Електронна комерція і право

НАВЧАЛЬНО-МЕТОДИЧНИЙ ПОСІБНИК

для студентів магістерської програми
«Міжнародне та порівняльне право
інтелектуальної власності»

Харків-2010

Програма Європейського Союзу TEMPUS

Проект: «Право інтелектуальної власності: нова магістерська програма для Національного Консалтингового Електронного Центру з управління інтелектуальною власністю»

Вищі навчальні заклади – учасники проекту:

Національна юридична академія України
імені Ярослава Мудрого

Національний аерокосмічний університет
ім. М.Є. Жуковського

Хмельницький національний університет

Королівський Технологічний Інститут (Швеція)
Kungliga Tekniska Högskolan

Університет м. Аліканте (Іспанія)
Universidad de Alicante

Університет Центрального Ланкашира (Великобританія)
University of Central Lancashire

Університет Любляни (Словенія)
Univerza v Ljubljani

Електронна комерція і право/ Уклад**.** А.А. Маєвська -Х.:2010.- 256 с.

Укладач: **Маєвська А.А.**, кандидат юридичних наук, доцент кафедри міжнародного права і державного права зарубіжних країн Національної юридичної академії України імені Ярослава Мудрого

Навчально-методичний посібник «**Електронна комерція і право**» видано відповідно до завдань проекту «Право інтелектуальної власності: нова магістерська програма для Національного Консалтингового Електронного Центру з управління інтелектуальною власністю». Посібник розрахований на студентів зазначеної магістерської програми, які мають освітній ступень бакалавра в галузі правознавства, він також буде корисним для юристів-практиків, підприємців, студентів юридичних факультетів та інших зацікавлених осіб.

Title the manual in English: E-commerce and law.

ЗМІСТ

1. ОРГАНИЗАЦІЙНО-МЕТОДИЧНИЙ РОЗДІЛ

1.1. Анотація навчального курсу

Курс орієнтований на широке коло слухачів, що мають спеціальну юридичну освіту (як мінімум ступінь бакалавра), але які бажають впевнено розбиратися в актуальних правових питаннях, пов'язаних з електронною комерцією. Знання в сфері електронної торгівлі потрібні фахівцям в різних сферах підприємницької діяльності і менеджерам різних рівнів.

Електронна комерція представляє собою середовище, в якому юридична або фізична особа, що знаходиться в будь-якій точці економічної системи, може легко контактувати із мінімальними витратами з будь-якою іншою юридичною або фізичною особою з метою сумісної роботи: торгівлі, обміну ідеями і «ноу-хау» або просто з метою отримання задоволення. І хоча електронна комерція загалом мало чим відрізняється від традиційного бізнесу, вона вимагає від своїх учасників знання спеціальних Інтернет-термінів, оскільки вони слугують підставою для прийняття того чи іншого рішення, пов’язаного із бізнесом. Це пояснюється специфікою підприємницької діяльності в Інтернеті, а саме із прийняттям, переробкою і наданням інформації.

Тому, для того щоб участь в електронному бізнесі була плідною, необхідно мати не тільки серйозну правову підготовку, а й знання про бізнес в Інтернеті, включаючи знання технічних термінів, знання програм електронної пошти, уявлення про World Wide Web, знання принципів роботи з телеконференціями; знання «своєї» аудиторії споживачів продукції, робіт (послуг); проводити дослідження діяльності конкурентів; виробляти стратегію рекламної політики тощо.

Інтелектуальна сфера в даний час відноситься до найголовніших ресурсів будь-якої держави, що визначає його науково-технічний і культурний потенціал, тому створена ціла система, яка регулює правовідносини, пов'язані зі створенням, охороною і використанням об'єктів інтелектуальної власності (в тому числі і у сфері електронної комерції). Ця система постійно розвивається, виникають нові об'єкти інтелектуальної власності, удосконалюються і розвиваються національні законодавства, розширюється міжнародне співробітництво.

Знання в цій галузі допоможуть правовласникам отримувати максимальну вигоду від належних їм прав, використовувати їх у конкурентній боротьбі, а іншим особам - запобігти нелегітимне використання чужих об'єктів інтелектуальної власності і тим самим уникнути можливих конфліктних ситуацій.

У цій програмі викладена тематика і основний зміст (тези) лекційних занять, вказана література та нормативні джерела, позначені контрольні питання для оцінки якості освоєння курсу й т.д.

1.2. Цілі і завдання дисципліни

Мета навчальної дисципліни полягає у формуванні знань про основні напрямки розвитку електронної комерції, способи її ведення, механізми підтримки та основних умінь по застосуванню цих знань, включаючи знання про базові основи функціонування Internet, правові аспекти електронної комерції.

Завданнями навчальної дисципліни є:

- опанування студентами необхідних теоретичних положень щодо охорони авторських прав;
- засвоєння нормативних документів, договорів та угод з авторського права;
- навички аналізу нормативної і економіко-технічної інформації в галузі електронної комерції;
- отримання уявлення про влаштування і принципи функціонування віртуальних крамниць, віртуальні підприємства і віртуальні продукти.

Засобами досягнення цілей та вирішення завдань є навчальні заняття у формі лекцій, практичних завдань, консультацій викладачів (як індивідуальних так і колективних), а також самостійна робота студентів під керівництвом викладачів. Методично студенти забезпечуються програмою

навчальної дисципліни, навчально-методичним посібником, що містить тексти лекцій та рекомендації для організації самостійної роботи, рекомендованою науковою літературою.

В результаті вивчення дисципліни студент повинен знати і вміти:

- аналізувати нормативно-правову і економіко-технологічну інформацію в галузі електронної комерції;

- обґрунтовувати прогностичні оцінки;

- здійснювати закупівлі в Internet;

- мати уявлення про влаштування і принципи функціонування віртуальних магазинів, віртуальні підприємства і віртуальні продукти.

1.3. Рекомендована література

Основна література

Алексеев И. Электронная торговля: правовые проблемы предпринимательской деятельности в Интернете //Юрист.- 2000.- № 3.-С. 43-45

Балабанов И.Т. Интерактивный бизнес. — СПб., 2001. — С. 73;

Балан Р.О. Регулювання діяльності небанківських електронних платіжних систем в Україні //Фінансове право.- 2009.- № 1.-С. 38-42

Батурин Ю.М., Жодзинский А. М. Компьютерная преступность и компьютерная безопасность. - М., 1991.

Борейко Н.М. Оподаткування електронної комерції: досвід іноземних країн // Вісник Академії митної служби України. Серія "Економіка". 2009 р. № 1(41).- Д.: Акад. митної служби України,2009.- С.143-147

Брижко В., Швець М. До питання е - торгівлі та захисту персональних данних //Правова інформатика.- 2007.- Електронний ресурс (№ 1).-С. 14-28

Войниканис Е.А., Якушев М.В. Информация. Собственность. Интернет. Традиция и новеллы в современном праве. – М.: Волтерс Клувер, 2004. – 176 с.

Гарибян А. Правоые аспекты организации электронных платежей //Российская юстиция.- 1996.- № 4.-С. 11-13

Гарибян А. Электронная цифровая подпись: правовые аспекты (Электронные платежи) //Российская юстиция.- 1996.- № 11.-С. 12-13

Грушко П. Міжнародно-правове регулювання електронної комерції та електронного обміну даними //Український Часопис Міжнародного Права.- 2002.- № 1.-С. 45-47

Гуцалюк М. Безпека Інтернет-торгівлі //Правова інформатика.- 2007.- Електронний ресурс (№ 1).-С. 28-30

Джафарли В.Ф. Проблемы безопасности "виртуальных" магазинов (правовой аспект) //Банковское право.- 2003.- № 1.-С. 35-37

Дутов М. Правовое обеспечение развития электронной коммерции //Підприємництво, господарство і право.- 2001.- № 4.-С. 33-35

Дутов М. Сравнительный анализ европейского законодательства в области электронного документооборота //Підприємництво, господарство і право.- 2002.- № 8.-С. 25-28

Європейська інтеграція та Україна. Навчально-методичний посібник. - К., 2002. - 480 с.

Желіховський В. Поширення електронної комерції в Україні //Правова інформатика.- 2007.- Електронний ресурс (№ 2).-С. 52-56

Жилінкова І. Правове регулювання Інтернет-відносин //Право України.- 2003.- № 5.-С. 124-128

Жук А. Правове регулювання здійснення комерційної діяльності в мережі Інтернет // Vivat Justitia!. Вип. 5: Міжнар. студент. наук.-практ. альманах.- Львів: Львів. нац. ун-т ім. І.Франка,2006.- С.70-74

Жучкова И., Коноплева А. Электронный бизнес (e-business): перспективы развития //Економіка, фінанси, право.- 2002.- № 12.-С. 3-6

Злобін С.В. Світовий та вітчизняний досвід організації систем електронної комерції //Науково-технічна інформація. - 2007.- № 3.-С. 36-41

Йогож. Юридические гарантии свободного использования электронной цифровой подписи в Украине // Підприємництво, господарство та право. — К., 2001. — № 9. — С. 24;

Карасюк В.В, Судейко М.А. Електронна комерція: проблеми правового забезпечення безпеки транзакції //Правова інформатика. - 2009.- № 2.-С. 58-69

Коваль Н.Б. Вчинення цивільно-правових угод через мережу Інтернет // Юридичні читання молодих вчених: Зб. матеріалів всеукр. наук. конф., 23-24 квіт.- К.: НПУ ім. Драгоманова,2004.- С.355-357

Копылов В. А. Информационное право: Учебник. 2-е изд., перераб. и доп. - М.: Юристъ, 2003.

Кохановська О.В. Інтернет-економіка України і роль права в процесі розвитку електроннох торгівлі // Вісник. Юридичні науки. Вип. 52-55.- К.: Київ. держав. ун-т ім. Т. Г.Шевченка,2003.- С.163-165

Курбатов А. Правовое регулирование электронных платежных систем по законодательству Российской Федерации //Хозяйство и право.- 2007.- № 9.-С. 68-84

Ларин В.В., Лебедев А.Н., Соловяненко Н.И. Правовое регулирование заключения сделок на современном этапе // http://www.vlarin.chat.ru/larin/diplom.htm.

Макарова М.В. Електронна комерція: Посібник для студентів вищих навчальних закладів. Київ. Видавничий центр „Академія».2002. - 272 с.

Меджибовська Н. Перспективи розвитку електронного бізнесу в Україні //Економіка України. - 2003. - №6. - С. 36-41.

Михайленко. Е. Правовые проблемы использования Интернет-технологий. Теоретический аспект //Адвокат, N 5, май 2004 г.

Міщенко В. Правове регулювання розвитку ринку фінансових послуг на основі електронної комерції // Підприємництво, господарство і право.- 2002.- № 11.-С. 70-73

Наумов В. Ключевые вопросы государственного регулирования Интернет-коммерции в РФ http://www.russianlaw.net..

Новицький А., Позняков С. Сутність та зміст поняття "електронна торгівля" //Правова інформатика. - 2007.- Електронний ресурс (№ 1).-С. 7-13

Пастухов О.М. "Електронна торгівля": nomen est omen? //Адвокат.- 2003.- № 5.-С. 14-15

Петровский С. Законы для электронной коммерции //Российская юстиция.- 2003.- № 7.-С. 72

Плескач В.Л., Затонацька Т.Г. Електронна комерція: Підручник. – К.: Знання, 2007. – 535 с.

Позняков С. Адміністративно-правові аспекти державного контролю і правоохоронної діяльності у сфері оподаткування електронної торгівлі //Правова інформатика. - 2007.- Електронний ресурс (№ 2).-С. 57-62

Правове регулювання електронної комерції. - Ірпінь: Нац. ун-т ДПС України, 2008.- 236 с.

Рассолов И. М. Право и Интернет. Теоретические проблемы.- М.: Издательство НОРМА, 2003.

Рыбалкин И.М., Международное налогообложение: применение понятия "постоянное представительство" к электронной коммерции //Налоговый вестник, №10, октябрь 2001г.

Саввина А. Проблемы защиты интеллектуальной собственности в сети Интернет // Адвокат, N 6, июнь 2004 г.

Свидрук О. Правове забезпечення електронної торгівлі //Підприємництво, господарство і право.- 2001.- № 10.-С. 35-37

Серго А.Г. Интернет и право. М., 2003.

Соколова А.Н., Геращенко Н.И. Электронная коммерция: мировой и российский опыт. – М.: Открытые системы, 2000. -224с.: ил.

Соловяненко Н. Правовое регулирование электронной торговли и электронной подписи (международный опыт и российская практика) //Хозяйство и право.- 2003.- № 1.-С. 27-37

Соловяненко Н.И. Правовые проблемы электронной коммерции в РФ // http://www.fe.msk.ru/otstavnov/Compunomika/vOn05a03.html.

Степаненко Е. Электронная коммерция в России. Основные вопросы //Хозяйство и право.- 2000.- № 12.-С. 23-37

Тедеев А. А. Электронная коммерция (электронная экономическая деятельность); правовое регулирование и налогообложение. - М.: Приор-издат, 2002.

Чубукова О. О формировании национального ринка информационных продуктов и услуг //Экономика Украины. - 1999. - №9. - С. 86-88

Чухно А. Актуальные проблемы стратегии экономического и социального развития на современном этапе //Экономика Украины. - 2004. - №5.- С. 14-23.

Чучковська А. Електронна комерція: деякі проблеми правового регулювання //Право України. - 2003.- № 1.-С. 111-116

Чучковська А.В. Електронна комерція як правове явище //Бюлетень Міністерства юстиції України. - 2006.- № 11.-С. 78-84

Чучковська А.В. Загальна характеристика правовідносин, які виникають у сфері електронної комерції //Бюлетень Міністерства юстиції України.- 2007.- № 3.-С. 58-64

Шамраев А. Электронная коммерция / Сборник документов. – 2003.

Шарма В., Шарма Р. Разработка Web-серверов для электронной коммерции (Комплексный подход). Учебное пособие: - М.: Издательский дом «Вильямс», 2001. – 400с.

Шевченко О. Електронна комерція в умовах чинного законодавства //Право України.- 2003.- № 10.-С. 142-143

Шутаєва О. Міжнародна електронна комерція: сучасний стан та перспективи розвитку в Україні // Схід (журнал), 2004.

Arnold, A *Can metatags and key word purchases constitute trade mark infringement?* (2004) Computer Law and Security Report, Volume 20, Issue 3, page 223.

Azmi, I D *Domain names and cyberspace: the application of old norms to new problems* (2000) IJL & IT Volume 8, number 2, pages 193-213.

Bainbridge, D *Introduction to Computer Law* Pearson, 5th Edition 2004, pp. 135-156, 303-310

Bainbridge, D *Introduction to Information Technology Law* Pearson Longman, 2008. Glossary and chapter 1, pages 1-5, chapter 21, pages 357-373

Boardman, R *Direct marketing -The new rules* (2004) Hertfordshire Law Journal, Volume 2, Issue 1, pages 3-30.

Butler, M *Spam – The meat of the problem* (2003) CLSR Vol. 19, No. 5, pp388-391.

Chaudri, A *Metatags and banner advertisements – do they infringe trade mark rights?* (2004) Computer Law and Security Report, Volume 20, Number 5, pages 402-404.

Cheng, T. S. L. *Recent international attempts to can spam* (2004) CLSR Vol. 20 No. 6, pp472-479.

Chetwin, M & Clarke, B T*he relative effectiveness of technology v legislation in curtailing spam* (2004) C.T.L.R. 10(8), pp192-197.

Chissisk, M & Kelman, A *Electronic Commerce – Law and Practice* 3rd Edition (Sweet & Maxwell, 2002), Chapter 10, pages 241-256.

Christensen, S, Mason, S & O'Shea, K *The international judicial recognition of electronic signatures – has your agreement been signed?* (2006) Communications Law, Volume 11, Issue 5, pages 150-160.

Clark, O *A Practical guide to E-commerce and Internet Law* (ICSA Publishing, 2002), pages 33-40.

Colston, C *Passing Off: the right solution to domain name disputes?* (2000) LMCLQ 523

Commission of the European Communities, Commission Staff Working Document- The implementation of Commission Decision 520/2000/EC

Deveci, H *Domain Names: Has Trade Mark Law Strayed From Its Path?* (2003) IJL & IT, Volume 11, Number 3, pages 203-225.

Downing, S & Harrington, J *The postal rule in Electronic Commerce: A reconsideration* Communications Law 2000, Volume 5, Issue 2, pages 43-47.

Edwards, L & Waelde, C *Law and the Internet: A framework for Electronic Commerce* 2nd Edition, Hart Publishing 2000, Chapter 2, pages 17-35, 309-329.

Freedman, C & Hardy, J *J Pereira Fernandes SA v Mehta: a 21st century email meets a 17th Century statute* (2007) Computer Law and Security Report, volume 23,Issue 1, pages 77-81.

Gringras, C *The Laws of the Internet* 2nd Ed, Butterworths 2002, Chapter 2, pp 14-42, 161-220

Hedley, S *The Law of Electronic Commerce and the Internet in the UK and Ireland*, Cavendish Publishing 2006, chapter 1 (pages 1-15), 165-205, 232-260.

Henderson, B R *Opt-in or Opt-out. Are these the only options?* (May 2005) Journal of Internet Law pages 1, 12-18.

Huston, G *ICANN, the ITU and WSIS, and Internet governance* (2004) World Internet Law Report, Volume 11, Issue 4, pages 26-30.

Information Commissioner *Guidance to the Privacy and Electronic Communications (EC Directive) Regulations 2003*, May 2004, Version 3 (Part 1).

Johnson, D & Post, D *Law and Borders – The rise of law in Cyberspace* (May 1996), Stanford Law Review, Volume 48, number 5, pp 1367-1402 (Available on JSTOR)

Klang,M & Murray, Human rights in the digital age

Kleinwachter, W *WSIS and Internet governance: the struggle over the core resources of the Internet* (2006) Communications Law, Volume 11, number 1, pages 3-12.

Leng, T. K. *Legal effects of input errors in eContracting* (2006) Computer Law and Security Report, Volume 22, Issue 2, pages 157-164.

Lessig, L *The Zones of Cyberspace* (May 1996) Stanford Law Review, Volume 48, Issue 5, pages 1403-1411.

Lloyd, I. J. *Information Technology Law* 4th Edition, Oxford University Press, 2004, Chapter 2 pages 27-43, 528-546.

Lloyd, I. J. *Information Technology Law* 5th Edition, Oxford University Press, 2008, Chapter 22, pages 425-453, 457-472, 477-486.

Middleton, R *Spamming and unsolicited commercial email from a European perspective* (2002) C.T.L.R 13

Munir, A B *Unsolicited Commercial Email: Implementing the EU Directive* (2004) C.T.L.R. 10(5) 105-110.

Murray, A. *The Regulation of Cyberspace,* Routledge Cavendish (2007), Chapter 1 (pages 3-21), Chapter 3 (Pages 57-73).

Murray, A *The use of Trade Marks as Metatags: Defining the boundaries* (2000) IJL & IT, Volume 8, Number 3, pages 263-284.

Niemann, J-M *Cyber Contracts- A comparative view on the actual time of formation* Communications Law 2000, Volume 5, Number 2, pages 48-53.

Office of Fair Trading Market Study *Internet Shopping* June 2007. Available at: http://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft921.pdf**.** (This Report is over 170 pages long. Please do not print it all off!)

Out-law.com article *The use of trade marks in meta tags* October 2005. Available at: http://www.out-law.com/page-6776

Penny, T *Key E-Commerce cases* E-Commerce Law and Policy (June 2006), page 16.

Reed Executive Plc and another v Reed Business Information Ltd and others [2004] 4 All ER 942.

Reidenberg, J *Lex informatica: The formation of Informaiton Policy Rules through Technology* (February 1998) Texas Law Review, Volume 76, Number 3, pp 553-584.

Rogers, K. M. *The Early Ground Offensives in Internet Governance* (2007) International Review of Law, Computers and Technology, Volume 21, Issue 1, pages 5-14.

Rogers, K. *Signing your e-life away* (2006) New Law Journal (19th May), volume 156, number 7225, page 833.

Rogers, K. M . *Snap-Happy consumers leave Kodak in the Dark* May 2002 Business Law Review, pages 112-114.

Rogers, K. M *Snap! Internet 'offers' under scrutiny again'* March 2002 Business Law Review, pages 70-72.

Rogers, K. M, *Spam Nation* (13th April 2007) New Law Journal, volume 157, number 7268, page 510.

Rogers, K. M, *The Privacy Directive and Resultant Regulations – The Effect on Spam and Cookies, Part I* (October 2004) BLR 271-274.

Rogers, K. M. *Contract Conclusion on the web – untangling the weakest link* (2002) The Law Teacher, Volume 36, Number 2, pages 220-240 (especially 220-228).

Schifreen, R *The Internet: where did IT all go wrong?* (2008) Script-Ed, volume 5, issue 2, August 2008.

Todd, P *E-Commerce Law*, Cavendish Publishing 2005, pages 3-21, Chapters 2, 3, Chapter 9, pages 169-196.

Tyacke, N *Internet Law – The legality of Internet «pop-up» ads* (2005) Computer Law and Security Report, Volume 21, pages 262-265.

Wegenek, R *E-Commerce* 3rd Edition, 2002 Chapter 1, E-World, pp. 1-10.

Wild, C, Weinstein, S & MacEwan, N *Internet Law* Old Bailey Press 2005, pp. 3-13, 44-50.

Working Group on Internet Governance *Report of the Working Group on Internet Governance* (2005). Available at: http://www.wgig.org (Click on 'WGIG Final Report' – you can choose any language you wish!)

World E-Commerce and Intellectual Property Report *IBA Session examines Trademark infringements by search engines* (October 2005), Volume 5, Issues 10, pages 12-14,

Додаткова література

Агеенко А.А., Погребинская Т.Ю. Товарный знак и доменное имя в Интернете //Основы государства и права.- 2000.- № 3.-С. 84-88

Андрієць В.С. Структурно-логічна схема оптимізації грошових потоків торговельних підприємств //Економіка, фінанси, право.- 2008.- № 7.-С. 3-6

Асеев Г.Г., Щербинина Е.П. Мобильная коммерция: [Електронний ресурс] // Соціальні комунікації в стратегіях формування суспільства знань [Електронний ресурс]. У 2 ч. Ч. 1 : матеріали міжнар. наук. конф., Харків, 26-27 лют. 2009 р..- Х.: ХДАК,2009.- С.202-204

Брагинский М.И., Витря В.В. Договорное право. — Кн. 1. Общие положения. — М., 2001. — С. 340.

Бредіхін В.М., Дмитрієв І.А.Академія праці і соціальних відносин

Брижко В., Базанов Ю., Швець М. Електронний банкінг у контексті захисту персональних даних.- К.: НДЦПІ АПрН України, 2008.- 141 с.

Використання можливостей ринку B2B у підприємницькій діяльності для виходу на міжнародні ринки // Вісник Академії праці і соціальних відносин Федерації профспілок України. 2008 р. №3/2(45).- К.: Курс,2008.- С.17-19

Винокуров Д. Реальные покупки в виртуальном Internet //.- .- № .-С. 36-41

Вовченко С. Торгуємо на замовлення та вдома //Бизнес (Бухгалтерія. Збірник систематиз. законодавства).- 2002.- 1-2, 18 листопада (№ 47).-С. 157-164

Головин В. Электронный кошелек [Новый способ электронной торговли] //Бизнес.- 2004.- 21 июня (№ 25).-С. 94-95

Голошевич І. Віртуальна торгівля. Це реально?! //Бизнес (Бухгалтерія. Збірник систематиз. законодавства).- 2002.- 1-2, 18 листопада (№ 47).-С. 175

Голошевич І. Інтернет-магазин: як його облаштувати? //Бизнес. Збірник систематизованого законодавства..- 2004.- травень (№ 5).-С. 189-192

Дашян М. //Бизнес-адвокат, №23, 2002 Защита потребителей в виртуальном пространстве

Деркач Т. Інтернет-розрахунки: облік у покупця та продавця //Бизнес. Бухгалтерия.- 2007.- 2 липня (№ 27).-С. 53-57

Дутов М. Юридические гарантии свободного использования єлектронной цифровой подписи в Украине // Підприємництво, господарство і право. – 2001. - №6. – С.24-26.

Єрмошенко М.М. Інформаційні технології у комерційній діяльності //Актуальні проблеми економіки.- 2003.- № 9.-С. 49-58

Желіховський В.М. Електронна комерція як стимулятор розвитку правовідносин у мережі Інтернет [Електронний ресурс] //Правова інформатика. - 2006.- Електронний ресурс (№ 4).-С. 72-78

Звєрєва О.В. Права споживачів у сфер торгівлі на замовлення і вдома у споживачів // Держава і право. Юридичні і політичні науки. Вип.39.- К.: Ін-т держави і права НАН України,2008.- С.370-376

Злобін С.В. Теоретичні засади організації систем електронної комерції //Науково-технична інформація.- 2007.- № 4.-С. 16-20

Золотухін О. Інтернет-магазин: особливості діяльності та обліку //Вісник податкової служби України.- 2009.- № 25.-С. 20-23, 6

Золотухін О. Поставки із "всесвітньої павутини". Як продати програмне забезпечення через Інтернет //Бизнес. Бухгалтерія.- 2006.- 27 марта (№ 13).-С. 89-92

Интернет-банкинг. Что это такое и какое оно бывает (Банковские операции через Интернет) //Бизнес. Бухгалтерия.- 2000.- 28 августа (№ 35).-С. 17-20

Карягіна Н.В. Деякі питання укладання угод комп`ютерним способом // Правові основи захисту комп`ютерної інформації від протиправних посягань: Матеріали міжвуз. наук.-практ. конф., 22 груд. 2000 р..- Донецьк: Донецьк. ін-т внутр. справ,2001.- С.118-122

Ковтунець В.В. Становлення електронного бізнесу в Україні //Актуальні проблеми економіки.- 2001.- (1-2) (№ 1).-С. 51-53

Корниюк О. Электронная коммерция получит защиту //Бизнес. Бухгалтерия.- 2000.- 11 сентября (№ 37).-С. 11-13

Корніюк О. Торгівля - віртуальна, правила - реальні... //Бизнес. Бухгалтерія.- 2006.- 30 жовтня (№ 44).-С. 74-75

Коташевська Т. Дистанційні покупки //Юридичний Радник.- 2008.- № 4.-С. 68-71

Кудрупов Д.О. Анализ источников получения дохода в сети Интернет и связанных с ним рисков // Збірник праць молодих учених Народної української академії.- Х.: Вид-во НУА,2008.- С.142-148

Кузнецов А. Электронные рынки и конкуренция //Вопросы экономики.- 2004.- № 2.-С. 72-81

Лігоненко Л.О., Танасюк П.В. Інтернет-торгівля: стан розвитку та особливості бізнес-планування //Актуальні проблеми економіки.- 2003.- (21) (№ 3).-С. 43-48

Луць В.В. Контракти у підприємницькій діяльності. — К., 2001. — С. 30. http://www.expert.org.ua/2001/01/08010108zls.html.

Материалы 10-й Всероссийской конференции "Проблемы законодательства в сфере информатизации" (г. Москва, 30 октября 2002 г.). М., 2002.

Меджибовська Н. Матеріально-технічне постачання промислових підприємств з використанням інтернет-технологій //Економіка України.- 2006.- № 10.-С. 59-65

Михайленко Е. Некоторые практические проблемы правового регулирования интернет-отношений //Адвокат, №6, июнь 2004г.

Нефьодов А. Інтернет-валюта, або Що таке електронні гроші в Інтернет //Бизнес. Збірник систематизованого законодавства. - 2004.- травень (№ 5).-С. 193-197

Одарюк А. Електронне сало [Электронные платежи] //Бизнес.- 2004.- 16 августа (№ 33).-С. 42-43

Плотица Е. Операторы мобильной связи могут стать конкурентами банков [Электронный бизнес] //Бизнес.- 2004.- 16 августа (№ 33).-С. 44-46

Поленок С. Електронний ринок стає реальністю //Урядовий кур`єр.- 2007.- 20 березня (№ 49).-С. 8

Проблема защиты информации в области электронной коммерции //Борьба с преступностью за рубежом.- 2001.- № 11.-С. 19-23

Руденко И. Суверенитет в паутине. Юрисдикция в контексте электронной торговли //Юридическая практика.- 2002.- 15 мая (№ 20).-С. 6

Руденко И., Капица Ю. Новое платье для короля — электронное // Телеком. Телекоммуникации и сети. — К., 2001. - № 3-4. - С. 40.

Саввина А. Проблемы защиты интеллектуальной собственности в сети Интернет // Адвокат, N 6, июнь 2004 г.

Саввина А. Проблемы защиты интеллектуальной собственности в сети Интернет // Адвокат, N 6, июнь 2004 г.

Симонович С.В. Інформатика для юристів та економістів. — СПб., 2001. — С. 345.

Соловьев В. Электронные документы. Какие они? // http://www.libertarium.ru.

Соловяненко Н. Совершение сделок путем электронного обмена данными (Принципы правового подхода) //Хозяйство и право, №№ 6-7.

Соловяненко Н.И. Разработка законодательства об электронной подписи // Банковское право. — М., 2001. — № 1(73).

Тарасов В.Б. Виртуальное предприятие – ключевая стратегия автоматизации и перестройки деловіх процессов // «Єлектронный офис», №10/1996, с.2-3.

Цыганок А. Держать дистанцию (Дистанционная торговля) //Бизнес.- 2002.- 16 сентября (№ 38).-С. 76-77

Цыганюк А. Интернет-магазин: для чего нужен, как создать, когда окупится //Бизнес. Бухгалтерия.- 2000.- 28 августа (№ 35).-С. 20

Чучковська А. Проблеми державного регулювання діяльності провайдерів сертифікаційних послуг в Україні //Підприємництво, господарство і право.- 2003.- № 11.-С. 21-26

Список корисних для вивчення курсу Інтертнет-ресурсів

1. http://e-commerce.com.ua/ - український портал електронної комерції.
2. http://www.bizmost.biz/ - публікації з електронного бізнесу західних авторів.
3. http://uelbu.org/ - Асоціація учасників електронного бізнесу України.
4. http://bizakademiya.ru/ - виртуальная Академия Интернет Бизнеса (Россия).
5. http://connect.rin.ru/cgi-bin/print.pl?id=2&s=internet - історія

розвитку глобальної мережі Інтернет.

6. http://www.bportal.com.ua/ - український бізнес-портал.
7. http://rubiznes.info/ - безкоштовні електронні книги, статті з електронного бізнесу на порталі RUBIZNES.
8. http://business-planet.ru/ - Інформаційно-аналітичний портал електронної комерції та Інтернет-маркетингу.
9. http://www.wilsonweb.com/ - Wilson Internet Services (Ресурси Інтернет-маркетингу).
10. http://www.inau.org.ua/ - Інтернет асоціація України.
11. http://internetworldstats.com/ - світова статистика Інтернету.
12. http://www.internetstatistic.com/ - світова статистика Інтернету.
13. http://bigmir-internet.com.ua/ - статистика українського Інтернету.
14. http://www.spylog.ru/ - статистика російського Інтернету.
15. http://www.internetnews.com/ - світові новини Інтернету.
16. http://www.idc.com/ - дослідницька агенція IDC Analyze the Future.
17. http://www.comcon-2.com/ - «Комкон-медиа» (дослідження ринку і ЗМІ. Росія).
18. http://ppc-seo.blogspot.com/ - моніторинг Інтернету
19. http://domenua.com.ua/ - реєстрація доменних імен.
20. http://www.imena.ua/ - реєстрація доменних імен.

Нормативно-правові акти

Окинавская Хартия глобального информационного общества от 22 июля 2000 г.

Совет Европы Конвенция «О защите физических лиц в отношении автоматической обработки персональных данных»от 28 января 1981 г. (Страсбург**).**

Соглашение по торговым аспектам прав интеллектуальной собственности (Марракеш, 15 апреля 1994 года)

Политическое послание Комитета министров Всемирной встрече на высшем уровне по вопросам информационного общества (ВСИС) (Женева, 10–12 декабря 2003 года)

Договор ВОИС по исполнениям и фонограммам (Женева, 20 декабря 1996 года)

Закон України «Про інформацію» *(ВВР), 1992, N 48, ст.650);*

Закон України «Про телекомунікації» - *(ВВР), 2004, N 12, ст.15;*

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» *(ВВР), 2005, N 26, ст.347;*

Закон України «Про Національну програму інформатизації» *(ВВР), 1998, N 27-28, ст.181;*

Закон України «Про науково-технічну інформацію» *(ВВР), 1993, N 33, ст.345);*

Закон України «Про електронні документи та електронний документообіг» *(ВВР), 2003, N 36, ст.275);*

Закон України «Про електронний цифровий підпис» *(ВВР), 2003, N 36, ст.276;*

Правила надання та отримання телекомунікаційних послуг, затв Постановою Кабінета Міністрів України від від 9 серпня 2005 р. N 720 // Офіційний Вісник України 2005, N 32, ст. 1935;

Правила Національної системи масових електронних платежів, затв. Постановою Правління Національного банку України 10.12.2004 N 620 // Офіційний Вісник України 2005, N 2, ст. 93

Концепція створення Єдиної державної автоматизованої паспортної системи (ЄДАПС), затв. Постановою Кабінету Міністрів України від 20 січня 1997 р. N 40 // Офіційний Вісник України 1997, 4.

Правила Національної системи масових електронних платежів, затв. Постановою Правління Національного банку України від 10.12.2004 N 620 // Офіційний Вісник України 2005, N 2, ст. 93.

2. ПРОГРАМА ДИСЦИПЛІНИ «ЕЛЕКТРОННА КОМЕРЦІЯ І ПРАВО»

Модуль 1. Основні поняття та принципи електронногобізнесу.

Тема 1. Місце електронного бізнесу в системі світового господарства

Нова (віртуальна) економіка в сучасному інформаційному суспільстві. Ознаки нової економіки та наслідки її розвитку.

Поняття електронного бізнесу та електронної комерції. Місце електронного бізнесу в системі світового господарства.

Історія розвитку електронної комерції.

Тема 2. Глобальна мережа Інтернет як база електронного бізнесу

Історія Інтернету. Інтернет: мережі, завдання, учасники.

Інтернет: юридичні проблеми. Міжнародний розмах. Електронний ринок. Швидко зростаючий звід норм.

Протокол передачі файлу (FTP), доменні імена, посилання.

Характеристика служб Інтернету та їх використання в електронному бізнесі. Комунікаційні характеристики Інтернету.

Перспективи розвитку мережі.

Тема 3. Принципи ведення бізнесу в Інтернеті

Реєстрація підприємства для ведення бізнесу в Інтернеті. Веб-сайт як основа бізнесу в Інтернеті. Класифікація Веб-сайтів.

Товарна політика в Інтернеті. Бізнес-моделі сайтів. Етапи створення

Веб-сайту. Варіанти розміщення Веб-сайту та їх економічна доцільність.

Принципи та економічне обґрунтування вибору провайдера Інтернет-послуг і способу підключення до Інтернету для ведення бізнесу. Поняття Інтернет-маркетингу та Інтернет-реклами.

Особливості Інтернет-реклами.

Принципи первісного залучення відвідувачів на Веб-сайт та їх утримання.

Аналіз роботи та оцінка економічної ефективності Веб-сайту.

Модуль 2. Міжнародна діяльність з просування торгівлі і надання послуг через електронні засоби.

Тема 4. Доменні імена

Реєстрація доменних імен і торговельних марок .

Маркетингові підходи до вибору доменного імені підприємства. Порядок реєстрації доменного імені.

Суперечки відносно доменних імен. Кіберсквоттинг.

Порушення торговельної марки.

Комерція під чужим ім'ям «Пассинг-оф».

Арбітражне врегулювання спорів

Тема 5. Захист інформації у комп’ютерних мережах

Шифрування інформації. Методи шифрування. Закриті та відкриті ключі.

Поняття цифрового підпису та електронного сертифіката.

Використання цифрового підпису та електронного сертифіката в практиці електронного бізнесу.

Протоколи і стандарти безпеки віртуальних платежів.

Тема 6. Міжнародна діяльність з просування електронної торгівлі і надання послуг через електронні засоби

ЮНСІТРАЛ

Типовий закон про електронну комерцію,

Директиви ОЕСД,

Директива ЄС,

Загальний звичай у міжнародній цифровій торгівлі

Модуль 3. Контракти в Інтернеті

Тема 7. Контракти в Інтернеті

Правовий статус угод, укладених в електронному вигляді.

Основні правові вимоги до електронних контрактів. Відповідальність за незаконну електронну інформацію. Відповідальність посередників

Відповідальність за електронну інформацію. Дифамація і Інтернет

Питання помилок і неправильного подання електронної комерції і недбалості; позиція розважливої особи і стандарти обережності

Тема 8. Правове регулювання електронного бізнесу

Правові проблеми реалізації схем електронного бізнесу.

Світовий досвід правового регулювання електронної комерції.

Українське законодавство в сфері електронного бізнесу.

Тема 9. Інтелектуальна власність у електронній торгівлі

Розуміння зв'язку між інтелектуальною власністю (ІВ) та електронною торгівлею

Інвентаризація активів ІВ, що мають значення для електронної торгівлі

Питання ІВ при проектуванні і створенні вашого веб-сайту

Питання ІВ у зв'язку з назвами доменів в Інтернеті

Вплив патентів на ділову практику в галузі електронної торгівлі

Питання ІВ при поширенні змісту через мережу Інтернет

Проблеми ІВ в міжнародних угодах в галузі електронної торгівлі

3. ЗМІСТ ДИСЦИПЛІНИ

Модуль 1. Основні поняття та принципи електронного бізнесу

Тема 1. Місце електронного бізнесу в системі світового господарства

Електронна комерція, е-комерція (*e-commerce*) — Всі форми торгівлі Товарами і послугами завдяки використанню електронних засобів, в тому числі і Інтернету. Електронна комерція є окремим випадком електронного бізнесу.

Електронна комерція — це широкий набір інтерактивних методів ведення діяльності з надання споживачам товарів та послуг. Також під електронною комерцією розуміють будь-які форми ділових операцій, де сторони взаємодіють через електронні технології, а не в процесі фізичного обміну чи контакту. Загалом же електронна комерція — це використання електронних комунікацій та технологій обробки цифрової інформації для встановлення та змін відносин створення вартості між організаціями та між організаціями і індивідами.

Електронна комерція — це ведення бізнесу в он-лайн режимі, яке на сьогодні присутнє в чотирьох наступних сферах: прямі продажі товарів і послуг; банківська справа та фактурування (платіжні системи); безпечне розміщення інформації; корпоративні закупівлі.

Прямі продажі — найдавніший вид електронної комерції, який став першою сходинкою до більш складних комерційних операцій для багатьох компаній. Успіх Amazon.com, Barnes & Noble, Dell Computer став каталізатором для цього сегменту.

Споживачі та представники малого бізнесу можуть зекономити час та кошти, проводячи банківські операції через Інтернет. Сплата рахунків, проведення транзакцій між рахунками, купівля-продаж акцій, облігацій, — все це може виконуватися за допомогою Інтернету.

Для багатьох видів бізнесу інформація є їх найбільш цінним активом. Незважаючи на те, що Інтернет дає можливість освоювати велику кількість нових ринків, паралельно виникає питання безпеки інформаційної та інтелектуальної власності, яке розв'язує Цифровий правовий менеджмент.

Також Інтернет дає можливість заощадити велику кількість часу і коштів на корпоративних закупівлях. Жодна інша модель бізнесу так не підкреслює необхідність тісної інтеграції між виробниками, постачальниками та дистриб'юторами, в процесі якої встановлюється ринкова ціна. Збільшення швидкості проходження цього ланцюжка за допомогою можливостей, які відкриває Інтернет, значно підвищує ефективність.

