне, а также личность этого лица.

Типовой закон 2001 года устанавливает некоторые стандарты, которые должны быть выполнены поставщиками сертификационных услуг. В статье 9 устанавливается:

1. В тех случаях, когда поставщик сертификационных услуг предоставляет услуги для подкрепления электронной подписи, которая может быть использована в качестве подписи, имеющей юридическую силу, такой поставщик сертификационных услуг:

a) действует в соответствии с заверениями, которые он дает в отношении принципов и практики своей деятельности;

b) проявляет разумную осмотрительность для обеспечения точности и полноты всех исходящих от него существенных заверений, которые относятся к сертификату в течение всего его жизненного цикла или которые включены в сертификат;

c) обеспечивает разумно доступные средства, которые позволяют полагающейся стороне установить по сертификату:

i) личность поставщика сертификационных услуг;

ii) что подписавший, который идентифицирован в сертификате, имел контроль над данными для создания подписи в момент выдачи сертификата;

iii) что данные для создания подписи были действительными в момент или до момента выдачи сертификата;

d) обеспечивает разумно доступные средства, которые позволяют полагающейся стороне установить, соответственно, по сертификату или иным образом:

i) метод, использованный для идентификации подписавшего;

ii) любые ограничения в отношении целей или стоимостного объема, в связи с которыми могут использоваться данные для создания подписи или сертификат;

iii) что данные для создания подписи являются действительными и не были скомпрометированы;

iv) любые ограничения в отношении масштаба или объема ответственности, оговоренные поставщиком сертификационных услуг;

v) существуют ли средства для направления подписавшим уведомления в соответствии с пунктом 1 b) статьи 8 настоящего Закона;

vi) предлагается ли услуга по своевременному аннулированию.

Поэтому обязательство поставщика сертификационных услуг включает обеспечение точности информации, содержащейся в сертификате, и того, что в момент его выдачи подписавшая сторона, указанная в сертификате, владела данными для создания подписи в момент выдачи сертификата.

Сертификат может содержать ограничения, касающиеся суммы сделки, для которой использован сертификат, или целей использования сертификата.

В пункте 2 статьи 9 предусмотрена ответственность поставщика сертификационных услуг за невыполнение этих юридических требований:

Поставщик сертификационных услуг несет ответственность за юридические последствия невыполнения требований пункта 1.

D. Защита данных

Использование Интернета и связи радиоэлектронными средствами, открывающее возможность обработки крупных массивов данных, заставляет серьезно задуматься о том, как реально будут использоваться данные, кем и для какой цели. В результате появившейся возможности хранения большого объема документов в виде, полностью пригодном для поиска, электронная среда увеличила масштабы сбора данных. Она также позволяет быстро и легко пересылать эти данные другим сторонам через международные границы. Наконец, данные становятся более уязвимыми для атаки со стороны в силу тех целей, для которых они

могут использоваться, - от мошенничества с кредитными картами с помощью похищенных персональных данных до манипуляций со счетами и документами.

Сбор данных ведется как частными, так и государственными структурами для целого ряда целей - от маркетинга, например, составления обобщенного портрета клиента для нацеливания на подходящий сегмент для конкретного товара, до ведения государственных баз данных налогоплательщиков, данных криминалистического учета или списков избирателей.

В разных правовых системах приняты разные подходы к сбору и использованию личных данных. Например, в Соединенных Штатах нет особых ограничений на покупку и продажу личных данных в виде списков рассылки, в то время как в ЕС принят более строгий подход, в соответствии с которым продажа такого рода списков ограничивается только списками физических лиц, согласившихся на передачу их личных данных.

Защита и использование сбора и передачи личных данных признается в некоторых правовых системах в качестве весьма важной. В частности, Европа находится в авангарде регулирования использования личных данных. Директива о защите данных ЕС предусматривает ограничения вида собираемых данных, целей их использования и методов, которые должны быть реализованы для защиты личных данных от случайного или незаконного уничтожения или случайной потери.

В этой области имеется спорный вопрос передачи личных данных между странами, в частности странами, придерживающимися совершенно разных подходов к защите данных. Такая передача часто будет вызывать обязательства со стороны компаний, находящихся в странах, в которых не имеется нормативных актов по защите данных, где они принимают данные из стран со строгими ограничениями, касающимися защиты данных. Эти обязательства могут быть выполнены на основе договорных требований, ограничивающих использование личных данных целями, отличными от согласованных целей, и удовлетворяющих требованиям регламентаций о защите данных в странах-отправителях.

E. Заключение

В этом разделе рассмотрены вопросы безопасности, непосредственно связанные с электронной торговлей. Хотя эти риски не могут быть полностью исключены, определив риски можно предпринять шаги по их более действенному сведению к минимуму.

Вопросы, связанные с этим разделом о юридической уверенности, заключаются в следующем:

- Определение рисков для безопасности, создаваемых электронной торговлей, и принятие мер по их сведению к минимуму
- Принятие мер по использованию и регулированию электронных подписей
- Определение соответствующих норм защиты личных данных.

F. Литература

International Chamber of Commerce (ICC), *General Usage for International Digitally Ensured Commerce*, 2001, есть на http://www.iccwbo.org/home/guidec/guidec.asp

Organisation for Economic Cooperation and Development (OECD) *Guidelines for the Security of Information Systems and Networks*, 2002, есть на http://www.oecd.org/dataoecd/16/22/15582260.pdf

OECD, *Privacy Online: OECD Guidance on Policy and Practice*, 2003, есть на http://www.oecd.org/

IV. ПРАВОВАЯ ЗАЩИТА

Движение информации и товаров через границы ставит в международном масштабе проблему правовой обеспеченности прав интеллектуальной собственности (ПИС), включая авторские и смежные права, патенты и товарные знаки. Если международная торговля товарами со временем возрастала постепенно, то масштабы торговли, которую делает возможной Интернет, и номенклатура товаров в такой торговле растут по экспоненте. Права интеллектуальной собственности, как правило, защищаются в масштабах страны, однако Интернет заставляет самым серьезным образом относиться к возможности защиты и обеспечению соблюдения этих прав в международном масштабе.