Сьогодні, приблизно 60 000 видів бізнесу обмінюються із своїми партнерами діловою документацією типу замовлень і рахунків за допомогою стандартного зв'язку і протоколу, що називається *Електронний Обмін Даних (EDI)*. Більшість реалізацій EDI використовують орендовані лінії або спеціалізовані мережі (value added networks, VANs), а це спричиняє необхідність значної інтеграції між всіма партнерами. Мережний дизайн, інсталяція й адміністрація можуть бути дорогими в термінах апаратних засобів, програмного забезпечення і штату. Фактично, ці витрати — ключова причина того, що EDI найбільше широко розгорнуті тільки в великих компаніях.

Проблеми впровадження

Незважаючи на очевидні переваги електронної комерції, розвинути і впровадити комерційну систему досить важко.

Компанії можуть зіштовхнутися з істотними проблемами, такими як: затрати, цінність, безпека, посилення існуючої системи, функціональна сумісність.

Затрати. Електронна торгівля вимагає істотних інвестицій у нові технології які можуть торкнутися багатьох із основних ділових процесів компанії. Як всі головні ділові системи, електронні системи торгівлі вимагають істотних інвестицій в апаратні засоби, програмне забезпечення, укомплектування персоналом, і навчання. Комерційна діяльність має потребу у всеохоплюючому рішенні, яке буде простим у використанні і сприятиме збільшенню рентабельності.

Цінність. Компанії хочуть знати, що їхні інвестиції в електронні системи торгівлі окуплять себе і принесуть прибутки. Досягнення цілей типу визначення кола потенційних споживачів, автоматизації ділових процесів, скорочення вартості повинно гарантуватися. Системи, які використовуються для розв'язання таких задач, повинні бути досить гнучкі, щоб змінитися, коли змінюється бізнес.

Безпека. Internet забезпечує універсальний доступ, але компанії повинні захистити їхні активи від випадкового або зловмисного неправильного використання. Системний захист, однак, не повинен створити перешкоджаючу складність або зменшити гнучкість. Інформація клієнта також повинна бути захищена від внутрішнього й зовнішнього неправильного використання.

Посилення існуючої системи. Більшість компаній уже використає інформаційні технології для ведення бізнесу поза межами Internet, в таких сферах як маркетинг, управління замовленнями, складання рахунків, обслуговування клієнтів, тощо. Internet надає альтернативний додатковий спосіб ведення бізнесу, але обов'язково електронні системи торгівлі повні бути інтегрованими із вже існуючими таким чином, щоб уникнути дублювання функціональних можливостей й підтримувалися їх застосовність, поточна робота і надійність.

Функціональна сумісність. Коли системи двох або більше видів комерційної діяльності здатні обмінюватися документами без безпосереднього втручання, бізнес досягає скорочення вартості, поліпшеної роботи і збільшення динамічності ланцюжків створення вартості. Невдача по будь-якому із зазначеним пунктів може привести до краху всіх зусиль по впровадженню системи. Тому стратегія комерції компанії повинна бути розроблена так, щоб вирішувати всі ці проблеми й допомагати клієнтам досягати вигід від електронної торгівлі.

Бачення компанією електронної торгівлі повинне також допомагати бізнесу встановлювати більш міцні відносини з партнерами й клієнтами.

Основні принципи технології електронної комерції

Щоб створити основу для швидкого росту електронної комерції, підприємства повинні прийняти ефективну політику технології електронної комерції, що полягає в наступних чотирьох критичних принципах:

1) Сильний захист інтелектуальної власності (сильне авторське право, патент, і інші форми захисту інтелектуальної власності є ключовими до підбадьорення інформаційної економіки).

2) Інтерактивна довіра: захист і таємність (без упевненості споживача в безпеці, захисті, і таємності інформації в кібер-просторі, не буде ніякої електронної комерції й ніякого росту).

3) Вільна й відкрита міжнародна торгівля (закриті ринки й дискримінаційна обробка будуть душити електронну комерцію. Інтернет — глобальне середовище, і правила інформаційної економіки повинні відбити той факт).

4) Вкладення в інфраструктуру технології електронної комерції (підтримка фізичної інфраструктури, необхідної, щоб поставляти цифровий зміст, життєвий для заохочення технологічного росту).

США

На сьогоднішній день лідером у сфері новітніх технологій електронної комерції є США. Цьому сприяло стійке економічне зростання1990-2000 рр., що супроводжувалося збільшенням продуктивності праці вдвічі за цей період. У той же час стрімко розвивалася індустрія комунікаційних технологій, значно підвищувалася кількість користувачів, радикально змінилася вартість комп'ютерів та їх комплектуючих. Якщо в 1990 р. лише 15% родин США мали комп'ютери, то сьогодні цей показник перевищує 50%. Причина полягає в тім, що в період з 1987 до 1994 року комп'ютери дешевшали на 10 - 12 %, а з 1995 р. - майже на 20% щорічно.

Галузь електронної комерції зростає надзвичайно динамічно - на початку століття вона подвоюється щорічно, а наприкінці 2003 року обсяг світової торгівлі через мережу Інтернет досяг майже 1,25 млрд дол. США (1).

Важливим компонентом розвитку є створення галузевих Інтернет-ринків. Так, наприклад, у 2000 році три світові автомобільні корпорації - "Форд мотор", "Дженерал моторс", "Даймлер-Крайслер" з метою сприяння закупівлі комплектуючих деталей та інших товарів, прискорення виробничого процесу та зниження собівартості кінцевої продукції оголосили намагання створити найбільший у світі спеціалізований автомобільний Інтернет-ринок, який також дозволить зменшити термін доставки комплектуючих та автомобілів покупцям з 2 місяців до 10 днів.

Важлива галузь електронної комерції - комерція "бізнес - споживач" - прискорює темпи розвитку. Незважаючи те, що більшість світових користувачів увійшли в Інтернет тільки два роки тому, за даними Forrester Research, у 1994 р. споживачі США витратили на купівлю в Інтернеті тільки 240 млн. дол., а в 2000 р. - уже близько 10 млрд. дол. США. З них 33% - на комп'ютерні товари, 23% - на подорожі, 13% - на розваги, 10% - на квіти і подарунки, 5% - на одяг. Близько 40 % покупців США використовують свої web-сайти для проведення хоча б деяких комерційних трансакцій.

Збільшується і кількість користувачів, що роблять регулярні покупки в он-лайні. Так, у 1998 р. це приблизно 6 млн. родин, а до 2010 р. ця цифра повинна досягти 20 млн.

Обсяг торгівлі через Інтернет вже обчислюється декількома трильйонами доларів. У найближчі роки він досягне 10 трлн дол., що еквівалентно всій економіці США. Безумовно, за рахунок виходу в он-лайн і завдяки скороченню або повному відмовленню від традиційних витрат, пов'язаних з веденням бізнесу, компанії в усьому світі заощадять кількасот млрд. дол.

Таким чином, вищевикладені факти дозволяють зробити висновок, що електронна комерція стане одним з наймогутніших сегментів національної економіки не тільки США, але й багатьох країн світу, що з успіхом упроваджують нові технології в усі сфери життєдіяльності суспільства.

Європа

Тенденції електронної комерції в Європі найближчим часом розвиваються в напрямку розширення Інтернет-економіки. У найближчі два роки очікується збільшення користувачів електронної комерції, що приведе до росту продажів у 20 разів. Швидке зростання числа користувачів Інтернет приведе до того, що в цьому регіоні світу половина населення буде мати доступ в Інтернет. Найбільший ринок електронної комерції в Європі у Німеччини (30% від загального обсягу, причому зараз вже 95% німецьких родин були підключені до Інтернету), далі йдуть Великобританія (23%), Франція (9%). Зміцнення позицій Інтернет-економіки пов'язано з очікуваним підвищенням рівня життя населення європейського континенту і збільшенням національного багатства. В Інтернет-сегменті ринку основними будуть продукти програмного забезпечення й послуги. Європейський ринок інформаційних технологій буде розвиватися в напрямку збільшення кількості послуг для різних секторів економіки: для промислового сектора - електронна торгівля "бізнес-бізнес", для фінансового сектора - Інтернет-банкінг, для енергетики - онлайновий білинг, для транспортного сектора - онлайнове планування і керування перевезеннями, для торгівлі - Інтернет-магазини, для освіти - дистанційне навчання. У найближчі три роки очікується активне використання нових форм електронної торгівлі: безпровідної, голосової, телевізійної. Понад 80% керівників європейських фірм від подібних технологій чекають більшого ефекту, ніж від звичайної електронної комерції.

Український сектор

За останні два роки ріст українського сегмента Інтернету (UAnet) спостерігається у всіх напрямках. Аудиторія UAnet подвоювалася щорічно за останні три роки, за різними оцінками, складає від 2 до 4% населення. UAnet містить у собі більш як 12 тис. українських сайтів. Очікується щомісячний ріст відвідувачів UAnet на 15%, 56% аудиторії UAnet представлена жителями України, 19% - Росії, 12% - США, 8% - Західної Європи, 5% - інші. Регулярна аудиторія користувачів UAnet, що проживають в Україні, - 450 тис., а користувачів Інтернету - від 750 тис. до 2 млн. чоловік. Швидке збільшення користувачів Інтернет стане рушієм Інтернет-сектора в Україні. Інтернет-економіка нашої

країни представлена галузями комп'ютерної техніки і комунікаціями, рекламою і медіа-індустрією, Інтернет-послугами, електронною комерцією.

Сфера Інтернет-комерції розвивається не так швидко, як інші сегменти вітчизняного Інтернет-ринку, і має більш скромні інвестиції, тому що Інтернет-магазини ще не одержали масового визнання українськими покупцями. В авангарді української електронної комерції Інтернет-магазини Molotok.com.ua, Bambook, Azbooke, Webshop. Kiev.ua. Через UAnet сьогодні добре продаються товари, що не вимагають контакту з покупцем: книги, касети, картки мобільного зв'язку, комп'ютери та комплектуючі. Багатообіцяючим є ринок туристичних послуг, ринок продажів та оренди житла, продажів автомобілів, коштовностей, рідкісних товарів. Водночас, за інформацією компанії TNS Interactive, всього 4% жителів України мають доступ до мережі Інтернет і лише 1% користувачів є одночасно Інтернет-покупцями.

Дуже перспективним в Україні є така форма організації інформаційної та торговельної взаємодії між компаніями через Інтернет, як електронна комерція "бізнес-бізнес". В умовах поглиблення міжнародного поділу праці, активного розвитку спільної комерції, коли підприємства не тільки купують один у одного продукцію, а й спільно працюють над виробництвом нових товарів та послуг, електронна комерція такого напрямку набуває особливого значення, оскільки вона передбачає формування тривалих партнерських відносин між підприємствами, які здійснюються через комунікаційні мережі.

В Україні вже створюються корпоративні портали, в межах яких систематизується корпоративна інформація та надається доступ до неї сертифікованим користувачам. Прикладом є корпоративні системи компаній "Квазар-Мікро" та Softline. Перспективним для України є також створення електронних ринків, систем управління ланцюжком комплектації, систем управління взаємовідносинами з клієнтами. Важливим кроком у напрямі впровадження будь-яких систем "бізнес-бізнес" є використання відкритих міжнародних стандартів. В Україні вже існують технічні умови застосування цих технологій - створено національний електронний каталог товарів.

Для активного включення України в міжнародний електронний бізнес необхідне:

1. активне впровадження базового устаткування, комп'ютерів та телекомунікацій, у тому числі й у сільській місцевості, що забезпечить розширення комп'ютерної грамотності населення і належний рівень розвитку інфраструктури;
2. стимулювання швидкого розвитку інфраструктури мережі: розвиток Інтернет-магазинів, мережних бізнес-структур, операторів мережі та створення декілька великих вітчизняних Інтернет-порталів;
3. навчання професійним і загальним навичкам роботи в Інтернеті на всіх рівнях освітньої системи, включаючи держслужбовців;
4. розвиток внутрішнього споживчого ринку, підвищення купівельної спроможності шляхом досягнення стабільного економічного росту.

Тенденції останніх років

На розвиток міжнародної електронної торгівлі в Україні та світі впливають ще й загальносвітові тенденції.

По-перше, в останні роки у зв'язку зі зниження цін на комп'ютерні системи і програмне забезпечення спостерігається бум у галузі продажів комп'ютерів.

Друга тенденція полягає у зростанні кількості користувачів Інтернетом. До 2020 р. приблизно більш як 1 млрд. людей почнуть виходити в он-лайн і буде створено понад 100 млн. сайтів. Український сегмент Інтернету в даний час являє собою більш як 12 тисяч сайтів, і також очікується щомісячний ріст відвідувачів на 15 % .

Третя тенденція - це ріст он-лайнових покупок, обсяг яких збільшився з 8 млрд. дол. у 1999 р. до більш ніж 100 млрд. у 2003 р.

Четвертий напрямок пов'язаний з різким ростом кількості домашніх компаній. Кількість людей, що працюють удома, підскочило з 4 млн. у 1990 р. до майже 16 млн. у 2000 р.

Широкому впровадженню електронної торгівлі на території держав-учасників ЄврАзЕС поки перешкоджають нерозвиненість інформаційних і комунікаційних технологій (ІКТ), недосконалість нормативно-правової бази, відносна слабкість багатьох фінансових і кредитних організацій, порушення взаємних зобов'язань учасниками торгових відносин, відсутність інформаційної структури товарних ринків, адекватної сучасним вимогам.

У зв'язку з цим існує необхідність у розробці і реалізації спеціальної міжнародної цільової програми на найближчі роки, яка сприяла б розвитку електронної торгівлі на інтеграційній основі. У країнах ЄврАзЕС є ряд національних проектів і програм, спрямованих на створення основ електронної комерції, наприклад, "Концепція розвитку електронної комерції в Республіці Казахстан", програма в Російській Федерації "Організаційно-правові стандарти електронної комерції", спільний проект Киргизької Республіки та Естонії "ІКТ для розвитку ".

У той же час в їх законодавчих системах не існує законодавства, повною мірою визначає параметри використання електронних еквівалентів відповідних договорів і розвитку сучасної системи електронних платежів. Це не дозволяє укладати контракти за допомогою обміну електронними даними, розвивати відносини між суб'єктами електронної комерції. До того ж для створення повноцінної заміни паперового еквіваленту електронним необхідно мати кілька типів договорів та контрактів.

У кожній країні ЄврАзЕС потрібні закони, що визначають юридичну силу електронного документа, повинні бути прийняті нормативні документи для юридичних осіб з метою забезпечення якісної експлуатації системи електронної торгівлі, вирішені правові питання щодо конфіденційності, оподаткування при електронній комерції, контролю за експортом криптографічних технологій, використання даних про характер поведінки відвідувачів сайту, інформації про покупки, забезпечення анонімності операцій і т. д.

Стратегічним завданням всіх країн ЄврАзЕС стає спільна розробка типового проекту про електронну торгівлю, який містив би перелік основних принципів регулювання електронної торгівлі і визначав її сферу, учасників, необхідний комплекс нормативних актів, параметри її саморегулювання за допомогою "кодексів поведінки", умови безперешкодного здійснення комерційної діяльності, вільного переміщення товарів, послуг і фінансових коштів у рамках ЄврАзЕС та гарантії судового захисту прав учасників електронної торгівлі.

У той же час такий типовий проект не має напряму коригувати національне законодавство про оподаткування, антимонопольних правилах, обіг цінних паперів, спадковому праві, нотаріат, захисту клієнтів, представництві в суді і т. д.

Подібні обмеження існують в зарубіжному законодавстві про електронну комерцію і відповідають положенням Директиви Європейського Союзу "Про електронні підписи" (1999р.). З урахуванням змін в законодавстві повинні змінюватися і акценти в системі управління - перш за все для прийняття рішень на рівні менеджменту у фірмах і розширення зворотного зв'язку з громадянами і громадськістю повинна розвиватися практика підключення юридичних осіб та громадян до системи державно фінансуються інформаційних послуг і покупки таких послуг через Інтернет. У зв'язку з цим необхідні і організація тендерів по послугах базової державної інформаційної мережі, і збільшення розмірів інвестування в Інтернет-мережі регіонів і муніципалітетів.

При створенні і вдосконаленні законодавства про електронну комерцію слід всебічно використовувати положення відповідних міжнародних конвенцій та досвід учасників Європейського союзу. У багатьох країнах ЄС прийняті спеціальні нормативно-правові документи, що регулюють електронні підписи, наприклад, в Німеччині вже в 1997 році - закон "Про електронний цифровий підпис". У США такі закони мають навіть окремі штати. Маються на увазі Закон Штату Юта "Про електронний цифровий підпис" (1996р.), відповідні закони штатів Каліфорнія і Массачусетс і т. д.

При вирішенні в період 2002-2010 рр. комплексу стратегічних завдань з розвитку економічної інтеграції держав-учасників Євразійського економічного співтовариства використання такого досвіду набуває особливого значення.

У першу чергу, це відноситься до Директиви Європейського союзу про правові основи використання електронних підписів (прийнятої 13 грудня 1999), що вводить в правозастосовну практику положення, згідно з якими держави - учасники інтеграційного утворення можуть формувати систему добровільної акредитації для підвищення якості сертифікованих інформаційних послуг, визнавати сертифікати, видані постачальниками послуг третіх країн, а також повинні приймати спільні заходи проти шахрайства з сертифікатами.

У Всесвітній організації торгівлі на рубежі XX і XXI століть почалися багатосторонні торгові переговори з питань міжнародного регулювання електронної комерції. Динамічне зростання операцій в цій сфері призвів до розвитку багатосторонніх торговельних переговорів з методів збору митних платежів, сплату ПДВ та деяких інших податків, щодо захисту прав інтелектуальної власності, визначення країни походження товару, поставленого за допомогою електронних засобів, проблем законності електронної угоди, автентичності комерційних документів, складених у письмовому вигляді або підписаних власноручно її учасниками, і т. д.

У травні 1998р. на Женевській конференції міністрів країн-членів СОТ прийнята Декларація про глобальну електронну комерцію. У ній міститься доручення Генеральній раді СОТ розробити програму з вивчення всіх торговельних аспектів електронної комерції, закріплена домовленість країн-членів СОТ продовжувати практику, що склалася щодо обкладання електронних торговельних операцій митними зборами. Ця домовленість, формально діяла до чергової міністерської конференції в Сіетлі, що відбулася в листопаді-грудні 1999р., була продовжена і згодом може придбати обов'язковий характер.

Паралельно з переговорами фахівцями вивчається питання про характер модифікації міжнародних правил торгівлі товарами і послугами, положень, що регулюють охорону прав інтелектуальної власності з урахуванням особливостей, властивих електронної комерції.

Досвід розвитку електронної комерції в США і Західній Європі показує, що повинні застосовуватися уніфіковані правила і на державному рівні, і на рівні взаємин фірм. Вони необхідні для ефективного функціонування торговельних систем (за допомогою угод в Інтернеті), платіжних систем (виконання грошових зобов'язань, що виникають при здійсненні операцій в Інтернеті), систем доставки товарів (гарантій при його поставці), систем арбітражу (для вирішення суперечок).

При створенні сучасного ринкового господарства виникає потреба у координаційній механізмі - для узгодженої розробки законопроектів у сфері інформатики та експертизи інших законопроектів з позиції використання інформаційних технологій при реалізації законів. При цьому загальна координація ІКТ може бути ефективною, якщо буде мати прямий вплив як на правові, так і на фінансові аспекти ІКТ.

У країнах Євразійського економічного співтовариства діяльність, пов'язана із запровадженням та використанням ІКТ, поступово починає розвиватися.

У Російській Федерації існує Федеральний закон "Про електронний цифровий підпис", прийнятий Державною Думою 13 грудня 2001 р. Він передбачає правові умови для використання електронного цифрового підпису в електронних документах - умови, за яких електронний цифровий підпис в електронному документі визнається рівнозначного власноручного підпису в документі на паперовому носії.

Роком раніше в Республіці Білорусь, 10 січня 2000 році, був прийнятий закон "Про електронний документ", в якому визначено правові засади застосування таких документів, вимоги до них, права, обов'язки і відповідальність учасників правовідносин у сфері обігу електронних документів.

На першому інформаційному саміті "ІКТ для розвитку" в Киргизькій Республіці (27-28 лютого 2001 року в Бішкеку) були всебічно обговорені основні завдання реалізації національної стратегії в області інформаційних і комунікаційних технологій.

До таких завдань були віднесені:

- Забезпечення прозорого і підзвітного управління державним сектором економіки;
- Сприяння створенню конкурентного економіки;
- Створення рівних умов для доступу до інформації;
- Формування законодавства, що забезпечує свободу інформації і разом з тим захист інтересів держави, підприємців, виборців, споживачів, інтелектуальної власності.

На практиці відповідні рішення означають: забезпечення вільного доступу всіх громадян та суб'єктів приватного бізнесу до правових державних актів, у тому числі для впевненого виходу на ринок ІКТ; створення сучасної державної комп'ютерної системи; формування системи громадського доступу до Інтернету та інформаційних центрів у регіонах і містах.

У Республіці Казахстан при розробці концепції розвитку електронної комерції до найважливішим стратегічним рішенням віднесені:

- Підготовка інформаційного проекту міжнародних торгових угод за допомогою електронної торгівлі;
- Створення регіональних центрів електронної торгівлі;
- Організація пілотної зони електронної торгівлі;
- Впровадження в систему електронного бізнесу апаратно-програмних комплексів "бізнес-бізнес" та "бізнес-споживач";
- Розробка закону "Про електронний документ та електронний цифровий підпис";
- Створення системи управління цифровими сертифікатами;
- Акредитація центрів сертифікації та випробувальних лабораторій у сфері електронного бізнесу;
- Організація навчально-консультаційних центрів з електронної комерції.

У Росії за планами експертно-координаційної ради при Комітеті з економічної політики та підприємництва Державної Думи робочою групою з електронної комерції у вересні 2000 року був прийнятий проект програми "Організаційно-правові стандарти електронної комерції". Визначено наступний перелік базових документів, необхідних з метою використання ІКТ: рекомендації з організації діяльності в області Інтернет-комерції; типовий контракт; типова угода про використання електронного цифрового підпису; регламент третейського суду та типова третейське застереження; регламент для внесення змін у документи. Рекомендації при цьому є елементом комплексної системи підтримки електронної комерції, що передбачає інформування громадськості, підтримку організацій, що використовують практичний досвід розвитку електронних угод, забезпечення доказів і захист прав споживачів, третейський вирішення спорів.

У розглянутому Державною думою проекті федерального закону про електронні угодах, що укладаються юридичними особами та індивідуальними підприємцями, з основою вказується на те, що, по-перше, законодавство про таких угодах має використовуватися поряд з іншим законодавством, що регламентує підприємницьку діяльність, охорону прав споживачів та авторських прав; по-друге, якщо в міжнародних договорах передбачено інші правила, ніж у законі про електронну комерцію, то застосовуються правила цих договорів.

28 січня 2002 Уряд РФ затвердив стратегічну програму "Електронна Росія (2002 - 2010 роки)", яка має забезпечити формування нормативно-правової бази у сфері ІКТ, розвиток інформаційної та телекомунікаційної інфраструктури, створити умови для підключення до відкритих інформаційних систем (через Інтернет, перш за все) і для ефективної взаємодії органів влади з громадянами і господарюючими суб'єктами на основі широкого використання ІКТ.

З 2002 року розробляється і використовується система моніторингу для оцінки ефективності витрачання коштів у сфері ІКТ та ефективності існуючої нормативної правової бази, що регулює цю сферу. З 2003-2004 рр. формуєтья сучасна нормативна база для електронних угод, основа єдиної інформаційної та телекомунікаційної інфраструктури, матеріально-технічна база для підготовки фахівців з ІКТ. У 2010 рр. передбачається завершити створення єдиної інформаційної та телекомунікаційної інфраструктури для органів державної влади, місцевого самоврядування, бюджетних і некомерційних організацій і забезпечити підключення населення та суб'єктів бізнесу до загальнодоступних інформаційних систем через спеціальні громадські пункти.

Найважливішим передбачених програмою заходів є формування системи електронної торгівлі, в тому числі для здійснення державних закупівель, з підсистемою інформаційно-маркетингових центрів і єдиною базою даних про продукцію і послуги, доступною (через комп'ютерні мережі) для всіх громадян, господарюючих суб'єктів і владних структур.

Міжпарламентська Асамблея Євразійського економічного співтовариства з метою гармонізації відповідного законодавства держав-учасників 25 березня 2002 прийняла типовий проект "Про електронний документ".

Електронна комерція вигідна і постачальникам, і клієнтам, оскільки забезпечує глобальний ринок збуту, підвищує конкурентоспроможність, створює можливість для ефективної індивідуальної діяльності, скорочення або усунення складної системи поставок, скорочення витрат, підвищення якості обслуговування, розвитку оперативної інформації про нові товари та послуги і т. п.

В даний час у всіх державах-учасниках ЄврАзЕС за поки нерозвиненою електронної комерції існує все зростаюча потреба у проведенні різних заходів для її розвитку та підвищення рівня єдності інформаційних систем в ЄврАзЕС.

Тема 2. Глобальна мережа Інтернет як база електронного бізнесу

Для того щоб повністю зрозуміти феномен Інтернету і, як юристи, визначити правові проблеми і запропонувати адекватну відповідь, необхідно чітке розуміння технічних аспектів середовища.

Введення в Інтернет та електронної комерції. Коротка історія Інтернету

Інтернет має своє коріння в Сполучених Штатах Америки, і був випробуваний під час "холодної війни". Новий протокол зв'язку, ARPANET, був розроблений з метою прискорення обміну інформацією. Згідно з цим протоколом, повідомлення розбивалося на кілька частин і відновлювалося після його доставки адресату. Зацікавлені щодо можливостей, що відкриваються завдяки такій мережі ARPANET, швидко після американської адміністрації приєдналися вчені. З часом, ARPANET вичерпав потенціал і був замінений NSF-Net, мережею Національного наукового фонду США, урядових агенції для фінансування досліджень. Підключення NSF-Net на інші мережі та комп'ютери сприяло появі Інтернету на початку 80-х.

Інтернет прибув до Європи в 1988 році через мережу EBONE, яка з'єднувала США і Європу. Він був відкритий для публіки в 1992 році зі створенням гіпертекстових зв'язків Тімом Бернерс-Лі. З тих пір Інтернет може бути визначений як мережа мереж, з міжнародним охопленням, у якій IT-прилади говорять однією мовою і використовують однакові методи для поширення інформації.

У 1995 році постановою Ради Федеральної мережі Інтернет (або "кіберпростор») визначений, як "... глобальна інформаційна система, що логічно пов'язує глобальний унікальний адресний простір на основі Інтернет-протоколу (IP) або його подальших розширень/наступних доповнень; (II) здатна підтримувати комунікації з використанням Transmission Control Protocol / Протокол Інтернету (TCP / IP) або наступних розширень / наступних доповнень та / або інших IP-сумісних протоколів, і (III) передбачає, що її використання робить доступним високий рівень обслуговувавання державного або приватного зв’язку"(цит. за Murray, стор 59).

Інтернет являє собою структуру, яка дозволяє користувачам обмінюватися інформацією на відстані, працювати, проводити дослідження, обговорення, передачі файлів і т.д. Кожне з цих завдань спирається на конкретні програми. Найбільш поширеними додатками в Інтернет є: Електронна пошта, World Wide Web, новини, Internet Relay Chat, віддаленість роботи та передачі файлів. В останні роки ми стали свідками подальшого розвитку додатків, включаючи VoIP (голос через Інтернет протокол), а також розвиток торгівлі і Wi-Fi.

Інтернет працює завдяки багатьом акторам, які забезпечують зв'язок у мережі Інтернет, надають послуги в мережі або забезпечують додатки. Споживачі як одержувачі послуг і як особи, що генерують інформацію, розміщену в Інтернет, і актори.

Директива від 8 червня 2000 р про електронну комерцію визначає в статті 2 (б) термін "постачальники послуг», як будь-яку фізичну або юридичну особу, що надає послуги інформаційного характеру. Поняття інформаційної служби визначається шляхом посилання на інші директиви.

Відповідно до статті 2 (е) директиви в галузі електронної торгівлі, споживач - це будь-яка фізична особа, яка діє в цілях, які не пов’язані із її торгівлею, бізнесом або професією.

Інтернет розвинувся в середині 1990-х років і в даний час займає центральне місце у здійсненні електронної торгівлі в діловому світі 21-го століття, пройшовши складний шлях.

В кінці 1990 і на початку 2000-х років Інтернет як засіб маркетингу себе дійсно не виправдав. Багато з рекламних компаній в Інтернеті, витрачаючи величезну кількість грошей, за порівняно короткий період часу збанкрутували, інші були оцінені в набагато завищені значення. Наприклад, Priceline.com (інтернет-компанія для відпочинку компаній і авіакомпаній, які й до сьогодні займаються торгівлею), які були представлені на фондовому ринку в 1999 році і протягом тижня втратили 25 млрд. дол США; це незважаючи на той факт, що в 1998 році Компанія втратила $ 114 млн. доларів.

Незважаючи на очевидні переваги електронного простору, споживачі неохоче ведуть бізнес в Інтернеті, що, мабуть, пояснюється певними недоліками в системі Інтернет.

Помилковість в Інтернет не є єдиною причиною для стриманості споживачів щодо укладання угод в Інтернеті. Незважаючи на те, що онлайн-транзакції продовжують зростати, безпека, видима відсутність виконання правил та відсутність довіри з боку споживачів (в основному через відсутність фізичної близькості) є тими причинами, через які є небажання укладати угоди в Інтернеті.

Ключовим питанням для розуміння Інтернет є питання природи кордонів. Жодна країна не має юрисдикції і не несе юридичної відповідальності від імені Інтернет. Це міжнародне середовище, яке працює за допомогою практично усіх країн світу.

Є конфлікт між комерційними потребами і захистом прав споживачів. Ця суперечка є не тільки в законодавстві, що стосується Інтернету, хоча існують різні приклади. Наприклад: бізнес-потреби (рекламувати, просувати і продавати товари) проти потреб споживачів (бути захищеним від поганої онлайн-практики)

Але характеристики мережі Інтернет, такі, як міжнародний характер середовища та дематеріалізація товарів і послуг, створюють нові проблеми. З одного боку, при використанні Інтернету часто пов'язані безліч держав, законів, приватних осіб, компаній і культур, які стикаються щодня. Це створює проблеми: наприклад, те, що прийнято в суспільстві в одній частині світу, не може бути схвалено в іншому. Так, наприклад, вихваляння нацизму є злочином у Франції, але допускається в США, згідно з Першою поправкою Конституції 1787 р. У реальному світі, що складається з фізичних кордонів, важко протистояти інтернаціоналізації, яка є суттю Інтернету.

З іншого боку, міжнародний вимір Інтернет надає необмежені можливості для отримання глобальної клієнтської бази. Це можна зробити з меншими витратами, тому що нема необхідності відкривати філіали за кордоном, щоб знайти свою клієнтуру. Хоча сайту не достатньо, щоб бути успішним, але можна отримати клієнтів, які можуть бути відсутні в більш традиційній формі торгівлі. Інтернет відкриває нову еру для нашого споживчого товариства. Це дозволяє в рамках різних програм і, головним чином World Wide Web купувати і отримувати послуги прямо в Інтернеті. Тим не

менш, не всі люди мають доступ до Інтернету і не можуть отримати ті переваги, що надає Інтернет. Це може бути з-за вартості, освіти, зв'язку і називається "цифрова прірва". Іншою потенційною перешкодою, яка на сьогодні долається, була необхідність паперового доказу існування певної угоди. Необхідність підпису документів, які існують у письмовому вигляді, створює проблеми для Інтернету. Введення Закону про електронні комунікації у 2000 зняло більшість цих перешкод.

Відповідальність посередників може виникнути у зв'язку з такими правопорушеннями, як наклеп і надання незаконних матеріалів. Є загальні положення, що стосуються відповідальності посередників відповідно до директиви про електронну торгівлю і щодо умов контрактів.

Відповідальність, пов'язана з незаконною електронною інформацією. Загальна відповідальність посередників

Стаття 12 передбачає, що постачальник послуг не повинен нести відповідальність, окрім як щодо забороненої інформації, що передається за умови, що постачальник

- не ініціює передачу;
- не вибирає отримувача передачі, а також
- не вибирає або змінює інформацію, що міститься в трансмісії.

Стаття 13 Директиви свідчить, що постачальник послуг не відповідає, за інформацію, надану одержувачу послуги, коли інформація є предметом автоматичного проміжного і тимчасового зберігання з єдиною метою зробити більш ефективної подальшу передачу інформації іншим одержувачам послуг на його прохання.

Відповідно до статті 14 Директиви про електронну торгівлю, постачальник послуг не несе ніякої відповідальності щодо зберігання інформації, якщо не має фактичного знання про незаконну діяльність або інформацію, і, у разі вчинення позову про відшкодування збитку, якщо йому не відомо про факти або обставини незаконної діяльності, але інформація мала б бути очевидною, у разі отримання таких знань та обізнаності, діє оперативно щодо її видалення або відключення доступу до інформації.

Без сумніву, що, як і раніше, «бум і спад» Інтернету продовжує розвиватися. У червні 2007 року Управління з чесної торгівлі випустило 176-сторінкову доповідь, що має назву Інтернет Shopping. Вона стверджувала, що покупки споживачів в Інтернеті - безумовно, успіх. За оцінками Доповіді, інтернет-покупки в Об'єднаному Королівстві сягають близько £ 21.4 млн на рік і охоплюють близько 20 мільйонів покупців, що використовують Інтернет в 2006 році, а кожен третій тратить понад £ 1000. У цьому звіті увага зосереджена на більш широких проблемах, в тому числі необхідності того, щоб споживачі в повній мірі були обізнані про свої права.

У поєднанні зі зростанням обсягів електронної комерції та інтернет-магазинів, розробка інтернет-спільнот (наприклад, Second Life), які є 3D віртуальним світом, повністю побудовані і належить його жителів. 22 червня 2007 було зареєстровано майже 7,5 жителів у всьому світі, які належать до Second Life.

Хоча, в той же час Інтернет розвивається і розвивається, існує значна група людей, які не мають доступу до благ World Wide Web, яким він недоступний з таких причин, як вартість послуг, мови, доступності та розуміння , це називається "цифрова прірва".

Перехід розвинутих країн світу до постіндустріальної економіки (останнім часом учені-економісти вдаються до терміна «нова економіка», який пов'язаний з поширенням Інтернет; виник він в середині 90-х років, коли на ринок вийшли перші Інтернет - компанії) та інформаційного суспільства став помітним явищем сучасної історії.

У цьому процесі сформувалася ієрархічна конструкція інформаційного комплексу: у велетенській сфері інформаційної діяльності людей окреслився інформаційний сектор економіки, основну частину якого становить суто інформаційна індустрія. В останні роки в інформаційній індустрії виокремлюється ще одна, поки що не дуже масштабна за обсягами, але найперспективніша структура — Інтернет-економіка.

Глобальна комп'ютерна мережа Інтернет вважається «четвертим каналом», що зв'язує людей між собою (після особистого спілкування, телефону і пошти). В інформаційному світі існують дві відомі технологічні тенденції:

1. Потужність комп'ютерів зростає вдвічі кожні десять місяців.

2. Корисність мережі для суспільства пропорційна квадрату числа користувачів

Надзвичайно високі темпи зростання глобальної комп'ютерної мережі Інтернет зумовлені тим, що вона базується на обох наведених вище закономірностях.

Нині світ бурхливо переживає ще один бум — зміщення акцентів з комунікаційної та інформаційно-пошукової функцій Інтернет на реалізацію з її допомогою сучасного бізнесу. Це відбувається завдяки здатності мережевих технологій докорінно змінювати спосіб взаємодії між людьми і компаніями, методи дослідницької діяльності, купівлі-продажу тощо. Інтернет не тільки забезпечує швидке «розкручування» нового, мережевого, бізнесу, а й змінює та підсилює конкуренцію в більшості традиційних галузей економіки, таких, як ЗМІ, роздрібна торгівля, інформатизація, телекомунікації, фінансові послуги, транспортування, освіта тощо.

Насамперед Інтернет охоплює найдешевші та найкращі на сьогодні технічні комунікації, що відкриває бізнесменам і споживачам можливості встановлювати і підтримувати в режимі реального часу постійний зв'язок з будь-яким респондентом у світі. Так, електронна пошта, програми електронних пейджерів, чати та інші засоби для спілкування у мережі забезпечують обмін між діловими партнерами пересічною, навіть стратегічною комерційною інформацією у лічені хвилини. Засоби захисту передавання електронних повідомлень роблять такий зв'язок надійним і ефективним. Завдяки цьому долаються географічні та національні кордони географічного простору. Весь світ стає клієнтом фірми, що визначає стратегію маркетингу, оскільки ареною боротьби за споживачів, а відповідно і конкуренції, стає весь світовий економічний простір. Це до небачених меж розширює можливості фірми, хоч і підвищує її ризики. Переваги такої роботи демонструють показники фірми Amazon.com, що, як стверджують, продала книги із свого офісу двом мільйонам осіб із 160 країн світу. Крім того, широкі можливості доступу до інформації створюють умови для досконалої конкуренції.

Глобальна мережа стала неперевершеним засобом для проведення маркетингу і здійснення прямих он-лайнових продажів, підвищення рівня обслуговування клієнтів, найпотужнішим інструментом управління фірмою і джерелом інформації для наукових і практичних розробок

Перетворення Інтернет на всесвітню торговельну платформу значно ослаблює необхідність у торговельному посереднику, тому його навіть називають «убивцею посередника».

Маркетинг у глобальній мережі забезпечує отримання й аналіз реакції споживачів на будь-які дії компанії через відстеження поведінки відвідувачів корпоративного web-сайту — вузла в Інтернет, що містить інформацію про компанію, її товари і послуги. У мережі практикуються цільові розсилання електронних повідомлень реальним і потенційним клієнтам фірми та розміщення реклами на часто відвідуваних тематичних сайтах.

Створення фірмою сайту власної електронної крамниці для прямих продажів через мережу сприяє значному підвищенню їх обсягу за рахунок необмеженого розширення ринку покупців — користувачів Інтернет, мережі, яка не має географічних кордонів. Прямі продажі через мережу дають змогу підвищити рівень «індивідуалізації» обслуговування певного клієнта, врахувати його особисті побажання і смаки.

Доступ співробітників філій великої компанії до централізованих корпоративних баз даних через Інтернет спрощує керованість такою установою через підвищення рівня інформованості. Водночас це значно скорочує операційні витрати, відчутно знижує собівартість і ціни товарів. Складне управлінське завдання з налагодження спільної роботи багатьох структурних підрозділів установи під час оброблення інформації вирішується шляхом створення і реалізації Інтернет — локальної комп'ютерної мережі підприємства, яка працює на основі Інтернет -технологій.

Глобальна мережа вміщує великі обсяги найкорисніших правових, економічних, наукових та інших відомостей, які слугують інформаційною базою для ведення бізнесу, досліджень тощо.

Інтернет породжує нові форми соціальної та економічної діяльності людей, найпоширеніші серед яких:

- телеробота — робота на відстані від офісу компанії;

- віртуальні підприємства — організаційна сукупність взаємодіючих господарюючих агентів, які працюють на відстані над спільним проектом, використовуючи мережеві технології;

- дистанційне навчання — надання платних освітніх послуг віддаленим слухачам через Інтернет та ін.

Протягом найближчого десятиріччя глобальна тенденція використання можливостей Інтернет для бізнесу вплине на десятки секторів світової економіки.

Яскраві вислови представників авторитетних у світі компаній, що активно використовують інформаційні технології, покликані переконати світову громадськість у великих перевагах переведення економіки на мережеву основу: «Інтернет, все змінює» (Крейг Барет, корпорація Intel); «Років через п'ять кожна компанія перетвориться на Інтернет - компанію або припинить своє існування» (Енді Гроув і Крейг Барет, Intel); «Усе, що вам здавалося можливим з допомогою Інтернет - технологій, швидко стане зовсім незначним у порівнянні з тим, що трапиться у найближчі декілька років» (Джеймс Річардсон, корпорація Cisco System); «Перемога у конкурентній боротьбі сьогодні часто залежить від одного клацання мишею» (Пол Отеліні, Intel).

Про ефективність і перспективність електронного бізнесу свідчить те, що акції Інтернет-компаній при первинному розміщенні виростали протягом дня в сотню і навіть тисячу разів.

Комунікаційні технології змінюють сутність бізнес - моделей — базових процесів створення продуктів і послуг виробниками та надання їх кінцевим споживачам. Перетворення основних бізнес-процесів з допомогою Інтернет -технологій, згідно з визначенням фахівців компанії IBM, і становить сутність електронного бізнесу (Е-бізнесу). Тобто будь-яка ділова активність, що використовує можливості глобальної інформаційної мережі для модифікації внутрішніх і зовнішніх зв'язків фірми з метою створення прибутку, охоплюється поняттям Е-бізнесу.

Електронна комерція (Е-комерція) є найважливішою складовою електронного бізнесу, хоча часто ототожнюється з ним. Це різновид бізнес-активності, в якій комерційна взаємодія суб'єктів бізнесу з купівлі-продажу товарів і послуг (як матеріальних, так і інформаційних) здійснюється з допомогою Інтернет або будь-якої іншої інформаційної мережі (мережі стільникового зв'язку, внутрішньої локальної мережі установи тощо).

Хоча Інтернет можна використовувати для обміну інформацією, оперативного зв'язку, реклами, для досліджень тощо, електронна комерція є сконцентрованою системою з використання усіх можливостей мережі для ведення бізнесу. Тобто електронна комерція є он-лайновою формою ведення бізнесу, яка використовує мережу як середовище для бізнесу і як засіб для його реалізації.

Нині виділяють чотири напрями Е-комерції залежно від взаємодіючих у її системах агентів: бізнес для бізнесу (B2B); бізнес для споживача (B2C); бізнес для адміністрації (B2A); споживач для адміністрації (C2A).

Електронна комерція передбачає:

- відкриття веб-сайтів компанії і віртуальної крамниці в Інтернет;

- наявність автоматизованої системи управління компанією;

- використання електронної реклами і маркетингу;

- використання певної моделі бізнес-взаємодії.

Типовим прикладом електронної комерції напряму B2C-механізму, який покликаний спростити роботу продавців і покупців, є Інтернет - крамниця; напряму B2B — торговельні майданчики для гуртової торгівлі в Інтернет.

Світовий бум електронної комерції почався в 1995— 1996 роках, а вже наприкінці 1998 — на початку 1999 року Інтернет стали розглядати як найперспективніший ринок, що перевершує за своїм потенціалом будь-який інший у світі.

Провідними країнами, в яких це економічне явище з'явилося і розвивається високими темпами, є Сполучені Штати Америки й Канада. Європа відстає від північноамериканських країн у використанні електронної комерції приблизно на рік, а відстань між країнами на пострадянському просторі і Європою становить 3—5 років. Однак реальна ситуація більш невизначена. Якщо західні компанії вже вичерпали усі резерви традиційних способів підвищення ефективності і з допомогою електронної комерції борються за кілька відсотків зростання, у наших національних підприємств можливості для росту ширші. Зміцнивши дисципліну праці або впровадивши ефективну автоматизовану систему обліку, можна отримати вагоміший результат, ніж від електронної комерції. Але можна поєднати з цими кроками й створення системи Е-комерції, одночасно реалізувавши комплекс заходів, до яких західні компанії послідовно вдавалися протягом декількох десятиліть.

Україна та інші країни на пострадянському просторі можуть отримати значні переваги від стійкого ринку електронної комерції, а саме:

- доступ до експортного ринку;
- робочі місця для кваліфікованої робочої сили;
- доступ до інвестиційного західного капіталу;
- зростання податкових надходжень від застосування електронних платежів.

Однак, щоб скористатися цими перевагами, слід усунути всі перешкоди на шляху ефективного впровадження електронної комерції, врегулювати використання механізмів її підтримки:

- систем електронних платежів в Інтернет;
- стрункої системи законів щодо правового визнання електронних документів і електронного підпису, законодавчого врегулювання електронної комерції загалом;
- розвитку електронного маркетингу і реклами;
- забезпечення захисту комерційної інформації під час передавання мережею тощо.

Найважливішими чинниками для покупців є можливість оплатити своє замовлення в Інтернет сучасними електронними засобами платежів, бути впевненими у безпеці такого платежу, в своєчасних доставці товару чи отриманні послуги і почувати себе захищеними законодавчо від будь-яких неправомірних дій продавців чи шахраїв. Подібні чинники важливі і для продавців.

Кредитні системи електронних платежів в Інтернет з допомогою пластикових карток і дебетові системи цифрових грошей поки що мало поширені на національному ринку електронної комерції через низький ступінь використання банківських карток українським населенням, невеликої кількості користувачів мережі.

Процес створення і розвитку систем електронних платежів у національних слов'яномовних сегментах Інтернет прискориться з прийняттям законів, які врегулюють правову базу реалізації електронної комерції: «Про електронну комерцію», «Про електронний цифровий підпис». Такі закони вже існують у розвинутих країнах Америки та Європи.

Безпека продавців і покупців у мережі може бути підтримана не тільки законодавчими заходами, а й програмно-технічними засобами. Виробники апаратних пристроїв і розробники програмних продуктів, усвідомлюючи важливість ринку електронної комерції як найперспективнішого в сучасній інформаційній економіці, приділяють велику увагу розробці надійних правил захищеного передавання інформації мережею — протоколів і стандартів (SET, SSL та ін.), розробці технологій цифрових грошей і розрахунків з допомогою смарт-карток.

Світовий ринок електронної комерції, обсяг якого нині оцінюється у $1,6 більйона доларів, висуває неабиякі вимоги до своїх учасників. Вони повинні володіти не тільки теоретичними знаннями й практичними навичками в сфері традиційного бізнесу — з маркетингу, логістики, управління кадрами, а й опанувати основи роботи у глобальній мережі Інтернет, користуватися її різними сервісами —

електронною поштою, телеконференціями, інформаційною веб - системою, мати уявлення про побудову комерційних веб-сайтів, форми роботи з клієнтами через них, механізми правового захисту продавців і покупців тощо. З цією метою в Україні, як і в усьому світі, будуть організовуватися професійні консалтингові команди з надання послуг певним компаніям щодо проектування і реалізації проектів електронної комерції, і «традиційні» бізнесмени будуть звертатися саме до них.

У середині 1990-х років, коли Інтернет тільки починав розвиватися, та академічні дискусії щодо "управління в Інтернет" знаходилися в зародковому стані, були дві основні точки зору:

- Cyber-визвольні теорії, які стверджують, що Інтернет схожий на "Дикий Захід". Втручання з боку уряду є мінімальним (необхідна децентралізація), а права на свободу слова і висловлень мають першорядне значення. Ця теорія пов'язує нові технології і визвольні ідеї, такі як свобода, суспільство та ринки, і що вони повинні бути захищені в кіберпросторі.

- Cyber-патерналістські теорії, які стверджують що, хоча в даний час існує «ерозія» суверенних кордонів в Інтернет, інший централізований нормативний контроль створюється державою. І вона забезпечує певні кордони, за якими люди не можуть перетинатися.

Оскільки Інтернет існує на міжнародному рівні, існує багато суперечок, хто є відповідальним за "управління" ним. Існує Інтернет-корпорація з присвоєння імен і номерів (ICANN). ICANN є органом, відповідальним за роздачу імен доменів верхнього рівня, і найбільше нагадує Інтернет-«уряд». Без доменного імені особа або компанія не існує в Інтернеті. Те, що ICANN розташовано у США, викликає значне занепокоєння у міжнародного співтовариства щодо «диктату» Сполучених Штатів в Інтернеті.

У 2003 році в Женеві було створено комітет для вивчення області управління Інтернетом, включаючи визначення питання державної політики і стратегічних підходів. Робоча група з управління Інтернетом (РГУІ) виклала в червні 2005 року в документі під назвою "Доповідь Робочої групи з управління Інтернетом свої висновки. Управління Інтернетом у цьому звіті було визначено як "... розробку та застосування урядами, приватним сектором та громадянським суспільством загальних принципів, норм, правил, процедур прийняття рішень і програм, що регулюють еволюцію і застосування Інтернету".

Було також відзначено, що якщо Інтернет - структури успішно вирішують такі проблеми, як спам, кіберзлочинність, питання конфіденційності та безпеки, то співробітництво на міжнародному рівні не потрібно. Поряд з офіційною аргументацією робочої групи, політичні аспекти питання були очевидні. Дилема була і залишається, і в основному має політичний характер. Такі країни, як Тайвань, Бразилія та Іран більше говорять про керівництво Інтернетом і намагаються перейти від методу ICANN регулювання (під контролем американського Департаменту торгівлі) до багатонаціональних структур управління, створених багатьма зацікавленими сторонами.

Американці виступають проти таких рішень. Так, наприклад, сенатор Норм Коулмен заявив, що «... немає раціонального обґрунтування для переміщення управління Інтернетом до органів при Організації Об'єднаних Націй ... ми не можемо залишатися байдужими, коли деякі уряди намагаються зробити Інтернет інструментом цензури та політичного придушення. Ми повинні стійко триматися проти всіх спроб змінити характер Інтернету як вільної та відкритої глобальної системи».

Угода 2005 р., досягнута в Тунісі, у ставленні до управління використанням Інтернет дозволила ICANN залишити загальний нагляд за Інтернет, у зв'язку з доменними іменами. Однак, поряд з ICANN, що не має обов'язкової сили, мав бути створений Форум з управління Інтернетом (IGF), який повинен був стати органом зацікавлених урядів у всьому світі. ООН взяла на себе провідну роль в розробці цього органу, і в лютому 2006 року організувала консультації в Женеві для обговорення її структури.

Тема 3. Принципи ведення бізнесу в Інтернеті

Дизайн веб-сайта

Взагалі звичайні норми щодо контракту застосовуються і до контрактів про дизайн веб-сайта. Необхідно розглянути кілька пунктів контракту, які відображають потреби сторін:

- специфікація й структура сайту - яка побудова, вигляд і характеристики будуть дані сайту;
- буде контракт розбитий по фазах, тобто чи будуть різні елементи сайту дороблятися в різний час;
- час доопрацювання й контрольні оцінки;
- оплата;
- володіння інтелектуальною власністю;
- експлуатація й навчання;

-Гарантії - дизайнер, щоб гарантувати, що матеріали, використовувані від третьої сторони, мають необхідні дозволи на інтелектуальну власність і навпаки, матеріали, які ви надаєте для включення, не спричинять відповідальність постачальника послуг Інтернету.

Права інтелектуальної власності на сайт. Існує невірне уявлення про те, що коли особа заплатила сторонньому консультанту за створення сайту або його частини, то всі права інтелектуальної власності на сайт або програмне забезпечення автоматично належать замовнику. Так буває не завжди, і замовник для того, щоб зберегти права інтелектуальної власності має укласти про це відповідну угоду. В зв'язку з цим адвокатам важливо ознайомитися з різними типами прав інтелектуальної власності, які можуть з'явитися в результаті створення сайта, а також з існуючим режимом їх захисту.

Сайт, який є мультимедійною продукцією, містить у собі безліч елементів, що вимагають захисту:

- письмові матеріали, музику, дзвоники, відео і таке інше, що є об'єктом авторських прав
- торгівельні марки, якщо сайт відображає емблеми, або захищені торгівельні назви.
- бази даних, якщо інформація представлена у вигляді баз даних.

Захист авторського права. Авторське право захищає інтереси автора на зазначені твори за допомогою надання прав інтелектуальної власності. Воно охороняє твір з моменту, коли він створений, протягом визначеного законодавством строку.

Моральні права на інтелектуальну власність - це права, які захищають інтереси автора в процесі створення творів і дають можливість протидіяти їх змінам. Комп'ютерні програми і твори, створені за допомогою комп'ютера – це винятки з існуючого правила, що вимагає ідентифікації моральних прав на них.

Пояснення до захисту авторського права. Автори повинні вміти користуватися своїми оригінальними творами. Авторське право та інші права інтелектуальної власності виникли і розвивалися, тому що, дуже мало людей хотіли б створювати роботи, не одержуючи матеріальну вигоду.

Авторське право - право інтелектуальної власності, що належить людині, яка створила твір. Закон про авторське право захищає продукт людських навичок, його праці, майстерності. Це означає, що наданий захист охоплює форму вираження людських думок, а не ідею, яка знаходиться поза межами охорони.

Створення твору, охоронюваного авторським правом. Авторське право виникає автоматично з моменту, як тільки твір створено в об'єктивній формі, і продовжує діяти протягом певного періоду. Для виникнення охорони немає необхідності реєструвати твори (як, наприклад, реєструються торговельні марки).

Типи захищених авторських прав. Існують три типи авторських прав, які захищаються Актом про авторські права, дизайн і патенти 1988 р. Якщо твір не відповідає одній з цих категорій, він не захищається правом.

1. Оригінальні літературні, драматичні, музичні і художні твори.

Твір повинен бути оригінальним, тобто не бути скопійованим. Поняття новизни не визначене в Законі (CDPA 1988). Однак, з цією метою використовуватися прецедентне право. Закон про авторське право не захищає ідею, що втілена у творі, тому твір має бути зареєстрованим. Форма вираження ідеї має бути оригінальною. Новизна - результат перемоги навичок, зусиль і капіталу автора. Авторське право в мовах, див. *Walter v. Lane (1900)*

Окремі слова твору не захищаються. Див. *Exxon Corporation v. Exxon Insurance (1982)*. Спірною є думка, що авторське право поширюється на газетні заголовки. Див. *Shetland Times .v Dr Jonathan Wills (1997)*.

Літературні твори - книги, статті і газети, інтерв'ю, мови, ліричні пісні, екзаменаційні документи тощо. У цю категорію попадають комп'ютерні програми (стаття 1 (1) Акта про авторські права, дизайн і патенти 1988 р.). Термін охорони комп'ютерної програми законодавством не визначений. Попередні матеріали для комп'ютерних програм також захищені відповідно до параграфа (c) статті 1 (1) Акта. Захист таких творів набуває все більшого значення через збільшення виробництва мультимедійних і цифрових робіт. Сайт у цілому може підпадати під цю категорію. Те ж саме стосується і кожного елементу сайта.

Заголовки Web сторінок і посилань гіпертексту. Див. *Shetland Times Ltd v. Jonathan Will and Zetnews Ltd* [1997] FSR 604; Контракт із *Exxon Corpn v. Exxon Insurance Consultants International Ltd*.

Драматичні твори - твори танцю або пантоміми, опера (існує імовірність їх виявлення на сайтах)

Музичні твори - твори, що складається винятково з музики. Це – музичне відтворення. Воно відрізняється від звукозапису, який охороняється як окремий об'єкт. (Дуже часто можна знайти сайт, який запускає мелодії при перегляді – мелодії, замовлені безпосередньо для сайта або мелодії, використання яких узгоджене з первісними володільцями авторського права на підставі виданої ліцензії. Найчастіше на сайті зустрічається популярна музика у форматі MP3)

Художні твори повинні бути оригінальними, але вони не вимагають реєстрації. Наприклад, такі художні твори, як фотографія, скульптура, архітектурний твір (будинок). Щодо цього об'єкту, то фактично рідко зустрічається твір, який не виражений матеріально (у сайт включається безліч фотографій)

2. Звукові записи, фільми, радіо - і кабельні програми

Це - похідні твори, оскільки вони складаються з інших добутків, які охороняються авторським правом. Наприклад, фільм буде базуватися на романі або сценарії (тобто на основному творі).

Звукові записи - касети, компакт-диски і міні диски. Авторське право на запис звуку відрізняється від авторського права на основний музичний твір.

Фільм - запис будь-яким способом, що допомагає сприймати рухомі зображення. Сюди можна віднести комп'ютерні програми. Наприклад, у фільмі «Історія іграшок» використані комп'ютерні програми для створення фільму. Також до цієї категорії можна включити відео кліпи, розміщені на сайтах.

Радіопередача - передача безпровідним зв'язком візуальних зображень, звуків або іншої інформації, законно отриманої і переданої для представлення публіці. До радіопередачі також може відноситись телевізійна програма, зміст якої відтворений у цифровій формі, і розміщений в Internet.

Кабельна програма - будь-який елемент, включений у кабельне програмне обслуговування (реклама, сайт Інтернету і т.д.) (див. справа Shetland Times).

3. Типографська домовленість щодо опублікованих видань

Це право існує для того, щоб захистити внесок видавця в процесі публікації. Таким чином фотокопіювання книги є порушенням права типографської домовленості (так само як і основне літературне авторське право автора). Типографською домовленістю захищені газетні сторінки.

Тривалість, авторство і власність. Авторство і володіння правами інтелектуальної власності можуть не співпадати. У розділі 11 (2) зазначається, що люди, які вперше створили твір, є володільцями авторських прав. Однак, якщо автор є найнятим для його створення, то авторське право належить замовнику-підприємцеві. У такому випадку підприємець - перший власник авторського права, якщо немає угоди про інше.

Після спливу строку охорони авторського права, твір стає державною власністю і може бути вільно копіюватися.

Табл. 1. Тривалість, авторство і власність

Твір, охоронюваний авторським правом	Авторство	Тривалість	Дата початку дії
Літературний, драматичний, музичний, художній	Творець роботи	70 років	Кінець календарного року смерті автора
Твори, створені комп'ютером	Особа, що здійснила дії, необхідні для створення	50 років	Кінець календарного року, у якому був зроблений твір
Запис звуку	Виробник	50 років	Кінець календарного року, у якому зроблена запис
Фільм	Виробник і головний директор	70 років	Кінець календарного року смерті a) головний директор b) автор сценарію c) автор діалогу d) композитор музики, спеціально створеної для фільму
Радіопередача	Журналіст	50 років	Кінець календарного року, протягом якого зроблена передача
Кабельна програма	Провайдер кабельної програми	50 років	Кінець календарного року, протягом якого програма була введена в обслуговування
Опубліковане видання	Видавець	25 років	Кінець календарного року публікації видання

Ділові відносини і передача прав. Власник авторського права може розпорядитися ним. Автор твору може передати права особі, яка замовила сайт. Це може відбутися шляхом передачі прав або ліцензування. Передача права – це передача (відчуження) прав інтелектуальної власності. Ліцензія - домовленість між сторонами про використання охоронюваного авторським правом матеріалу протягом деякого часу. Передача права надає право інтелектуальної власності, ліцензія надає право користування, що основане на контракті.

Передача прав. Офіційні вимоги до передачі прав:

- письмова форма;
- підпис власника, який передає право.

Тривалість передачі прав: той, хто передає право, визначає термін передачі. Можлива повна передача авторського права або тільки на певний строк.

Дії, права на які передаються:

- право інтелектуальної власності, зокрема авторське право, може бути розділене на безліч прав, оскільки це - право на нематеріальне благо. Наприклад, право видавати книгу у твердому

плетінні або на театральну адаптацію книги. Кожен елемент авторського права може бути переданий окремо. Права на книгу можуть бути передані для створення фільму при збереженні права зробити комп'ютерну гру, засновану на книзі.

Ліцензія. Ліцензія дозволяє використовувати певним чином твір, охоронюваний авторським правом. Це право, яке випливає з контракту і виключає можливість передачі його ліцензіатом третій особі.

Виключні і звичайні ліцензії:

- виключна ліцензія повинна бути в письмовій формі. Дає ліцензіату право пред'явити позов за порушення авторського права (аналогічно передачі прав). Ліцензіар не може надати ніяких аналогічних ліцензій щодо зазначеного у ліцензії права.

- звичайна ліцензія - право, що випливає з контракту. Відсутність повноважень пред'являти позов за порушення, тому ліцензіат буде мати потребу в обіцянці ліцензіара вжити заходів проти порушників. Ліцензіар має право видавати аналогічні ліцензії щодо того ж права.

Порушення авторського права. Два типи порушень:

- первинне порушення має місце, коли людина здійснює «обмежену дію» без дозволу власника авторського права, порушення існує незалежно від того, чи знала особа про авторське право, чи ні. (сувора відповідальність).

- вторинне порушення має місце, коли людина виконує «обмежену дію», знаючи або маючи причини вважати, що ця дія порушує авторське право власника.

«Обмежені дії» визначені розділом 16. Порушення має місце, коли обмежена дія відбувається в цілому або в «істотній частині» авторського права без згоди власника авторського права.

«Істотна частина» визначається не використовуваною кількістю, а якістю, яку зацікавлена сторона представляє відносно цілого. Див. *Ladbroke (Football) Ltd v. William Hill* [1964] 1 W.L.R. 273.

Деякі обмежені дії: копіювання, публікація копій для публіки, орендна плата або надання.

Копіювання. Розділ 17 (1) – стосується літературного, драматичного або музичного твору - копіювання носіїв, що містять твір або його істотну частину в будь-якій матеріальній формі. Наприклад, фотокопіювання, відтворення витягів, фотографування. Розділ 17 (2) - збереження будь-якого твору в будь-якому електронному виді відноситься до копіювання. Завантаження сторінки від Internet – це виконання її копії. Постачання змісту в Internet, відповідно до визначення, призводить як до відтворення первісного змісту, так і його представлення іншим особам.

Потенційні порушення авторського права:

- завантаження web-сторінки або програмного забезпечення в пам'ять вашого комп'ютера;

- автоматичне кешування web-сторінки - стандартна особливість фактично всього програмного забезпечення браузера;

- друкування web-сторінки;

- репродуцирування матеріалу, завантаженого із сайта

- мережний зв'язок (гіперз'єднання, глибоке з'єднання)

- мережний підбор

- spamdexing

Публікація копій для публіки. Цей тип порушень рідкий. Регулюється Розділом 18 (2).

Орендна плата або надання. Розділ 18 (2): орендна плата – це «створення копії роботи, доступної для використання, на умовах, що вона буде або може бути використана з метою прямої або непрямої економічної або комерційної вигоди». Наприклад, орендна плата за відео.

Надання означає «створення копії роботи, доступної для використання за умови, що вона буде або може бути використана для загального доступу з метою прямої або непрямої економічної чи комерційної вигоди». Наприклад, діяльність суспільної бібліотеки.

Авторське право і зв'язані з ним інструкції з прав (2003). Виконання Директиви Авторського права у Великобританії. Інструкції вводять у британському законі про авторське право нову концепцію

суспільних зв'язків, що випливає із угоди про авторське право 1996 BOIC, яку Директива прагне здійснювати по всій Європі. Це має пряме відношення до сайтів. Інші зміни включають право на рівноправну винагороду. CDPA 1988 тепер виправлений таким чином, щоб дозволити виконавцеві запобігати запису суспільної радіопередачі або включення її в кабельне програмне обслуговування. Замість цього виконавцеві надавали право на рівноправну винагороду за їхнє використання.

Дія Зв'язку з громадськістю стає однією з дій, обмежених авторським правом у:

а) літературному, драматичному, музичному або художньому творі;

б)звуковому записі або фільмах,

в) радіопередачі.

Вона містить два взаємно виключаючих типів зв'язку:

- радіомовлення твору;

- створення доступного твору на інтерактивній підставі.

Для цього потрібно, щоб мала місце фіксація (початкове завантаження). Якщо передача є інтерактивною, то пізніше вона не може бути відтворена по радіо. Дане створення доступного твору в дійсності повинне передбачати право на розміщення охоронюваного твору у сайті або іншому електронному місці таким чином, щоб представники публіки могли звернутися до нього, коли вони побажають. Згідно ЕС критичним аспектом цього права є те, що будь-який представник публіки може звернутися до твору будь-який момент за їх вибором. Однак, це не відноситься до відео за вимогою, коли неінтерактивна програма передана по радіо кілька разів паралельно через короткі інтервали.

Директива пропонує ряд звільнень від порушень, які держави-члени можуть дозволити. Тільки одне з цих звільнень є примусовим: звільнення для *перехідних* копій. Це передбачає виключення відповідальності за створення копії творів у мережі, оскільки файли обмінюються через Internet, і ця тимчасова копія не має ніякого економічного значення. Це повинно бути зв'язане з директивою 2000 р. по Електронній комерції, що містить правила, які стосуються Захисту авторського права і відповідальності провайдерів Internet. Тимчасові дії відтворення були вже охоплені s.17 (6) CDPA 1988: «створенням копій, які є перехідними або призначені для іншого використання роботи», але директива 2000 р. по Електронній торгівлі, встановлює, що *перехідні і непередбачені дії відтворення, що є складеною й основною частиною технологічного процесу …, будуть звільнені*. Також додатково передбачено, що кешування припустиме.

Захист бази даних. З 1 січня 1998, нова норма права інтелектуальної власності була встановлена в британському законі. Європейською директивою від 11 березня 1996 щодо юридичного захисту бази даних, OJ 1996 L 77/20 передбачені нові *sui generis* права, які ефективні проти витягу і/або перевикористання істотної частини змісту бази даних. Це право може існувати одночасно з авторським правом на елементи, що складають базу даних.

У цілому сайт може також бути базою даних, якщо це відповідає юридичним{законним} вимогам. База даних визначена таким способом у Розділі 3 (А) - (1): *«У цій частині бази даних утворює сукупність незалежних робіт, даних або інших матеріалів, які (а) розміщені систематичним або методичним способом, і (b) є індивідуально доступними електронними або іншими засобами»*

Традиційно, одне з основних вимог для функціональної бази даних було те, що її зміст збережений у певній структурі. З розвитком програмного забезпечення пошуку все менше і менше інформації необхідно зберігати відповідно до такої визначеної структури. Якщо база даних включає суміш даних і програмного забезпечення пошуку, буде необхідно для програмного забезпечення зібрати індекси слів, використаних у даних. Такі індекси використовуються в наступних діях пошуку.

Більш проблематичні питання виникнуть там, де програмне забезпечення пошуку є окремим від баз даних, що обшукуються, як у випадку з www.

Іншими словами переліки предметів матеріально-технічного забезпечення, ідентифікуються пошуковим сервером як зустріч запиту користувача безпосередньо з базою даних. Подальші

проблеми виникають, якщо елементи, що складають дані - не є самостійними об'єктами авторського права.

Відповідно до діючого законодавства нове право бази даних виникне, коли здійснюється *істотний* внесок в одержання, підтвердження або представлення змісту бази даних. Виготовлювач бази даних буде першим прямим власником бази даних, крім випадку, коли робота створена службовцем. У такому випадку наймач буде володіти авторським правом (Інструкції 13 і 14).

*Що є істотним?*Не ясно, який внесок необхідний для визначення прикметника «істотний». Див**.** *Mars Uk Ltd v Teknowledge Ltd* [2000] FSR 138 і *British Horseracing Board Ltd v. William Hill Organisation Ltd* [2001] EWCA Civ 1268.

Як можна було б припустити, для існування права, не є головним, чи захищена база даних або її зміст юридичним авторським правом. Право буде порушено особою, яка відповідно до інструкції 16: *... без згоди власника ... витягає або перевикористовує всі або істотну частину змісту бази даних*. ' Воно може прийняти форму або єдиної дії, або низки менших витягів.

Традиційна умова торговельної чесності, що присутня у деяких аспектах авторського права, знову визначена у зміненій формі відповідно до положення 20. Ця умова забезпечує використання *доступної громадськості бази даних будь-яким способом, з метою ілюстрації, для навчання або дослідження (за винятком комерційного навчання або дослідження),із позначенням джерела,, не порушуючи при цьому торговельної чесності в експлуатації істотної частини бази дани.*

Порушення права бази даних дає право на позов про стягнення збитків, судові заборони (ст. 96 Акта 1988 р.)

Однак умови Акта 1988 р., що стосуються злочинних штрафів не розповсюджуються на порушення бази даних, і також неможливою є конфіскація незаконних копій.

Термін дії права. Право з'явиться, коли база даних стане доступною для опублікування, і буде охоронятися протягом 15 років. Однак, в інстр. 17 закріплено, що «б*удь-яка істотна зміна в змісті бази даних, включаючи нагромадження послідовних доповнень, видалень або змін, що можна вважати істотно новим внеском, і привело б до створення нової бази даних, повинне надавати новій базі даних власний термін захисту»*. Додаток цієї умови не повинний бути проблематичним там, де бази даних (наприклад, телефонний довідник) випускаються щорічно.

Принцип Пітера. Крім відомого винятку Питера Пэна, авторське право не безстрокове, хоча має довгий термін. Відповідно до 15-літнього періоду *sui generis* права, додаток інструкції 17 може бути проблематичним. Що є істотною зміною? 1 %, 2 % і за який період? Зміна на 0.01 % незначна, але якщо повторюється щотижня протягом року або двох років? Якщо невеликі зміни можуть накопичуватися, тоді в дійсності надається безстроковий захист.

Супроводження (ведення) програми сайта.

Ведучий - ключовий актор у стратегії торговця. Якщо сайт доступний не завжди, існує можливість втрати доходу. Якщо клієнти не можуть звернутися до вашому сайту, вони не будуть робити закупівлю і якщо це відбувається занадто часто, вони можуть переключитися до більш надійного джерела.

Наступна потреба ретельно розглядається при складанні проекту контракту або прийняття відповідних термінів і умов:

- підстава сервісної умови - список обладнання або постачання обслуговування – який доступ гарантується, коли здійснюється обслуговування і т.д.

- специфікація обслуговування – чи включає обслуговування модифікації, сайт або дає доступ, необхідний для обслуговування

- обов’язки по обслуговуванню обладнання

- сервісні рівні

- дублювання і відновлення після нещастя

- зміст сайта і дисплея - сайт будуть показувати, як передбачалося або будуть відбуватися деякі зміни

Ваш ведучий може нести відповідальність на основі контракту, якщо всі погоджені пункти виконані незадовільно. Також, стосовно третіх осіб ведучий часто був адресатом судових процесів за такі правопорушення, як наклеп, оскільки ведучі можуть бути легко виявлені. Відповідальність посередників може базуватися на таких правових порушеннях, як наклеп і використання незаконних матеріалів.

Відповідальність, зв'язана з незаконною електронною інформацією: загальна відповідальність посередників

Європейська Директива 2000/31/ЕС по Електронній Торгівлі, видана у Великобританії в Інструкції Електронної Торгівлі (Директива ЕС) 2002, розглядає загальну відповідальність систем інформаційних суспільних служб. Положення, власне кажучи, забезпечують три спеціальних захисти ISP's. Вони охоплюють три головних види діяльності, що є основними для функціонування ISP: просте керівництво, кешування (збереження) і ведення програми.

Просте керівництво. Стаття12 [див. положення 17 Директиви] говорить, що провайдер несе відповідальність, тільки відповідно до судової заборони щодо переданої інформації за умови, що провайдер (a) не починає передачу; (b) не вибирає одержувача передачі; і (c) не вибирає або змінює інформацію, що утримується в передачі.

Дії передачі й умова доступу, згадані в параграфі 1, включають автоматичне, проміжне і перехідне збереження інформації, переданої для того, щоб єдиною метою було виконати передачу в мережі зв'язку, і за умови, що інформація не зберігається довше, ніж необхідно для передачі.

Стаття 15 [див. положення 22] говорить далі, що держави-члени не повинні накладати загальне зобов'язання на провайдерів при забезпеченні послуг, охоплених статтями 12 - 14, щоб контролювати інформацію, що вони передають або зберігають, як загальне зобов'язання неактивне для фактів, так і обставини, що вказують на незаконну діяльність.

Кешування (збереження). Це відбувається там, де системна служба розміщає інформацію в тимчасовій пам'яті, щоб збільшити ефективність системи, дозволяючи здійснювати негайний перегляд сторінки без потреби витягу з первісного джерела.

Стаття 13 Директиви говорить, що провайдер не відповідальний там, де обслуговування складається з передачі в системі комунікацій інформації, забезпеченої одержувачем обслуговування, де інформація - тема автоматичної, проміжної і тимчасової пам'яті з єдиною метою зробити більш ефективну прогресивну передачу інформації іншим одержувачам даної служби.

Ведення програми. Це місце, де ISP зберігає інформацію для одержувача служби, тобто збереження електронної пошти для наступного доступу користувача.

У відповідності зі статтею 14 Директиви про Електронну Торгівлю, провайдер не несе відповідальність за збереження, якщо у провайдера немає зведень про незаконну діяльність або інформацію і де пред'явлена вимога про відшкодування збитку, а провайдер не знає про факти або обставини незаконної діяльності й інформації або після виявлення таких провайдер негайно видаляє або відключає доступ до інформації. Захист не застосовується, якщо одержувач обслуговування (тобто одержувач, що забезпечений розглянутою інформацією), діяв під керівництвом або контролем системної служби. Умови для визначення, чи має системна служба фактичне повідомлення, ті ж самі, що застосовуються до кеширування відповідно до положення 22 з Електронної Торгівлі (Директива ЕС) Інструкції 2002.

Відповідальність, зв'язана з електронною інформацією - наклеп і Internet

Щоб виграти справу про наклеп, позивач повинний довести три речі зробленого твердження: воно повинно дискредитувати, воно може дійсно відноситися до позивача і воно було опубліковано. Кожний з цих трьох елементів важко довести, але в останні роки Internet як система комунікацій також додав труднощі в системі права.

Вимога публікації. Щоб мати позовну силу, необхідно, щоб твердження було повідомлено принаймні ще одній особі, крім суб'єкта. Діапазон поширення не повинний бути широким. Листа або електронної пошти третій особі буде достатньо, як і коментарю на дошці суспільних оголошень. Див. *Slipper v British Corp* [1991] 1 QB 283.

У Великобританії виникає новий мотив для відповідної дії після кожної публікації твердження, що дискредитує. В іншій юрисдикції, наприклад у США, є 'правило єдиної публікації". Це означає, що тільки перша публікація може викликати мотив до відповідної дії. Наступні публікації можуть бути прийняті в увагу при встановленні грошової компенсації, але ніякого права для подальшої відповідної дії немає. Це має значення протягом обмеженого періоду часу. У США час обмеження має силу тільки з моменту першої публікації. У Великобританії право відповідної дії має силу з моменту кожної нової публікації. Див. *Loutchansky v Times Newspaper* [2002] QB 783.

Виникають наступні проблеми:

1) наклеп і юрисдикція - який суддя є компетентним для слухання суперечки (будь ласка, зверніться до Модуля 4 розділу 1 для уточнення деталей і особливостей прецедентного права, що відноситься до електронної комерції);

2) чи існує правило єдиної публікації (свого роду глобальна публікація) або правило багаторазової публікації, як у Великобританії? Див. *Berezovsky v Michaels* [2000] 2 All ER 986);

3) що, якщо тільки деякі особи в специфічній юрисдикції можуть мати доступ, що є правилом *de minimis?* Ще з часів *Whittaker v Scarborough Post*[1896] британські суди не прийняли ніякого правила *de minimis* про наклеп. Подібне рішення було прийнято в справі з Internet: *Macquarie Bank v Berg*[2002] NSWC 1110.

Чи може суд відхилити юрисдикцію на основі *forum non conveniens*? Рішення відмовитися від юрисдикції на основі forum non conveniens знаходиться у Великобританії і базується на рішенні в *Spiliada Maritime Corp v Cansulex (Spiliada)* [1987] 1 AC 460. Лорд Гоффс пред'являє 6 вимог, щоб здійснити такий намір.

Хто відповідальний за коментарі, що дискредитують? Відповідальність виготовлювача.

Немає сумніву, що людина, що робить дискредитуюче висловлення, буде нести відповідальність. Хоча можна стверджувати, що відправник повідомлення, що дискредитує, може піддатися ризикові судового позову, задача ідентифікації відповідальний сторони може бути нелегкою. Навіть якщо повідомлення походить від визначеної особи, може виникнути необхідність установити його дійсність.

В американському випадку *Stratton Oakmont v Prodigy*(1995) 195 NY Misc. LEXIS 229, повідомлення, здавалося, прийшло з рахунка визначеного користувача. Користувач, однак, заперечував, що повідомлення послав він або його обладнання. У визначеній справі, проблема не мала великого значення, оскільки відповідна дія спричинила кримінальну справу проти провайдера, що завжди була головним адресатом позову. В інших справах, позивачеві можливо необхідно установити, що повідомлення посилала ідентифікована сторона. У Великобританії подібні факти спираються на справу *Takenaka (UK) Ltd v Frankl* (неповідомлене) 11-ого жовтня 2000. Воно може бути уособленням ідентичності користувача. Прикладами були підроблені поштові повідомлення, що, як припускалося, виходили з Білого дому.

Відповідальність підприємця. Оскільки все більше компаній використовують електронну пошту як спосіб зв'язку з персоналом, таким чином буде розкриватися все більша кількість справ, заснованих на відповідальності за чужу провину щодо використання або неправильного вживання системи комунікацій. У 1997 компанія Norwich Union досягла врегулювання по питанню наклепу, з боку страхової компанії на випадок хвороби Ассоциациии Western Provident. Відповідно до угоди Norwich Union погодився заплатити 450 000 фунтів стерлінгів збитків і витрат, що стосуються наклепницьких повідомлень щодо фінансової стабільності асоціації, що утримуються в електронних повідомленнях, якими обмінювався персонал компанії Norwich Union. (Times, 18 липня 1997).

Тому контроль за електронною поштою на робочому місці може бути необхідний. Перехоплення згідно з Актом про Зв'язки 1985 р. буде керувати перехопленням електронних повідомлень, що проходять через мережу суспільного телезв'язку, це положення застосовується до приватних мереж, але див. RIPA 2000. Див. *Halford v UK* [1997] IRLR 471.

Відповідальність провайдеру. У Великобританії Акт про Наклеп набрав сили в 1996, починаючи спробу обновити закон, що стосується наклепу. Це пішло за дослідженням, проведеним Юридичною Комісією, що рекомендувала введення нового захисту невинного поширення'. Актом відповідно передбачено:

Розділ 1 (1) На слуханнях у справі про наклеп особа має захист, якщо показує, що:

(a) він не був автором, редактором або видавцем оскаржуваного твердження, (b) він виявляв розумну турботу щодо його публікації; і (c) він не знав і в нього не було ніякої причини думати, що те, що він зробив, викликало або вплинуло на публікацію твердження, що дискредитує чи виявляла людина розумну турботу або мала причину думати, що те, що вона зробила, викликало або вплинуло на публікацію твердження, що дискредитує, необхідно звернути увагу на ступінь її відповідальності за зміст твердження або рішення видавати його; характер або обставини публікації; і попереднє поводження або характер автора, редактора або видавця.

Розділ продовжує визначати терміни «автор», «редактор» і «видавець». Важливо звернути увагу на те, що ці визначення застосовуються тільки для цілей розділу. Видавець визначається як «. комерційний видавець, тобто людина, бізнес якої полягає в передачі матеріалу публіці або частини публіки, що видає матеріал, що містить твердження в ході цієї діяльності».

Чи дійсно ISP – «видавець» відповідно до Акта про наклеп 1996? Суди вказали, що оператор або провайдер доступу до системи зв'язку, за допомогою якого передане твердження або зроблене доступним особам, над якими він не має ніякого ефективного контролю - не видавець.

Див. *Totalise plc v. Motley Fool Ltd* ([2001]) All ER 213), що, очевидно, підтверджує думку про те, що оператор сайта не несе відповідальність за публікацію про неповагу до суду тому, що там не було ніякого редакційного змісту.

Див. також *Godfrey v. Internet \Demon Internet* ([1999]) 4 All ER 342, де Internet Demon не здійснював розумне керування за виданою інформацією і, таким чином, не міг уникнути відповідальності. У справі Godfrey v Demon [1999] EMLR542 Мореленд Дж. затверджував, що:

1. Демона не можна розглядати як видавця поштових відправлень і таким чином виконана перша вимога захисту.

2. Положення, однак, були зв'язані з обов'язком Демона продемонструвати, що вони взяли розумну турботу і не усвідомлювали факт, що їхні дії викликали публікацію твердження, що дискредитує. Дія наклепу була зв'язана тільки з періодом після 17 січня 1997, коли прибув факс позивача і, оскільки відповідач не почав ніякої дії, щоб досліджувати питання, отже не було можливості продемонструвати початок розумної турботи.