Имеется ряд международных соглашений по различным аспектам интеллектуальной собственности, включая Парижскую конвенцию об охране промышленной собственности[21] (1883 года) и Бернскую конвенцию об охране литературных и художественных произведений[22] (1986 года), которые подписаны большинством стран - участниц СПЕКА, включивших соответствующие нормы в свое законодательство. Наиболее серьезные инициативы по унификации этой области - Соглашение по торговым аспектам прав интеллектуальной собственности (ТАПИС), осуществление которого находится в ведении ВТО[23].

Интернет также изменил облик торговых связей между предприятиями и между предприятиями и потребителями. Он открыл каналы торговли с потребителями в международных масштабах, которых ранее не существовало. Хотя это приводит к росту объема торговли, это же способно также вызвать юридические проблемы особого рода, касающиеся клиентов, прежде всего проблемы защиты данных и защиты прав потребителей.

A. Товарные знаки

Товарный знак - это слово, эмблема, рисунок или другое изображение, которое используется в торговле в связи с определенными товарами и услугами для обозначения источника этих товаров и услуг, а также для того, чтобы отличить их от товаров и услуг других производителей. Владельцы товарных знаков имеют право воспрепятствовать другим использовать их товарный знак на идентичных или сходных товарах в ходе торгового оборота. Общая цель законодательства о товарных знаках - предотвращение введения потребителей в заблуждение относительно источника данного товара, а также предотвращение ущерба репутации марки в результате его использования в связи с товарами или услугами более низкого качества.

Товарные знаки обычно защищаются с помощью регистрации в национальных масштабах в связи с конкретными товарами или услугами. Поэтому возможно, а во многих случаях вероятно, что тот же знак будет зарегистрирован в связи с другими категориями товаров и услуг. Регистрация товарного знака имеет силу только в данной стране, поэтому

---

[21] Конвенцию подписали 164 страны, а из числа стран-участниц СПЕКА ее не подписал только Афганистан.

[22] Конвенцию подписали 150 стран, а из числа стран-участниц СПЕКА ее не подписали только Афганистан и Туркменистан.

[23] Общие сведения см. на http://www.wto.int/english/tratop_e/trips_e/trips_e.htm.

регистрация должна быть произведена в каждой стране, в которой владелец товарного знака желает получить его защиту. Предпринимались различные меры по унификации регистрации и классификации в системах товарных знаков. Кроме того, в некоторых странах названия или эмблемы, используемые в связи с данными товарами или услугами, могут защищаться даже без регистрации. Например, в Соединенном Королевстве деликт введения в заблуждение может быть с успехом вменен лицу, ложно представляющему связь с товаром конкурента в попытках использования престижа фирмы, связанного с данным товаром, для продажи своих товаров. Для того чтобы такой иск был удовлетворен, необходимо наличие ущерба или вероятность ущерба, причиненного товарному знаку истца.

1. Доменные имена

Область, которая вызвала больше всего споров, - это использование доменных имен, включая товарные знаки. Система доменных имен действует совсем иначе, чем система товарных знаков, например, доменное имя не связано с данным товаром, что и вызвало большое число споров.

Когда компьютер соединяется с Интернетом, ему присваивается отдельный идентификационный номер, или IP-адрес. При поиске сайта необходимо использовать этот IP-адрес для определения компьютера, на котором размещается сайт. IP-адрес состоит из четырех чисел, каждое от 0 до 255, разделенных точкой. Поскольку сами по себе эти цифры трудно запомнить, была разработана система доменных имен, чтобы сделать пользование этими адресами более удобным. Доменное имя используется для отображения IP-адреса компьютера, что и позволяет легко определять компьютер. Среди категорий доменных имен имеется два домена верхнего уровня - страновые коды, такие как .uk, и общие коды, такие как .org.

Для отождествления сайта часто в доменное имя включается товарный знак. Поэтому доменное имя, включающее товарный знак, имеет для владельца товарного знака большую ценность.

Хотя доменные имена тоже должны быть зарегистрированы, система доменных имен работает совсем иначе: здесь заявки регистрируются в порядке поступления и практически не рассматриваются по существу. Доменные имена также могут регистрироваться для коммерческого или некоммерческого использования, и, что самое важное, они не регистрируются в связи с каким-либо конкретным классом товаров или услуг. Имеются категории общих доменных имен верхнего уровня, таких как .org, .com и .edu, однако они используются гораздо реже, чем доменные имена, используемые в масштабе стран, связанные с торговыми марками.

Хотя товарные знаки допускают использование одного и того же наименования несколькими пользователями в разных классах или категориях, для того чтобы доменное имя служило адресом отдельного компьютера и могло привлекать прямых пользователей, оно должно быть уникальным. Эти различия между доменными именами и товарными знаками неизбежно вели к спорам. Сначала это были споры между владельцами товарных знаков с одним и тем же названием, но на разные товары. В системе доменных имен это название будет закреплено за тем, кто первым зарегистрирует доменное имя. Во-вторых, возникают

споры в тех случаях, когда физические лица приобрели некоторые доменные имена, желая перепродать их с прибылью владельцу товарного знака с этим наименованием. Такую деятельность часто называют кибersквоттингом. Некоторые страны, например Соединенные Штаты, в которых принят закон о защите потребителей от кибersквоттинга, уже выработали меры регулирования, призванные не допустить злоупотреблений при регистрации доменных имен.

За управление системой доменных имен отвечает Международная корпорация по присвоению доменных имен (ИКАНН). Для разрешения возникающих споров по поводу доменных имен в 1999 году в ИКАНН были введены в действие единообразные общие правила урегулирования споров. Поэтому споры, возникающие в связи с доменными именами, могут быть переданы либо одному из аккредитованных ИКАНН поставщиков услуг по регулированию споров, такому как Центр арбитража и посредничества Всемирной организации интеллектуальной собственности (ВОИС) применительно к спорам о доменных именах[24] либо национальным судам.

2. Гиперссылки и кадрирование

Еще одна область, в которой возникают юридические споры, - представление гиперссылок, в частности глубоких ссылок. Речь идет о проставлении ссылок на страницу владельца сайта, размещенных на внутренней странице другого сайта. Это вызывает определенные споры, поскольку из-за того, что ссылка дана на страницу внутри сайта, а не на начальную страницу владельца сайта, пользователь, идя по ссылке, может обойти начальную страницу и, возможно, любые рекламные материалы, размещенные на этой начальной странице.

Кадрирование происходит тогда, когда сайт дает ссылку на информацию, содержащуюся на другом сайте, которая представлена в определенном кадрированном формате без переадресации пользователя непосредственно к этому другому сайту. Может возникать путаница относительно источника информации.