Хоча Демон Інтернет не класифікувалися як видавці з метою захисту безвинного поширення, визначення, обговорені вище, застосовуються тільки по цьому захисту. Також проблемним виявилося питання, чи міг Дэмон розглядатися як видавець у відповідності з загальним законом. ***Byrne v Deane*,** [1937] 1 Кбайт 818, де директори *клуба аматорів гольфа* вважалися відповідальними як видавці за повідомлення, що дискредитує, поміщеною третьою особою на дошці оголошень у клубі. У даному випадку суд дотримувався загальної думки: якщо дія особи, що опубликовала наклеп, не було якою-небудь дією, а була лише стримуванням від виконання деяких дій, вона не може бути винною у публікації. Я зовсім не згодний з такою загальною думкою.

У справі *Thompson and Venables v. Newsgroup Newspapers*, Order of Dame Elizabeth Butler-Schloss у відділенні по сімейних справах Високого Суду , 10 липня 2001, про яке не повідомлялося, Високий суд підкреслив, що відмовлення ISP здійснювати всі розумні кроки, щоб запобігти публікації прикладених матеріалів спричинить відповідальність.

У США Акт про Пристойні Зв'язки 1996 47 USC §230 заявляє, що ніякий провайдер або користувач інтерактивного комп'ютерного обслуговування не повинний розглядатися як видавець або постачальник якої-небудь інформації, забезпеченої іншим постачальником оперативної інформації ніякої інформації, забезпеченої іншим інформаційним постачальником оперативної інформації. Це було відповіддю на побоювання, що ISPs більше не буде самостійно регулювати зміст матеріалу, забезпеченого їхньою службою після таких випадків як:

Stratton Oakmont Inc v Prodigy Services Co, 1995 NY Misc. LEXIS 229, [вже згадується] основна відповідальність лежить на провайдері, що перевіряв зміст, таким чином забезпечуючи можливість для саморегулювання.

Zeran v America Online Inc (1997) 129 F 3d 327, позивач скаржився на передбачувані дискредитуючі повідомлення, що були відправлені поштою непізнаною третьою особою по лінії служби America Online. Він затверджував, що 47 USC 523 не допомагали службі America Online, як тільки стало відомо, що матеріал дискредитучий. Суд не погодився, служба America Online могла все ще використовувати захист.

Інтернет з глобальної поштової та інформаційно-пошукової системи перетворюється на інструмент ведення сучасного бізнесу, заснованого на принципах мережевої економіки.

Електронний бізнес (Е-бізнес) — ділова активність, що використовує можливості глобальних інформаційних мереж для перетворення внутрішніх і зовнішніх зв'язків компанії з метою створення прибутку.

Найважливішою складовою Е-бізнесу є Е-комерція, яка охоплює не тільки операції купівлі-продажу, а й супровід процесів створення попиту на продукцію і послуги, автоматизацію адміністративних функцій, пов'язаних з он-лайновими продажами і обробленням замовлень, а також із вдосконаленням обміну інформацією між партнерами.

Електронна комерція (Е-комерція) — різновид бізнес-активності, в якій взаємодія суб'єктів бізнесу з купівлі-продажу товарів і послуг (як матеріальних, так й інформаційних) здійснюється з допомогою глобальної комп'ютерної мережі Інтернет або будь-якої іншої інформаційної мережі.

Виділяють кілька класичних етапів ведення електронної комерції: он-лайновий маркетинг, оформлення замовлень, здійснення платежів і підтримку інформації про доставку.

Розвиток моделей електронної комерції, впровадження пілотних проектів у цій галузі, а також розробка загальних юридичних і правових основ ведення бізнесу в Інтернеті підтримуються Європейською комісією в ESPRIT.

ESPRIT — програма Європейської спільноти, спрямована на прискорення і розширення досліджень з використання інформаційних технологій (IT).

Виокремлюють такі напрями електронної комерції:

- бізнес — бізнес (B2B) — визначає взаємодію компаній з компаніями в електронному середовищі;
- бізнес — споживач (B2C) — визначає взаємодію компаній з кінцевими споживачами в мережі;
- бізнес — адміністрація (B2A) — визначає взаємодію компаній з адміністративними органами;
- споживач — адміністрація (C2A) — визначає взаємодію споживачів з адміністрацією.

Згідно із статистичним дослідженням у мережі, напрям B2B посідає перше місце (70 відсотків від загальної кількості усіх угод, що укладаються в Інтернет). Починаючи з великих корпорацій, таких, як Cisco Systems, прагнення збільшити обіг коштів через глобальну мережу в галузі *бізнес — бізнес* поступово поширюється й на дрібні фірми, які бажають розширити свою діяльність з меншими витратами часу й матеріальних ресурсів.

Однак пересічним користувачам більш відомі компанії, що торгують в Інтернет товарами і послугами для кінцевих користувачів, тобто представники напряму B2C. Прикладом може слугувати Amazon.com — найвідоміша у світі електронна крамниця з торгівлі книжками, компактами тощо.

Перспективними вважають напрями B2A і C2A. Держава є значним постачальником послуг для громадян і підприємств, які сплачують податки за комплекс певних послуг у сфері безпеки і суспільного порядку, освіти, охорони здоров'я тощо. Все більша кількість місцевих і центральних органів влади в різних країнах надає послуги своїм громадянам через Інтернет. Найпомітнішим проектом для всього світу в цій галузі є державний портал Сінгапуру, на який перенесено практично все спілкування громадян з владою.

У матеріалах Європейської комісії в ESPRIT наводяться такі моделі електронної комерції: електронна крамниця; електронний довідник-каталог; електронний он-лайновий аукціон; електронний торговельний центр; віртуальне співтовариство; віртуальний центр розробки; інформаційний брокер; провайдер бізнес-операцій; інтегратор бізнес-операцій тощо.

Електронна крамниця — спеціалізований веб-сайт, що належить фірмі-виробнику, торговій фірмі тощо й призначений для просування товарів на ринку, збільшення обсягу продажів, залучення нових покупців.

На таких сайтах є змога вибрати товари, оформити замовлення і зробити оплату через мережу, оформити документи в режимі он-лайн для здійснення оплати звичайним способом і відстежити доставку.

Електронний довідник-каталог — спеціалізований веб-сайт для проведення тендерів серед постачальників. Зазвичай існує у вигляді каталогу-довідника, з допомогою якого клієнт може вибрати постачальників товарів для проведення переговорів з ними. Відбір робиться, виходячи з характеристик товарів, цін, умов постачання, номенклатури або будь-яких інших специфічних умов. Електронні довідники-каталоги застосовуються компаніями для полегшення участі в тендерах, для просування своєї торгової марки і зниження витрат з маркетингу.

Електронний он-лайновий аукціон — одна з найперспективніших галузей електронної комерції; програмно-інформаційна тематична база з пошуковими засобами, в якій містяться описи товарів, допущених до торгів.

Електронний аукціон аналогічний до процедури торгів по лотах на звичайному аукціоні. «Господар» такої веб-системи заробляє на відсотках від трансакцій, а також на продажах програмного забезпечення для участі в торгах. Вдалий приклад такого Інтернет - аукціону — www.e-bay.com.

Електронний торговельний центр (E-mall, електронний мол) - веб-сайт, що містить безліч електронних крамниць і каталогів, об'єднаних загальним місцем розташування (інколи під відомою маркою), які спільно виконують додаткові функції, використовують систему здійснення захищених платіжних трансакцій тощо.

Інші моделі електронної комерції (за класифікацією Європейської комісії в ESPRIT) пов'язані з інтенсифікацією обміну інформацією і процесами спільного виробництва.

Переваги електронної комерції порівняно з традиційними видами ділової активності вагомі. Використання нових електронних форм комунікації істотно знижує витрати на організацію і підтримку всієї інфраструктури бізнесу. Можливості Е-комерції дають змогу також перепроектувати стратегію ведення бізнесу. Фундаментальне переосмислення і радикальна зміна бізнес-процесів може помітно поліпшити такі найважливіші характеристики, як витрати, якість, сервіс і швидкість обслуговування.

Впровадження Е-комерції, можливо, стане саме тим економічним важелем, який зможе змінити ідеологію, засоби і принципи традиційного бізнесу. Розвиток потенціалу електронної комерції зумовить створення нових ринкових моделей і відносин.

Бізнесмен, який підключився до Інтернет і вирішив стати активним учасником, гравцем на полі віртуального бізнесу, отримує неперевершене знаряддя для проведення маркетингу і здійснення продажів; найкращу на сьогодні систему комунікацій, яка дає змогу встановлювати й підтримувати постійний зв'язок з будь-яким абонентом у світі (за умови його підключення до мережі); можливість підвищення рівня обслуговування клієнтів; найпотужніший інструмент управління; джерело інформації для наукових і практичних розробок. Інтернет забезпечує отримання та аналіз реакції споживачів на

будь-які дії компанії, до того ж миттєво. Бізнесмени та їх менеджери можуть отримувати від відвідувачів веб-сайту компанії детальну й різноманітну зворотну інформацію.

У мережі є можливість цільового розсилання електронних повідомлень різним клієнтам, які зареєструвалися на комерційному сайті. Але зловживати цим не слід — можна викликати обурення користувачів Інтернет непотрібною інформацією.

Торговець може вибрати електронні інформаційні видання — певні веб-вузли, які відвідуються певною аудиторією, і розташувати на них свою рекламу, що дає змогу здійснити цільове охоплення певної аудиторії. Існує можливість відкрити власну електронну крамницю для безпосередніх продажів у мережі. Однак за статистикою, 70—80% крамниць, які відкриваються, є збитковими. Серед причин цього — непрофесійність їх розробників.

Маркетингові дослідження в Інтернет щодо охоплення аудиторії, швидкості оброблення результатів, повноти інформації, яка надається, не мають аналогів. Багато керівників західних компаній вважають, що підключатися до Інтернету доцільно хоча б заради цих досліджень.

До послуг бізнесменів — найпотужніші комунікації Інтернет. У лічені хвилини електронні листи доходять до адресата у будь-якій точці світу. Користуючись програмами захисту інформації, можна бути впевненим, що навіть дуже зацікавленим службам (не кажучи про хакерів - одинаків), буде складно прочитати вашу кореспонденцію. Поставивши під листом свій електронний підпис, можна позбавити потенційного злодія можливості змінити навіть кому в тексті підписаного документа.

Електронний підпис *— код (послідовність одного або декількох символів), який є електронним еквівалентом письмового підпису.*

До послуг бізнесменів численні тематичні електронні конференції, списки розсилань, Інтернет - пейджери для прямого спілкування із співрозмовником, відправлення факсів у СІЛА і Канаду за ціною 10 центів за аркуш, IP-телефонія (можливість не тільки розмовляти, а й бачити співрозмовника).

Особливі переваги у менеджменті Інтернет надає компаніям, що мають віддалені філії або співробітників, яким потрібно часто їздити. Маючи модем і комп'ютер, працівники компанії завжди матимуть надійний зв'язок з головним офісом, доступ до корпоративних баз даних і можуть швидко скористатися необхідною інформацією або отримати консультацію провідних фахівців фірми.

Якщо компанія велика і має багато структурних підрозділів, то налагодження їх спільної роботи є важким управлінським завданням.

За останні п'ять років кількість користувачів мережі зросла в десятки разів і продовжує швидко зростати. Це стосується таких країн, як СІЛА, де користуються Інтернет у половині родин. У зв'язку з досягнутим рівнем «інтернетизації» американського суспільства темпи зростання ринку Інтернет - послуг у США знизяться.

Загальна чисельність користувачів Інтернет у всіх пострадянських країнах навряд чи перевищує декілька відсотків від їх загальносвітової кількості. Це перешкоджає розвитку національної електронної комерції. Однак бізнесменам цих країн не забороняється продавати товари і послуги іншим 90—98% користувачам Інтернету, хоча на практиці такі можливості обмежуються їхнім законодавством.

Проте чисельність національного мережевого контингенту постійно зростає. Відсоткове співвідношення навряд чи зміниться найближчим часом, але критичної маси користувачів пострадянських країн, за якої починається лавиноподібний розвиток комерційних проектів в Інтернет, буде досягнуто невдовзі. Підтвердженням цього є поява великої кількості публікацій з електронної комерції в пресі й мережі, а також зацікавленість комерційних структур і банків, готових оплачувати Інтернет -проекти.

Бум електронної комерції у світі почався в 1995— 1996 рр. У 1996 р. багато маркетологів та інформаційних агенцій робили прогноз розвитку комерції в Інтернет.

Очікувані цифри зростання на той час вважалися надмірно оптимістичними, але вже наприкінці 1998 р. загальний прибуток від операцій в Інтернет перевищив 8 млрд. доларів, а прибуток

від реклами — 2 млрд. доларів на рік. Саме наприкінці 1998 — на початку 1999 року про Інтернет заговорили як про абсолютний ринок, що перевершує за своїм потенціалом будь-який інший у світі.

Засади створення системи Е-комерції

Для створення системи електронної комерції спершу слід з'ясувати, яку з ланок торговельного ланцюжка займає певна компанія, яку частину своїх бізнес-процесів вона хотіла б перевести в електронну форму і які саме сфери діяльності можна оптимізувати, використовуючи Інтернет - технології.

Система електронної комерції (торговельна Інтернет - система (ТІС), Інтернет-крамниця) - форма відображення у веб-вигляді прайс-листа, комори, системи замовлень торговельної компанії, фірми-виробника тощо, яка забезпечує дієвий зв'язок віртуального світу з реальним, внутрішнім життям цієї установи.

Важливе значення має логічна система виробничо-комерційних відносин, коли компанії будують бізнес у здоровій і «прозорій» економіці, прагнучи до прибутку і стабільності. І цей «прозорий» оф-лайновий бізнес природним шляхом стає основою для он-лайнового.

Оф-лайновий бізнес — бізнес, який здійснюється у традиційній формі без використання можливостей глобальних інформаційних мереж.

Он-лайновий бізнес — бізнес, який здійснюється з використанням апаратних і програмних можливостей глобальної комп'ютерної мережі Інтернет.

Виробничі та комерційні відносини часто з різних причин побудовані «нелогічно». Тому впровадження інформаційних систем, в тому числі й систем електронної комерції, у вітчизняних компаніях відбувається повільно. Бізнес-процеси необхідно перебудовувати так, щоб вони органічно вписалися до електронної комерції

Бізнес-процес — сукупність пов'язаних між собою процедур або операцій (функцій), які реалізовують певне бізнес-завдання або політичну мету підприємства, як правило, в межах його організаційної структури.

Інформаційні технології та Інтернет — потужний стимул для перебудови, а деколи — навіть для побудови бізнес-процесів. Отже, починати слід з логічної організації бізнес-взаємодії між учасниками торговельного процесу.

Виокремлюють чотири рівні взаємовідносин учасників торговельного процесу, які слугують базою для створення системи електронної комерції:

— виробник — дистриб'ютор;

— дистриб'ютор — дилер;

— продавець — дистриб'ютор;

— покупець.

Будь-який з цих рівнів може бути частково або цілком переведений у систему електронної комерції. Важливо пам'ятати, що електронна комерція — це лише одна з форм ведення бізнесу.

Кожній компанії необхідно визначити найвигідні-іпе або найважливіше місце в бізнес-ланцюжку і зробити ставку саме на нього. Якщо, наприклад, виробнику вигідно працювати з дистриб'юторами, бо це найбільш рентабельно, — тоді з допомогою системи електронної комерції треба оптимізувати роботу з дистриб'юторами. Виробнича компанія. Для такої компанії перенесення частини процесів зі збуту своєї продукції чи послуг до глобальної мережі набуває форми прямих продажів через Інтернет.

Прямі продажі через Інтернет (он-лайнові роздрібні продажі) — продажі товарів чи послуг кінцевим користувачам, які здійснюються через Інтернет - крамницю компанії або з допомогою інших форм підтримки електронної торгівлі.

Компанії-виробнику найкраще починати з впровадження торговельної Інтернет - системи і засобів електронної комерції в роботу підрозділів збуту продукції компанії.

Для максимального економічного ефекту від впровадження системи електронної комерції інформаційна система збуту повинна бути з'єднана із системою планування виробництва і системою

організації постачань. Таким чином можна мінімізувати окремі статті видатків: ТІС дає змогу уникнути витрат на оф-лайнові комірні запаси готової продукції, комплектуючих тощо

Електронна підтримка каналів збуту і постачання здійснюється різними засобами. Для того, щоб їх зв'язати, необхідна наявність інформаційної системи підприємства чи ERP-системи.

ERP (Enterprise Resource Planning) — система планування ресурсів підприємства; програмне забезпечення нового покоління для планування ресурсів підприємства.

Крім стандартних послуг, у ній пропонуються й нові, наприклад управління якістю виробничих операцій і створення постійних звітів.

Під час розробки торговельної Інтернет - системи, інтерфейсів її програмного забезпечення й інформаційного наповнення розробники повинні виходити з принципу, що будь-який Інтернет - ресурс повинен орієнтуватися на певну групу користувачів. Якщо, наприклад, виробник орієнтується на роботу з дистриб'юторсько-дилерською мережею, то його ТІС повинна, передусім, привертати увагу дистриб'юторів-дилерів. Було б помилкою використовувати Інтернет для накопичення інформації за принципом «заходь, хто хоче, бери, що потрібно».

Інтернет - система повинна бути максимально зручною і простою для входу до неї певного споживача ззовні. Однією з таких систем є електронна платіжна система PayCash, яка пропонує розміщувати Інтернет - крамниці безпосередньо на своєму сайті, тим самим об'єднуючи їх у торговельну систему.

Побудова торговельної Інтернет - системи компанії відрізняється від побудови її традиційної інформаційної системи. Розробникам ТІС величезні можливості надають веб-технології. Одна з особливостей полягає в тому, що вони вимагають наявності в колективі розробників бригади, яку прийнято називати контентною. Робота цієї бригади близька до редакційної роботи з інформацією (текстами, числовими даними, графікою), пов'язаної з систематизацією, редагуванням і наданням даних на екрані монітора для користувачів ТІС. Електронна торговельна система є частиною іміджу компанії, її обличчям в Інтернет. Тому для користувачів мережі вагому роль відіграє можливість працювати на сайті компанії у зручному і зрозумілому для споживача просторі.

Чи потрібно виробнику організовувати прямі продажі, використовуючи електронну комерцію? Якщо виробнича компанія хоче діяти, активно використовуючи Інтернет, вона повинна мати і канали для прямих продажів. Однак далеко не кожний виробник може собі дозволити прямі продажі через мережу. Щодо цього існую принаймні дві проблеми:

1. Під час переходу на прямі продажі компанії доведеться подбати про взаємодію з традиційними дистриб'юторсько - ділерськими каналами збуту. Чим потужніший виробник, тим легше йому вирішити це питання.

2. Невеликим виробничим компаніям складно встановити зв'язки з кур'єрськими службами. Послуги великих кур'єрським систем (наприклад, UPS, DHL, TNT) недешеві, але вони гарантують високий рівень сервісу по всьому світу. В невеликих кур'єрських компаніях послуги дешеві, але при цьому знижується рівень гарантій доставки товару кінцевим споживачам і охоплення регіонів. Тобто в першому випадку товар невеликого виробничого підприємства може виявитися неконкурентним за ціною доставки (оскільки обсяги доставки невеликі), а в другому випадку компанії доведеться домовлятися з декількома кур'єрськими службами, що також позначиться на ціні товару.

Виробник може обмежити зону своїх прямих продажів до локального рівня (наприклад — Київська область і 2—3 райони навколо неї) й укласти договір з однією-двома кур'єрськими службами. При цьому виробник входить у новий для себе бізнес із взаємодії з системами кур'єрської доставки (адже раніше він працював тільки з великими дистриб'юторами). Цей новий бізнес може бути для фірми нерентабельним, бо тут усе — «локальне» (обсяги маленькі, ціни високі). Якщо компанія має намір здійснювати прямі продажі, використовуючи Інтернет -технології, їй необхідно звернутися до консалтингових компаній, які допоможуть проаналізувати ситуацію і прийняти правильне рішення

Дистриб'юторська компанія. Ініціатива створення торговельної Інтернет - системи на рівні *виробник— дистриб'ютор* може виходити й від дистриб'ютора. В такому разі це буде Інтернет - система постачання дистриб'ютора. Більшість етапів у побудові такої системи постачань для дистриб'ютора такі самі, що й для системи збуту виробника. Для дистриб'юторської компанії також важливо створити торговельну Інтернет - систему для підтримки продажів.

Перед керівництвом дистриб'юторської компанії під час створення системи електронної комерції одразу постає питання: продавати товар кінцевому покупцю за схемою прямих продажів через Інтернет і «обходити» роздрібних продавців чи продовжувати працювати через дилерів? Рішення повинна прийняти сама компанія. Можливо, потрібен моніторинг існуючої дилерської мережі з метою визначення найслабших місць. Якщо вони є, то можна перейти на прямі постачання в цих регіонах.

Дилерська частина торговельної системи дистриб'ютора обов'язково повинна бути гнучкою: дистриб'ютору важливо підтримати не тільки великих дилерів, а й тих, які тільки починають працювати. Перехід на електронно-комерційну систему відносин може дати їм змогу вийти на новий рівень бізнесу

Електронно-комерційна система, яка підтримує дилерську мережу, відкриває для дистриб'ютора нові можливості, наприклад «обхід» проміжних ланок на шляху реалізації товару кінцевому покупцю. Можлива організація електронно-комерційної взаємодії між регіонально розподіленими дистриб'юторами. В цьому разі торговельна Інтернет - система виконуватиме такі функції:

— передавання дистриб'юторами один одному регіонально розподілених замовлень;

— передавання інформації про стан комор, розташованих у різних місцях;

— надання інформації про роботу системи кінцевим покупцям.

Ці функції обов'язкові для всіх ТІС. Кожен дистриб'ютор повинен з'ясувати, який його «ареал розповсюдження». Коли моніторинг буде проведений (самостійно або з допомогою консультантів), стане можливим створення «правильної» торговельної Інтернет -системи. Дилером у ланцюжку *дистриб'ютор — дилер* може бути регіональний покупець, дрібний гуртовик, а може, й роздрібна крамниця. Все це слід чітко визначити до початку створення системи електронної комерції.

Продавець (роздрібний продаж). Організація електронно-комерційної системи під роздрібний продаж має свої особливості. Традиційний роздріб вже має ціну на товар, близьку до межових сум. Роздрібному торговцю складно почати займатися прямими постачаннями в інші регіони. Чим більша відстань, тим менш перспективно займатися глобальними прямими постачаннями. Єдиний виняток — торговельна мережа (наприклад, «Сьомий континент» або «Копійка» — система крамниць-дискаунтерів у Росії). Якщо торговельна мережа, яка вже існує, розглядає питання про створення декількох крамниць - дискаунтерів, їй обов'язково потрібно використати Інтернет -торгівлю. Інтернет - крамниці — це і є крамниці-дискаунтери. В дискаунтері ціни нижчі, ніж у звичайній крамниці, але в такій крамниці все зручно спаковано, розфасовано за певними ваговими категоріями, є широке коло порівняно дешевих товарів. І ця технологія дуже зручна для Інтернет - крамниці, тому крамниці в мережі обов'язково треба будувати як дискаунтери, тобто з низькими цінами, нормованими упаковками.

Покупець (споживач). Якщо споживач — велика організація, холдинг, то з допомогою технологій електронної комерції вона може упорядкувати стосунки між партнерами, контрагентами, а також внутрішні корпоративні зв'язки.

Холдинг — сукупність двох чи *більше юридичних осіб, пов'язаних відносинами, за яких один з учасників (головна компанія) управляє діяльністю інших.*

Більшість холдингів працюють між собою за схемою взаємних зобов'язань. Навіть якщо холдингові відносини вже побудовані, рішення електронної комерції надають економію операційних витрат на підтримку функціонування холдингу в зручному і швидкому режимі. З іншого боку, будь-якій

компанії потрібно упорядкувати відносини між суб'єктами компанії — службами збуту, доставки тощо. Електронно-комерційна база дасть змогу вирішити це нелегке завдання швидко. Великим корпораціям слід для початку з'ясувати, хто, що, кому і коли постачає. Тоді з'ясується, яким саме підрозділам потрібно в першу чергу застосовувати засоби електронної комерції, для кого це найнеобхідніше.

Однією з проблем Інтернету э спами. Інтернет відкрив широкі можливості для реклами і просування продукції в Інтернеті. Але разом з цим приходить бажання захистити споживачів від так званих спамів - явища масової розсилки небажаної пошти.

Є безліч способів реклами в Інтернеті, до них належать рекламні банери, спливаючі вікна і спам по електронній пошті.

В державі мають існувати стандарти і контроль щодо реклами. Так, наприклад, Велика Британія має ряд нормативних актів щодо контролю, регулювання як традиційної реклами, так і в Інтернеті. До них відносяться:

- Британські кодекси реклами і стимулювання збуту. Основний принцип той, що реклама має бути а) законною, пристойною, чесною та правдивою, б) підготовленою з почуттям відповідальності перед споживачами і суспільством, і в) відповідно до принципів чесної конкуренції, загальноприйнятих у бізнесі.

- Комітет з рекламної діяльності. Колектив рекламодавців, агентств і постачальників послуг та власників засобів масової інформації

- Стандарти у рекламі. Вони регулюють в тому числі спливаючі вікна-рекламу

- Інтерактивне бюро з реклами Великобританії. Торгова асоціація інтерактивної реклами, електронної комерції та маркетингу в Інтернеті, яка вимагає від своїх членів дотримуватися кодексів.

- Асоціація маркетингу Великобританії є контролером дотримання кодексу у практиці прямого маркетингу промисловості в галузі електронної торгівлі

- Закон про захист даних 1998 р. При зборі даних для цілей маркетингу електронною поштою, рекламодавці повинні надати людям можливість відмовитися від отримання небажаних повідомлень електронної пошти. Рекламодавці, які купують або використовують загальнодоступні списки особистих даних, а не збирають свої власні дані, зобов’язані надати людині можливість відмовитися від отримання небажаних повідомлень електронної пошти в першому пункті контакту.

- Норми про захист прав споживачів («на відстані») 2000 р. Їх можна застосовувати до «контрактів на відстані» про поставку товарів або надання послуг між постачальником і споживачем, укладених через, в тому числі, електронною поштою

- Директива ЄС 2000/31/ЕС про електронну комерцію 2002 р., яка набула чинності 21 серпня 2002. ЇЇ вимоги щодо електронної пошти в цілому стосуються і спаму і всіх електронних листів. Всі повідомлення повинні містити ім'я, географічну адресу, адресу електронної пошти відправника та детальну інформацію про компанію, так щоб одержувачі могли легко прийняти заходи, щоб уникнути отримання таких повідомлень у майбутньому. Всі небажані маркетингові повідомлення електронної пошти повинні бути визначені як такі й мають визначити особу, від імені якої вони були відправлені. Всі небажані маркетингові повідомлень електронної пошти повинні бути чітко визначені як такі, як тільки вони будуть отримані, з тим щоб їх можна було видалити, не читаючи їх. Спам, спрямований на стимулювання економічної діяльності, повинен бути визначений як "комерційні зв'язки" і від імені кого відправлений. Якщо спам містить інформацію про гру, повинні бути легко доступні і чітко і недвозначно представлені умови, що відносяться до цієї оферти або гри

- Тлумачення Закону про торгівлю 1968 р. Цей закон передбачає кримінальну відповідальність за застосування помилкових торгових описів будь-яких товарів або послуг. Це включає вказівку на кількість або розмір, спосіб виготовлення, призначення, дату виготовлення тощо

- Закон про Торгові марки 1994 р. Товарний знак є знаком того, що відрізняє товари або послуги одного підприємства від іншого. Маркетинг і реклама товарів може вимагати згоди власника товарного знаку, наприклад, якщо логотип, назва та форма виробу є торговою маркою. Жертва

незаконного використання товарного знака має ряд засобів правового захисту: судову заборону, відшкодування збитку, вилучення і знищення товарів або брошур порушника.

- Закон про дифамацію 1996 р. спрямований на запобігання компаніям або приватним осам образливо висловлюватись про інших. Рекламна інформація має бути вірною й правдивою.

- Норми про порівняльну рекламу 2000 дозволяють рекламодавцеві порівняти свою продукцію з діяльністю конкурентів, якщо: рекламодавець порівнює подібне з подібним, а це означає, що реклама повинна порівняти товари або послуги, які відповідають вищевказаному чи призначені для однакової мети; реклама повинна об'єктивно порівнювати один або кілька відповідних матеріалів, що піддаються перевірці, і типові риси товарів і послуг (які можуть включати в ціну), а також реклама не повинна дискредитувати або очорнити торгові марки конкурентів.

- Закон про захист споживачів 1987 р. встановлює, що введення споживачів в оману щодо ціни товару або послуги є незаконним.

Спливаючі вікна з рекламою. Ці рекламні оголошення, які буквально спливають на екрані комп'ютера, коли ви в мережі. Вони є привабливими і в деякому сенсі вводить в оману, коли людина може натиснути на "X" у верхньому правому куті, щоб видалити їх, а насправді спрямовується на їх сайті.

Спам в електронній пошті - в загальному, реклама часто образливого, такого, що вводять в оману, характеру, отримана на електронну поштову скриньку. Ці повідомлення часто - хоча і не обов’язково - порнографічного, сексуального чи фінансового характеру.

Важливо, що є різниця між спамом і законно посланою комерційною електронною поштою. Передбачається, що спам є одним з найважливіших питань у розвитку електронної комерції. Орієнтовна оцінка загальносвітового обсягу спаму тримається на рівні близько 60-70%.

Spamhaus це організація, яка активно виступає проти спаму. На своєму сайті (http://www.spamhaus.org) вона викладає список серверів, окремих осіб і країн, які мають неналежно борються зі спамами.

Проблеми спаму - це міжнародна проблема. Саме тому ЄС і Сполучені Штати взяли на себе провідну роль у виданні анти-спам законодавства з метою покласти край спаму. Директива про конфіденційність електронних комунікацій (2002/58/ЕС) та Директива про обробку персональних даних і захист недоторканності приватного життя в секторі електронних комунікацій має ключове значення для боротьби зі спамом.

У ст. 1 Директиви зазначено, що вона «... гармонізує положення держав-членів, необхідні для забезпечення еквівалентного рівня захисту основних прав і свобод, і зокрема права на недоторканність приватного життя стосовно обробки персональних даних у секторі електронних комунікацій і забезпечити вільне пересування таких даних і електронних засобів зв'язку в Співтоваристві». З цієї статті видно, що Директива призначена для узгодження заходів. Її основна мета полягає в забезпеченні дотримання балансу між особистим життям і вільним поширенням інформації.

Модуль 2. Міжнародна діяльність з просування торгівлі і надання послуг через електронні засоби

Тема 4. Доменні імена

Щоб бути визнаними споживачами й мати справи в Інтернеті, електронним торговцям потрібно мати те, що відомо як доменні імена.

Комерціалізація Интернету вимагає від фірм учасників електронної комерції встановити свою присутність у кіберпросторі. Комп'ютери в Інтернеті зв'язані один з одним рядом цифр, таких як 324.546.576.29., інакше називаних протоколом адреси Інтернет. Доменне ім'я - це визнаний вербальний код, еквівалентний адресі постачальника інформації, який краще запам'ятовується людьми.

Для доменного імені важливо, що воно а) повинне бути унікальним; б) встановлювати ім'я власника, в) встановлювати або сутність власника – com.org.gov. тощо, або міжнародну присутність або країну перебування – com. або co.uk.

Доменні імена не обов'язково є торговельними марками, але вони вони виконують ту ж саму роль в Інтернеті, дозволяючи встановлювати особу-виготовлювача товарів або постачальника послуг.

Для користування Інтернетом слід мати на увазі наступне.

1. Будь-який електронний адрес, який містить символ @ («мавпа», «собака»), є адресом електронної пошти. Зліва від символу @ стоїть ім’я користувача або логін, тобто частина адреси, яка відповідає на питання: «Кому?». То, що стоїть зправа від @, відповідає на питання: «Куди?». Наприклад, info@bolero.ru. (bolero. – це доменне ім’я (містить вказівку на назву організації; ru-домен вищого рівня, що вказує на те, в якій країні знаходиться організація)).

Кожний домен верхнього рівня має своє значення - com – комерційна (підприємницька) організація; as, u, ca, jp, ru, ua, rz - відповідно: США, Велика Британія, Канада, Японія, Росія, Україна, Казахстан; edu – університет або організація освіти; net – мережева організація; org – некомерційна (непідприємницька) організація; gov – державна організація.

2. Зустрічаються такі електронні адреси, які не містять символу @, наприклад, http: //www.name/com. Цей різновид електронної адреси носить назву (URL Univerzal Resource locat or – універсальний показчик ресурсів). Перша частина адреси в форматі URL використовується для вказівки засобу Інтернету, який треба використовувати для доступу до цієї адреси; http:// - означає Hyper Text Trausfer Protocol (протокол передачі гіпертексту). Але навіть якщо символ http не використано, це - web–адреса, яка, за правило, починається з www. Все що стоїть після одинарної косої риски (/), вважається назвою файла або каталогу.

3. Адреса інтернету, за правило, ніколи не містить прогалин між словами.

Торгівельні марки. Торгівельні марки дозволяють власникові зареєструвати її при підтвердженні кваліфікації. Коли це зроблено, можна чекати більший ступінь захисту з боку держави. Торгівельна марка визначена в розділі 1 Акту 1994 року як будь-який знак, здатний бути представленим графічно, що здатний відрізняти товари або послуги одного підприємства від товарів або послуг інших підприємств. Торгівельна марка може, зокрема, складатися зі слів (включаючи особисті імена), малюнків, букв, цифр на товарах або їхньому впакуванні. Головна вимога до марки укладається в тім, що вона повинна відрізняти одного торговця від іншого. Прикладами можуть бути особисті імена (приправа до салату Ньюмена) або підпису (Кэдберри, Кока кола, написані рукописно) або те, до чого власники часто прибігають, винайдене слово або слова, але не слова, які б суперечили тим, що вони, крім усього іншого описували б фізичні характеристики продукту або послуги, і тим самим перешкоджали б конкурентам.

Варто також помітити, що в умовах Інтернету могли б бути зареєстровані монограми, наприклад, ‘JPS’, ‘BSA’. Звичайно треба три букви, але коли марка добре відома, могли б бути прийняті й дві букви (‘BP’ було дозволено).

У такий же спосіб можуть бути прийнятними числа ‘4711’, ‘911’. Міра успіху таких марок може бути продемонстрована питанням є чи необхідність повідомляти, до яких продуктів або компаній ставляться ці марки.

Акт 1994 додав ряд пунктів, які можна класифікувати, як характерні і які не були включені в класифікацію попередніми актами. Вони включають: заходи (наприклад, Шанель № 5) ; звуки (дзвінок прямої лінії страхування), назви місць (Йорк (трейлери), Уімблдон (теніс))

Визначаючи, що могло б становити торговельну марку, Бюро патентів опублікувало оголошення: «Практика щодо торговельної марки, що включає слово 'net'» і «Про реєстрації в Інтернеті доменних імен як торгівельних марок»

Власне кажучи такими термінами, як .com або .co.uk варто зневажати. Про марку повинні судити за звичайними критеріями розпізнавальної чинності за умовами, як прийнятності, так і порушення.

Реєстрація доменних імен і торгівельних марок. Торгівельні марки реєструються у різних країнах по категоріях (класам). Реєстрація торгівельних марок у Великобританії відбувається відповідно до Акту про торгівельні марки 1994, а заявки на реєстрацію приймає Бюро патентів. Можна зареєструвати торгівельну марку Співтовариства і вона буде дійсна у всіх державах-учасниках, якщо подати центральну заявку в Керування по Координації на внутрішньому ринку (торговельні марки й проектування), розташоване в Аликанте, Іспанія. На міжнародному рівні Мадридська угода й Протокол про міжнародну реєстрацію торгівельних марок передбачають систему міжнародного визнання торгівельних марок таким чином, що визнання в одній державі-учасниці буде загальноприйнято й в іншому. Ця система підготовлена ВОІВ (Всесвітньою організацією по охороні інтелектуальної власності) і гарантує загальне визнання.

Існує 45 міжнародних категорій товарів і послуг, яким потрібен захист. Кожна категорія вимагає окремої реєстрації, якщо особа, що подає заявку на реєстрацію, не йде на реєстрацію, що складається з багатьох категорій. Ту саму торговельну марку можна зареєструвати в різних категоріях або та сама торговельна марка може співіснувати в декількох різних категоріях.

Реєстрація доменних імен. Домени вищого рівня. Уся система компетенції й реєстрації доменних імен в усьому світі контролюється Новою некомерційною організацією по призначенню адрес і імен в Інтернеті, параметрів протоколів, керуванню системами доменних імен (ICANN). Вона була створена в 1998 році.

Існують різні доменні імена, з яких можна вибирати: характерні вищі доменні імена, наприклад, .com, .org, .edu, .mil, .net; деякі вищі доменні імена субсидіюються (.aero, .coop, .museum); деякі не субсидіюються (.info, .biz); вищі доменні імена коду країни, наприклад, .uk, .fr, .eu

Яке вище доменне ім'я зареєструвати? Доменні імена є ключовими для електронних фірм, і для успішного бізнесу необхідна їхня відповідна реєстрація. Фірми можуть зареєструвати свої (доменні) імена або торговельні марки за прикладом декількох з вищевказаних вищих доменов для гарантії того, що покупці знайдуть їх, не використовуючи механізм пошуку, і щоб уникнути того, що конкурент використає це ім'я під іншим вищим доменним ім'ям.

Як зареєструвати доменне ім'я? Є три способи одержання доменного імені: зареєструватися у відповідному системному реєстрі (наприклад, Номинет у Великобританії), заплатити за послуги реєстраційного брокера, купити ім'я в існуючого власника. Можна використовувати такі системні реєстри: вищі доменні імена можна зареєструвати через одне з акредитованих реєстраційних бюро ICANN, а вищі доменні імена коду країни всі мають свою власну організацію. Наприклад, для Великобританії - це НОМИНЕТ.

Суперечки про доменні імена. Торговельні марки захищені проти зазіхань. Позов про «пассинг-оф» по загальному праву є новим і основним типом надаваного захисту. Однак головною проблемою з «пассинг-оф» є вимога до позивача підтвердити існування репутації, на яку, за його заявою, зазіхав відповідач. «Пассинг-оф» часто використається для торговельних марок, які не задовольняють характерним вимогам торговельних марок.

Такі позови також часто пред'являють у випадку незаконного використання доменних імен, або коли доменне ім'я реєструється як торговельна марка, або коли доменне ім'я є шановною маркою («пассинг-оф»). Незаконне використання доменного імені може створюватися кіберсквоттингом або реєстрацією доменного імені, що спантеличує своєю подібністю на добре відоме ім'я. Наприклад, зрівняєте www.Royalmail.co.uk і www.Roymail.co.uk.

Альтернатива судочинству про доменні імена доступна відповідно до УДРП (UDPR) і здійснюється різними реєстраційними бюро.

Кіберсквоттинг - це практика, що укладається в реєстрації добре відомих назв як доменні імена й витягу вигоди із правила «першим прийшов, першим обслужений», що залишалося до недавніх часів характеристикою реєстраційної системи доменних імен.

Кіберсквоттинг у дійсності з'явився через те, що відповідні реєстраційні бюро діяли по цьому принципі при видачі доменних імен. Ніхто з них не шукав підтвердження на право використати це ім'я. Цее положеннння ускладнюваловалося через дв інш способи одержання імені ... власне кажучи покупки в так називаного агента/власника, хто вже зареєстрував ім'я з наміром продати й ні по як інш причині. У більшості випадків кіберсквоттинга існує натяк на вимагання.

Див. справа British Telecommunication plc, Virgin Enterprises Ltd, J Sainsbury plc, Marks & Spencer plc, Ladbroke Group plc v One in a Million [1999] FSR 1, що було першою справою на цьому рівні, що ставиться до незаконного придбання й використання доменного імені. У цій справі One in a Million Ltd зареєструвала такі імена, як Ladbroke.com, sainsbury.com, sainsburys.com, marksandspencer.com, bt.org і virgin.org. Згодом вони звернулися до відповідних компаній із пропозицією продати ці доменні імена.