Хотя ссылки - необходимая часть Интернета, по-прежнему в определенной степени сохраняется вопрос о законности глубоких ссылок. В некоторых странах судам было предложено определить, вызывают ли глубокие ссылки и кадрирование вопросы введения в заблуждение, недобросовестной конкуренции или нарушения авторских прав.

Сами владельцы сайтов могут попытаться помешать ставить такие глубокие ссылки, используя идентификационные файлы, сохраняемые на клиентской системе, или другие технические меры.

[24] Общие сведения см. на http://www.wipo.int/amc/en/domains/index.html

3. Метатеги

Метатеги используются для обеспечения того, чтобы страница попала в зону поиска по данной теме. Вопросы или темы, связанные с данной страницей, незаметно вставляются в язык гипертекста, использованного для создания страниц, чтобы поисковые машины могли включить соответствующие страницы в результаты поиска. Чем чаще данное слово используется в метатеге, тем больше шансы на попадание в список результатов поиска. Хотя метатеги могут служить полезным средством описания содержимого вебстраницы, они также могут использоваться для увеличения числа заходов на страницу. Это может достигаться, например, включением в метатег товарных знаков конкурентов. Возник ряд споров в тех случаях, когда владельцы товарных знаков утверждали, что метатеги были использованы конкурентами для незаконного использования репутации фирменного наименования владельца товарного знака.

Для решения таких вопросов используются такие меры, как предупреждение о снятии ответственности, в которых, например, поясняется, что сайт никак не связан с владельцами данного товарного знака. Полезными могут быть соглашения о ссылках и различные технические методы, такие, как куки-файлы или просьбы сайта о фильтрации с некоторых адресов в Интернете.

B. Авторские права

Защита авторских прав охватывает оригинальные литературные, художественные, музыкальные и драматические произведения, а также фильмы, звукозаписи и типографские аранжировки. Не существует какого-либо официального процесса регистрации защищаемых авторскими правами произведений, поэтому уже материальная фиксация произведения, например, составление вебстраницы, влечет за собой защиту авторских прав. Поэтому содержимое вебстраницы, как правило, подлежит защите вне зависимости от наличия на ней символа ©.

Авторские права обеспечивают защиту выражения идеи, однако не могут использоваться для охраны самой идеи. Поэтому копирование текста вымышленной истории будет считаться нарушением, а использование идеи, на которой построена история, может нарушением не считаться. Владелец авторских прав обладает исключительным правом осуществления некоторых видов деятельности, связанных с произведением, таких, как его копирование, издание копий для других лиц и переделка произведения. Право осуществления таких видов деятельности может быть передано другим лицам или лицензировано. Нарушение авторских прав происходит в случае осуществления такой деятельности без разрешения владельца авторских прав.

1. Открытый источник

Защищенные авторскими правами работы, как правило, предоставляются в распоряжение на условиях "лицензии", в которой детально устанавливаются условия использования произведения. С юридической точки зрения "лицензия" может характеризоваться либо как одностороннее предоставление лицензиаром разрешения использовать произведение определенными способами, либо может включать в себя

договорное соглашение между лицензиаром и лицензиатом. В интерактивном контексте такие лицензионные соглашения часто называют лицензиями, подтверждаемыми "согласительной" кнопкой. Юридическое согласие пользователя достигается выражением им своего согласия с условиями путем нажатия кнопкой мыши на специальную иконку.

Массовая культура открытости, выражаемая многими пользователями Интернета, в частности технически подготовленными пользователями первых лет, также привела к росту альтернативных систем лицензирования, специально предназначенных для того, чтобы способствовать обмену информацией, а не ограничивать ее использование с помощью авторских прав. В области программного обеспечения (ПО) появилась система "Линукс": она была разработана совместными усилиями на основе механизма лицензирования, в соответствии с которым любой мог свободно копировать и изменять это произведение при том условии, что любой результат работы, основанный на первоначальной работе, также должен быть лицензирован на условиях свободного и бесплатного использования. Это получило название лицензирование "открытого источника". Термин "открытый источник" используется в целом ряде контекстов, однако главным образом он обозначает модель разработки программного обеспечения и/или лицензирования. Что касается модели разработки ПО, то сообщество программистов или составителей кодов - от частных лиц до сотрудников компаний - вносит свой вклад в составление исходного кода программы, такой, как "Линукс", который в свою очередь распространяется в соответствии с моделью лицензирования "открытого источника". Имеется множество лицензий "открытого источника", однако их объединяют некоторые общие черты[25]. Во-первых, лицензиат вправе реализовывать программы. Во-вторых, лицензиату должен быть предоставлен доступ к исходному коду, языку, на котором написана программа (например, C+), а также объектному коду (т.е. машинному коду). В-третьих, лицензиар должен разрешить внесение в первоначальное произведение исправлений или производные произведения. В-четвертых, не должно быть дискриминационных условий лицензий в отношении либо использования, либо пользователя программы. В-пятых, лицензиату не должно навязываться каких-либо прочих видов обеспечения или связывающих ограничений. Наиболее известная из лицензий с открытым источником - общедоступная лицензия (ОДЛ) проекта ГНУ, выдаваемая Фондом свободно доступного программного обеспечения.

В отличие от "открытого источника" были также созданы системы так называемых материалов "общедоступной сферы" (например, http://www.creativecommons.org), когда юридический владелец авторских прав отказывается от своих авторских прав на материалы и разрешает свободное повторное использование, переделку и реализацию. Если лицензирование "открытого источника" использует ныне действующие системы авторских прав для содействия массовому распространению, использованию и разработке сходного кода, то общедоступное программное обеспечение и информация вообще отказываются от применения режима авторских прав.

[25] Подробнее см. об инициативе открытого источника (ИОИ) на http://www.opensource.org.

2. Нарушения

Копирование произведений в сети, безусловно, позволяет говорить о нарушении авторских прав, если владелец авторских прав не дал своего разрешения. Некоторые утверждают, что помещение произведения в сеть предполагает согласие на копирование произведения, хотя суды не поддержали такой точки зрения. Разработка оцифрованных продуктов также создает новые возможности для тех видов произведений, которые могут копироваться и бесплатно распространяться по Интернету.

Сайты, которые разрешают пользователям размещать информационное наполнение, должны знать, что такое информационное наполнение само по себе может нарушать авторские права. Им также следует требовать от пользователей предоставления хосту телеконференции неисключительных лицензий или передачи ему авторских прав, чтобы хост мог редактировать, копировать и стирать информационное наполнение.

3. Ответственность поставщиков Интернет-услуг

Размещение произведения в Интернете может вызывать несколько вопросов, связанных с авторскими правами. Даже методы загрузки и просмотра вебстраниц связаны с копированием произведения. Поставщики Интернет-услуг (ПИУ) часто хранят копии популярных вебстраниц в своих "кешах", чтобы повысить эффективность вывода этих страниц. Если такое копирование будет считаться нарушением, то это, возможно, станет сдерживать развитие электронной торговли. ПИУ также могли бы быть признаны несущими ответственность за передачу вебстраниц или хранение защищенных авторскими правами произведений в ходе своей повседневной деятельности. Поэтому во многих странах в законодательстве предусматривается, что такая деятельность, которая необходима для загрузки и просмотра вебстраниц, не считается нарушением.

В законе Соединенных Штатов о защите прав в цифровое тысячелетие 1998 года предусмотрено изъятие из положений об ответственности ПИУ за нарушение авторских прав применительно к нарушениям, возникающим в результате передачи, кеширования или хостинга защищаемых авторскими правами материалов, если владелец авторских прав не знал о том, что данные материалы нарушают авторские права. Узнав о нарушении авторских прав данными материалами, ПИУ должен удалить их или заблокировать доступ к ним. ЕС также предусматривает аналогичный уровень иммунитета для ПИУ, если те не знают о том, что данные материалы нарушают авторские права.

4. Технологические меры защиты

Некоторые из шагов, предпринятых для содействия защите ПИС, связаны с разработкой технологических мер защиты. Такие технологические методы, например использование средств защиты от копирования, в свою очередь вызвали новые юридические проблемы. Механизмы защиты от копирования позволяют владельцу авторских прав ограничивать доступ к их произведениям и их копирование. Некоторые утверждают, что это лишает законных пользователей возможности получения доступа к произведениям для добросовестного свершения сделок или добросовестного использования. В ряде правовых систем, включая ЕС и Соединенные Штаты, были приняты нормативные акты о

предотвращении использования технических средств для обхода мер по защите от копирования.

Интернет создает множество проблем для владельцев ПИС. Быстрый и эффективный способ показа и пересылки продуктов через границы между странами одновременно вызывает проблемы международного обеспечения соблюдения прав.

C. Защита прав потребителей

Ныне действующие законы о защите прав потребителей часто охватывают сделки с использованием Интернета, для чего не требуется внесения в них поправок[26]. Однако был принят ряд мер по повышению уверенности потребителей в связи со сделками в Интернете - от предоставления конкретной информации о поставщике и товаре до усиления защиты от мошеннического использования платежных карт в сетевых сделках.

1. Прозрачность

Предоставление потребителям информации, благодаря которой они могут должным образом идентифицировать поставщика и сравнить характеристики нескольких товаров, позволяет им принимать продуманные решения о покупке товаров.

Директива об электронной торговле также предусматривает предоставление некоторой информации потребителям, указывая, когда такая информация должна быть предоставлена.

2. Мошенническое использование платежных карт

Потребители особо озабочены безопасностью использования в сети реквизитов их кредитных карт (или других платежных карт). Вопросы безопасности возникают в связи с потенциальным перехватом реквизитов карт в результате совершения сделки или недобросовестного использования этих платежных реквизитов получателем. Для обеспечения более безопасной передачи платежных реквизитов могут использоваться различные технические меры, такие, как протокол безопасных соединений веб-обозревателей, защищающих эти реквизиты от перехвата при передаче. Однако невозможность надлежащим образом идентифицировать поставщика по-прежнему вызывает у потребителей неуверенность в их защищенности. Хотя электронные подписи обеспечивают такую идентификацию, использование подобного рода электронных подписей оказалось чересчур обременительным и дорогостоящим для розничных сделок на небольшую сумму.

Для усиления уверенности потребителей в своей директиве о дистанционной продаже ЕС обязывает эмитентов кредитных и дебетовых карт компенсировать потребителям любые потери, вызванные мошенническим использованием их платежных карт в Интернете. Статья 8 устанавливает:

---

[26] Например, закон Республики Кыргызстан "О защите прав потребителей", декабрь 1997 года.

Государства-члены обеспечивают действие надлежащих мер, позволяющих потребителю:

- *требовать отмены платежа в случае мошеннического использования его платежной карты в связи с дистанционными договорами, охватываемыми настоящей директивой,*

- *получать повторное зачисление списанных сумм или их возвращение в случае мошеннического использования.*

Эти меры повышают уровень потребительской уверенности, однако не менее важно рассмотреть соответствующие методы урегулирования споров при их возникновении.

3. Урегулирование споров

Серьезные проблемы урегулирования споров о защите прав потребителей в связи с электронной торговлей связаны с проблемами иностранных претензий, неопределенностью в отношении применимого права и с проблемами обеспечения соблюдения законодательства о защите прав потребителей. Жалобы отдельных потребителей связаны с небольшими суммами, поэтому обращение в суд не подходит из-за связанных с этим затрат времени и денег. При возникновении международных споров затраты времени и денег и трудности получения доступа к суду оказываются еще больше. Были предприняты шаги по усилению международного сотрудничества и унификации норм по защите прав потребителей, однако необходимо рассмотреть и другие малозатратные меры по урегулированию потребительских претензий.

В области защиты прав потребителей альтернативные методы урегулирования споров можно было бы предусмотреть с использованием кодексов поведения и знаков доверия, а также альтернативных систем урегулирования споров, предоставляющих малозатратные возможности удовлетворения претензий за пределами судебной системы.

D. Заключение

Электронная торговля создает новые способы нарушения прав интеллектуальной собственности. Эти новые угрозы необходимо изучить, чтобы обеспечить защиту правообладателей в соответствии с ныне действующими законодательными нормами. Товары и услуги, защищаемые ПИС, представляют собой столь важную часть электронной торговли, что игнорировать эту область нельзя.

Для создания условий для развития электронной розничной торговли необходимо рассмотреть меры повышения потребительской уверенности.