Справа розглядає таке незаконне придбання й звертається до «пассинг-оф» і зазіхання на торговельну марку.

Порушення торговельної марки. Реєстрація торговельної марки дає монопольні права на торговельну марку. Деякі дії, виконані без згоди власника, є порушенням. Правопорушуючі дії перераховані в розділі 10. Права власника мають чинність від дня реєстрації, що фактично є датою заповнення заяви про реєстрації відповідно до розділу 40(3).

Відповідно до розділу 10 Акту про торговельну марку 1994 *змішання* означає, що а) особа порушує зареєстровану торговельну марку, якщо вона використає в ході торгівлі знак, що ідентичний торговельній марці товарів або послуг, які ідентичні зареєстрованим товарам або послугам, б) особа порушує зареєстровану торговельну марку, якщо вона використає в ході торгівлі знак, тому що знак ідентичний торговельній марці й використовується для товарів або послуг схожих на ті, на які зареєстрована торговельна марка, або знак схожий на торговельну марку й використовується для товарів або послуг ідентичних або схожих на ті, на які зареєстрована торговельна марка.

Існує ймовірність плутанини з боку суспільства, що включає ймовірність асоціації з торговельною маркою.

Ослаблення як порушення означає, що особа порушує зареєстровану торговельну марку, якщо вона використає в ході торгівлі знак, що ідентичний або схожий на торговельну марку, і використовується для товарів і послуг, які не схожі на ті, на які зареєстрована торговельна марка,коли торговельна марка має репутацію в Об'єднаному Королівстві й використання знака без належної причини має несправедливу перевагу або приносить збиток характерній рисі або репутації торговельної марки.

Ніщо в попередніх положеннях цієї статті не повинне тлумачитися, що як запобігає використання зареєстрованих торговельних марок будь-якою особою з метою розпізнавання товарів або послуг як товари або послуги власника або ліцензіата.

Але будь-яке таке використання іншим образом, а не відповідно до чесної практики в промислових або комерційних справах повинне розглядатися як порушення зареєстрованої торговельної марки, якщо використання знака без належної причини має несправедлива перевага або приносить збиток характерної риси або репутації торговельної марки.

Див. приклад у відношенні Інтернету Hasbro Inc v Internet Entertainment Group C96 130 WD. Хазбро робить іграшки, включаючи гру для маленьких дітей, називану Кэнди Лэнд. ИИГ створила домен, названий 'candyman.com' для розваги дорослих. Була видана судова заборона.

Чесне співпадаюче використання. Для застосування прецедентного права в ситуації з Інтернетом див., наприклад, справа Pitman Training Limited і PTC Oxford Ltd v Nominet UK Ltd і Pearson Professional Ltd. [1997], що не втримується в збірниках судових рішень.

Обмеження на дію зареєстрованої торговельної марки має місце у випадку, коли дві торговельні марки законно зареєстровані в різних категоріях, у принципі не існує порушення. Торговельна марка також у принципі не порушується, коли особа використає своє власне ім'я або адресу, вказівки про тип, якість, кількість, призначення й т.д. товарів і послуг.

«Пассинг-оф» (комерція під чужим ім'ям). Головні елементи сучасного позову були встановлені в провідній справі: Erven Warnink Besloten Vennootschap v J. Townend & Sons [Hull] Ltd. [1979]. Суд при рішенні на користь позивача встановив основні вимоги для позову, а саме: перекручування фактів, зроблене торговцем у ході свого бізнесу, щодо перспективного клієнта або, якщо це послуга остаточному споживачеві послуги розрахована на те, щоб нашкодити бізнесу або репутації іншого торговця, ... або те, що це був передбачуваний наслідок його дій, навіть якщо й не розраховане, що викликає або ймовірно заподіяло б збиток іншому торговцеві.

Див. Glaxo plc and another v Glaxowellcome Ltd [1996] FSR 388, де Дж. Лайтмен ухвалив, що суд …не схвалює будь-яка така перевага при реєстрації компаній з іменами, коли в інших є репутація в цих іменах, а сторона, що реєструє, потім вимагає заплатити за зміну імен.

Див. також справа British Telecommunication plc, Virgin Enterprises Ltd, J Sainsbury plc, Marks & Spencer plc, Ladbroke Group plc v One in a Million [1999] FSR 1.

Репутація позивача. Перед тим, як позивач почне обвинувачувати іншого торговця в підриві репутації, повинне бути встановлене, що існує така репутація, яку можна підірвати. Наприклад, для цього використаються наступні фактори: тривала практика, обсяг продажів, витрати на рекламу, свідоцтво інших торговців на тім же самому ринку про положення на цьому ринку, висновку споживачів у межах ринку в результаті ринкового опитування. Жоден із цих факторів не є вирішальним.

Перекручування фактів відповідачем. Для того щоб успішно переслідувати відповідача судом, позивач повинен установити «змішання, що володіє позовною чинністю». Ключове питання – «Кого повинні змішувати?» Суди не думають, що суспільство гарне інформоване. Див., наприклад, Morning Star v Express Newspapers [1977].

Арбітражне врегулювання спорів. Необхідність мати кошти для рішення спорів виявилася в справі Питмана. Реєстраційному бюро доменних імен, Номинет, загрожувала судовим позовом одна сторона, якщо ім'я не буде перепризначено, і позовом інша сторона, якщо це відбудеться. Класичний приклад ситуації «без переможців». З появою Нової некомерційної організації по призначенню адрес і імен в Інтернеті, параметрів протоколів, керуванню системами доменних імен (ICANN) як організаційного органа для системи доменних імен був прийнятий новий підхід. Будь-яка організація, що бажає діяти як реєстраційне бюро у відношенні характерних доменних імен, зобов'язана вести справу відповідно до «Єдиної політики рішення спорів про доменні імена».

Вона вимагає від заявників на доменні імена надати обов'язкові процедури рішення спорів затвердженим постачальникам послуг з рішення спорів у випадку будь-якого позову про те, що:

доменне ім'я відповідача ідентичне або спантеличує своєю подібністю на торговельну марку або марку послуг, на які позивач має права; а відповідач не має прав або правових інтересів відносно доменного імені; зареєстроване доменне ім'я використовується несумлінно. Позивач зобов'язаний довести всі ці пункти позову. Якщо позовні вимоги обґрунтовані, тоді ім'я буде перепризначене або скасоване.

Тема 5. Захист інформації у комп'ютерних мережах

Шифрування використовується для автентифікації і збереження таємниці. *Шифрування* — метод перетворення первісних даних у закодовану форму. Шифр (код) — сукупність правил для шифрування.

Криптографічні технології (методи захисту даних з використанням шифрування) забезпечують три основних типи послуг для електронної комерції: автентифікацію, неможливість відмови від здійсненого, збереження таємниці.

Автентифікація — метод перевірки не тільки особистості відправника, а й наявності чи відсутності змін у повідомленні. Реалізація вимоги *неможливості відмови* полягає в тому, що відправник не може заперечити, що він відправив певний файл (дані), а отримувач — що він його отримав (це схоже на відправлення замовного листа поштою). *Збереження таємниці* — захист повідомлень від несанкціонованого перегляду.

Шифрування, або кодування, інформації з метою її захисту від несанкціонованого читання — головне завдання криптографії. Щоб шифрування дало бажаний результат, необхідно, щоб і відправник, і одержувач знали, який шифр був використаний для перетворення первісної інформації на закодовану форму (зашифрований текст). Шифр визначає правила кодування даних.

В основу шифрування покладено два елементи: криптографічний алгоритм і ключ.

Криптографічний алгоритм — математична функція, яка комбінує відкритий текст або іншу зрозумілу інформацію з ланцюжком чисел (ключем) з метою отримати незв 'язний (шифрований) текст

Новий алгоритм важко придумати, але один алгоритм можна використовувати з багатьма ключами. Існують ще спеціальні криптографічні алгоритми, які не використовують ключів.

Шифрування з ключем має дві переваги.

1. Новий алгоритм шифрування описати важко, і навряд чи хтось захоче це робити щоразу під час відправлення таємного повідомлення новому респонденту. Використовуючи ключ, можна застосовувати той самий алгоритм для відправлення повідомлень різним людям. Головне — закріпити окремий ключ за кожним респондентом.

2. Якщо хтось «зламає» зашифроване повідомлення, щоб продовжити шифрування інформації, достатньо лише змінити ключ. Переходити на новий алгоритм не потрібно (якщо був «зламаний» ключ, а не сам алгоритм). Чим більше комбінацій, тим важче підібрати ключ і переглянути зашифроване повідомлення.

Надійність алгоритму шифрування залежить від довжини ключа.

Довжина ключа — кількість біту ключі, яка визначає число можливих комбінацій.

Алгоритми шифрування:

DES (Data Encryption Standard). Цей шифр розроблений фахівцями фірми IBM і затверджений урядом США у 1977 р. Використовує закритий 56-бітовий ключ і оперує блоками даних по 64 байт. Відносно швидкий, застосовується під час одноразового шифрування великої кількості даних.

Потрійний DES. Шифрує блок даних три рази трьома різними закритими ключами. Запропонований як альтернатива DES, оскільки загроза швидкого і легкого його «злому» швидко зростає.

RC2, RC4, RC5. Шифри із змінною довжиною ключа для дуже швидкого шифрування великих обсягів інформації. Діють трохи швидше від DES і здатні підвищувати ступінь захисту через вибір довшого ключа.

IDEA (Internatiomal Data Encryption Algorithm). Створений у 1991 р. і призначений для швидкої роботи в програмній реалізації. Дуже стійкий шифр, використовує 128-бітовий закритий ключ.

RSA (названий на честь його розробників Rivest, Shaimr, Adelman). Алгоритм з відкритим ключе підтримує змінну довжину ключа, а також змінний розмір блоку тексту, що шифрується. Розмір блоку відкритого тексту повинен бути меншим від довжини ключа.

DSA (Digital SignatureAlgorithm). Може створювати підписи швидше від RSA. Поширюється як стандарт цифрового підпису фщіїаі (Digital Signature Standard, DSS), поки що не має загального визнання.

Симетричне шифрування або шифрування з таємним ключем - це найдавніша форма шифрування з використанням ключа. Під час шифрування за такою схемою відправник і одержувач володіють одним ключем, з допомогою якого обидва можуть зашифровувати і розшифровувати інформацію.

Однак існують проблеми з автентичністю, оскільки особистість відправника або одержувача повідомлення гарантувати неможливо. Якщо двоє володіють одним ключем, кожен з них може написати і зашифрувати повідомлення, а після цього заявити, що це зробив інший. Це не дає змоги реалізувати принцип неможливості відмови. Проблему відмови від авторства може вирішити криптографія з відкритим ключем, що використовує асиметричні алгоритми шифрування. У симетричному шифруванні використовується один секретний ключ для шифрування і розшифровування повідомлень.

*Криптографія з відкритим ключем***.** Заснована на концепції *ключової пари.* Кожна половина пари (один ключ) шифрує інформацію так, що її може розшифрувати тільки інша половина (другий ключ). Одна частина ключової пари — особистий ключ — відома тільки її власнику. Інша половина — відкритий ключ — розповсюджується серед усіх його респондентів, але зв'язана тільки з власником.

Ключові пари володіють унікальною властивістю: дані, зашифровані будь-яким з ключів пари, можуть бути розшифровані тільки іншим ключем з цієї пари.

Відкрита частина ключової пари може вільно розповсюджуватися, і це не перешкодить використовувати особистий ключ. Ключі можна використовувати і для забезпечення конфіденційності повідомлення, і для автентифікації його автора.

Кожен, хто має копію відкритого ключа, здатний прочитати повідомлення, зашифроване ним. У комерційних трансакціях прийнята стандартна процедура: покупець шифрує повідомлення своїм особистим ключем, а підтвердження продавця, в свою чергу, шифрується його особистим ключем. Це означає, що кожен, кому відомий відкритий ключ продавця, спроможний це підтвердження прочитати. Для збереження в таємниці інформації, надісланої продавцем, необхідні додаткові кроки.

Оскільки певний користувач — єдиний, хто має можливість зашифрувати інформацію особистим ключем, то той, хто використовує його відкритий ключ для розшифрування повідомлення, може бути впевнений, що воно саме від цього користувача. Отже, шифрування електронного документа користувача особистим ключем подібне до підпису на паперовому документі. Але, на жаль, немає жодних гарантій, що таке повідомлення не прочитає сторонній.

Використання криптографічних алгоритмів з відкритим ключем для шифрування повідомлень — це дуже повільний обчислювальний процес, тому фахівці криптографи знайшли засіб швидко генерувати коротке унікальне подання особистого повідомлення — дайджест.

Дайджест. Незважаючи на назву, дайджест повідомлення не є його стислим викладенням.

Існують криптографічні алгоритми для генерації дайджестів повідомлення — *однобічні хеш-функції.* Однобічна хеш-функція не використовує ключа. Це звичайна формула для перетворення повідомлення будь-якої довжини в один рядок символів (дайджест повідомлення). При використанні 16-байтової хеш-функції оброблений нею текст матиме на виході довжину 16 байтів. Наприклад, повідомлення може бути надане ланцюжком символів VCC349RTYasd904. Кожне повідомлення формує свій випадковий дайджест. Якщо зашифрувати дайджест особистим ключем, то можна

отримати цифровий підпис. Припустимо, що продавець А перетворив своє повідомлення на дайджест, зашифрував його особистим ключем і відправив В цей цифровий підпис разом з відкритим текстом повідомлення. Після того як В використає відкритий ключ А для розшифрування цифрового підпису, у нього буде копія дайджесту повідомлення А. Оскільки він зумів розшифрувати цифровий підпис відкритим ключем А, то А є її автором. Після цього В використовує ту ж саму хеш-функцію (про яку обидва домовилися заздалегідь) для підрахунку власного дайджесту для відкритого тексту повідомлення А. Якщо отриманий рядок збігається з тим, що надіслав А, то В може бути впевнений в автентичності цифрового підпису. А це означає не тільки те, що відправник повідомлення є А, а й те, що повідомлення не було змінене.

Проблема полягає лише в тому, що саме повідомлення надсилається відкритим текстом, а, отже, його конфіденційність не зберігається. Для шифрування відкритого тексту повідомлення можна додатково використовувати симетричний алгоритм із секретним ключем. Але це ускладнить процес.

Отже, названі способи не забезпечують «абсолютного» захисту інформації. Однак вони:

— гарантують мінімально необхідний час для «зламу» ключів: від декількох місяців до декількох років; за цей час інформація, що передається, стає неактуальною;

— гарантують, що вартість «зламу» у кілька разів перевищує вартість самої інформації.

Не дуже стійкий криптозахист може бути «зламаний» на звичайному комп'ютері з використанням спеціалізованого програмного забезпечення (ПЗ). Таке ПЗ можна отримати в Інтернет як безкоштовно, так і за невеликі гроші. А що стосується стійких з точки зору криптографії систем, то їх, як правило, вдається «зламувати» іншими, організаційними шляхами. Наприклад, одного дня всі абоненти провайдера одержують листа немовби від системного адміністратора. У листі пропонується якась додаткова (звісно, безкоштовна) послуга. Щоб отримати її, користувачам слід надіслати листа зі своїм логіном і паролем. З декількох сотень клієнтів провайдера обов'язково знайдеться кілька не дуже досвідчених користувачів, які відправлять дані, не звернувши уваги на те, що системному адміністратору не потрібно знати пароля користувача і що електронна адреса, на яку вони надсилають листи, зовсім не адміністраторська. Таким чином зловмисник водночас стає власником декількох паролів. Найменша халепа, яка очікує довірливих користувачів, — те, що їх рахунок у провайдера буде використаний іншими.

Роль цифрових сертифікатів і сертифікаційних центрів. Щоб використовувати систему криптографії з відкритим ключем, необхідно згенерувати відкритий і особистий ключі. Як правило, це робиться програмою, яка буде використовувати ключ (web-браузером або програмою електронної пошти). Після того як ключова пара генерована, користувач повинен зберігати свій особистий ключ у таємниці від сторонніх. Потрібно розповсюдити відкритий ключ серед своїх респондентів. Для цього можна використовувати електронну пошту. Однак такий підхід не забезпечує автентифікації: хтось може згенерувати ключову пару і, приховуючись за іменем певного користувача, розіслати відкритий ключ респондентам. Після цього ніщо не завадить йому відправляти повідомлення від імені цього користувача.

Найнадійніший спосіб розповсюдження відкритих ключів — послуги сертифікаційних центрів — сховищ цифрових сертифікатів.

Цифровий сертифікат — електронний ідентифікатор, який підтверджує справжність користувача, містить інформацію про нього, слугує електронним підтвердженням відкритих ключів.

Сертифікаційні центри несуть відповідальність за перевірку особистості користувача; надання цифрових сертифікатів; перевірку їх справжності.

Сертифікаційний центр приймає відкритий ключ разом з доказами особистості (якими — залежить від класу сертифіката). Після цього респонденти користувача можуть звертатися до сертифікаційного центру за підтвердженням відкритого ключа користувача.

Відомі сертифікаційні центри (VeriSign, Cybertrust і Nortel) видають цифрові сертифікати, що містять ім'я власника, назву сертифікаційного центру, відкритий ключ для шифрування

кореспонденції, термін дії сертифіката (як правило, від шести місяців до року), клас та ідентифікаційний номер цифрового сертифіката.

Виданий цифровий сертифікат може належати до одного з чотирьох класів, які вказують на ступінь верифікації власника. Сертифікат першого класу отримати найлегше, оскільки тут вимагається мінімальна перевірка біографічних даних (лише імена й адреси електронної пошти). Під час видачі сертифіката другого класу сертифікаційний центр перевіряє посвідчення особистості, номер картки соціального страхування і дату народження. Користувачі, які бажають отримати сертифікат третього класу, повинні бути готові до того, що, крім інформації, необхідної для отримання сертифіката другого класу, сертифікаційний центр перевірить їх кредитоздатність, використовуючи спеціальні установи. Сертифікат четвертого класу містить ще й інформацію про посаду власника в його установі, але відповідні верифікаційні вимоги тут ще не вироблені остаточно. Чим вищий клас сертифіката, тим вищий ступінь верифікації.

Щоб отримати цифровий сертифікат у комерційному або урядовому сертифікаційному центрі, користувач повинен внести певну плату (є й винятки). її розмір зростає з класом сертифіката (у тому числі й через додаткову роботу, необхідну для перевірки особистих даних користувача). Завдяки точній перевірці даних біографії власників сертифікатів вищих класів, сертифікати можуть вважатися надійним підтвердженням особистості користувача.

Сертифікаційні центри несуть відповідальність і за ведення й публікацію списку недійсних сертифікатів. Існують комерційні сертифікаційні центри (VeriSign, Cybertrust і Nortel) і державні (Поштова служба США). Компанія може стати сертифікаційним центром і після цього видавати сертифікати своїм службовцям або іншим компаніям

Інші системи захисту інформації, що передається в Інтернет. Для безпеки електронної комерції розроблено низку протоколів і програмних застосувань, які використовують криптографічні методики. Крім того, всупереч думці про Інтернет як про ненадійний носій інформації через його децентралізацію, трансакції тут можуть бути добре захищені шляхом використання багатьох стандартів, які охоплюють усі рівні мережі — від пакета даних до програмного застосування.

Стандарти забезпечують захист сполучень і програмних застосувань.

Сполучення (connection) — зв'язок між вузлами мережі або вузлами та їх абонентами.

Програмне застосування — програма (впорядкована послідовність команд) для комп'ютера, яка працює під керуванням певної оперативної системи

Табл.2 Призначення стандартів для захисту всіх рівнів мережі

Стандарт (протокол)	Виконувана функція	Місце використання стандартів
Secure HTTP (S-HTTP)	Захист трансакцій у Web	Програми-браузери, web-сервери, програмні застосування для Інтернет
Secure Sockets Layer (SSL)	Захист пакетів даних на мережевому рівні	Програми-браузери, web-сервери, програмні застосування для Інтернет
Secure MIME (S/MIME)	Захист електронних повідомлень, які передаються за поштовим протоколом MIME	Поштові програми з підтримкою шифрування і цифрового підпису RSA
Secure Wide Area Networks (S/WAN)	Шифрування однорангових сполучень між брандмауерами і маршрутизаторами	Віртуальні приватні мережі
Secure Electronic Transaction (SET)	Захист трансакцій з кредитними картками	Смарт-картки, сервери трансакцій, електронна комерція

Розглянуті стандарти можна класифікувати відповідно до того, що саме вони захищають — сполучення чи програми. Такі стандарти, як SSL і S/WAN, призначені для захисту комунікацій в Інтернет; хоча SSL використовується насамперед з web-застосуваннями. S-HTTP і S/MIME спрямовані на забезпечення автентифікації і конфіденційності (8-HTTP — для ЧАГеЬ-застосувань, а 8/MIME — для електронної пошти). SET забезпечує тільки захист трансакцій електронної комерції.

Захист web-застосувань: S-HTTP і SSL. Web-застосування захищені двома протоколами — S-HTTP і SSL, які забезпечують автентифікацію для серверів і бра-узерів, а також конфіденційність і цілісність даних для сполучень між web-сервером і програмою-браузером

S-HTTP — захищений HTTP-протокол, розроблений компанією Enterprise Integration Technologies (EIT) спеціально для Web. Він дає змогу забезпечити надійний криптозахист тільки для HTTP-документів web-сервера. Його використання неможливе для захисту інших прикладних протоколів (FTP, TELNET, SMTP тощо). S-HTTP призначений насамперед для підтримки протоколу передачі гіпертексту (HTTP), забезпечує авторизацію і захист web-документів.

SSL — розробка компанії Netscape — пропонує ті ж самі засоби захисту, але для комунікаційного каналу.

Канал — лінія зв'язку між двома вузлами мережі або вузлом і одним з його абонентів.

За SSL кодування інформації здійснюється на рівні порту.

Порт — ідентифікаційний номер, який відповідає кожному програмному застосуванню або процесу, що використовують базовий протокол Internet TCP як транспортний.

SSL — наймасовіший механізм захисту інформації, який застосовується у www – системі. Однак він не призначений для забезпечення безпеки на основі автентифікації, що відбувається на рівні програмного застосування або документа. Для управління доступом до файлів і документів потрібно використовувати інші засоби.

Отже, SSL — універсальний протокол захисту сполучення, що використовує криптографію з відкритим ключем і є єдиним універсальним засобом, який дає змогу динамічно захистити будь-яке сполучення з використанням будь-якого прикладного протоколу (HTTP, DNS, FTP, TELNET, SMTP тощо).

SSL вже оформився як офіційний стандарт захисту для HTTP-сполучень, тобто для захисту web-серверів. Його підтримують домінуючі на ринку програми-браузери компаній Microsoft і Netsscape. Як правило, для встановлення SSL-сполучення з web-сервером ще необхідне й програмне забезпечення для нього. Такі версії web-серверів існують (наприклад, SSA-Apache).

Однак поки що жоден з існуючих криптопротоколів не оформився як єдиний стандарт захисту сполучення, який би підтримувався всіма виробниками мережевих операційних систем (ОС). Якби протокол SSL підтримували всі мережеві ОС, не було б потреби в розробці спеціального програмного забезпечення SSL-сумісних серверів (DNS, FTP, TELNET, WWW тощо). Але виробники мережевих ОС не можуть домовитися про єдину позицію і певним чином перекладають рішення проблем інформаційної безпеки безпосередньо на користувачів Інтернет.

Отже, S-HTTP захищає дані, а SSL — комунікаційний канал.

Захист *електронної пошти***.** Для захисту електронної пошти в Інтернет існує безліч різноманітних протоколів, але лише кілька з них поширені.

PEM (Privacy Enhanced Mail). Це стандарт Інтернет для захисту електронної пошти з використанням відкритих або симетричних ключів. Він застосовується усе рідше, оскільки не призначений для оброблення нового MIME-формату електронних повідомлень і вимагає жорсткої ієрархії сертифікаційних центрів для видачі ключів.

S/MIME**.** Відносно новий стандарт, у якому задія-но багато криптографічних алгоритмів, запатентованих і заліцензійованих компанією RSA Data Security Inc. S/MIME використовує цифрові сертифікати і, отже, при забезпеченні автентифікації спирається на використання сертифікаційного центру.

PGP (Pretty Good Privacy). Це родина програмних продуктів, які використовують найстійкіпіі криптографічні алгоритми. В їх основу покладено алгоритм RSA. PGP реалізує технологію, відому як *криптографія з відкритими ключами,* яка дає змогу обмінюватися зашифрованими повідомленнями і файлами каналами відкритого зв'язку без наявності захищеного каналу для обміну ключами, а також накладати на повідомлення й файли цифровий підпис. Іншими словами, програма побудована за принципом «павутини довіри» (Web of Trust) і дає змогу користувачам розповсюджувати свої ключі без посередництва сертифікаційних центрів.

PGP була розроблена американським програмістом, громадським діячем Ф. Цимерманом, стурбованим порушенням особистих прав в інформаційну епоху. В 1991 р. у США існувала реальна загроза прийняття закону, який забороняв би використання стійких криптографічних засобів без так званого «чорного ходу», використовуючи який, спецслужби могли б безперешкодно читати зашифровані повідомлення. Тоді Цимерман почав безкоштовно розповсюджувати PGP в Інтернет. PGP став найпоширенішим криптографічним пакетом у світі (понад 2 млн. копій), а Цимермана три роки переслідувала влада, підозрюючи його в незаконному експорті озброєнь.

Нині PGP розповсюджується на комерційних засадах основаною Цимерманом фірмою PGP, Inc. Експорт PGP у програмному коді, що виконується, заборонений у США, тому в інших країнах використовуються міжнародні релізи цієї програми, які обходять заборону.

PGP випускається для всіх основних операційних систем, і повідомлення з його допомогою можна шифрувати до використання програми відправлення електронної пошти. Деякі поштові програми (наприклад, Eudora Pro), дають змогу підключати спеціальні PGP-модулі для оброблення зашифрованої пошти.

Нагадаємо, особливість систем шифрування з відкритим ключем полягає в тому, що вони працюють не з одним ключем, а з парою. Те, що зашифроване першим ключем, може бути розшифроване тільки з допомогою другого, і навпаки. Отже, користувач зберігає у себе перший — таємний — ключ і нікому його не повідомляє. Другий ключ — публічний — користувач повідомляє усім, розсилає по телеконференціях, вставляє до коментарів власних архівів тощо. Якщо хтось інший побажає передати користувачу важливу інформацію, він зашифрує її публічним ключем користувача і відправить. У термінах програмної родини PGP тут описаний так званий *PGP puЬlic кеу.* Розшифрувати таку інформацію можна тільки з допомогою таємного ключа користувача, невідомого іншим.

Так само можна організовувати електронний підпис (певний аналог механізму Authencity verification, який реалізується в більшості програм-архіваторів). У цьому випадку за вмістом інформації певного користувача розраховується спеціальна контрольна сума, яка шифрується таємним особистим ключем. Після цього кожний, у кого є публічний ключ користувача, може розрахувати таку ж суму і порівняти її з результатом розшифрування. Якщо вони не збігаються, хтось мав несанкціонований доступ до цієї інформації і щось у ній змінив. Цей механізм називається *PGP Signature.*

Однак PGP має й недоліки. По-перше, його теж можна зламати шляхом перебирання, оскільки вхідні тексти програми PGP розповсюджуються відкрито. Але алгоритм шифрування достатньо складний і працює довго, тому при нинішньому рівні швидкості комп'ютерів це поки що нереально. По-друге, існує небезпека в можливості підробки публічного ключа. Якщо хтось почне розповсюджувати свій публічний ключ, підписуючись ім'ям іншого користувача, то він зможе одержувати листи, які інші надсилатимуть цьому користувачу, думаючи, *що* ключ передав він. Крім того, зловмисник зможе розсилати будь-яку інформацію, в тому числі й шкідливу, використовуючи ім'я іншого користувача і його публічний ключ.

Щоб запобігти цим зловживанням, передбачені можливість сертифікації публічного ключа і механізм *PGP public key fingerprint,,* за яким можна за контрольними цифрами перевірити справжність ключа, зателефонувавши у сертифікаційну установу. Свій ключ бажано пересилати не відкрито, а

через посередника — людину, якій довіряєш **і** чий публічний ключ відомий споживачам твоєї інформації, щоб цей посередник міг супроводити твій ключ своєю PGP-сігнатурою.

Захист мереж: міжмережеві екрани (брандмаузери, Firewall). Віртуальні приватні мережі. Коли з'єднуються ресурси корпоративної мережі установи, її сегмента чи окремого комп'ютера з відкритою мережею, наприклад, Інтернет, підвищується ризик атакування і пошкоджень як самих даних у мережі, так і комп'ютерної системи загалом.

Корпоративна мережа — тут — TCP/IP-мережа установи з підключенням до Інтернет і з улаштуванням спеціального додаткового захисту.

Міжмережеві екрани (брандмауери, Firewall) слугують для захисту даних і комп'ютерних систем.

Міжмережеві екрани (Firewall) — програмне забезпечення, розташоване на комп'ютері, що містить певні інформаційні ресурси на окремому спеціалізованому комп'ютері чи пристрої" з метою захисту цих ресурсів або ресурсів корпоративної мережі від користувачів із зовнішньої мережі.

Firewall здатні забезпечити захист окремих протоколів і програмних застосувань. Вони здійснюють контроль доступу ззовні до внутрішньої мережі, її окремих сегментів тощо на основі вмісту пакетів даних, що передаються між двома сторонами, або пристроями мережею.

Міжмережеві екрани працюють з програмами маршрутизації та фільтрами всіх мережевих пакетів, щоб визначити, чи можна пропустити інформаційний пакет, а якщо можна, то відправити його до певної комп'ютерної служби за призначенням. Для того щоб міжмережевий екран міг зробити це, необхідно визначити правила фільтрації. Отже, міжмережевий екран є немовби віртуальним кордоном, на якому перевіряється цілісність фрагментованих пакетів даних, що передаються, їх відповідність стандарту тощо.

Налагодивши відповідним чином міжмережевий екран, можна дозволити або заборонити користувачам як доступ із зовнішньої мережі до вузлів сегментів внутрішньої мережі, що захищається, так і доступ користувачів із внутрішньої мережі до відповідних ресурсів зовнішньої мережі.

Методика міжмережевих екранів завжди була привілеєм великих локальних мереж, які передбачали високий ступінь надійності. З розповсюдженням по всій глобальній мережі програм, що атакують, пересічні комп'ютерні користувачі відчули себе в небезпеці. Оскільки не кожен Інтернет - провайдер може підключити через Firewall індивідуального користувача мережі, з'явилася потреба в захисних програмах, які б виконували функції Firewall для окремого комп'ютера.

Декілька фірм розташували в Інтернет свої версії такого програмного забезпечення. Причому в назві кожної версії обов'язково є слово Firewall, що приваблює численну армію користувачів. Серед них одним з найвизначніших є продукт фірми ConSeal.

Часто корпоративні мережі зв'язують офіси, розкидані в місті, регіоні, країні або всьому світі. Ведуться роботи щодо захисту на мережевому рівні *IP-мереж* (саме такі мережі формують Інтернет). Провідні постачальники міжмережевих екранів і *маршрутизаторів* запропонували технологію S/WAN. Вони взяли на себе впровадження і тестування протоколів, що пропонуються Робочою групою інженерів Інтернет (Inernet Engineering Task Force, IETF) для захисту пакетів даних. Ці протоколи забезпечують автентифікацію й шифрування пакетів, а також засоби обміну та управління ключами для шифрування й автентифікації. Протоколи S/WAN допоможуть досягти сумісності між маршрутизаторами і брандмауерами різноманітних виробників, що дасть змогу географічно віддаленим офісам однієї корпорації, а також партнерам, що утворюють віртуальне підприємство, безпечно обмінюватися даними по Інтернет. Іншими словами, компанії зможуть створювати власні *віртуальні* приватні *мережі* (virtual private networks, VPN) і використовувати Інтернет як альтернативу традиційним каналам зв'язку, які орендуються за високу плату.

Віртуальні приватні мережі (virtual private networks, VPN) — територіально розподілені корпоративні мережі, які використовують для зв'язку між окремими сегментами Інтернет.

Однак міжмережеві екрани не є універсальним вирішенням усіх проблем безпеки в Інтернет. Наприклад, вони не здійснюють перевірку на віруси і не здатні забезпечити цілісність даних.

Інтерфейси прикладного програмування. Існує два основних набори інструментів, призначених для спрощення впровадження криптографічних засобів захисту розробникам програмних застосувань для персональних комп'ютерів — CryptoAPI від фірми Microsoft і CDSA (Common Data Security Architecture) від Intel.

CryptoAPI. Є важливим компонентом інтегрованої системи безпеки Інтернет від Microsoft — Internet Security Framework, сумісної з операційними системами Windows. Цей інтерфейс прикладного програмування (API) діє на рівні операційної системи і надає розробникам засоби виклику криптографічних функцій через стандартний інтерфейс у середовищі Windows. Оскільки CryptoAPI має модульну структуру, він дає змогу розробникам залежно від їх потреб замінювати один криптографічний алгоритм іншим. CryptoAPI також містить засоби для оброблення цифрових сертифікатів.

CDSA від Intel. Пропонує практично ті ж самі функціональні можливості, *що* й CryptoAPI, але цей набір інструментів призначений для використання на багатьох інших платформах, а не тільки для Windows. Деякі компанії (в тому числі Netscape, VeriSign) вже включили підтримку CDSA до своїх продуктів.

Система електронної торгівлі являє собою характерний приклад розподіленої обчислювальної системи. У ній кілька клієнтів працюють з одним сервером, рідше з декількома серверами. Таким чином, електронного магазину загрожують всі внутрішні і віддалені атаки, притаманні будь-якій розподіленої комп'ютерної системи, що взаємодіє за допомогою передачі даних по відкритих мереж. Ми бачимо, що обидва учасники цього бізнес-процесу виявляються уразливими перед ними і незахищеними в плані відображення атак і їх відстеження.

Крім інформаційних атак і погроз, в електронній комерції існують ще багато вразливостей іншого аспекту, більше пов'язаних з організаційними, правовими і фінансовими проблемами в економічній діяльності фірми в цілому. Тому, потрібно відзначити, що тільки технічних засобів для вирішення задачі побудови комплексної системи захисту недостатньо. Необхідний цілий комплекс організаційних, законодавчих, фізичних та технічних заходів.

Так в чому ж причина гальмування зростання електронної комерції? На наш погляд, вона криється в недоліках законодавчого регулювання та, як наслідок, в ризиках, обумовлених проблемами забезпечення необхідного рівня безпеки.

Втім, існують і інші - це, може бути, і необхідність ліцензійного оформлення діяльності для кінцевих споживачів технологій, а також необхідність придбання сертифікованих засобів захисту інформації та ряд інших. З іншого боку, потрібно звернути увагу, що комп'ютерні технології дуже молоді, але при цьому розвиваються стрімкими темпами. І дуже складно встигнути продумати всі тонкощі захисту і реалізувати їх належним чином.

Усім спеціалістам, постійно працюють у сфері електронної торгівлі добре відомо поняття ЕЦП. Аутентифікація електронного документа здійснюється за допомогою перевірки електронно-цифрового підпису (ЕЦП). При перевірці ЕЦП файлу перевіряється, застосовувався чи при виробленні даної цифрового підпису конкретний ключ, що належить відправнику документа, і не зазнав чи файл змін у процесі пересилання адресату. Якщо програма перевірки підпису формує запис "ЕЦП вірна", то файл "аутентифікований". При аутентифікації файлу не має значення, яку корисну інформацію він містить і чи містить взагалі. Для подальшої ідентифікації файлу - документа потрібно механізм переведення бінарної інформації, що становить файл, в читану людиною форму і певним чином трактуються вміст даної форми. Очевидно, що тільки при наявності подібного механізму може бути забезпечена доказова сила електронного документа. Закон "Про електронний цифровий підпис" є підставою доказової сили цифрового підпису.

Доказова ж сила електронних документів ґрунтується на фіксації мови їх прочитання або, іншими словами, механізму ідентифікації цифр - нулів та одиниць, що утворюють документ. Найчастіше мова ідентифікації електронних документів в договірних відносинах не регламентований. Тому, за відсутності будь-яких правил, норм і вимог, ситуація необтяжливої хаосу в цьому питанні породжує додаткові ризики, які є принциповим гальмом розвитку технологій електронної комерції. Безперервний розвиток мережевих технологій при відсутності постійного аналізу безпеки призводить до того, що з плином часу захищеність мережі падає. З'являються нові невраховані загрози та вразливості системи. Є поняття - адаптивна безпека мережі. Вона дозволяє забезпечувати захист у реальному режимі часу, адаптуючись до постійних змін в інформаційній інфраструктурі. Складається з трьох основних елементів - технології аналізу захищеності, технології виявлення атак, технології управління ризиками. Технології аналізу захищеності є дієвим методом, який дозволяє проаналізувати і реалізувати політику мережевої безпеки. Системи аналізу захищеності проводять пошук вразливостей, але нарощуючи кількість перевірок і досліджуючи всі її рівні. Виявлення атак - оцінка підозрілих дій, які відбуваються в корпоративній мережі.

Будь-якому програмному забезпеченню властиві певні уразливості, які призводять до реалізації атак. І уразливості проектування системи e-Commerce (наприклад, відсутність засобів захисту), та вразливості реалізації і конфігурації. Останні два типи вразливостей найпоширеніші і зустрічаються в будь-якій організації. Все це може призвести до реалізації різного роду атак, спрямованих на порушення конфіденційності і цілісності даних, що обробляються. Розглянемо, які загрози підстерігають фірму на різних етапах здійснення покупки через Інтернет

Загрози існують на різних етапах здійснення покупки через Інтернет:

1) Замовник вибирає продукт чи послугу через сервер електронного магазину і оформляє замовлення : підміна сторінки Web-сервера електронного магазину. Основний спосіб реалізації - переадресація запитів користувача на інший сервер. Проводиться шляхом заміни записів у таблицях DNS-серверів або в таблицях маршрутизаторів. (Особливо це небезпечно, коли замовник вводить номер своєї кредитної картки).

2) Замовлення заноситься до бази даних замовлень магазину. Проникнення в базу даних і зміна процедур обробки замовлень дозволяє незаконно маніпулювати з базою даних.

Перевіряється доступність продукту або послуги через центральну базу даних. Якщо продукт не доступний, то замовник отримує про це повідомлення. Залежно від типу магазину, запит на продукт може бути перенаправлений на інший склад. Реалізація атак типу "відмова в обслуговуванні" і порушення функціонування або виведення з ладу вузла електронної комерції.

У разі наявності продукту або послуги замовник підтверджує оплату та замовлення поміщається в базу даних .

3) Створення помилкових замовлень з боку співробітників електронного магазину. Електронний магазин посилає замовнику підтвердження замовлення. Перехоплення даних, які передаються в системі електронної комерції.

Клієнт в режимі on-line оплачує замовлення. Особливу небезпеку становить собою перехоплення інформації про кредитну картку замовника.

Товар доставляється замовнику. Шахрайство з боку співробітників електронного магазину.

На всіх етапах роботи системи електронної торгівлі можливе проникнення у внутрішню мережу компанії і компрометація компонентів електронного магазину. За статистикою більше половини всіх комп'ютерних інцидентів пов'язано з власними співробітниками, адже вони, як ніхто інший, знають всю роботу «зсередини».

Які ж наслідки у разі здійснення цих загроз? У результаті всіх цих загроз компанія втрачає:

а) довіру клієнтів; б) гроші від недосконалих угод.

У деяких випадках цієї компанії можна пред'явити позов за розкриття номерів кредитних карт. У разі реалізації атак типу "відмова в обслуговуванні" на відновлення працездатності витрачаються

тимчасові і матеріальні ресурси на заміну обладнання. Перехоплення даних не залежить від використовуваного програмного й апаратного забезпечення. Це пов'язано з незахищеністю версії протоколу IP(v4). Рішення проблеми - використання криптографічних засобів або перехід на шосту версію протоколу IP (v6).