Проблемы, возникающие в связи с этим разделом о защите юридических прав, включают следующие:

- влияние доменных имен на законодательство о товарных знаках
- новые формы возможных нарушений товарных знаков, такие, как метатеги, глубокие ссылки и кадрирование
- ответственность ПИУ за нарушение авторских прав
- разработка и правовая защита мер защиты от копирования
- обеспечение надлежащего уровня защиты прав потребителей применительно к электронной торговле, в частности в связи с предоставлением информации и использованием платежных карт
- доступ к надлежащим механизмам урегулирования споров.

E. Литература

ВОИС, "Интеллектуальная собственность в Интернет: обзор проблем", 2003 год, имеется на http://www.wipo.int/ebookshop

OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999), имеется на http://www.oecd.org/dataoecd/18/13/34023235.pdf

V. ПРАВОВЫЕ СДЕРЖИВАЮЩИЕ СРЕДСТВА

Электронная торговля создает новые риски для безопасности и новые способы совершения преступлений. Глобальный доступ, предоставляемый Интернетом, будучи полезным с коммерческой точки зрения, также открывает много возможностей для киберпреступников. Например, при том что Интернет позволяет заключать коммерческие соглашения на международном уровне, он же способен давать киберпреступникам доступ к компьютерным системам предприятий на другом конце земного шара.

A. ИКТ-преступность

Использование информационного общества породило разнообразные новые виды преступности и новые способы совершения неновых преступлений, таких, как отмывание денег, мошенничество и терроризм.

Новые формы преступных деяний включают:

1. Воздействие, вызывающее отказ в обслуживании законных пользователей

Воздействие, вызывающее отказ в обслуживании законных пользователей, - это методы нарушения нормальной работы вебсайта. Атака на сайт совершается путем посылки большого объема ложных запросов информации, которые замедляют работу сайта или перегружают его до такой степени, что система, на которой размещен сайт, дает сбой. Для анонимного проведения такого рода атак часто используются компьютеры третьих сторон, над которыми устанавливается контроль без ведома владельца. Эти компьютеры получают задачу бомбардировать сайт до тех пор, пока система не перестанет функционировать.

2. Вирусы и вредоносные коды

Это программы, которые должны запускаться на домашних и служебных компьютерах. Они имеют различные злонамеренные цели и способны временно или окончательно вывести компьютеры из строя. Некоторые программы, такие, как "черви", самотиражируются и поэтому способны заразить большое число систем за самое короткое время.

3. Несанкционированный доступ

Несанкционированный доступ к электронным данным или к компьютерной системе способен привести к незаконному использованию этих данных. Например, в ряде случаев мошенники взламывали базы данных о кредитных картах различных компаний и реквизиты кредитных карт всех их клиентов были размещены в сети.

B. Регулирование и ИКТ-преступность

Развитие технологий связи не только создало новые способы совершения преступлений, но и дало различные методы их расследования. Один из методов, используемых для предупреждения и пресечения правонарушений в сфере информации и инфраструктуры, - группы реагирования на чрезвычайные ситуации, такие, как группа

реагирования на связанные с компьютерами чрезвычайные ситуации в Университете Карнеги Меллона в Соединенных Штатах.

Уголовно-процессуальное законодательство наделяет правоохранительные органы определенными правомочиями по расследованию преступной деятельности, такими, как право перехвата сообщений и проведения обыска и выемки предметов, возможно связанных с преступной деятельностью. Разработка информационно-коммуникационных технологий поставила новые вопросы, связанные с этими процессуальными правами. Например, теперь уже может быть недостаточно изъять компьютер, использовавшийся подозреваемым в преступлении; возможно, теперь уже потребуется обеспечить принятие мер по предотвращению потери или уничтожения данных. Имеется также возможность того, что преступная деятельность охватывает несколько стран, что затрудняет ее выявление и деятельность правоприменительных органов.

Во многих странах приняты новые нормативные акты, ставящие цель предупреждения или по крайней мере ограничения компьютерной преступности. Эти нормативные акты, как правило, предусматривают уголовную наказуемость несанкционированного доступа к компьютерной системе, обычно известного как "хакерство", а также несанкционированного воздействия на компьютеры или программы и содержащиеся в них данные в результате использования "вирусов" и других форм вредоносных программных средств. Среди стран-участниц СПЕКА Азербайджан, Казахстан, Кыргызстан, Таджикистан, Туркменистан и Узбекистан приняли нормативные акты, предусматривающие преследование деяний, направленных против конфиденциальности и целостности и работоспособности компьютеров[27].

Считается, что для обеспечения эффективной работы правоохранительных органов необходимо внесение поправок в уголовно-процессуальное законодательство в следующих областях:

- обыск и выемка,
- перехват сообщений и
- регулирование криптографических продуктов.

1. Обыск и выемка

Обыск и выемка электронной информации могут быть связаны с особыми трудностями ввиду научно-технического прогресса. Изменения в законодательстве должны учитывать такие разнообразные факторы, как возможность сохранения целостности доказательств с момента их выемки до момента их представления в суде или же возможность преодоления шифрования или другие технические аспекты, которые могут затруднять доступ к информации. Для достижения этой цели необходимо соответствующее финансирование для обучения соответствующих работников криминалистической экспертизы методам раскрытия полученной информации и ее тщательного сохранения.

[27] Соответствующие положения уголовных кодексов см. http://www.crime-research.org/library/Criminal_Codes.html.

2. Перехват сообщений

Хотя перехват сообщений - не новая область, появилось много новых способов передачи сообщений, которые может потребоваться перехватывать, включая Интернет, мобильную телефонию и другие системы связи. Определение того, в каких системах необходим перехват и позволяет ли законодательство перехватывать сообщения данного вида, - эти вопросы требуют своего рассмотрения.

Поэтому положения законодательства в этой области должны быть технологически нейтральными, чтобы они могли регламентировать новые виды технологий связи. Необходимо также рассмотреть вопрос о средствах содействия перехвату и о том, следует ли привлекать другие стороны, такие, как поставщиков услуг связи, например к обеспечению возможности перехвата. Имеется также вопрос о том, следует ли сохранять определенные данные и в течение какого-периода, а также кто должен нести соответствующие расходы.

3. Регулирование шифрования

Шифрование - это важный механизм защиты и обеспечения сохранности информации. Вместе с ростом информационно-коммуникационных технологий происходит и стремительное расширение использования средств шифрования. Даже такие стандартные приложения, как просмотровые программы Интернета и почтовые программы обычно используют технологии шифрования, чтобы их программное обеспечение позволяло поддерживать безопасную связь.