Крім усього сказаного, може відбутися: 1) порушення доступності вузлів електронної комерції; 2) неправильне налаштування програмного і апаратного забезпечення електронного магазину.

Всі перераховані раніше загрози не страшні, якщо проти них існують дієві засоби захисту. Який же арсенал засобів сьогодні існує і чому все ж і його не завжди достатньо? Для відповіді на це питання потрібно розглянути всі чотири рівні, що є у будь-який інформаційної системи.

1 і 2-й рівні (нижні) - рівень операційної системи й рівень мережі. Рівень операційної системи (ОС), що відповідає за обслуговування СУБД і прикладного програмного забезпечення. Приклади - ОС MS Windows NT, Sun Solaris, Novell Netware.

Рівень мережі, що відповідає за взаємодію вузлів інформаційної системи. Приклади - протоколи TCP / IP, IPS / SPX і SMB / NetBIOS.

Ці рівні важливі особливо. Уявімо, що зловмисник отримав ідентифікатор та пароль користувача бази даних магазину або перехопив їх у процесі передачі по мережі, або підібрав за допомогою спеціальних програм. Це дуже небезпечно, потрібні такі засоби і механізми захисту, які швидко і точно виявляють і блокують мережеві атаки типу "відмова в обслуговуванні", а також атаки на операційну систему.

В даний час на рівні мережі застосовуються маршрутизатори і міжмережеві екрани, на рівні ж ОС - вбудовані засоби розмежування доступу. Одним із прикладів засобів виявлення атак є система RealSecure, розроблена компанією Internet Security Systems, Inc.

Наступний рівень - третій рівень прикладного програмного забезпечення (ПО), що відповідає за взаємодію з користувачем. Прикладом елементів цього рівня - текстовий редактор WinWord, редактор електронних таблиць Excel, поштова програма Outlook, броузер Internet Explorer.

Четвертий рівень системи управління базами даних (СКБД) відповідає за зберігання і обробку даних інформаційної системи. Прикладом елементів цього рівня - СУБД Oracle, MS SQL Server, Sybase і MS Access.

Система захисту повинна ефективно працювати на всіх рівнях. Інакше зловмисник зможе знайти уразливості системи і реалізувати атаку на ресурси електронного магазину. Тут допоможуть засоби аналізу захищеності та сканери безпеки.

Ці кошти можуть виявити і усунути багато вразливостей на сотнях вузлів, в т.ч. і віддалених на значні відстані. У цій області також лідирує компанія Internet Security Systems зі своїм сімейством SAFEsuite. Система включає функції пошуку вразливостей, що працюють на всіх чотирьох рівнях - Internet Scanner, System Scanner і Database Scanner. Спільне застосування різних засобів захисту на всіх рівнях дозволить побудувати надійну систему забезпечення інформаційної безпеки eCommerce. Така система корисна й користувачам, і співробітникам компанії-провайдера послуг. Вона дозволить знизити можливі збитки від атак на компоненти і ресурси електронного магазину.

З історії створення SAFEsuite

Розроблений одним з експертів з комп'ютерних систем захисту Крістофером Клаусом, цей пакет повинен виявляти "дірки" в системах безпеки Web-серверів, брандмауерів, серверів і робочих станцій на базі ОС Unix, Windows 95 і NT і повідомляти про них користувачеві. Ці "дірки" SAFEsuite виявляє шляхом імітації всіх відомих способів, що використовуються "зломщикам" для проникнення в мережу. Відмінною особливістю пакету SAFEsuite, що складається з програм Intranet Scanner, Firewall Scanner, Web Security Scanner і System Security Scanner, є його орієнтація виключно на оцінку стану комп'ютерних систем захисту. На відміну від відомих програм, наприклад SATAN, яка тестує мережу тільки "зовні", або COBS, що перевіряє мережу тільки "всередині", пакет SAFEsuite покликаний об'єднати всі функції цих програм в єдине ціле.

З комерційних російських засобів, що реалізують велику кількість захисних функцій можна назвати системи сімейства SecretNet, розроблені підприємством "Інформзахист". Не можна забувати також і про шифрування і ЕЦП (електронного цифрового підпису). Ступінь захищеності безпосередньо залежить від алгоритму шифрування і від довжини ключа, яка вимірюється у бітах. Чим довший ключ, тим краще захист, але тим більше обчислень треба провести для шифрування і дешифрування даних.

Основні види алгоритмів шифрування - симетричні й асиметричні. Симетричні методи шифрування зручні тим, що для забезпечення високого рівня безпеки передачі даних не потрібно створення ключів великої довжини. Це дозволяє швидко шифрувати і дешифрувати великі обсяги інформації. Разом з тим, і відправник, і одержувач інформації володіють одним і тим же ключем, що робить неможливим аутентифікацію відправника. Крім того, для початку роботи із застосуванням симетричного алгоритму сторонам необхідно безпечно обмінятися секретним ключем, що легко зробити при особистій зустрічі, але дуже важко при необхідності передати ключ через будь-які засоби зв'язку.

Прикладом деяких алгоритмів симетричного шифрування є:

1) DES (Data Encryption Standard).

Розроблений фірмою IBM і широко використовується з 1977 року. В даний час трохи застарів, оскільки вживана в ньому довжина ключа недостатня для забезпечення стійкості до розтину методом повного перебору всіх можливих значень ключа.

2) Triple DES.

Це удосконалений варіант DES, що застосовує для шифрування алгоритм DES три рази з різними ключами. Він значно стійкішими до злому, ніж DES. Rijndael. Алгоритм розроблений в Бельгії. Працює з ключами довжиною 128, 192 і 256 біт. На даний момент до нього немає претензій у фахівців з криптографії. Skipjack.

Алгоритм створений і використовується Агентством національної безпеки США. Довжина ключа 1980 біт. Шифрування і дешифрування інформації проводиться циклічно (32 циклу).

IDEA. Алгоритм запатентований в США та низці європейських країн. Держатель патенту компанія Ascom-Tech. Алгоритм використовує циклічну обробку інформації (8 циклів) шляхом застосування до неї ряду математичних операцій. RC4. Алгоритм спеціально розроблений для швидкого шифрування великих обсягів інформації. Він використовує ключ змінної довжини (у залежності від необхідного ступеня захисту інформації) і працює значно швидше інших алгоритмів. RC4 відноситься до так званих потоковим шифру.

Електронний цифровий підпис (ЕЦП) є електронним еквівалентом власноручного підпису. ЕЦП служить не тільки для аутентифікації відправника повідомлення, а й для перевірки його цілісності. При використанні ЕЦП для аутентифікації відправника повідомлення застосовуються відкритий і закритий ключі. Процедура схожа на здійснювану в асиметричному шифруванні, але в даному випадку закритий ключ служить для шифрування, а відкритий - для дешифрування.

Алгоритм застосування ЕЦП складається з ряду операцій:

1) Генерується пара ключів - відкритий і закритий.

2) Відкритий ключ передається зацікавленій стороні (одержувачу документів, підписаних стороною, згенерованої ключі).

3) Відправник повідомлення шифрує його своїм закритим ключем і передає одержувачу по каналах зв'язку.

4) Одержувач дешифрує повідомлення відкритим ключем відправника.

Принципово новий підхід до здійснення електронних платежів сьогодні полягає в негайній авторизації і шифруванні фінансової інформації в мережі Інтернет з використанням протоколів SSL (Secure Sockets Layer) та SET (Secure Electronic Transaction). Протокол SSL припускає шифрування інформації на канальному рівні, а протокол SET, розроблений компаніями VISA, MasterCard та інші, - шифрування виключно фінансової інформації. Оскільки мережа Інтернет розрахована на одночасну

роботу мільйонів користувачів, то в комерційних додатках "у чистому вигляді" неможливо використовувати ні традиційні системи, засновані виключно на "закритих ключах" (DES, ГОСТ 28147-89 та ін), ні методи шифрування тільки на " відкритих ключах ", в тому числі і російський стандарт електронного підпису.

Застосування одних закритих ключів неможливо у зв'язку з тим, що розкриття (перехоплення) навіть одного ключа відразу ж приведе до "злому" усієї системи захисту. Тому при реалізації електронної комерції в Інтернет разом з системами шифрування за допомогою закритих ключів використовуються системи шифрування за допомогою відкритих ключів. Це пов'язано з тим, що шифрування лише відкритими ключами вимагає великих витрат обчислювальних ресурсів. Тому краще всього шифрувати інформацію, передану по мережах, за допомогою закритого ключа, який генерується динамічно та передається іншому користувачу зашифрованим з допомогою відкритого ключа.

Така система шифрування буде працювати і швидше, і надійніше.

У додатках, заснованих на використанні алгоритму SET, покупець, не розшифровуючи платіжних реквізитів продавця, розшифровує всі дані замовлення, а банк, не маючи даних про структуру замовлення, має доступ до платіжних реквізитами і продавця і покупця. Це досягається завдяки використанню подвійний (сліпий) електронного підпису, і в даній ситуації банку надсилається одна частина повідомлення, а покупцеві - інша. Крім того, протокол SET описує стандартні види фінансових транзакцій між банками, центрами авторизації і торговими точками. При шифруванні з використанням закритих ключів передбачається, що і продавець і покупець мають загальний ключем, який вони використовують для шифрування / дешифрування інформації. У шифруванні ж з використанням відкритих ключів передбачено, що і продавець і покупець мають по два ключі: один - "відкритий", який може бути відомий будь-якої третьої стороні, а інший - "приватний", завжди відомий лише одній стороні - його власнику. При цьому по одному ключу неможливо відновити інший.

Який є висновок на сьогодні? Як захистити угоду від несанкціонованого доступу?

Для захисту угод в Інтернет в даний час організовані спеціальні центри сертифікації. Вони стежать за тим, щоб кожен учасник електронної комерції отримував унікальний електронний "сертифікат", в якому за допомогою ключа центру сертифікації підписаний відкритий ключ даного учасника комерційних угод. Сертифікат генерується на певний час. Щоб його отримати, в центр сертифікації необхідно надати документ, що засвідчує особу учасників угоди (для юридичних осіб таким документом є свідоцтво про реєстрацію). Кожен учасник, маючи "на руках" відкритий ключ центру сертифікації, може за допомогою сертифікатів перевірити справжність відкритих ключів інших учасників і здійснювати операції.

З самого початку впровадження електронної комерції було очевидно, що методи ідентифікації власника картки, що застосовуються у звичайних транзакціях, є незадовільними для транзакцій електронної комерції. Дійсно, при здійсненні операції купівлі у фізичному магазині продавець має право розглянути пред'являється для розрахунку пластикову картку на предмет її відповідності вимогам платіжним системам (зокрема перевірити наявність голограми, спеціальних секретних символів, звірити підписи на панелі і торговому чеку і т. п.). Крім того, продавець може вимагати від покупця документ, що засвідчує його особу. Все це робить шахрайство по підробленій карті досить дорогим підприємством.

У разі транзакції в електронній комерції все, що потрібно від шахрая - знання реквізитів картки. Витрати, пов'язані з виготовленням підробленої фізичної карти, в цьому випадку не потрібно. У світі пластикових карт із магнітною смугою самим надійним способом захисту транзакції від шахрайства є використання PIN-коду для ідентифікації власника картки його банком-емітентом. Секретною інформацією, якою володіє власник карти, є PIN-код. Він являє собою послідовність, що складається з 4-12 цифр, відому тільки власнику картки і його банку-емітенту. PIN-код застосовується завжди при проведенні транзакції підвищеного ризику, наприклад при видачі власнику картки готівки в банкоматах.

Видача готівки в банкоматах відбувається без присутності представника обслуговуючого банку (ситуація схожа на транзакцію електронної комерції). Тому звичайних реквізитів картки для захисту операції "зняття готівки в банкоматі" недостатньо і використовується секретна додаткова інформація - PIN-код. Власники карток, емітенти яких тримають свою базу даних карток на хост STB CARD, можуть отримати додатковий PIN-код, званий PIN2. Цей код являє собою послідовність з 16 цифр, яка роздруковується у PIN-конверті, передаваному власникові картки, та обчислюється емітентом за допомогою симетричного алгоритму шифрування, застосованого до номера картки та використовує секретний ключ, відомий тільки емітенту карти.

Повертаючись до схеми STB CARD, відзначимо, що, звичайно ж, у заповненій клієнтом формі PIN2 не міститься, а в дійсності все виглядає наступним чином: торгова точка (точніше, сервер Assist), визначивши, що має справу з картою банку STB CARD, передає власникові картки форму, що містить підписаний java-аплет, який реалізує деякий симетричний алгоритм шифрування. При цьому PIN2 грає роль секретного ключа цього алгоритму шифрування, а шифровані дані виходять в результаті застосування хеш-функції до номера картки, сумі і дату транзакції, а також випадкове число Nn генерується торговою точкою. Таким чином, у заповненій власником картки формі присутня тільки результат шифрування перерахованих вище даних про транзакції на ключі PIN2.

Таким чином, технологія перевірки PIN-коду, прийнята в системі STB CARD, насправді забезпечує не тільки спільну аутентифікацію клієнта, а ще й гарантує "наскрізну" цілісність деяких даних про транзакції (сума транзакції, номер картки). Під "наскрізної" цілісністю тут розуміється захист від модифікації даних на всьому протязі від їх передачі від клієнта до банку-емітента. А як же інші карти? В інших системах немає поки такого високого ступеня захисту. Доведеться власникам інших карт тримати в суворій таємниці свій PIN-код і намагатися не втрачати карту. До тих пір, поки їхня система не буде належним способом захищена від шахрайства.

З усього вищесказаного видно, що робота з проведення захисних заходів ведеться, але складнощі ще залишаються. Ця діяльність передбачає створення великого числа все більш складних алгоритмів шифрування, спеціальних програм для перехоплення і нейтралізації атак. Фахівці в цій галузі, як у нашій країні, так і за кордоном багато корисного вже здійснили у сфері розробок нових програмних засобів для «відстеження» і «уловлювання» атак, чого не можна не помітити. Однак у систем електронної комерції все ще залишаються багато неусуненених небезпек. Тому їх необхідно ретельно вивчати і намагатися швидше усувати. Від цього залежить як-не-як обсяг продажів, а значить, і прибутковість даного сектора комерції.

Тема 6. Міжнародна діяльність з просування електронної торгівлі і надання послуг через електронні засоби

Як вже зазначалося вище, в світі вже почалася активна робота по створенню належного правового забезпечення електронної комерції і вже є певні результати. Почати треба з Типового закону Юнсітрал «Про електронну торгівлю», прийнятого Комісією ООН по праву міжнародної торгівлі в 1996 р. В рамках Європейського Союзу прийнято ряд актів, спрямованих на регулювання електронної комерції. Серед них: Директива ЄС «Про електронну торгівлю», «Про електронний підпис», «Про деякі аспекти електронної торгівлі на внутрішньому ринку», «Про захист споживачів у випадку укладення контрактів на відстані» тощо.

Ряд країн вже прийняли закони, які встановлюють правові підстави використання електронних документів. Одним з найскладніших питань електронної комерції є використання електронного цифрового підпису, тому корисним є досвід деяких країн, в яких це питання врегульоване окремим законом:

— так, Європейський парламент та Рада Європейського Союзу розробили Директиву від 13 грудня 1999 р. «Про правові підстави для використання електронних підписів»;

— комісією ООН з права міжнародної торгівлі (ЮНСІТРАЛ) 5 червня 2001 р. було прийнято Типовий закон «Про електронний підпис»;

— Міжпарламентська асамблея країн-учасниць СНД розробила Модельний закон від 9 грудня 2000 р. «Про електронний цифровий підпис»;

— у США прийнято Федеральний Закон від 1 жовтня 2000 р. «Про електронні підписи у міжнародних та внутрішньодержавних торгових відносинах»;

— штат Юта США ще 1 травня 1995 р. прийняв Закон «Про електронний підпис»;

— Німеччина у 1997 р. прийняла Закон «Про регулювання основних умов надання інформаційних та комунікаційних послуг». Стаття 7 цього Закону присвячена електронним підписам. Саме тому 8 жовтня 1997 р. Федеральний уряд видав окрему постанову «Про електронний підпис»;

— Італійська Республіка 1 березня 1997 р. прийняла «Закон Басаніні»;

— у Російській Федерації у січні 2002 р. прийнято Закон «Про електронний підпис» тощо.

Питання правової регламентації електронного цифрового підпису потребують окремого ретельного дослідження. Але вже зараз можна виділити найцікавіші визначення електронного цифрового підпису, які, на мій погляд, заслуговують на увагу. Так, в Директиві Європейського парламенту та Ради 1999/93-/ЄС від 13 грудня 1999 р. «Про правові підстави Співдружності для використання електронних підписів» в ст. 2 дається визначення «електронного підпису» як даних в електронній формі, що приєднані або логічно пов'язані з іншими електронними даними, та які виступають як метод аутентифікації. Разом з тим Директива містить також поняття «вдосконаленого електронного підпису», під яким розуміється електронний підпис, котрий відповідає наступним вимогам: а) унікальне пов'язаний з особою, яка підписує; б) достатній для її ідентифікації; в) створюється з використанням засобів, які перебувають під виключним контролем особи, яка підписала; г) пов'язаний з даними, до яких він відноситься, таким чином, що наступні зміни даних стають наочними.

В Законі Німеччини від 22 липня 1997 р. «Про цифровий підпис» та в аналогічній постанові Федерального уряду від 8 жовтня 1997 р. застосовується поняття «цифрового підпису», яке визначається як створена за допомогою приватного ключа печатка до цифрових даних, яка, за допомогою відповідного відкритого ключа, що має сертифікат ключа підпису, виданого сертифікуючим центром або державною установою, дозволяє визначити володільця ключа підпису та істинність даних.

Прийнятий Міжпарламентською асамблеєю країн-учасниць СНД Модельний закон «Про електронний цифровий підпис» визначає останній як електронні дані, одержані в результаті перетворення вихідних електронних даних з використанням закритого ключа підпису, які за допомогою відповідної процедури з використанням відкритого ключа підпису дозволяють: підтвердити незмінність вихідних даних після підписання їх електронним цифровим підписом; встановити, що електронний цифровий підпис, створений з використанням закритого ключа, відповідає відкритому; встановити володільця реєстраційного свідоцтва на відкритий ключ електронного цифрового підпису, за наявності такого свідоцтва.

Кожне з визначень, розкриваючи поняття електронного підпису, виділяє його різні риси. На мій погляд, у визначенні електронного цифрового підпису мають знайти відображення такі його основні риси: 1) він є невід'ємною частиною електронного документа; 2) унікальне пов'язаний з особою, яка підписує; 3) надає можливість ідентифікувати особу, яка підписала електронний документ; 4) створюється з використанням засобів, які перебувають під виключним контролем особи, яка підписала; 5) дозволяє встановити, що створений з використанням закритого ключа, він відповідає відкритому ключу; 6) містить положення про сертифікацію ключа підпису та посилання на установи, які вправі його видавати.

Одразу треба вказати, що серед фахівців (насамперед в технічній сфері) існує вкрай негативне ставлення до самої ідеї правового регулювання відносин, які виникають в Інтернет-

середовищі. В Мережі навіть була розповсюджена «Декларація незалежності кіберпростору» (автор - Джон Барлоу), в якій проголошувалося право на свободу Інтернет-простору та принцип невтручання жодної з країн у регулювання Інтернет-відносин. Прихильники такої позиції вважають, що Мережа повинна залишитися «чистою» від законодавчого нормування і складати зону вільного пересування інформації, ідей, думок, висловлювань тощо. Утім, такий дещо «ідеалізований» погляд на справу останнім часом зазнав значного тиску. Порушення особистих та майнових прав, навіть злочинні дії, що виникли за допомогою Інтернет-технологій, наочно показали, що Інтернет не може бути тільки зоною свободи людини і з необхідністю стає об'єктом правового втручання. Крім того, свобода ніколи не означала хаосу, а правове регулювання не обов'язково пов'язане з установленням заборон та обмежень. Тому думка щодо виведення Інтернет-відносин за межі правового регулювання є просто безпідставною.

Інша справа — якою буде концепція регулювання Інтернет-відносин в тій чи іншій країні, якою мірою і за допомогою яких саме засобів держава буде впливати на їх формування. Діапазон вирішення цього питання є значним. З одного боку, — практично повна заборона доступу громадян до Інтернету (досвід Китаю), з іншого — практично повна комп'ютеризація та дозвіл на розміщення в Інтернеті будь-якої інформації, навіть пов'язаної з пропагандою нацизму (США).

Сьогодні вже визначилися певні різновиди Інтернет-відносин, які в першу чергу потребують правового опосередкування та визначення. До них, зокрема, належать такі.

По-перше, це відносини, які пов'язані з функціонуванням самої Мережі й доступом до Інтернету. У зв'язку з тим, що Інтернет є складним та багатофункціональним технічним засобом, виникають специфічні відносини між виробниками, споживачами та володільцями різноманітних ресурсів серверів, сайтів, адрес електронної пошти, доменних імен тощо. Особливо гостро останнім часом постає питання щодо використання доменних імен, зокрема доменних імен другого рівня, які збігаються із зареєстрованими товарними знаками юридичних осіб. В Україні були прийняті і діють «Правила домену.ua», які вже регулюють відповідні відносини в Українському сегменті Мережі, що свідчить про необхідність і можливість їх нормування.

По-друге, відносини, що виникають у сфері електронної комерції (електронного бізнесу). Цей термін уже отримав досить широке розповсюдження. З правової точки зору він означає сукупність правочинів, які укладаються за допомогою Інтернет-технологій — договорів купівлі-продажу, перевезення, страхування, надання послуг, банківських розрахунків тощо. На 29 сесії Комісії ООН по праву міжнародної торгівлі прийнято Типовий закон про електронну торгівлю, який рекомендовано резолюцією 51/162 Генеральної Асамблеї від 16 грудня 1996 р. У сфері електронної торгівлі найбільшу проблему складає сьогодні питання електронного цифрового підпису, який буде застосовуватися при укладенні електронних угод. В деяких країнах питання електронного цифрового підпису знайшло своє законодавче вирішення. В Україні правовий статус електронного документа та електронного цифрового підпису, який його засвідчує, вже визначені Законом «Про платіжні системи та переказ грошей в Україні» від 5 квітня 2001 р.

По-третє, відносини щодо захисту авторських та інших виключних прав на об'єкти інтелектуальної власності, які розміщені в Інтернеті, а також ті, що пов'язані з функціонуванням у Мережі засобів масової інформації. Тут постає багато питань, які мають бути вирішені в тому числі за допомогою правових засобів. Насамперед це пов'язано з тим, що розміщення об'єктів виключних прав в Інтернеті дає широкі можливості для їх неправомірного використання (несанкціонованого розповсюджування, тиражування тощо). Тому традиційні механізми захисту авторських та інших прав в Інтернеті в багатьох випадках виявилися не ефективними. Фахівці вважають, що поява Інтернету взагалі поставила під сумнів саму концепцію копірайта. Справа в тому, що традиційна офф-лайнівська концепція щодо всебічного захисту володільців виключних прав зіткнулася з концепцією свободи інформаційного Інтернет-простору. Прибічники останньої концепції вважають, що «Інтернет із самого початку був задуманий і реалізований як засіб вільного розповсюдження інформації». Таким чином

особа, яка свідомо розмістила в Інтернеті будь-які результати своєї творчої діяльності, тим самим уже погодилася з їх використанням широким загалом споживачів. Утім, такий однобічний підхід навряд чи може бути визнаний правильним. Тому визначення певного балансу інтересів користувачів Інтернету та володільців авторських та інших виключних прав має бути знайдено.

По-четверте, відносини, що виникають стосовно захисту конфідиційної інформації в Інтернеті, забезпечення цілісності систем, інформаційної безпеки, запобігання розповсюдженню інформації, що має кримінальний зміст (порносайти, ведення промислового шпіонажу тощо). Регулювання Інтернет-відносин такого роду певною мірою вже здійснюється як на міжнародному, так і на державному рівнях. Насамперед це стосується найбільш небезпечних різновидів дій, пов'язаних із використанням Інтернет-технологій. Так, на 109 сесії Комітету Міністрів Ради Європи (8 листопада 2001 р.) була прийнята «Конвенція про кіберзлочинність» («Convention on Cybercrime»). Боротьба з кримінальними зловживаннями зводиться до чотирьох головних напрямів: запобігання несанкціонованому доступу до інформації; пошкодження систем; маніпуляції даними; розповсюдження інформації злочинного змісту. Кримінальне законодавство різних країн останнім часом також доповнилося нормами щодо злочинів у сфері застосування комп'ютерів та комп'ютерних мереж. Відповідний розділ включено і до Кримінального кодексу України (Розділ XVI. «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж»). Хоча цього недостатньо. Верховною Радою України 26 грудня 2002 р. прийнято за основу Закон про внесення змін до КК України, відповідно до якого Кодекс буде доповнено ст. 363 «Незаконне втручання у роботу мереж електрозв'язку». В спеціальній літературі також відзначалося, що «КК України не встановлено чіткого визначення злочинів про сексуальну експлуатацію дітей через Інтернет, хоча окремі його статті передбачають покарання за подібні злочинні діяння» тощо.

Недостатньо відпрацьованими є правові методи боротьби з такими специфічними для Інтернету явищами, як спам та злісне сквотерство, хоча останнім часом ситуація починає змінюватися на краще, і такі закони приймаються. В ряді країн спам розглядається як серйозне правопорушення, за яке винуватець має принаймні сплатити штраф і може бути притягнений до кримінальної відповідальності.

Інтернаціональний характер Інтернет викликає ряд проблем, пов'язаних з застосуванням національних законодавств. Наприклад, якщо ділові партнери живуть в різних країнах і ведуть бізнес через Інтернет, законодавством якої саме країни повинні регулюватися пов'язані з цим аспекти? Якщо громадянин України живе в Німеччині, зареєстрував підприємство в США, а веб-сайт - у колумбійській зоні, його партнери знаходяться в Таїланді, а сайт використовується для торгівлі наркотиками - за законодавством якої країни він повинен відповідати за скоєне?

Лише один приклад: у 1999 році проти Amazon.com був поданий судовий позов, який звинувачував компанію в продажі забороненої літератури на території Німеччини (в цій країні заборонена книга Гітлера "Майн Кампф" та інші нацистські твори). Компанія відповідала на позов тим, що клієнти з інших країн, які замовляють книги на її сайті, повинні розглядатися як туристи, які самі відповідають за ввезення книжок до своєї країни.

Модуль 3 Контракти в Інтернеті

Тема 7. Контракти в Інтернеті

Коли споживач і професійний торговець не зустрічаються, контракт укладається на відстані, тим самим збільшуючи ризики для споживача. Він не може в дійсності перевірити товари, які він збирається купувати, на відповідність своїм очікуванням або задати питання продавцеві. Регулювання таких контрактів на відстані не є новим, наприклад, для Великобританії. Положення загального права, Закону про продаж товарів від1979 року, Регламенту про Захист Споживачів (скасування контракту, укладеного далеко від приміщення підприємства) від 1987 року й таке інше забезпечувало в минулому деякий захист.

Директива ЄС по захисту споживачів щодо контрактів, укладених на відстані, висуває вимоги до контракту на споживання, укладеному без зустрічі сторін. Це зміцнює захист споживача. Наприклад, Директива була імплементована у Великобританії Регламентом про Захист Споживачів (при продажі на відстані) від 2000 року, що набув чинності 31 жовтня 2001 року. Деякі з вимог, встановлених Регламентом про продаж на відстані, повинні дотримуватися відповідно до вимог Директиви про Електронну комерцію (якщо діяльність підпадає під дію обох нормативно-правових актів).

Сфера дії Регламенту про продаж на відстані. Контракти на відстані визначаються як «будь-який контракт, що стосується товарів або послуг, і укладений між постачальником і споживачем при організованому продажі на відстані або організованій схемі надання послуг, якою управляє постачальник. Останній здійснює виняткове використання одного або більше коштів комунікації на відстані аж до моменту виконання контракту й у момент його укладення».

Регламент не застосовується до всіх контрактів. Зі сфери його застосування виключаються контракти:

- на продаж або інше розпорядження землею;
- на будівництво будинку;
- щодо надання фінансових послуг;
- ті, що укладаються за допомогою автоматизованого торговельного автомата;
- з телекомунікаційним оператором за допомогою суспільного телефону - автомату
- що укладаються на аукціоні.

Деякі положення застосовуються тільки частково:

- Положення 7 - 20 не застосовуються до контракту, що є "угодою тайм-шера»;
- Положення 7 - 19 (1) не застосовуються до контрактів на поставку їжі, напоїв або інших товарів, призначених для щоденного споживання;. контракти на надання послуг з розміщення, транспортування, громадського харчування або послуг дозвілля;
- Положення 19 (2) до (8) і 20 не застосовуються до контракту про " відпочинок по путівці)".

Обговорення запропонованих змін Регламенту про захист споживача при продажі на відстані 2000 р. Слід відмітити, що у січні 2004 року, DTI видав документ по обговоренню запропонованих змін у Регламент по Захисту Споживачів (при продажі на відстані) від 2000 року. Метою обговорення є рішення по складанню більш ясних інструкцій (регламенту), більш здійсненних і менш дорогих для постачальників і споживачів. Обговорення припинилося 23 квітня 2004 року.

Ключові пропозиції:

1. Переддоговірна інформація надається споживачеві щоб охопити існування або відсутність права на розірвання договору. Для послуг, надання яких повинно початися протягом 7 днів, обов'язкова інформація про те, що право розірвати договір минає з моменту початку надання послуг.

2. Споживачі повинні протягом надання послуг одержувати інформацію про втрату права на розірвання договору в письмовій або іншій надійній формі.

3. Дозвіл споживачам розірвати контракти по телефону.

Визначення електронного контракту. Електронний контракт – це домовленість двох сторін, що спрямована на досягнення певного результату.

Пропозиція (оферта) - це чітка вказівка сторони про бажання бути зв'язаною умовами пропозиції. Про це може бути повідомлено декількома способами, включаючи електронні комунікації. Запрошення розглянути пропозиції не є юридично обов'язковим, але, на жаль, може тлумачитися споживачем таким чином. Отже, кібертрейдеру необхідно забезпечити, щоб його комунікації онлайн були викладені й складені таким чином, щоб не викликати невизначеності. Він або вона повинні також гарантувати, щоб комунікації не тлумачилися як однобічні пропозиції (Carlill v Carbolic Smoke Ball Co [1893] 1 QB 256).

Варто розрізняти пропозицію й запрошення (до розгляду, веденню переговорів). При цьому важливий намір сторін, тому що пропозиція являє собою перший щабель взаємин і у зв'язку із цим характеризується зв'язаністю умов сторони, що висунула. Запрошення розглянути пропозицію такої зв'язаності не містить, однак, на жаль, може тлумачитися споживачем таким чином. Закон закріпив різні загальні норми, що охоплюють стандартні комерційні ситуації, такі як демонстрація товарів у магазині – Fisher v Bell [1961] 1 QB 394, Pharmaceutical Society of G.B. v Boots [1953] 1 QB 401 і реклама товарів і послуг на продаж - Partridge v Crittenden [1968] 2 All ER 421. Між тим усе ще не вирішено, як ці загальні норми, які можуть бути виключені протилежним наміром сторін, будуть застосовуватися у звичайних ситуаціях з електронним контрактом.

Тому кібертрейдеру необхідно забезпечити, щоб його комунікації онлайн були викладені й складені таким чином, щоб не викликати невизначеності й не тлумачити як сполучні пропозиції (Carlill v Carbolic Smoke Ball Co [1893] 1 QB 256).

У процесі укладення електронних контрактів виникає безліч проблем. Доконтрактні проблеми – це юридичні проблеми, що виникають у процесі формування контракту до його підписання. Щоб захистити споживачів, відповідно до існуючих правил, на професіоналів покладаються певні зобов'язання навіть до укладання контракту і, таким чином, сторони юридично зв'язані. Наприклад, важливий набір правил стосується реклами товарів і послуг. Також у процесі підготовки контракту законодавство гарантує, що споживачам дають усю необхідну інформацію для схвалення контракту.

Є дві головних причини контролю реклами, використовується реклама в Інтернеті чи ні:

- захист споживачів від введення в оману рекламою, що дає помилкове зображення виробу або забезпечення обслуговування;

- захист торговців від рекламних заяв, що ґрунтуються на нечесній конкуренції.

У Великобританії, зміст і методи реклами регулюються за допомогою законодавства ЄС – стосовне до загального середовища електронної комерції, особливо угод або особливих видів реклами, і законодавства Великобританії.

Зняття пропозиції. Взагалі, пропозиція може бути знята до її прийняття. Однак відмова від пропозиції повинна бути отримана до того, як контракт вважається укладеним. Пропозиція може блокуватися контрпропозицією. У випадку вільного текстового вікна здається, що будь-яка зміна умов пропозиції могла би розглядатися контрпропозицією, між тим навмисне використання вільного текстового вікна повинно вказувати користувачеві на передбачувану згоду зміни деяких умов пропозиції.

Прийняття (акцепт). Акцепт відрізняється від контрпропозиції тим, що є закінченням процесу досягнення домовленості. Сторони, що є підприємницькими структурами, звичайно перевагу надають своїм власним стандартним умовам. При веденні ними переговорів по укладання договору, кожна буде наполягати на тому, щоб він містив саме її умови. Це може закінчитися так званою „боротьбою форм». Кожна сторона, що відповідає інший пред'явленням своїх власних стандартних умов, тим самим робить контрпропозицію.

Обговорення акцепту. За загальним правилом акцепт повинен обговорюватися, бо в правочинах онлайн він буває надзвичайно суперечливим. Складність у тім, що процес обговорення

акцепту відбувається з машиною (комп'ютером), або він пропонується машиною. Це викликає питання, чи визнає англійське або українське право комп'ютер у якості належної договірної сторони? Так, коли, наприклад, споживач шляхом здійснення конклюдентних дій укладає той чи інший договір закон відносить дії й бездіяльність машини до особи, що на ній працює. Проведення аналогії між цими випадками дає підставу прийти до висновку, що власник або особа, що контролює комп'ютер, зв'язані правовими повідомленнями, зробленими комп'ютером, якщо такі повідомлення були запрограмовані в комп'ютер саме вказаними особами. А звідси, англійське право повинно розглядати веб-сервер як простого агента кібертрейдера або кіберспроживача, що може укладати контракти від їхнього імені за умови, що ці повідомлення були заздалегідь запрограмовані фізичними або юридичними особами, що мають до цього відношення.

Власник або особа, що контролює комп'ютер, зв'язані правовими повідомленнями, зробленими комп'ютером, якщо такі повідомлення були запрограмовані в комп'ютер саме вказаними особами. Таким чином, виявляється, що англійське право повинно розглядати веб-сервер як простого агента кібертрейдера або кіберспроживача, що може укладати контракти від їхнього імені за умови, що ці повідомлення були заздалегідь запрограмовані фізичними або юридичними особами, що мають до цього відношення.

Держави-учасники також повинні гарантувати, що постачальник послуг укаже будь-які значимі кодекси поводження, які він розділяє, і інформацію про те, яким чином ці кодекси можна прочитати в електронному виді.

На торговці також лежить обов'язок гарантувати, щоб умови, показані в онлайн, могли бути завантажені й збережені для відтворення споживачем.

Слід зазначити, що такі положення не застосовуються там, де контракт укладений винятково обміном електронної пошти або подібних індивідуальних повідомлень. Вони застосовуються тільки до контрактів, укладеним через Інтернет (звичайно інтерактивним способом).

Електронні послання повинні розглядатися по-іншому, тому що вони не є повідомленнями «реального часу», оскільки вони не миттєві. Одержувач повинен дістати їх з „поштової скриньки». Тим часом інтерактивний веб-контракт Інтернету одержує й обробляє комп'ютер одержувача майже миттєво.

В праві Англії це приводить до таких наслідків. По-перше, поштова норма буде застосовуватися до акцептів електронної пошти, але не до інтерактивних акцептів. По-друге, останні, будучи миттєвими повідомленнями, вважаються дійсними тільки після їхнього одержання (Brinkibon v Stahag Stahl [1983] 2AC 34). Акцепт же електронної пошти, імовірно, буде вважатися дійсним, як тільки вона відправлена, у незалежності від того чи була вона отримана або прочитана.

Застосування електронного підпису. Ризик відмови – беручи контракт в Інтернеті, сторони не зустрічаються. Це означає ризик, що збільшується, у контрактному процесі. З погляду споживача може трапитися так, що продавець зникне з оплатою до одержання замовленого. З погляду професіонала може бути ризик відмови оплати, коли товар уже відправлений. Відмова може відбутися, тому що картка була украдена або використалася по-шахрайському. Більшість контрактів між банками й торговцями припускають, що у випадку відмови торговець несе тягар ризику.

Вимога «письмового документа» – не всі контракти, укладені між професіоналом і споживачем вимагають письмового й підписаного документа. Характеристики дистанції й дематеріалізації Інтернету означають, що у випадках, де письмовий документ не є вимогою для законності контракту, сторони можуть бути в невизначеній ситуації відносно особистості іншої сторони, бажання іншої сторони бути юридично зобов'язаної контрактом тощо.

Електронний підпис – це засіб засвідчення особою комп'ютерним кодом, а не рукописним підписом. Цей код звичайно створюваний з використанням кнопок, що кодують, додається до електронного документа як кошти підписання документа.

Використання цифрових підписів і кодування може зменшити заклопотаність щодо ризику відмови й вимоги письмового документа. Цифровий підпис виконує декілька функцій. Встановлює особистість договірних сторін, окрім сумнівів щодо повноважень кожної сторони в контракті. Підтверджує, що встановлена особа прийняла запропоновані умови. Підтверджує дату складання контракту й, крім цього, підтверджує точний час цього. Цю функцію не можуть виконувати письмові документи. У відповідності до статті 5 (1) Директиви про електронний підпис держави-учасниці повинні гарантувати, щоб сучасні електронні підписи задовольняли юридичні вимоги підпису (дієвість) і були припустимі як докази у суді.

Однак простим електронним підписам не можна відмовляти в юридичній дієвості й допустимості тільки на підставі того, що вони не мають того ж самого рівня надійності (стаття 5(2)). Це означає, що зараз суддям не потрібно дивитися на підпис в електронному бланку й оцінювати її надійність і допустимість для встановлення юридичних фактів.

Директива про цифровий підпис 1999 року встановлює рамки для юридичного застосування електронних підписів у Європейському Союзі. Застосування цієї Директиви відбувалося на різних стадіях шляхом внесення її положень у відповідні національні законодавчі акти.

Відповідно до цього акту постачальники послуг Інтернет (такі як постачальники доступу) зобов'язуються давати доступ до цільових пересилань і розкривати будь-які захищені електронні повідомлення або дані в зрозумілій формі.

Де й коли укладається контракт? Момент обговорення акцепту також важливий для встановлення, де й коли укладається контракт. В звичайній угоді ці моменти не викликають труднощів, але коли сторони обговорюють (угоду) на відстані, як в електронних контрактах, точний момент укладення контракту може бути спірним. Між тим цей момент дуже важливий, оскільки він встановлює:

а) коли договірна сторона втрачає право на однобічну відмову;

б) який акцепт вважається першим за часом, якщо є конкуруючі акцепти для обмеженої кількості контрактних можливостей;

в) де укладений контракт, бо для угод між резидентами різних країн це може допомогти визначити, право якої юрисдикції застосовується до контракту – Brinkibon v Stahag [1983] AC 34.

Відповідно до чинного законодавства акцепти дійсні тільки тоді, коли вони отримані, але є виключення, коли для відправлення акцепту використовується пошта. Моментом відправлення акцепту вважається відправлення (пошти) («поштова норма») – Adams v Lindsell (1818) 1 B.&Ald. 681. Застосування поштової норми обмежено певними умовами (див. приклад, Holwell Securities v Hughes [1974] 1 All ER 399) і може бути виключено наміром сторін, вираженим певним чином або таким, що мається на увазі.