Имеется озабоченность тем, что такие технологии могут использоваться для разнообразных преступных целей. Поэтому в некоторых странах введены ограничения на использование или импорт или экспорт таких технологий. Например, в Казахстане регулируется ввоз и вывоз криптографической продукции, а также внутренняя разработка, производство, восстановление и продажа[28]. Вассенаарские договоренности по экспортному контролю за обычными вооружениями, товарами и технологиями двойного применения предусматривают определенный уровень международной унификации в этом вопросе[29].

Строгие меры контроля за использованием шифровальных продуктов могут, тем не менее, создавать неоправданные ограничения на их использование внутри хозяйственных организаций. В результате, например, в Соединенных Штатах были ослаблены меры регулирующего контроля за некоторыми видами шифровальной технологии. В ОЭСР было разработано руководство для правительств в этой области - его Руководящие принципы политики в области криптографии[30].

---

[28] Соответственно постановление № 1037, статья 266 (от 30 июня 1997 года) и постановление № 29; а также постановление № 967, статья 240 (от 13 июня 1997 года), а также постановление № 27.

[29] http://www.wassenaar.org.

[30] http://www.oecd.org/dsti/sti/it/secur/prod/e-crypto.htm.

C. Международное сотрудничество

В области борьбы с киберпреступностью международная координация и сотрудничество имеют огромное значение. Киберпреступление не ограничивается национальными границами, и точно также обнаружение и привлечение к ответственности за такие деяния потребуют выхода за эти границы. Киберпреступники могут, если захотят, пересылать свои сообщения через несколько стран, чтобы добиться скрытности, как и доказательства их преступлений могут находиться в самых разных странах.

Поэтому необходимы международные договоренности о содействии расследованию и судебному преследованию за преступления. В 2005 году Интерполом была создана виртуальная глобальная целевая группа, связанная с национальными группами в Соединенном Королевстве, Соединенных Штатах, Австралии и Канаде, для борьбы с детской порнографией.

Был выдвинут ряд инициатив, нацеленных на развитие международной координации в этой области, включая Директивы по проблеме безопасности информационных систем и сетей: формирование культуры, обеспечения безопасности ОЭСР[31].

Совет Европы разработал Конвенцию о компьютерных преступлениях Совета Европы, которая с 2001 года была подписана 38 из 47 членов Совета Европы; хотя Азербайджан, единственный член СПЕКА, являющийся также членом Совета Европы, еще не подписал ее. Эту Конвенцию также подписали Канада, Коста-Рика, Мексика, Соединенные Штаты, Южная Африка и Япония[32]. В Конвенции рассмотрены вопросы материального и процессуального уголовного права, в связи с которыми государства-члены обязуются принять меры по осуществлению в своем законодательстве, а также вопросы международного сотрудничества.

Что касается правонарушений, то в разделе 1 Конвенции проводится различие между четырьмя категориями правонарушений:

- "Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем", т.е. противозаконный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование систем и противозаконное использование устройств (статьи 2-6).

- "Правонарушения, связанные с использованием компьютерных средств", т.е. подлог и мошенничество (статьи 7-8).

- "Правонарушения, связанные с содержанием данных", т.е. детская порнография (статья 9).

- "Правонарушения, связанные с нарушением авторского права и смежных прав" (статья 10).

---

31 http://www.oecd.org/pdf/M0034000/M/00034292.pdf.

32 http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

В части 2 Конвенции рассмотрены процессуальные нормы, которые государства-члены обязуются включить в свое законодательство. В их числе меры, призванные "оперативно обеспечивать сохранность хранимых компьютерных данных" (статья 16), "оперативное обеспечение сохранности данных о потоках информации" (статья 17), предъявление и обыск и выемка компьютерных данных (статьи 18-19), "сбор в режиме реального времени данных о потоках информации" (статья 20) и перехват данных о содержании (статья 21). В части 3 рассмотрен вопрос о юрисдикции (статья 22).

В плане международного сотрудничества в Конвенции рассматриваются вопросы выдачи (статья 24), взаимной правовой помощи между национальными правоохранительными органами (статьи 25-34) и создания обеспечивающих такую помощь контактных центров, работающих 24 часа в сутки семь дней в неделю (статья 35). Контактная сеть основана на концепции, впервые принятой государствами "восьмерки" для содействия сотрудничеству с использованием неофициальных каналов связи, дополняющих официальные процедуры взаимной правовой помощи. Сеть уже охватывает свыше 39 стран-участниц.

Всеобъемлющий характер Конвенции, а также ее географический охват в плане подписавших ее стран означает, что она, вероятнее всего, останется в обозримом будущем наиболее авторитетным международно-правовым актом в этой области. В 2005 году Международная организация уголовной полиции, Интерпол, приняла резолюцию, в которой Конвенция была названа "обеспечивающей минимальные международные юридические и процессуальные стандарты" и рекомендовалось ее 186 странам-членам рассмотреть возможность присоединения к ней[33]. Все страны - участницы СПЕКА являются также членами Интерпола.

После принятия в 2001 году Конвенции ее государствами-участниками в январе 2003 года был согласован дополнительный протокол "о криминализации деяний расистского и ксенофобного характера, совершенных с помощью компьютерных систем"[34]. Такие вопросы были рассмотрены в ходе работы над самой конвенцией, однако из-за невозможности тогда прийти к консенсусу потребовалось разработать отдельный протокол.

[33] http://www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp.
[34] European Treaty Series No. 189 (‘Additional Protocol’).

D. Заключение

Конвенция о компьютерных преступлениях Совета Европы устанавливает четкие положения о такого рода поведении, которое должно преследоваться в уголовном порядке, и процессуальные требования, необходимые для содействия расследованию и наказанию за такие деяния. Поэтому она представляет собой очень хорошую отправную точку для любой правовой системы, в которой предпринимаются попытки укрепления законодательства о киберпреступности.

В этом разделе о правовых средствах сдерживания затрагиваются следующие вопросы:

- необходимость внесения поправок в законодательство с учетом новых форм уголовных деяний
- необходимость адаптации уголовно-процессуальных методов с учетом новых видов уголовных деяний.

Необходимо сохранить и повысить уровень международного сотрудничества и правоохранительной деятельности.

E. Литература

Explanatory Report to the Council of Europe Convention on Cybercrime (ETS No. 185) есть на http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

VI. ЗАКЛЮЧИТЕЛЬНЫЕ ЗАМЕЧАНИЯ И РЕКОМЕНДАЦИИ

В этом руководстве рассмотрены основные юридические и законодательные вопросы, связанные с использованием ИКТ и их внедрением в электронной торговле, электронных приложениях и электронных услугах либо в деловой или потребительской среде, либо в практике органов государственного управления. В руководстве также представлены соображения о том, как рассматривать любые выявленные вопросы, чтобы способствовать согласованной правовой реформе для развития электронной торговли и связанной с ней деятельности, а также как сдерживать при необходимости некоторые вредные виды поведения для защиты стран - участниц СПЕКА и их народов.

Проблемы юридической действительности, обеспеченности правовой санкцией и допустимости юридических актов, осуществленных в электронной форме, могут сдерживать распространение электронной торговли. Юридическая неопределенность представляет собой препятствие для внедрения вне зависимости от того, насколько серьезны эти проблемы, и организации часто будут не в состоянии установить истинную юридическую ситуацию и могут воздержаться от принятия риска. Законы, нормативные акты и административная практика стран будут часто требовать того, чтобы юридические акты были осуществлены с использованием физических документов вместе с подписями и процедурами засвидетельствования, что исключает использование электронных альтернатив. Такого рода требования формы во многом связаны с инерцией и консерватизмом, внутренне присущим государственным органам власти, включая судебную систему, и к тому же по этому поводу имеются конкретные правовые нормы. Хотя правовая реформа, прямо признающая юридическую действительность, правовую обеспеченность и допустимость электронных средств связи, является решающим шагом в направлении установления юридической уверенности, важно также, чтобы государство проводило кампанию развития использования таких методов работниками государственных органов.

Цель содействия развитию электронной торговли и достижения юридической определенности получила достаточно большое внимание среди международных межправительственных учреждений. В этой связи был достигнут значительный прогресс в направлении поощрения унифицированного подхода к различным вопросам, затрагиваемым в области юридической определенности. Наиболее важный форум рассмотрения таких вопросов - Комиссия по праву международной торговли Организации Объединенных Наций (ЮНСИТРАЛ), выдвинувшая с 1985 года ряд инициатив по реформе в этой области, кончая Конвенцией 2005 года.

Что касается юридической безопасности, то остается задача обеспечения того, чтобы электронная торговля, электронные приложения и электронные услуги внедрялись безопасным образом. Соображения безопасности охватывают вопросы подтверждения подлинности (например, подтверждения личности другой стороны общения), целостности (например, уверенности в неизменности содержания сообщения), конфиденциальности (например, уверенности в том, что несанкционированное лицо не имело доступа к вашему сообщению), наличия (например, уверенности в том, что система при необходимости будет работоспособной), и ответственности (например, уверенности в том, что отчет о событиях может быть создан позднее). Хотя вопросы безопасности в основном затрагивают физические, организационные и логические меры, законодательство может содействовать

внедрению таких мер безопасности. Особое внимание уделяется двум областям, в которых законодательство играет ключевую роль в деле обеспечения юридической безопасности, - электронным подписям и защите данных. Электронные подписи призваны обеспечить то, чтобы юридические акты, совершенные в электронной форме, были аутентичными и целостными, в то время как защита данных имеет своей целью недопущение злоупотреблений личной информацией, полученной в ходе электронной торговли и связанной с ней деятельностью.

Электронные подписи одновременно связаны категориями правовой определенности и надежности. Что касается правовой определенности, то требование "подписания" юридических актов означает, что электронные альтернативы традиционным рукописным подписям должны получить юридическое признание. Однако, поскольку такие требования часто продиктованы соображениями безопасности, вопрос политики заключается в том, в какой мере различные виды электронной подписи должны получить юридическое признание. Используемые методы варьируются от положения имени лица в конце электронного сообщения до использования сложных криптографических методов, обеспечиваемых инфраструктурой пользующихся доверием третьих сторон, которых обычно называют сертификационными органами, способных подтвердить надежность применяемых методов. В зависимости от подхода страны можно в общем плане подразделить на две группы: страны, применяющие разрешительный нейтральный по технологии и методике режим, и страны, устанавливающие более подробное регулирование методов, считающихся приемлемыми, и вводящими режим регулирования, призванный обеспечить такой подход. В свете нынешних тенденций развития рынка развивающимся странам, таким, как страны - участницы СПЕКА, рекомендуется первый из этих двух подходов.

Законы о защите данных в основном связаны с использованием и злоупотреблениями личной информации, т.е. с данными, которые прямо или косвенно идентифицируют человека. Один из элементов такого рода режима касается необходимости реализации соответствующих мер по обеспечению безопасности данных, по защите как от случайного, так и от преднамеренного воздействия на такие данные. В некоторых странах, например в Соединенных Штатах, организации также обязаны уведомить лиц или регулирующие органы о нарушении режима безопасности. Законы о защите данных обычно не считаются непосредственным средством содействия развитию ИКТ и электронной торговли. Кроме того, относительно низкий уровень общей распространенности ИКТ среди населения развивающихся стран уменьшает вероятность массовых злоупотреблений личными данными. В краткосрочном плане наиболее вероятно, что главной задачей принятия законодательства по защите данных станет содействие тому, чтобы предприятия развитых стран размещали свои аутсорсинговые структуры по обработке данных, поскольку озабоченности вопросами безопасности данных и конфиденциальности в развитых странах воспринимаются как потенциальные препятствия для такого рода выноса производств.

Раздел о вопросах юридической защиты затрагивает два ключевых вопроса, защита интеллектуальной собственности и защита потребителей от недобросовестных продавцов в сетевой среде. В международном масштабе имеется высокий уровень унификации материальных мер защиты, предоставляемой основным формам интеллектуальной собственности, включая патенты, товарные знаки и авторские права. Различия часто возникали в отношении национальных процедур, регламентирующих предоставление и

обеспечение осуществления таких прав, которые выходят за рамки настоящего доклада. Рассматриваются некоторые области, в которых рост Интернета как среды ведения дел бросает вызов нынешним режимам и/или создал новые проблемы для директивных органов. Взаимодействие национальных режимов товарных знаков и международной системы доменных имен и связанная с этим практика - наглядный пример проблем, стоящих перед сетевыми предприятиями.