Розміщення замовлення он-лайн: норми Директиви про електронну комерцію

Директива ЄС про електронну комерцію, включає положення і відносно принципів, які повинні застосовуватися державами-учасниками, щоб гарантувати захист споживачам, які розміщують замовлення он-лайн, а саме акцепти он-лайн.

Стаття 11(1) визначає ці принципи в такий спосіб:

- постачальник послуг повинен підтвердити одержання замовлення одержувача (адресату) без недоречної затримки й електронних коштів (це не застосовується там, де контракт був укладений винятково (за допомогою обміну) електронною поштою;

- замовлення й підтвердження одержання вважаються отриманими, коли сторони, яким вони адресовані, мають можливість одержати до них доступ.

Стаття 11(2) вимагає від держав-учасників передбачити в законодавстві положення про те, щоб постачальники послуг мали обов'язок застосовувати кошти, за допомогою яких одержувачі послуг могли б визначити й виправити помилки в контракті. Додатки Європейського Парламенту представляють подальшу вимогу про те, що контракти й інформація до них «повинні мати можливість бути надрукованими одержувачем і відтворені незмінно». (Спочатку) Вважалося, що це занадто

надмірно й відволікає від використання електронних повідомлень. (Тому) Прийшли до наступного компромісу: ‘ постачальник послуг робить доступними для одержувача послуг відповідні ефективні й доступні технічні кошти, що дозволяють йому визначити й виправити помилки до розміщення замовлення’. Стаття 11(2) не застосовується там, де контракт був укладений винятково за допомого обміну електронною поштою.

Що стосується угод бізнес для бізнесу (Б2Б), сторони вільні скасовувати ці положення за домовленістю (див. статтю 11(1)(2)). Але такий підхід не враховує інтереси малих і середніх підприємств, чиї важелі при веденні переговорів не завжди настільки сильні, як це припускає закон.

Об'єднання (включення) умов в Е-контракти на споживання. Умови контракту життєво важливі у визначенні прав і відповідальності сторін у випадку виникнення суперечок. Більшість торговців воліє мати контракти на їх власних умовах. Перевагою такого підходу є впевненість і передбачуваність договору для торговця, а також те, що стандартні умови розробляються з урахуванням інтересів торговця. Тому, однієї з найважливіших проблем для е-торгівця є впевненість, що його стандартні умови включені в контракти з його клієнтами. Якщо умови не будуть включені, то в Э-торговца не буде можливості посилатися на них.

Традиційні методи включення умов у договори. Проблемою для Е-торгівця є збереження з одного боку, балансу між забезпеченням доступу клієнтів до умов), а, з іншого боку, не поставити під загрозу комерційну привабливість й презентацію вебсайта. Є три методи включення, визнані відповідно до закону: - *за допомогою підпису*, *відповідно до повідомлення*, *відповідно до загальноприйнятої практики ведення ділових операцій.*

Включення за допомогою підпису За загальним правилом особа зв'язана умовами документу, що вона підписала, навіть якщо вона не читала його або не розуміла його значення - *L’Estrange v Graucob* [1934] 2 KB 394. Є обмежене число виключень із цього правила, якщо підпис отриманий шляхом введення в оману - *Curtis v Chemical Cleaning* [1951] 1 KB 805 або шахрайства або якщо доступно прохання *non est factum (не встановлений акт)*.

Також людина, що підписує документ, повинна розумно вважати, що документ містить умови, про які сторони домовилися - *Grogan v v Robin Meredith Plant Hire* (1996). чи може таке натискання на кнопку, підтвердити, що стандартні умови е-торговця були прочитані й погоджені, і бути розцінене як еквівалент підпису в цьому випадку? Chissick і Kelman заперечили це ствердження, оскільки споживачі за загальним правилом можуть бути уведені в оману, тому що не розцінюють такий крок як натискання на кнопку настільки ж серйозно, як підписання документа.

Включення (умов) шляхом повідомлення. Умови можуть бути включені шляхом розумного повідомлення. Власне кажучи повинні бути дотримані 3 умови: вибір часу (див., наприклад, *Olley v Marlborough Court* [1949] 1 KB 532), повідомлення повинне бути в договірному документі (на відміну від *Chapelton v Barry UDC* [1940] 1 KB 532 з *Parker v South Eastern Railway* (1877) 2 CPD 416), розумні міри повинні бути прийняті, щоб повідомити про договірні умови іншу сторону (*Thompson v LMS Railway* [1930] 1 KB 41).

Якою мірою на розумність повідомлення може вплинути характер пункту або розглянутої умови? Чим незвичніша й необтажувальніша ця умова, тим сильніше повідомлення{уваги} буде потрібно *Thornton v Shoe Lane Parking* [1971] 2 QB 163, *Spurling v Bradshaw* [1956] 1 WLR 461 HL, *Interfoto Picture Library v Stiletto* [1989] QB 433, CA.

Включення (умови) по сформованим діловим відносинам. Умова може бути включена навіть якщо явно не згадана в конкретній угоді, якщо попередньо були тривалі, постійні й послідовні ділові відносини між сторонами на основі цієї умови - *McCutcheon v David MacBrayne Ltd* [1964] 1 WLR 125, HL. In *Hollier v Rambler Motors* [1972] 2 QB 71, зокрема три або чотири контракти протягом приблизно п'яти років не можуть уважатися сформованими діловими відносинами для цих цілей.

Е-торговці тепер використають безліч методів. Існує баланс між юридичною визначеністю й комерційною привабливістю вебсайта. Посилання на джерело off-line (автономний, поза мережею)

можуть бути недостатньої. Відображення стандартних умов унизу сторінки або у зворотному зв'язку, що повинен переглянути користувач, є набагато більш юридично певними методами. Компроміс, до якого прибігають багато Э-торговцы – заява-посилання з гіперпосиланням. Позиція американських судів усе ще не визначена - див. *Ticketmaster V. Tickets.com* (2000) і *Specht v. Netscape* (2002).

Контракти через Е-пошту. Стандартні умови ймовірно повинні бути включені. Посилання або додатки, імовірно, будуть недостатні, якщо немає сформованих ділових відносин.

Використання обов'язкових умов в Е-контрактах. Е-торговці повинні знати про обов'язкові умови, які не можуть бути виключені. Див. умови, які мається на увазі в Акті про продаж товарів і Акт про поставку товарів і надання послуг; *St Albans City and District Council v ICL* [1996] 4 All ER 481, CA; Акт про несправедливі умови договору й Регламент (Інструкція) про несправедливі умови в договорах на споживання.

*Незапитувані товари***.** Ст.24 Регламенту забороняє поставку незапитуваних товарів і послуг споживачам. Ст.24 з виправленнями заміняє ст. 1 Закону про незапитувані товари й послуги від 1971 року. Згідно до ст.24 (2) одержувач може розцінити товари як беззастережний подарунок.

Шахрайство при оплаті. Платежі в Інтернеті були проблематичні, картки підроблялися й використалися в режимі онлайн. Ст.21 захищає споживачів і встановлює, що у випадку шахрайського використання картки споживача для оплати по контрактах на відстані, споживач буде мати право анулювати оплату. Якщо оплата вже була зроблена, у споживача буде право на рекредитування або повернення всіх сум емітентом картки. Регламент вносить виправлення в ст. ст. 83 і 84 Закону про Кредит Споживача від 1974 року, усуваючи потенційну відповідальність боржника перед кредитором за згодою про кредит споживача за втрату перших 50 £ через неправильне вживання символу кредиту (картки) у зв'язку з контрактом на відстані.

Право на розірвання контракту (ст.10).

Форма й процедура розірвання. На відміну від Закону про кредит споживача від 1974 року немає ніяких вимог до права на розірвання договору, за винятком того, що це повинно бути зроблене:

- у письмовій або іншій надійній формі
- у межах періоду для розірвання
- і виражати ясний намір розірвати договір

Після розірвання контракт буде розглядати, як такий, що не був укладений. Повідомлення повинно бути направлено постачальникові або іншим, позначеним постачальником, особам. Ст.10 (4) встановлює, що повідомлення є таким, що належним чином спрямовано, якщо споживач:

- залишає/залишив його по останній відомій адресі
- посилає/послав його поштою по останній відомій адресі
- відправляє/відправив факсом його по останньому відомому номеру
- посилає/послав по електронній пошті його по останній відомій адресі в е-пошті

Наслідки розірвання контракту. Після розірвання сторони повертаються в положення, у якому вони були до укладення контракту. Тому, згідно ст.14, у випадку забезпечення контракту цінним папером, при розірванні договору цінний папір підлягає поверненню. Ст.15 установлює, що, якщо контракт укладався разом з кредитною угодою (що згідно Закону про кредит споживача називається зв'язаною угодою), тоді розірвання торкнеться обох контрактів. Товари, отримані за розірваним контрактом, підлягають поверненню. До моменту повернення товарів споживач повинен піклуватися про товари. Професійний торговець зобов'язаний відшкодувати гроші, заплачені споживачем.

Період, протягом якого можливе розірвання контракту. Він відмінний для товарів і послуг. Якщо товар поставлений (ст.11), то після закінчення періоду семи робочих днів, що починаються від дня після того, у який споживач одержав товари.

- якщо постачальник не виконав умови - протягом трьох місяців, що починаються від дня після того, у який споживач одержав товари,

- після закінчення періоду семи робочих днів, що починаються від дня після того, у який споживач одержує інформацію.

Якщо жодна із зазначених вище ситуацій не має місце, - після закінчення трьох місяців і семи робочих днів, що починаються від дня після того, у який споживач одержав товари.

Для послуг (ст.12) застосовуються ті ж самі періоди часу, але час починає текти від дня після того, у який контракт укладений, але не з моменту початку надання послуг.

Виключення із правила про розірвання. Розірвання неможливо, якщо сторони не домовилися про інше:

- постачальник послуг виконав умови (ст. 8) і обслуговування почалася, за згодою споживачів;
- товари або послуги піддаються коливанням фінансового ринку;
- товари по особистих вимогах/специфікаціям покупця;
- аудіо, відео матеріали або програмне забезпечення;
- журнали, газети;
- лотерейні послуги або послуги з парі.

Тема 8. Правове регулювання електронного бізнесу

У юридичному аспекті електронна комерція — це укладення в електронній формі низки підприємницьких угод купівлі-продажу, постачання, про розподіл продукції, страхування, про перевезення вантажів або пасажирів повітряним, морським, залізничним транспортом, банківських угод та ін.

Торговельні відносини традиційно впливали на право з метою спрощення регулювання даної сфери, а також способів вирішення конфліктів. В результаті деякі країни пішли шляхом розвитку дуалізму приватного права і нарівні з громадянським право розробляли торгове право. Обсяг і поняття останнього розрізнялися (приміром, у Франції і Німеччині). При цьому поняття комерції в праві не збігалося з його економічним значенням. З точки зору права торгівля могла охоплювати різні види діяльності (у тому числі банківську, страхову), що має мета отримання прибутку. Якщо в XX столітті відзначалася комерціалізація цивільного права, і деякі країни відмовилися від дуалізму приватного права (Швейцарія, Італія), то наприкінці століття проблема правового регулювання торговельних відносин знов виникла у зв'язку з розвитком електронної комерції.

Поняття електронної комерції в національних правових системах не має однакового значення. Його обсяг варіюється і визначається тим, наскільки національне законодавство приділяє увагу цьому інституту. Тобто, якщо раніше національні юрисдикції виробляли критерії торгового права (наприклад, німецьке право відносить до торгових операціях угоди, що здійснюються комерсантами, а французьке право визначає коло угод, що відносяться до торговельних), то в даний час вони визначають зміст електронної комерції. Приміром, в європейських країнах застосовується ряд обмежень. Через Інтернет не укладаються договори, що вимагають нотаріального посвідчення, договори, що вимагають реєстрації в органах державної влади, договори в області сімейного та спадкового права. Тим не менш, електронна комерція охоплює різноманітні відносини, які здійснюються з використанням Інтернету. Сюди відносяться не тільки продаж через Інтернет, але і надання послуг (медичні, юридичні, інші професійні консультації, а також банківські, фінансові послуги). У такому значенні електронна комерція стає умовним поняттям. Однак, як вуж вказувалося, для права традиційно розширене розуміння комерційних відносин і перенесення особливості правового регулювання комерційних відносин на суміжні відносини.

В даний час відбувається переоцінка підходу до правового регулювання Інтернету. Численні роботи, головним чином американських вчених, про Інтернет як новий інформаційно-соціальному просторі, де формується своя нормативна система регулювання і потрібно вироблення особливої концепції правового регулювання, залишилися в минулому. Практика пішла шляхом «втягування» Інтернету у національні юрисдикції. У зв'язку з цим не виправдалося і припущення інших юристів, що

прогнозували стрибок у розвитку міжнародного права і посилення його ролі в уніфікації національного законодавства. Регіон, де такі тенденції спостерігаються, - це Європа, оскільки Європейський Союз прагне встановити єдине правове простір, в тому числі і в сфері електронної комерції, і як наслідок гарантувати захист інтересів учасників електронної комерції.

Таким чином, США стали більш тверезо, хоча разом з тим досить активно, а Європа більш виважено і обережно регулювати нове явище.

Електронна комерція ставить питання про те, наскільки дана сфера вимагає особливого правового регулювання. Регулювання електронної комерції здійснюється на основі загальних правових норм, і тільки в ряді випадків потрібне спеціальне правове регулювання. Припущення того, що дана сфера вимагає виключно нового правового регулювання, не підтвердилися практикою. Більшість країн обережно визначають специфіку правового регулювання. Приміром, загальновизнана необхідність законодавчого регулювання електронного підпису, однак договірне право не зазнає особливих змін.

Електронна комерції має ряд істотних переваг, як для продавця, так і для покупця. Однак найчастіше переваги, пов'язані з великим інформаційним обміном, визначають і недоліки, зокрема можливе шахрайство з боку учасників. Тому потрібна додаткова захист інтересів. Суди захищають права споживача незалежно від використання технічних засобів. Проте виникають моменти, що вимагають уточнення.

Закордонне законодавство приділяє увагу укладенню договору через Інтернет. Місце і час укладання договору мають важливе значення для визначення національного законодавства, вибору суду при вирішенні конфлікту. Сторони можуть використовувати різні технічні засоби для вираження своєї волі - Інтернет (як електронну пошту, так і веб-сторінки), або факс, телекс, або скористатися телефоном (в тому числі телефоном з використанням Інтернету). Від продавця вимагається більш чітко визначити, в якій формі має бути отримана відповідь.

Спілкування по телефону або поштою підкоряються загальним положенням договірного права. У такому випадку час та місце укладання договору визначається місцем знаходження оферента. Якщо використовується пошта, то оферта вважається прийнятим з моменту, коли лист було надіслано, але не коли воно було отримано. Відносно електронної пошти діє різні правила, що фіксують момент отримання.

Якщо в традиційних випадках прийняття оферти контрагентом не вимагає додаткового підтвердження, то при використанні Інтернету продавець, як правило, підтверджує, що він отримав інформацію (через електронну пошту, або через веб-сторінку). Для того, щоб між сторонами не виникало непорозумінь з питання характеру пропозицій, зроблених через Інтернет, і в даному випадку захистити особа, яка зробила оголошення в Інтернеті, зокрема англійська практика проводить відмінність між офертою і «пропозицією звертатися». У першому випадку слід прийняття оферти, у другому можлива в свою чергу оферта. Така відмінність проводитися для того, щоб усвідомити, наскільки оферент вважає себе зв'язаним своєю пропозицією. Продавець може мати обмежений набір товару для продажу, або має намір продавати обмеженому колу осіб (наприклад, певного віку), або визначає територію («юрисдикцію»), на яку поширюється її пропозицію, або визначити порядок розрахунку. Разом з тим, при оцінці оферти і акцепту слід враховувати особливості їх регулювання не тільки в країнах загального та романо-германського права, але і в країнах романського та германського права. Таким чином, специфіка національних правових систем визначає особливості укладання договорів через Інтернет.

Разом з тим Інтернет змушує країни визначитися у визнанні електронної форми договору, а також надати юридичне значення цифрового підпису.

Більш складно вирішується питання про захист порушеного права, зокрема вибір національної юрисдикції. Незважаючи на те, що Інтернет є світовою інформаційною системою, електронна комерція з точки зору права не набула настільки «світової» характер і традиційно продовжує залишатися в

рамках національних юрисдикції. Проте можливий більш складний «національний» склад учасників процесу загострює проблему вибору права. У більшості випадків спори вирішуються відповідно до міжнародного приватного права. Переважно в договорі визначати, право якої країни застосовується в даному випадку, і суду якої національної юрисдикції буде розглядати справу. Якщо сторони не обумовлюють це, то діє міжнародне приватне право. У договорах купівлі-продажу застосовується право звичайного місця проживання покупця. Такої позиції дотримується і право Європейського Союзу. Необхідно вдаватися до певних правових підходів і засобів, щоб оперативно й ефективно відповісти на появу нових можливостей у бізнесі. Передусім, це особлива законодавча регламентація електронної комерції, яка поєднувала б застосування традиційних, базових юридичних норм і правил (таких, як положення Цивільного або Цивільно-процесуального кодексу) і створення нових правових інститутів і процедур. Серед найважливіших юридичних питань, які потребують негайного законодавчого вирішення, слід назвати:

— вимоги до форми укладення електронних угод;
— оподаткування мережевих тарифів;
— захист інформації і використання електронних підписів;
— охорона прав споживачів у мережі, інтелектуальної власності тощо.

Деякі представники іноземної юридичної доктрини стверджують, що законодавство щодо мережевої економіки повинно бути міжнародним і «прозорим». Глобальний і розгалужений характер он-лайнової економіки не дає змоги регулювання її будь-яким урядом або державним органом. Як наслідок — домінування на практиці способу саморегулювання

Глобальний бізнес-діалог в Інтернет повинен бути спрямований на створення уніфікованих правил або «кодексів поведінки» всіх учасників електронної економіки. Тому країни, де правова система ґрунтується на судовому прецеденті (рішенні суду), мають більше можливостей для саморегулювання Е-комерції порівняно з країнами, в яких застосовуються виняткова нормативні правові акти. В них електронна комерція часто не в змозі подолати правові перешкоди, які виникають під дією національних законів, зміна яких вимагає спеціальної процедури.

На пострадянському просторі право і юридична практика останніх років швидше сприйняли, ніж «відштовхнули» електронний бізнес, становлення якого збіглося з процесом загальної модернізації правових систем пострадянських країн. Однак, як правило, відносини між учасниками електронної комерції й досі не регулюються спеціальними законами або іншими джерелами права. На практиці створюються і постійно модифікуються різні угоди про електронний обмін даними або про електронний документообіг, які певною мірою відповідають чинному законодавству. Загалом правовим нормам властива нерозвинутість і фрагментарність, які порушують електронну форму бізнесу. Такі норми є юридичними бар'єрами для електронної комерції та її інтеграції до глобального електронного ринку. Позбутися таких перешкод можна через встановлення оптимального співвідношення норм адміністративного і приватного права щодо електронної комерції, введення в дію низки нових законів.

В Україні існує низка нормативних актів щодо відносин у сфері інформатизації, але тільки один документ присвячений безпосередньо глобальній мережі Інтернет. Це Указ Президента № 928/2000 «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31.07.2000 р. Він носить декларативний характер, але при цьому визначає основні напрями правового регулювання Іпіегпеі у нашій країні.

Міжвідомчою Робочою групою з питань спрощення і модернізації процедур в управлінні, торгівлі та н транспорті Міністерства економіки за участю представників Робочої групи Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України у листопаді 2000 р. було розроблено проекти Законів України «Про електронні документи та електронний документообіг» та «Про електронний цифровий підпис »(ЕЦП). На їх думку, проекти загалом відповідають подібним

закордонним проектам і вже прийнятим законам, однак необхідно забезпечити їх зв'язок із загальним законодавством України.

Під час опрацювання проекту Закону про ЕЦП використовувалося законодавство ФРН та Австрії, було взято до уваги досвід законотворчої діяльності у цій сфері Російської Федерації та Білорусі [див.: Закон України Про електронний цифровий підпис, Відомості Верховної Ради України (ВВР), 2003, N 36, ст.276, із змінами, внесеними згідно із Законом N 879-VI **(** 879-17 **)** від 15.01.2009, ВВР, 2009, N 24, ст.296].

Електронний цифровий підпис є тим інструментом, що дає змогу створити правові основи для електронного документообігу, укладати угоди, створювати платіжні системи нового типу, електронні цінні папери тощо. Він використовується для підтвердження цілісності, дійсності та авторства будь-яких електронних документів: текстових, графічних, окремих рядків або записів у базах даних тощо.

Під час укладення угод в електронній комерції електронний підпис виконує такі юридичні функції:

— вказує, ким підписаний документ або повідомлення, і є складним для відтворення будь-якою іншою, не уповноваженою на те особою;

— ідентифікує те, що підписано, і не допускає підробки або змін;

— виконує процедурну роль, тобто символізує виявлення волі певної сторони до угоди (схвалення, дозвіл тощо). В електронній комерції процедури створення і перевірки підпису є гарантією справжності та дійсності договірних зобов'язань, а також захистом від їх односторонньої зміни або порушення.

Розроблений відповідно до чинного законодавства України закон про ЕЦП враховує рекомендації Європейського Союзу і зокрема Директиву Європейського Парламенту та Ради Міністрів Європейського Союзу 1999/93/ЄС від 13 грудня 1999 року «Про політику ЄС щодо електронних підписів». Так, за ст. 24 Закону, центри сертифікації ключів несуть відповідальність за заподіяну шкоду перед користувачами та третіми особами; тим самим підтверджена вимога ст. 6 Директиви 1999/93/ЄС щодо обов'язків центрів сертифікації ключів відшкодувати збитки, заподіяні іншим особам внаслідок використання цифрового підпису. Відповідно до вимог ст. 6 щодо визнання іноземних сертифікатів, взаємне визнання сертифікатів ключів, виданих центрами сертифікації ключів, розташованими в Україні і за кордоном, здійснюється згідно з міжнародними договорами за участю України (ст. 26, 27 Закону).

У багатьох державах законодавство щодо електронних підписів уже діє. Крім того, розповсюдження забороненої інформації через мережу призвело до того, що в Австралії прийняті закони, спрямовані на врегулювання змісту інформації в Інтернет, а в Німеччині діє Закон «Про відповідальність провайдера».

Розвиток іноземного законодавства в цій галузі відбувається через гармонізацію і формування загальних принципів, які дають змогу створити на міжнародному рівні універсальну правову інфраструктуру електронного підпису.

Водночас світ Інтернету висуває занадто високі вимоги до держави і права щодо захисту інтересів учасників електронного комерційного обігу. Дієздатність демократичних держав у світі електронних мереж обмежена, бо вони не мають відповідної правової бази, але дозволяють кожному бажаючому приєднатися до загальнодоступних глобальних процесів. Цілеспрямоване втручання будь-якої держави у функціонування всесвітньої мережі Інтернет, яка децентралізована за своєю сутністю, не дає бажаного результату. В цій сфері жодна держава не має ні монополії, ні влади, ні можливості застосувати примусові засоби. Захист індивідуальних і суспільних інтересів тільки шляхом дозвільних або заборонних заходів не спрацьовує у нематеріальному світі мереж.

Під час розроблення юридичних норм, які обґрунтовують використання електронного підпису, стратегія будь-якої держави повинна бути замінена новим підходом.

1. Якщо демократична держава не має змоги на достатньому рівні захистити учасників ринку

в новому соціальному просторі мереж, то вона повинна надати їм право на самозахист.

Сучасні інформаційні технології дають змогу створити систему самозахисту, яка передбачає юридично рівноправну різнобічну систему безпеки кожного учасника електронного ринку. Юридичні норми не мають суперечити технічним засобам самозахисту. Право повинно тільки надавати можливість користуватися технічними засобами самозахисту. Кожен учасник правоздатний і сам вирішує, який з цих засобів він бажав би використати. Деякі технічні засоби можуть застосовуватися без будь-якої спеціальної регламентації. У такому разі держава мусить відмовитися від обмежувального регулювання.

3. Усі інші засоби (наприклад, цифровий підпис) повинні спиратися на відповідну нормативну базу, яка допоможе юридичній або фізичній особі довести свої права.

4. Система наведеного вище являє собою спеціальний правовий механізм. Законодавцям необхідно лише доповнити систему самозахисту необхідними юридичними гарантіями з боку держави.

5. В обов'язкових державних гарантіях особливе місце повинно бути відведено забезпеченню недоторканості приватного життя та особистої інформації користувачів Інтернет.

Закон про ЕЦП вирішує кілька юридичних завдань. Насамперед, принципове визнання ЕЦП як аналога власноручного підпису для широкого кола юридичних дій. Цивільний кодекс України не визнає електронних документів навіть як письмову угоду. Разом з тим існує велика кількість юридичних документів, про які не йдеться в Цивільному кодексі (наприклад, трудові контракти). Питання про можливість використання ЕЦП у таких випадках залишається відкритим. Для його вирішення Цивільного кодексу недостатньо.

Закон необхідний також для того, щоб легалізувати використання ЕЦП як функціонального еквівалента власноручного підпису у випадках, коли це безпосередньо не заборонено законодавством. У законодавстві про електронний підпис деяких країн такі заборони стосуються заповіту, процесуальних документів тощо. Звичайно, необхідні певні зміни та доповнення до діючих законів.

Нині питання електронної комерції в Україні Національний банк України врегульовує своїми нормативними документами. У серпні 2000 р. НБУ розробив проект «Вимог з організації електронної комерції в Україні», в якому висвітлено питання з організації електронних крамниць, формування і виконання електронних замовлень, їх оплати з допомогою різних платіжних систем, у тому числі через банківські платіжні картки, систему типу *клієнт-банк* тощо. НБУ також планує надавати комерційним банкам України програмне забезпечення для організації центрів сертифікації ключів для участі їх клієнтів в електронній комерції.

Законом України від 05.04.2001 р. № 2346-ІП «Про платіжні системи та переказ грошей в Україні» теж було легалізовано електронний підпис. Згідно з пунктом 18.2 статті 18 Закону, електронний цифровий підпис на електронному документі має однакову юридичну силу з підписом на паперовому документі, а з пунктом 18.1 статті 18 — електронний документ має однакову юридичну силу з паперовим документом. Тепер у суді Інтернет -крамниці можуть виступати з електронним документом і приймати платежі клієнтів з електронним цифровим підписом, щоправда, лише за угодою з банком.

Проблеми розвитку електронної комерції, які вимагають законодавчого вирішення. Не менш важливою умовою розвитку електронної комерції є прийняття комплексного Закону «Про електронну комерцію», який повинен забезпечувати юридичне визнання угод, що укладаються шляхом електронних повідомлень, гарантії їх дійсності, захист інформації від несанкціонованого доступу, а також охорону прав споживачів у сфері електронної комерції.

Захист інформації — сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи інформаційної системи та осіб, які користуються інформацією.

Несанкціонований доступ —доступ до інформації, що здійснюється з порушенням встановлених у певній інформаційній системі правил.

Електронна комерція безперспективна, якщо її учасники не матимуть можливості захисту своїх прав і законних інтересів у суді. Тому законодавство повинно передбачати правила подання судових доказів в електронній формі з цифровим електронним підписом.

На пострадянському просторі законодавству в сфері електронної комерції поки що приділяється незначна увага. Такий стан речей, виходячи зі світових тенденцій швидкого розвитку цієї галузі, не може залишатися надовго. Нормативні документи з префіксом «Е» покликані врегулювати правові й технологічні питання використання системи електронної комерції. Тому чим швидше держави вирішать ці питання, тим швидше електронна комерція почне приносити реальний зиск

Різновиди шахрайства в електронній комерції. Невпинне зростання користувачів Інтернет в останні роки спричинило появу в мережі багатьох негативних явищ. Покупки товарів з чужими кредитними картками, крадіжки інтелектуальної власності в Інтернет набули величезного розмаху і нікого вже не дивують.

Основною проблемою безпеки електронної комерції в Інтернет з часу її виникнення була проблема передавання закритої інформації (номерів кредитних карток, сум платежів тощо) через відкриту мережу. Існує низка ймовірних загроз безпеці інформації, яка передається в мережі, які вимагають певних рішень, що дають змогу організувати і значно підвищити захищеність даних, у тому числі й у ситуаціях, не пов'язаних безпосередньо з електронною комерцією (наприклад, під час відправлення конфіденційної інформації електронною поштою).

Найпоширенішою є крадіжка ідентифікаційної інформації (різновид загрози під номером 1): злодії збирають персональну інформацію — імена, адреси, номери соціального страхування й інші важливі дані, а після цього замовляють картки під цими іменами. Хоча крадіжки такого типу — річ не нова, Інтернет значно полегшив їх здійснення. Хакери і кракери «зламують» сайти, які зберігають цю інформацію. В деяких випадках злочинці вдають із себе легітимних он-лайнових торговців і збирають інформацію в покупців, які нічого не підозрюють.

Хакер — фахівець у галузі комп'ютерної техніки, який «зламує» системи захисту з метою задоволення власних професійних амбіцій, отримання «інтересу».

Кракер — хакер, який «зламує» комп'ютерні системи захисту з метою крадіжки й отримання фінансових доходів.

Дійсні номери карток також можуть бути автоматично згенеровані. Інтернет перенасичений хакерськими сайтами, які пропонують програмне забезпечення для генерації номерів кредитних карток, що здаються дійсними. Ці програми використовують складний алгоритм створення номерів, у яких, наприклад, перші чотири цифри відповідають дійсним цифрам банків-емітентів. Генератори створюють 12 додаткових цифр, які під час перевірки відповідають параметрам дійсних карток. Навіть якщо жоден банк ніколи не емітував картку з цим згенерованим номером, може так статися, що вони будуть авторизовані при електронних платежах

Існує ще й старий перевірений спосіб: кредитні картки викрадають у фізичному світі і використовують для он-лайнових закупівель.

Важливість вирішення проблеми шахрайства з кредитними картками в Інтернет неоднозначно оцінюється різними агентами електронної комерції. Часто говорять про загрозу безпеці споживачів. Однак, наприклад, американські споживачі ризикують незначною сумою: за федеральними законами, їх максимальна відповідальність обмежується 50 $, але це не стримує кредитні асоціації в експлуатації фобії шахрайства при просуванні різноманітних схем захисту.

Від реального ризику потерпають продавці. Саме вони несуть відповідальність за шахрайські он-лайнові трансакції. Співвідношення шахрайства такого типу становить від 2% продажів в одних товарних категоріях до 40% — в інших. Наприклад, такий гігант електронної комерції, як Amazon.com, визнає серйозність цієї проблеми і заявляє, що його спроможність протистояти шахрайству з боку

третіх сторін через трансакції з допомогою кредитних карток є одним з ключових чинників, які визначають позитивні результати діяльності компанії.

Рівень шахрайства в 2% у 20 разів перевищує оцінки компаній Visa і MasterCard — найвідоміших емісіо-нерів кредитних карток. У роздрібному он-лайновому бізнесі 2% шахрайських продажів при справжніх трансакціях могли б принести половину прибутку компанії. Крім того, постраждалі продавці платять штраф за кожне повернення, відшкодування власнику картки за неавторизований продаж. Якщо повернення стають частими, продавець сплачує підвищену комісію за трансакції або втрачає цю послугу взагалі.

Шахрайські Інтернет -замовлення можна поділити на дві категорії: товари, що можна легко обміняти на наявні, і трансакції, які не потребують фізичної доставки. До першої категорії належать споживча електроніка, діаманти і презентаційні сертифікати. До другої — програмне забезпечення, яке можна завантажити з мережі, і передплата на сайти «для дорослих». На цих сайтах (переважно американських) практично 100% трансакцій з деяких країн Східної Європи — шахрайські.

Головними вимогами до здійснення комерційних операцій в Інтернет є конфіденційність, цілісність, автентифікація, авторизація, гарантії і збереження таємниці. Перші чотири вимоги можна забезпечити технічними засобами, а досягнення гарантій і збереження таємниці залежить від технічних засобів, від відповідальності окремих осіб та установ, а також від дотримання законів, що захищають споживача від можливого шахрайства.

Ще у 1998 р. Верховна Рада України вперше заявила про свої наміри стати рівноправним учасником світових інформаційних відносин. Так, 4 лютого 1998 р. вона прийняла Закон «Про Національну програму інформатизації». Того ж дня була схвалена Концепція Національної програми інформатизації та прийнято Закон «Про затвердження завдань Національної програми інформатизації на 1998—2000 роки».

Головною метою Національної програми інформатизації є забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією на основі широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави.

Загальні положення Концепції Національної програми інформатизації (Програма) та Закон «Про Національну програму інформатизації» (ст. 1) визначають інформатизацію як сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, спрямованих на створення умов для задоволення інформаційних потреб, реалізацію прав громадян і суспільства на підставі розвитку, використання інформаційних систем, мереж, ресурсів та інформаційних технологій, створених на основі застосування сучасної обчислювальної та комунікаційної техніки.

Наступним кроком став Указ Президента України № 928 від 31 липня 2000 р. «Про заходи по розвитку національної складової глобальної інформаційної мережі Інтернет та забезпеченню широкого доступу до цієї мережі в Україні». Основна цінність його в тому, що він визначає розвиток національної складової глобальної інформаційної мережі Інтернет, забезпечення широкого доступу до цієї мережі громадян та юридичних осіб усіх форм власності в Україні.

Постановою Національного банку України від 10 червня 1999 р. № 280 затверджено Правила організації захисту електронних банківських документів. Вони оперують поняттям електронні банківські документи, не розкриваючи його. Основна мета Правил — регламентувати порядок отримання, обліку, передачі, використання та зберігання засобів криптозахисту НБУ, виконання правил інформаційної безпеки в установах, що є учасниками інформаційно-обчислювальної мережі НБУ.

Поняття електронного документа та електронного цифрового підпису використовується у прийнятому 5 квітня 2001 р. Законі «Про платіжні системи та переказ грошей в Україні» для регулювання загальних засад функціонування платіжних систем в Україні, загального порядку проведення переказу грошей в межах країни, а також для встановлення відповідальності суб'єктів

переказу. Вказаний нормативний акт вперше на рівні закону дає визначення електронного документа та електронного цифрового підпису.

Сам факт того, що законодавець нарешті звернув увагу на електронний цифровий підпис та законодавче закріпив це поняття хоча б в межах спеціального закону, є позитивним моментом. В той же час, щодо визначення електронного документа та електронного цифрового підпису вказаний Закон викликає й дискусійні питання, які стосуються як самого визначення електронного цифрового підпису, так і його правового статусу. Зважаючи на істотне значення цього поняття для суспільства та держави, вважаю, що не можна обмежитися зазначеним Законом для регулювання відносин, пов'язаних з використанням електронного цифрового підпису, а тому щодо цього необхідно прийняти окремий закон.

Інших законів, які хоча б опосередковано регулювали б електронну комерцію в Україні, немає. Ні чинний в нашій державі Цивільний кодекс, ні Цивільний процесуальний, ні Господарський процесуальний кодекси жодною нормою не сприяють становленню та розвитку електронної комерції в Україні.

Розвиток техніки та технології дозволяють істотно спростити укладення угод. Однією з основних категорій електронної комерції є електронна угода, поняття якої наше законодавство не передбачає.

Норми, що регулюють форму угод, знаходяться в Цивільному кодексі на трьох рівнях: вони містяться у главі 3 «Угоди», главі 14 «Виникнення зобов'язання», а також в різних главах ЦК, присвячених окремим видам договорів. Правове регулювання форми договорів виражається у встановленні вимог до неї (форми) та наслідків її порушення. Висуваючи відповідні вимоги, закон сприяє тому, що відносини сторін стають більш визначеними, знімаються підстави для спорів у майбутньому щодо самого факту укладення угоди та її змісту.

Стаття 42 ЦК передбачає, що угоди можуть укладатися в усній або письмовій формі. Письмовий договір укладається шляхом складання відповідного належним чином підписаного документа. Як зазначають російські вчені, ЦК РФ врахував та визнав існуючу практику застосування різноманітних способів факсимільного відтворення підпису за допомогою засобів механічного чи іншого копіювання, електронно-цифрового підпису та інших аналогів власноручного підпису. Використання цього способу визнається припустимим, якщо в законі, іншому правовому акті або угоді сторін буде встановлена сама можливість таких підписів та визначено їх порядок. Порушення хоча б однієї з цих вимог може бути достатньою підставою для оспорювання договору.

Деякі вітчизняні автори зазначають, що в сучасних умовах розширилися технічні можливості вияву волевиявлення сторін на укладення договору, зокрема за допомогою електронного зв'язку. Однак не вказується як трактувати електронну форму угоди.

Далі, ст. 154 ЦК передбачає, що коли сторони домовились укласти договір у певній формі, він вважається укладеним з моменту надання йому обумовленої форми. Отже, укладаючи угоду в письмовій формі, сторони мають скласти відповідний, належним чином підписаний документ. Таким чином, якщо навіть припустити, що ст. 42 та ст. 154 ЦК дозволяють нам укласти електронний договір (як договір, електронна форма якого обумовлена сторонами), документ, що містить погоджене волевиявлення сторін на виникнення між ними зобов'язання, повинен набрати юридичної сили договору, що відбувається після його посвідчення електронними підписами сторін. Чинне цивільне законодавство не передбачає такого поняття як електронний (цифровий) підпис, а також й поняття електронного документа, електронного документообігу.

22 травня 2003 р. Верховна Рада України прийняла Закон «Про електронні документи та електронний документообіг» (Відомості Верховної Ради України (ВВР), 2003, N 36, ст.275, із змінами, внесеними згідно із Законом N 2599-IV (2599-15) від 31.05.2005, ВВР, 2005, N 26, ст.349)

Він пропонує визначення електронного документа та електронного документообігу, пропонує закріпити світові тенденції щодо визнання юридичної сили електронного документа, вказує на права та обов'язки суб'єктів електронного документообігу, їх відповідальність, тощо.

В законі дотриманий функціонально-еквівалентний підхід до розуміння електронного документа, запропонований Типовим законом Юнсітрал «Про електронну комерцію». Функціонально-еквівалентний підхід ґрунтується на дослідженні цілей та функцій традиційних вимог до складання документів на папері для того, щоб визначити, як ці цілі та функції можуть бути досягнуті або виконані за допомогою методів, що використовуються при електронній передачі даних.

Однак цей закон чітко не визначає його сфери дії; крім того, необхідно доопрацювати визначення електронного документа, зробити його більш конкретним; визначитися з тим, що є паперовою копією електронного документа, та передбачити порядок її оформлення; треба більш ретельно підійти до визначення умов зберігання електронних документів; вказуючи на права та обов'язки суб'єктів електронного документообігу, слід все ж таки їх зазначити, а не відсилати до іншого нормативного акту.

В юридичній літературі справедливо зазначається, що основними недоліками правового регулювання електронних угод є:

1. Невизначена юридична сила договорів, які укладаються у електронній формі, а звідси відсутність судового захисту у разі порушення прав та обов'язків, що випливають з таких договорів.

2. Чинне законодавство не містить положень щодо того, які документи можуть або не можуть бути використані у господарському обігу у вигляді електронного документа та які вимоги передбачаються до структури та форми його.

3. Вітчизняний законодавець не визначився щодо правового статусу електронного підпису.

4. Посередники, особи, що поставляють послуги з організації електронного зв'язку, не зобов'язуються зберігати, надавати за запитом сторін чи офіційних органів, а також підтверджувати справжність створених та переданих за їх допомогою електронних документів.

5. Не зрозуміло, яким чином буде здійснюватися оподаткування угод, що здійснюються у електронній формі.

Тема 9. Інтелектуальна власність у електронній торгівлі

Розуміння зв'язку між інтелектуальною власністю (ІВ) та електронною торгівлею. Інтелектуальна власність (далі ми використовуємо скорочення ІС) - це правовий термін, який означає промислову власність, а також авторське право і суміжні права. Промислова власність включає охорону патентів, товарних знаків, промислових зразків та географічних зазначень. Вона також включає охорону корисних моделей, товарної упаковки і топології інтегральних мікросхем, коли така охорона існує, а також захист від недобросовісної конкуренції ключа / або охорону нерозкритою інформації / комерційної таємниці.