Законодательство об охране прав потребителей обычно преследует цель защиты потребителей исходя из неравенства позиций на рынке и невозможности надлежащим образом защитить от недобросовестной практики. Государство традиционно играет роль защитника тех, кто, как считается, находится в уязвимом положении в коммерческих связях. Однако инициативы по охране прав потребителя можно также рассматривать как механизм на стороне спроса, поддерживающий развитие электронной торговли. Если потребители будут доверять Интернету как среде, в которой они ведут все более широкий круг своих повседневных видов деятельности, от простых операций до представления налоговых деклараций, то тогда электронная торговля продемонстрирует рост.

Необходимо рассмотреть ряд проблем, касающихся защиты прав потребителей. Из-за анонимности Интернета стало труднее подтверждать личность людей, взаимодействующих в Интернете. Эту проблему частично можно решить с привлечением методов обеспечения юридической безопасности, о чем говорилось выше. С этим связан вопрос о применимом праве и возмещении для потребителей в международных сделках. Помимо того, что часто не ясно, какое именно законодательство действует в отношении таких сделок, в случае возникновения трудностей потребителям гораздо сложнее и дороже получить возмещение. Для решения таких проблем созданы совместные механизмы национальных органов по защите прав потребителей, разрабатываются и альтернативные сетевые процедуры урегулирования споров.

Еще одна общая проблема, затрагивающая потребителей, а также граждан в целом, - это проблема социальной изоляции. Большие массы населения мира по-прежнему не имеют доступа к инфраструктуре телесвязи, компьютерам или к компьютерной грамотности. Такие проблемы "цифрового разрыва" выходят за рамки этого доклада, однако всегда должны учитываться при формировании политики.

Последний раздел о правовых средствах сдерживания посвящен вопросу преступности, которая неизбежно использует возможности, создаваемые ИКТ. Инициативы по проведению правовой реформы затрагивали как материальное, так и процессуальное уголовное право. Что касается материального права, то национальные уголовные кодексы, возможно, ненадлежащим образом охватывают использование ИКТ в преступных деяниях, в то время как появляются новые виды преступлений, такие, как хакерство и вирусы, требующие положений sui generis. Процессуальное уголовное право касается правомочий правоохранительных органов по расследованию преступных деяний и привлечению к ответственности виновных. Необходимы новые правомочия для поддержки правоохранительных усилий в среде электронной торговли.

A. Правовая реформа

Важный вопрос для стран с переходной экономикой - как с успехом провести процесс правовой реформы от первоначального признания наличия проблемы и подготовки проекта мер до их официального утверждения политическими институтами страны и осуществления таким образом, чтобы они реально влияли на установки и практику в хозяйственной и административной сфере.

Проведение процесса эффективной правовой реформы часто будет связано с рядом элементов и шагов. Во-первых, необходима прямо выраженная политическая поддержка процесса правовой реформы на самом высоком уровне руководства. Во-вторых, соответствующее министерство должно нести ответственность в этом вопросе и быть готово к выделению достаточных внутренних ресурсов как для проведения необходимой работы внутри министерства, так и для поддержания контактов и активной координации с другими соответствующими участниками этого процесса, в частности другими министерствами и ведомствами. Третий элемент - необходимость выявления и назначения соответствующих технических и юридических экспертов для поддержки ведущего министерства внутри данного органа и/или вне его, находящихся как внутри страны, так и в других странах. После этого работа эксперта или экспертов должна быть поддержана путем создания обзорной группы участников под руководством ведущих министерств, включая представителей общественности и частного сектора. Очевидные потенциальные кандидаты включают представителей министерства юстиции, национальной комиссии по правовой реформе и местных хозяйственников. Любые проекты мер, подготовленные экспертами, после этого проходили бы процесс тщательного изучения обзорной группой участников, которой следует как существенно повысить качество окончательного проекта, так и распространить информацию и усилить поддержку предложения в более широких кругах. Наконец, ведущему министерству следует провести проектные меры через процесс парламентского утверждения, следя за тем, чтобы были предприняты шаги для того, чтобы подробно объяснить политическим представителям задачи, цель и последствия этой меры.

Составление плана правовой реформы всегда значительно проще, чем ее реальное проведение. Успешное обеспечение юридической стороны развития ИКТ требует того, чтобы государства выделяли столько же времени и ресурсов для процесса правовой реформы, что и для различных конкретных тем, указанных в этом руководстве.

B. Рекомендации

В этом Руководстве разобраны некоторые важные вопросы, которые странам - участницам СПЕКА, возможно, потребуется принять во внимание в их будущих реформах политики в вопросах сектора ИКТ. Наиболее важные из них следующие:

- Политическая приверженность руководства государств стран - участниц СПЕКА была бы ключевым предварительным условием успешных правовых реформ в поддержку национальных стратегий ИКТ в конкретные сроки.

- Необходимо предпринять дополнительные усилия по ознакомлению стран - участниц СПЕКА с юридическими и регулятивными последствиями использования ИКТ и электронной торговли.

- Необходимо предпринять усилия по содействию обмену опытом в этой области между странами - участницами СПЕКА на основе региональных учебных семинаров и рабочих совещаний.

- Странам - участницам СПЕКА было бы целесообразно лучше ознакомиться с международным передовым опытом по различным темам и с имеющимися типовыми законами и другими международно-правовыми актами. Имеется достаточное число типовых законов и правовых актов, которые могли бы помочь странам - участницам СПЕКА в решении различных указанных выше вопросов. В частности, рекомендуется, чтобы страны - участницы СПЕКА рассмотрели вопрос о подписании и ратификации Конвенции Совета Европы о компьютерных преступлениях (2001 года) и Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах (2005 года).

- Между странами - участницами СПЕКА следует развивать координированные и согласованные инициативы, позволяющие добиваться значительной экономии в плане времени, опыта и ресурсов, необходимых для такой деятельности.

- В ходе обсуждения на уровне стран, нацеленного на содействие правовым реформам, должны быть представлены все различные участники от предприятий органов государственного управления и гражданского общества.

- Странам - участницам СПЕКА необходимо лучше признать ту особую роль, которую органы государственного управления способны сыграть в деле внедрения и развития электронных средств хозяйственной деятельности и поддержания контакта с органами государственного управления.