Інтелектуальна власність дійсно є одним із видів власності або активів, настільки ж цінним (або навіть більш цінних) ніж фізична або реальна власність, хоча подібно до знань вона є невловимої. Цінність активів ІВ в порівнянні з матеріальними активами зросла з причини важливості технологій та творчої праці для сучасної економіки. Інтелектуальна власність складається з нових ідей, оригінальних виразів, відмінних назв і зовнішнього вигляду, які роблять продукцію унікальною і цінною. Інтелектуальна власність часто стає об'єктом торгівлі (або ліцензій) сама по собі без торгівлі які лежать в її основі продуктом або послугою, шляхом передачі правотримателів патенту або інших ліцензій ІС іншій особі.

Є декілька причин, що пояснюють, чому інтелектуальна власність є настільки важливою для електронної торгівлі. Більшою мірою, ніж інші ділові системи, електронна торгівля часто пов'язана з продажем продуктів і послуг, заснованих на інтелектуальній власності, і її ліцензування. Музика, картини, фотографії, програмне забезпечення, дизайн, навчальні модулі, системи і т.д. - Все це може

бути об'єктом електронної торгівлі. У всіх цих випадках ІС є основним компонентом вартості. Інтелектуальна власність є важливою, оскільки цінні об'єкти, що продаються в Інтернеті, повинні охоронятися з використанням технічних систем безпеки та законів інтелектуальної власності, бо вони можуть стати предметом крадіжки чи піратства, а вся справа може бути розорена.

Інтелектуальна власність також забезпечує ефективність електронної торгівлі. Системи, що дозволяють доступ до Інтернету діяти, - програмне забезпечення, мережі, проекти, інтегральні схеми, перехідники і перемикачі, інтерфейс користувача і т.д. є різними формами інтелектуальної власності і часто охороняються правами інтелектуальної власності. Товарні знаки є важливою частиною сфери електронної торгівлі, оскільки постачання товару торговою маркою, визнання споживача та доброзичливість - основні елементи всієї діяльності на основі веб-сайтів - охороняються товарними знаками і законом про недобросовісну конкуренцію.

Діяльність у сфері електронної торгівлі і в Інтернеті заснована на ліцензування продукції або патенту. Оскільки для створення продукту необхідні багато різні технології, компанії часто передають розробку деяких компонентів продуктів на бік або використовують технологію спільно з ким-небудь завдяки ліцензійним угодам. Якщо б кожна компанія повинна була самостійно розробляти та виробляти всі технічні компоненти кожного продукту, розвиток високотехнологічних продуктів було б неможливо. Економіка електронної торгівлі залежить від компаній, що діють спільно і спільно використовують завдяки ліцензій можливості, і також що піддаються загальним ризиками. Багато хто з цих компаній є малими і середніми підприємствами.

І нарешті, цінність операцій у сфері електронної торгівлі звичайно в значній мірі пояснюється інтелектуальною власністю, тому оцінка вашого бізнесу в сфері електронної торгівлі буде залежати від того, охороняєте ви вашу інтелектуальну власність. Багато компаній, що займаються електронною торгівлею, подібно іншим технологічним компаніям мають у своїх активах портфелі патентів і товарних знаків, які підвищують цінність їх діяльності.

Інвентаризація активів ІВ, що мають значення для електронної торгівлі. Важливим початковим кроком для будь-якої діяльності в сфері електронної торгівлі є інвентаризація активів ІВ. Візьміть ручку і складіть список будь-яких патентів, патентних заявок або інновацій, які ви зробили і які на вашу думку можуть бути патентоздатності винаходу. Включіть також до списку все, що на вашу думку відноситься до сфери авторського права. Цей список буде включати програмне забезпечення, проекти, документацію або технічні запису, структурний опис програмного забезпечення, матеріали інтерфейсу користувача, схеми, твори мистецтва, дизайн веб-сайту, музику, фотографії і т.д. Охорона авторського права діє автоматично в більшості країн і не потребує реєстрації (хоча реєстрація у депозитарію авторського права, в тих випадках, коли це можливо, звичайно бажана).

Тепер напишіть, які відмітні знаки або назви як зареєстровані, так і незареєстровані компанія використовує. Такі знаки користуються охороною в якості товарних знаків або знаків обслуговування після реєстрації або, якщо це передбачено законом, просто в разі використання, навіть без реєстрації. До їх числа можуть ставитися назви продуктів, якщо назва не є просто описом продукту (наприклад, сіль, тканина, хороше програмне забезпечення, швидкі комп'ютери), а також емблеми та ділові назви.

Вкажіть, будь ласка, будь-які промислові секрети; така інформація має для вас комерційну цінність, вона зазвичай невідома і будь-який розумна людина не може її просто так уявити собі. Вона включає формули продукту, списки клієнтів, ділову стратегію, плани технічного оснащення для випуску продукції, і т.д. Вкажіть будь-яку іншу інформацію, яка, на вашу думку, може бути цінною, хоча і не матеріальної.

І нарешті, вкажіть будь-які контракти, які, на вашу думку, можуть вплинути на активи ІВ, які ви перерахували (наприклад, контракт про консультації з дизайнерської фірмою, яка розробила ваш веб-сайт, угода про розробки з університетом, дозвіл на самостійну діяльність від вашого колишнього роботодавця, угоди про нерозголошення інформації, угоди з співробітниками).

Тепер ви можете показати ваш список юристу і попросити його або її оцінити, скільки коштуватиме проведення «ревізії ІК». Ревізія ІС має на меті проаналізувати, яку ІВ компанія має, і визначити, як охороняти, використовувати і підвищувати цінність цієї ІВ. Ваш юрист повинен мати у своєму розпорядженні знаннями про ІВ. Він або вона підкаже вам як краще використовувати правову систему для охорони вашої ІС від використання або розкрадання конкурентами і краще використовувати її як в режимі он-лайн, так і в іншому режимі, з тим щоб підвищити цінність ІС як активу компанії. Якщо у вас немає юриста, зверніться в ваше національне відомство ІВ і з'ясуйте чи мають вони можливість допомогти вам.

Додаткову інформацію

• щодо ревізії ІС див. «Ревізія вашої інтелектуальної власності»• з загальних питань ІВ і її стратегічного використання див http://www.patentcafe.com і

посилання, вказані вище, в розділі «Розуміння зв'язку між інтелектуальною власністю (ІВ) та електронною торгівлею»

• з питань авторського права див. «Авторське право і суміжні права»

Питання ІВ при проектуванні і створенні веб-сайту. Одним з основних елементів діяльності в сфері електронної торгівлі є проектування та нормальне функціонування веб-сайту компанії. При проектуванні і створенні вашого веб-сайту ви перш за все повинні знати, чи належить вам зовнішній вигляд веб-сайту, зміст і кожен аспект що знаходиться на ньому ІВ. Можливо ви цього і не знаєте, але вам необхідно знати, що вам належить, що ви маєте право використовувати, що вам не належить і що ви не маєте право використовувати. Якщо ви користуєтеся послугами консультанта або компанії при проектуванні вашого веб-сайту, уважно ознайомтеся з положеннями угоди, що стосується права власності та прав інтелектуальної власності. Кому належить дизайн веб-сайту та текст? Перевірте, які зобов'язання компанія несе, щоб переконатися в тому, що вона не використовує в ході своєї роботи будь-яку ІВ, що належить третій стороні.

Якщо ви користуєтесь базою даних, системою електронної торгівлі або іншим технічним інструментарієм Інтернет, отриманим за ліцензією від іншої компанії, перевірте умови ліцензійної угоди з тим, щоб з'ясувати кому належить система.

Переконайтеся, що у вас дійсно є письмова угода, і дайте його на перевірку юристу, перш ніж підписати його і почати будь-яку роботу з проектування, виготовлення або встановлення сайту.

Вам знадобиться письмовий дозвіл (також згадується як ліцензія, згода або угода) на використання будь-яких фотографій, відеозаписів, музики, голоси, ілюстрацій або програмного забезпечення і т.д., що належать будь-кому іншому. Той факт, що ви отримали матеріал в Інтернеті, зовсім не означає, що він є суспільним надбанням. Можливо вам доведеться заплатити за дозвіл використовувати ці матеріали. У багатьох країнах для отримання дозволу вам знадобиться звернутися до суспільства зі збору роялті або до асоціації артистів.

Вам необхідно переконатися в тому, що, якщо законодавство вашої країни (або законодавство, що застосовується до вашої діяльності) вимагає цього, у вас є дозвіл показувати що належать іншим компаніям товарні знаки, на які ви посилаєтесь на вашому веб-сайті, і що ви визнаєте їх .

Чи не поширюйте і не завантажуйте на ваш веб-сайт будь-який зміст або музику, які вам не належать, якщо тільки ви не отримали від власника письмового дозволу поширювати їх в Інтернеті.

Проявляйте обережність при відсилання на інші веб-сайти. Посилання - це важливий інструмент електронної торгівлі і корисна послуга для ваших клієнтів, але в багатьох країнах немає чіткого законодавства про те, коли і як ви можете використовувати ці посилання. Найбільш обережна практика полягає в тому, щоб запросити і отримати дозвіл іншого сайту, перш ніж робити на нього посилання.

Структурна інтеграція - це більш спірна практика, ніж відсилання до іншого сайту. Така практика означає включення великих компонентів іншого веб-сайту в ваш веб-сайт, при цьому

створюється враження, що вони є частиною вашого веб-сайту. Завжди отримаєте письмовий дозвіл, перш ніж робити це.

Додаткову інформацію про товариства зі збору роялті, див: BOIB: колективне управління авторським правом і суміжними правами

Питання ІВ у зв'язку з назвами доменів в Інтернет. В наші дні вибір назви домену став важливим діловим рішенням. Назва домену - це назву, що використовується для ідентифікації сайту вашої компанії в Інтернеті. Воно має бути відмінною і в ідеальному випадку досить відмінною, щоб отримати охорону на підставі законодавства про товарні знаки. Причина цього полягає в тому, що якщо ви вибрали дуже загальне або родову назву домену (наприклад, «хороше програмне забезпечення»), вашої компанії буде мабуть важко завоювати особливу репутацію і показати доброзичливість у цій назві. До того ж як правило ніщо не може перешкодити іншій компанії використовувати ваше ім'я домену в якості торгової марки або описового терміна в торгівлі, можливо обманюючи або вводячи в оману ваших споживачів.

Ви повинні вибрати назву домену, яка не є товарним знаком іншої компанії. Це пояснюється тим, що більшість законів розглядають реєстрацію товарного знака іншої особи в якості домену як порушення прав товарного знака і вашому МСП можливо доведеться припинити його використовувати і також відшкодувати збитки. Є різні бази даних, в яких ви можете провести пошук і визначити, чи не вибрали ви назву домену, яка зареєстрована як товарний знак в будь-якій конкретній країні.

Назви доменів компанії можуть бути в будь-якому числі «доменів верхнього рівня», які називаються «ДВУ». Ви можете вибрати з «родових доменів верхнього рівня» («рДВУ»), таких як. Com,. Net,. Org. Або ви можете вибрати з спеціалізованих або обмежених доменів верхнього рівня, якщо ви відповідаєте поставленим умов (наприклад, Aero для повітряних перевезень та індустрії транспорту). Ви можете також зареєструвати назву вашого домену в рамках «кодів країн доменів верхнього рівня» (ксДВУ) у вашій власній країні (наприклад,. Bn для Болгарії,. Cn для Китаю,. Ch для Швейцарії).

Управління назвами доменів зазвичай входить до компетенції корпорації Інтернет з присвоєння назв та номерів («ICANN»). Проте реєстрації здійснюють багато акредитовані ICANN реєстратори Інтернет, яких ви можете знайти на сайті ICANN за адресою: http://www.icann.org**.**

Якщо ви виявили, що хтось інший використовує назву вашої компанії в якості назви домену, як вам слід чинити? Деякі несумлінні люди використовують практику «кіберсквотінга», яка означає реєстрацію назв доменів із використанням назв і товарних знаків, які належать іншим компаніям, як правило для вивудження грошей у законного власника назви. Якщо ви виявили, що назва вашої компанії або товарний знак став об'єктом кіберсквотінга, є проста процедура, якою ви можете скористатися в режимі он-лайн для одержання рішення про можливе повернення вам назви домену. Така процедура називається Єдина політика з врегулювання спорів у галузі назв доменів (ЕПУСД) і ви можете знайти інформацію про це на сайті ICANN за адресою: http://www.icann.org.

Крім товарних знаків розумно уникати використання назв доменів, які включають деякі інші слова, такі як географічні назви (наприклад, Шампанське, Божоле), імена відомих людей, родові назви ліків, назва міжнародних організацій і торгові назви (наприклад, назва справи іншої особи).

Додаткову інформацію про назви доменів в цілому, див. http://ecommerce.wipo.int/domains/

Вплив патентів на ділову практику в галузі електронної торгівлі. Патенти існують не тільки для великих компаній. Патенти видаються не тільки стосовно високих технологій. Деякі з найбільш успішних компаній, що займаються електронною торгівлею, використовували патенти для ділових методів і для винаходів «низьких технологій».

Патенти можуть допомогти вашої діяльності в сфері електронної торгівлі з цілого ряду напрямків. Вони стимулюють службовців, які люблять вирішувати проблеми і які можуть отримувати винагороди та інші пільги, що надаються компанією. Вони допомагають фіксувати і розвивати нові ідеї.

Вони можуть підвищити цінність вашої компанії в умовах операцій з інвестування, фінансуванню, злиття і придбання. Вони можуть сприяти збільшенню цін на вашу продукцію, надаючи продукції вашої компанії виняткові особливості, недоступні для ваших конкурентів. Вони можуть сприяти збільшенню обсягу продажу вашої продукції, надаючи продукції вашої компанії виняткові особливості, недоступні для ваших конкурентів.

Вони можуть стати джерелом надходження роялті в рамках ліцензійних угод, тим самим збільшуючи доходи вашої компанії. Такі роялті можуть надходити у вигляді одноразово виплачується суми, часткових платежів в розрахунку на одиницю проданої продукції або з урахуванням відсоткової частки доходів від продажу продукції. Вони можуть дозволити вашої компанії, у випадку надання нею ліцензії на патент, розширити свої ринки і / або створити базу, на якій володарі ліцензій зможуть розвивати і диференціювати продукцію, засновану на патент.

Вони можуть використовуватися у зв'язку з участю в стандартних органах або консорціумах, де різні компанії об'єднуються для створення взаємодії технології або її просування. Вони можуть використовуватися для захисту в тому випадку, якщо ваша компанія обвинувачується в порушенні патентних прав іншій компанії; ви можете захистити вашу компанію від судової тяганини та / або пред'явити ваш патент проти затверджується патенту яка звинувачує компанії. Ви можете допомогти вашій компанії укласти стратегічні союзи з іншими компаніями, які хочуть взяти ліцензію на патенти вашої компанії і тим самим збільшити свої власні портфелі патентів.

Патенти, мабуть, володіють великою кількістю переваг, але нижченаведений перелік - це лише початок. Ці переваги мають значення не лише для компаній, що займаються електронною торгівлею, вони особливо важливі в сфері електронної торгівлі. Це відбувається тому, що електронна торгівля тісно пов'язана з об'єктами, які в тих країнах, де патентна охорона є для цих областей технологій, стали об'єктом патентної діяльності: телекомунікації, напівпровідники, ділові методи та програмне забезпечення.

В наші дні все більше число виробів програмного забезпечення та ділових методів охороняються у Сполучених Штатах патентами (http://www.uspto.gov/web/menu/pbmethod/). У Японії комп'ютерні програми та ділові методи можуть бути запатентовані за умови, що вони розглядаються як технічних, а не просто абстрактних ідей (див. веб-сайт Японського патентного відомства http://www.jpo.go.jp/infoe/tt1211- 055.htm). У відповідності з Європейською патентною конвенцією і патентним законодавством ряду країн-членів Європейської патентної організації комп'ютерні програми та ділові методи як такі поки ще виключені зі сфери охорони патентів. Однак на практиці в останні роки підхід до цього змінився в результаті тривалих, активних і суперечливих дискусій і багатьох рішень. Вважається, що в наші дні більшість заявок не заявляють про абстрактних програмах або ділових методах, а описують, наприклад, такі технічні засоби як комп'ютерні мережі, необхідні для здійснення цих програм або методів. Щоб бути патентоспроможним програми або методи повинні вирішити яку-небудь проблему неочевидним шляхом; іншими словами патентоспроможним вони стають не завдяки комерційної винахідливості (див. веб-сайт ЕПО за адресою: http://www.european-patent-office.org/news/ pressrel/2000_08_18_e.htm і http://www.european-patent-office.org/epo/pubs/oj000/7_00/7_3070.pdf і. У ряді інших країн комп'ютерні програми та ділові методи поки що не є патентоспроможним.

Як приклад можна навести наступні ділові методи: патенти на використання єдиного натискання клавіші для замовлення товарів у рамках угоди в режимі он-лайн, патенти на систему бухгалтерського обліку в режимі он-лайн і на систему заохочення ініціативи в режимі он-лайн. Багато було написано про патенти на ділові методи. У більшості країн патенти видаються на широкий ряд винаходів. У сфері електронної торгівлі розумно отримати юридичну консультацію з питання про те, чи можуть бути патентоспроможним будь-які нові ділові методи, що розвиваються вашою компанією.

Патенти в електронній торгівлі важливі, оскільки електронна торгівля пов'язана з великим обсягом ліцензування, укладання контрактів, передачі роботи на бік і стратегічними відносинами.

Ви захочете, наприклад, розглянути питання про доцільність здійснення у вашій компанії програми стимулювання винахідницької діяльності серед своїх співробітників. Такі програми дуже поширені, особливо в країнах, де немає законодавства про винагороду співробітників за винахідницьку діяльність, а також у великих компаніях, і звичайно вони передбачають надання бонусних акцій та / або виплату готівкових грошей службовцю або групі службовців - авторам винаходів. Винагорода зазвичай відбувається поетапно, причому невелику винагороду дається в момент, коли розкриття винаходу співробітника реєструється тією особою в компанії, яка відповідає за це. Інша частина винагороди дається в момент подачі заявки на патент і ще одна частина дається в момент видачі патенту. Причому остання частина винагороди є найбільшою. Публічні об'яви та церемонії нагородження є гарним засобом для підтримки моралі та заохочення творчої діяльності.

Як правило, патенти реєструються спочатку в патентному відомстві вашої власної країни, але в більшості інших країн будь-яка особа може також зареєструвати патент у відповідному національному патентному відомстві або, коли умови для цього виконані, може використовувати Міжнародне бюро ВОІВ для подачі заявки на патент відповідно до Договором про патентну кооперацію (PCT). Використання PCT дає вам можливість подачі заявки на патент в цілому ряді країн. Є також регіональні патентні відомства, наприклад, Європейське патентне відомство (ЄПВ), Патентне відомство Ради зі співробітництва країн Затоки, Африканська регіональна організація промислової власності (АРОПС) і Африканська організація інтелектуальної власності (AOIC). Див: «Охорона вашої інтелектуальної власності за кордоном».

Якщо ви займаєтеся електронною торгівлею як вашим основним бізнесом або важливою частиною вашого бізнесу, то вам знадобиться прийняти рішення про те, чи є охорона патентів на винаходи ваших службовців корисним інструментом для вашої компанії, і якщо так, то куди ви повинні подавати заявку.

Додаткову інформацію про ділові методи в сфері патентів див.:

Відомство США по патентах і товарних знаках (ВПТЗ)

http://www.uspto.gov/web/menu/pbmethod/)

NOLO (http://www.nolo.com/encyclopedia/articles/ilaw/method_patents.html)

споживчий проект за технологією (http://www.cptech.org/ip/business/ # survey)

з питання подачі заявок на регіональний або міжнародний патент см.:

Договір про патентну кооперацію (PCT) (http://www.wipo.int/pct/en/index.html)

Європейське патентне відомство (ЄПВ) (http://www.european-patent-office.org)

Японське патентне відомство (ЯПВ) (http://www.jpo/go/jp)

Африканська регіональна організація промислової власності (АРОПС) (http://www.aripo.wipo.net/)

з питання про ліцензування патентів та інших видах ліцензування див: http://www.les.org

Питання ІВ при поширенні змісту через мережу Інтернет. В останні роки дуже багато говорилося про незаконне поширення в Інтернеті творів мистецтва, фотографій, рукописів та програмного забезпечення («зміст»). Ця недозволених завантаження часто порушує національні закони про авторське право. З урахуванням тої простоти, з якою цифрові файли можуть бути завантажені, недозволене копіювання змісту стало однією з найважливіших проблем, які ведуть до втрати мільйонів доларів в доходи власників цих прав.

Займаючись електронною торгівлею, важливо охороняти свої права інтелектуальної власності на Інтернеті. Це можна зробити різним шляхом. Завжди чітко ідентифікуйте ваш зміст або за допомогою позначки про авторське право, або за допомогою будь-якого іншого вказівки про право власності. Можливо ви просто захочете вказати користувачам, що вони можуть і що вони не можуть робити з вашим вмістом. Ніколи не поширюйте самі і не дозволяйте завантажувати третім особам зміст, який не належить вашій компанії, і встановлюйте програми, що допомагають переконатися в тому, що ваші співробітники розуміють політику вашої компанії в цьому відношенні.

Справа Напстера в Сполучених Штатах отримало міжнародний резонанс у зв'язку з невирішеною завантаженням музичних файлів. Це справа, в результаті розгляду якого суд прийняв рішення про постійне заборону Напстеру користуватися своєю системою обміну файлів, стало справою про «непрямому порушення», оскільки позивач стверджував, що Напстер не копіював файли сам, а полегшував незаконне копіювання для користувачів системи. Інші справи стануть пробним каменем для законодавства у цій галузі. Можливо будуть розглядатися інші питання і будуть отримані різні результати в різних країнах, але урок Набстера полягає в тому, що для компанії, що займається електронною торгівлею, важливо переконатися в тому, що вона проводить чітку політику проти незаконного копіювання файлів і проти будь-яких дій, які заохочують або полегшують таке копіювання. для компанії, що діє в сфері електронної торгівлі, також важливо переконатися в тому, що службовці не отримали доступ і не мають у своїх системах будь-яких недозволених копій програмного забезпечення або іншого змісту. Ваша компанія повинна мати у своєму розпорядженні системою профілактики, виховання та контролю, з тим щоб переконатися, що ваші службовці не вдаються до незаконному копіюванню програмного забезпечення, навмисне чи не навмисне.

Всі службовці повинні знати про проведену компанією політиці протидії незаконному використанню інтелектуальної власності, а вище керівництво повинно відповідати за регулярний огляд ділової практики компанії з тим, щоб переконатися, що така політика дійсно проводиться в життя. Доцільно оцінювати ситуації, в яких виявляється порушення цієї політики, з тим щоб визначити, які слід вжити дисциплінарних заходів.

Деякі компанії все ширше використовують технічні засоби для охорони вмісту в Інтернеті за допомогою маркування, шифровки та інших систем позначення та блокування. Ділові консорціуми та окремі компанії пропонують електронні системи управління авторським правом і вважають ці системи одним із видів застосування технічних засобів для контролю за використанням змісту.

З питання про піратство програмного забезпечення див:

Альянс по програмному забезпеченню фірм і корпорацій (http://www.bsa.org)

Про піратство в музиці див.:

Американська асоціація звукозаписної промисловості (http://www.riaa.org)

Асоціація музичних видавців (http://www.mpa.org)

Про системи електронного управління авторським правом див.:

Асоціація американських видавців (AAI) (http://www.publishers.org/home/drm.pdf)

Всесвітній консорціум веб (http://www.w3.org/2000/12/drm-ws/)

Обережність при розкритті інформації в Інтернеті. Успіх бізнесу в сфері електронної торгівлі в значній мірі пояснюється маркетингом продукції та послуг в Інтернеті, часто через веб-сайт компанії або через листування, що здійснюється керівництвом і співробітниками компанії. У процесі цієї діяльності по збуту важливо охороняти вашу інтелектуальну власність в сфері електронної торгівлі. Необережне розголошення інформації може зашкодити і навіть звести нанівець ваші права інтелектуальної власності. Це відбувається тому, що відповідно до законодавства багатьох країн охорона не може бути надана патенту, якщо винахід було оприлюднено навіть на короткий період часу до подачі заявки на патент.

Оприлюднення комерційної таємниці може також зашкодити її охорону в якості інтелектуальної власності. Публікація текстів, творів мистецтв, програмного забезпечення та інших творів, що охороняються відповідно до законодавства про авторське право, в деяких випадках може призвести до втрати прав інтелектуальної власності.

Перш ніж розкрити вашу інтелектуальну власність в Інтернеті (див. ревізію ІВ, яку ви провели), переконайтеся з вашим юридичним радником в тому, що ви необережно не завдає шкоди будь-якому активу ІВ.

У рівній мірі важливо уникати розкриття інтелектуальної власності третьої сторони. Виявляйте обережність при афішування винаходів або творів інших компаній на вашому веб-сайті, як зазначено вище. Додаткову інформацію про розкриття ІВ див. http://www.uspto.gov

Важливі контракти та ІВ. При розробці та охорони ІВ вашої компанії, що займається електронною торгівлею, вам треба бути уважним у відношенні контрактів. Контракти і ІС нерозривні один від одного. Будь-який контракт, підписаний вашої компанією, є важливим і має бути зроблено все, щоб переконатися, що ви сприяєте підвищення цінності, а не завдаєте шкоди вашим активів ІВ. Це відбувається тому, що в рамках контрактів права ІВ можуть бути продані, стати об'єктом ліцензії або просто віддані. Неправильно складені контракти можуть призвести до суперечок і невиправданих витрат.

Небезпечні ризиками контракти з співробітниками та підрядниками, угоди про розробки, угоди про проект веб-сайту, угоди про передачу ліцензії на вашу продукцію або ІВ іншої компанії (віддача в ліцензію), угоди про отримання ліцензії на продукцію або ІВ іншої компанії (отримання ліцензії) , угоди про поширення, угоди про ліцензування назв доменів та товарних знаків і патентні ліцензії, перехресні ліцензії та пули. Це досить не повний перелік.

Якщо ви використовуєте співробітників, підрядників, консультантів або інші компанії для розвитку вашої ІС (наприклад, підрядника, що становить програмне забезпечення), важливо укласти контракт з цією особою або органом до початку роботи. Вже на самій ранній стадії роботи можуть виникнути важливі права і підрядчик може стати автором або власником своєї роботи або можливо спільним власником. В контракті повинно бути зазначено, кому належить створена ІВ і яка її подальша доля.

Найбільшу економічну цінність ІС представляє її використання в цілях ліцензування. Це може бути зроблено у вигляді ліцензування продукції (наприклад, ліцензування продукту, який містить таку ІВ, як програмне забезпечення та матеріали курсу) або у вигляді чистих ліцензій ІС (наприклад, ліцензії, за допомогою якої інша компанія отримує право використовувати патент).

Як зазначено вище в позиціях 3 та 6 контрольного списку важливо укласти контракти, в яких чітко зазначено, які права ви маєте або які права ви дали іншим для цілей використання ІВ.

У більшості країн передбачається, що контракти не повинні бути занадто довгими або навіть занадто формальними. Вони повинні бути чіткими та містити точні формулювання, що стосуються прав ІВ. Як зазначено вище, важливо отримати пораду експерта в цій області. Часто корисно, щоб експерт дав вам ряд зразків, які можна використовувати в якості стартової бази для вирішення різних ситуацій, пов'язаних з ІВ. У цьому випадку ви можете діяти ефективно, але завжди корисно перевірити з вашим юридичним радником текст будь-якої угоди, що стосується ІВ, до його укладення, яким би простим він не представлявся.

Гарна думка для ділової практики в сфері електронної торгівлі зберігати копії всіх контрактів, що торкаються ІВ. Це дисциплінує і дозволяє вам поглянути на питання, коли вони стають раптом важливими пізніше. В якості прикладу слід відзначити, що, що торкаються ІС контракти, стануть виключно важливими, якщо ваша діяльність у сфері електронної торгівлі пов'язана з придбанням, злиттям, продажем активів або інвестиційної угодою. Звертайте увагу на положення контрактів, які впливають на вашу можливість продавати, віддавати в ліцензію, передавати або передавати ІС вашої компанії.

Проблеми ІВ в міжнародних угодах в галузі електронної торгівлі. Однією з найбільш характерних особливостей електронної торгівлі є той факт, що вона здійснюється у всьому світі. Інтелектуальна власність може використовуватися і ставати об'єктом ліцензій у багатьох країнах одночасно. Глобальність операцій у сфері електронної торгівлі торкається інтелектуальну власність з цілого ряду напрямків. Вона ускладнює пошук порушника та захист прав інтелектуальної власності, які були порушені в Інтернеті. Не дуже ясно, яким судам підсудні спори, пов'язані з електронною

торгівлею та інтелектуальною власністю. Крім того, що стосуються ІС закони зовсім різними в різних країнах і тому різним може бути й рівень охорони.

Щодо ваших дій в сфері електронної торгівлі можуть бути подані судові позови і навпаки ви можете шукати захисту в національних судах. Однак на такі справи впливають різні процедурні питання. Якщо сторони в суперечці знаходяться в різних країнах, то досить важко встановити, в який суд можна і необхідно звертатися. Суд може прийняти або не прийняти справу до розгляду в залежності від багатьох факторів, перш за все від зв'язку між сторонами і країною. На практиці для того, щоб позов досяг своєї мети, відповідач повинен проживати в тій країні, в якій подано позов. Також складним є питання про те, який закон слід застосовувати, особливо, якщо законодавство країн-учасників спору є досить різним. І нарешті, навіть якщо справа виграна, буде вельми складно забезпечити виконання судового рішення в іншій країні.

Міжнародний арбітраж є одним з шляхів вирішення міжнародних спорів у сфері електронної торгівлі, хоча як правило участь у ньому є добровільним і не може бути примусовим. Положення про арбітраж можуть бути узгоджені в тексті контрактів, і в цьому випадку сторони пізніше зобов'язані вдаватися до послуг арбітражу. Вам слід подумати про те, щоб вказувати на обов'язковість звернення в міжнародний арбітраж у всіх, пов'язаних з електронною торгівлею контрактах, що передбачають міжнародні угоди. Центр ВОІВ з арбітражу та посередництва спеціалізується на врегулювання міжнародних суперечок і таким чином чудово підходить для вирішення міжнародних проблем ІС, що виникають в електронній торгівлі. Стандартні положення про договірному арбітражі викладені на веб-сайті (див. нижче).

Додаткову інформацію про арбітраж і посередництво див.:

Центр ВОІВ з арбітражу та посередництва (http://www.arbiter.wipo.int)

Примітка.

При написанні змістовної частини модулів були використані, зокрема, такі джерела:

Дутов М. М. Правове забезпечення розвитку електронної комерції. – Автореф… дис. Канд. Юрид.наук: 12.00.04 // www.iub.at.ua

Ефремкина О.В. Электронная торговля в ЕС (основные правовые аспекты) // http://eulaw.edu.ru/documents/articles/eu12.htm

Жилінкова І., Правове регулювання Інтернет-відносин //Право України.- 2003.- № 5.-С. 124-128

Интеллектуальная собственность в электронной торговле // http://www.wipo.int/ru/sme

Макарова М.В. Електронна комерція: Посібник для студентів вищих навчальних закладів. Київ. Видавничий центр „Академія».2002. - 272 с.

Плескач В.Л., Затонацька Т.Г. Електронна комерція: Підручник. – К.: Знання, 2007. – 535 с.

Чучковська А., Електронна комерція: деякі проблеми правового регулювання//Право України. - 2003.- № 1.-С. 111-116

Шевченко О., Електронна комерція в умовах чинного законодавства //Право України.- 2003.- № 10.-С. 142-143

E-commerce Law (MLAW0139). Module Guide 2008/9 //

http://www.studynet1.herts.ac.uk/crs/09/MLAW01390909.nsf/Homepage?readform

4. Перелік питань для самоконтролю

1. Поняття «нової» (віртуальної) економіки Ознаки нової економіки та наслідки її розвитку.
2. Поняття електронного бізнесу.
4. Поняття електронної комерції.
5. Служби Інтернету.
6. Web-сайт - як основа бізнесу в Інтернеті.
7. Поняття доменного імені.
8. Принципи вибору доменного імені.
9. Порядок реєстрації доменного імені.
10. Методи шифрування інформації в комп'ютерних системах та мережах.
11. Поняття цифрового підпису.
12. Методи забезпечення захисту у платіжних системах в Інтернет.
13. Поняття електронного сертифікату.
14. Порядок отримання електронного сертифікату
15. Поняття мобільної торгівлі
16. Поняття телевізійної торгівлі.
17. Основні види правопорушень у сфері електронної комерції та їх характеристика.
18.. Правові проблеми реалізації схем електронної комерції.
19. Українське законодавство у сфері електронної комерції.
20. Міжнародно-правове регулювання електронної комерції

Самотестування з електронної торгівлі

1. Чи включає чи інтелектуальна власність:
a) патенти?
b) корисні моделі?
c) товарні знаки?
d) товарну упаковку?
e) географічні вказівки?
f) промислові зразки?
g) топології інтегральних мікросхем?
h) захист від недобросовісної конкуренції, включаючи / або охорону комерційної таємниці?
i) авторське право?
j) суміжні права?
Дивись посилання для відповіді: http://www.wipo.int/ru/sme/e_commerce/ip_ecommerce.htm

2. Чи може програмне забезпечення охоронятися авторським правом і патентами?
Дивись посилання для відповіді (про авторське право і патенти):
http://www.wipo.int/ru/sme/e_commerce/ip_assets.htm
http://www.wipo.int/ru/sme/e_commerce/patents.htm

3. Щоб пред'являти свої авторські права на який-небудь об'єкт, чи повинен він бути зареєстрований в урядовій установі?
Дивись посилання для відповіді: http://www.wipo.int/ru/sme/e_commerce/ip_assets.htm

4. Чи є патенти цінними для компанії, що займається електронною торгівлею, чи збут продукції є більш важливим?

Дивись посилання для відповіді: http://www.wipo.int/ru/sme/e_commerce/patents.htm

5. Чи рекомендується складати та підписувати угоди про дизайн веб-сайту після того як дизайн веб-сайту зроблено і веб-сайт діє?
Дивись посилання для відповіді: http://www.wipo.int/ru/sme/e_commerce/design_issues.htm

6. Перш ніж використовувати або поширювати музику на веб-сайті необхідно перевірити, кому належить ця музика, і отримати дозвіл від тієї особи, корпорації, товариства по збору роялті або іншої установи, хто має право на розповсюдження?
Дивись посилання для відповідей (про дизайн веб-сайту та розповсюдженні):
http://www.wipo.int/ru/sme/e_commerce/design_issues.htm
http://www.wipo.int/ru/sme/e_commerce/internet_content.htm

7. Чи можна зареєструвати назву домену, яка включає товарний знак іншої компанії, так як не існує ефективного способу забезпечення міжнародних прав інтелектуальної власності?
Дивись посилання для відповіді: http://www.wipo.int/ru/sme/e_commerce/domain_names.htm

8. Чи правильно починати роботу над проектами в області високих технологій, не чекаючи підписання контракту, затримуваного підготовкою тексту, і з'ясувати правові аспекти пізніше?
Дивись посилання для відповіді: http://www.wipo.int/ru/sme/e_commerce/contracts.htm

9. Чи можуть національні закони вимагати передачі в арбітраж міжнародних спорів у сфері ІВ?
Дивись посилання для відповіді: http://www.wipo.int/ru/sme/e_commerce/transactions.htm

10. Чи можуть фахівці, що працюють над технічними проектами, використовувати Інтернет для обміну ідеями та новими винаходами, оскільки заявки на патенти щодо таких ідей завжди можуть подаватися пізніше, без шкоди інтересам ?
Дивись посилання для відповіді: **http://www.wipo.int/ru/sme/e_commerce/disclosures.htm**

ДОДАТКИ

Додаток 1. Директива 2000/31/ЄС Європейського парламенту та Ради від 8 червня 2000 року про деякі правові аспекти інформаційних послуг, зокрема,електронної комерції, на внутрішньому ринку.

("Директива про електронну комерцію")*Офіційний журнал L 178, 17.07.2000, с.0001-0016*

ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ ТА РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ,

Беручи до уваги Договір про утворення Європейського Співтовариства та його статті 47(2), 55 та 95,

Беручи до уваги пропозиції Комісії (1),

Беручи до уваги висновки Економічного і Соціального Комітету (2),

Діючи відповідно до порядку, передбаченого статтею 251 Договору (3),

Враховуючи, що:

1) Європейський Союз прагне розвивати якомога тісніші зв'язки між державами та народами Європи з метою забезпечення економічного та соціального прогресу; відповідно до статті 14(2) Договору, внутрішній ринок включає в себе зону без внутрішніх кордонів, в якій забезпечується вільний рух товарів, послуг та свобода організації; розвиток інформаційних послуг в межах зони без внутрішніх кордонів життєво важливий для скасування бар'єрів, які розділяють європейські народи.

2) Розвиток електронної комерції в межах інформаційного суспільства пропонує істотні можливості зайнятості в межах Співтовариства, зокрема, в малих та середніх підприємствах, та стимулюватиме економічне зростання і інвестування європейськими компаніями в інноваційні технології, а також може посилити конкурентоспроможність європейської промисловості, забезпечуючи доступ до Інтернету всім громадянам.

3) Законодавство та характеристики правопорядку Співтовариства є життєво важливими для наділення громадян та операторів європейських держав можливістю, незважаючи на кордони, повноцінно користуватися перевагами, які надає електронна комерція; таким чином, ця Директива має на меті забезпечити високий рівень правової інтеграції держав Співтовариства з тим, щоб сформувати реальну зону без внутрішніх кордонів для обміну інформаційними послугами.

4) Важливо забезпечити отримання переваг для електронної комерції від внутрішнього ринку і, таким чином досягти високого рівня інтеграції в межах Співтовариства, як це передбачає Директива Ради 89/552/ЄЕС від 3 жовтня 1989 року про координацію визначених положень, передбачених законом, постановою чи адміністративним актом в державах- членах стосовно заняття діяльністю в сфері телевізійного мовлення (4).

5) Розвиткові інформаційних послуг в межах Співтовариства перешкоджає ряд правових перепон на шляху до ефективного функціонування внутрішнього ринку, які роблять реалізацію свободи організації та свободи надання послуг менш привабливою; ці перешкоди виникають з розбіжностей в законодавстві та з правової невизначеності щодо вибору тих норм національного законодавства, які мають бути застосовані до таких послуг; за умов відсутності координації та адаптації законодавства у відповідних сферах, перешкоди можуть бути обґрунтовані на підставі прецедентного права, відповідно до якого здійснює судочинство Європейський Суд Справедливості; має місце правова невизначеність щодо того, до якої міри держави-члени можуть контролювати послуги, що надаються іншою державою-членом.

6) Беручи до уваги цілі держав Співтовариства, статей 43 та 49 Договору та вторинного права держав Співтовариства, ці перешкоди мають бути скасовані шляхом координації певних національних законів та шляхом уточнення правових концепцій на рівні Співтовариства до міри, необхідної для ефективного функціонування внутрішнього ринку; регулюючи лише окремі питання, які спричиняють виникнення проблем для внутрішнього ринку, ця Директива повною мірою узгоджується із потребою поважати принцип субсидіарності, як визначено в статті 5 Договору.

7) З тим, щоб досягти правової визначеності та забезпечити впевненість споживача, ця Директива повинна закласти чітку та загальну структуру з метою регулювання визначених правових аспектів електронної комерції на внутрішньому ринку.

8) Метою цієї Директиви є створення правової структури для забезпечення вільного переміщення інформаційних послуг між державами-членами, а не гармонізація сфер дії кримінального права, як такого.

9) Вільне переміщення інформаційних послуг в багатьох випадках може відобразити в праві держав Співтовариства більш загальний принцип, а саме – принцип свободи вираження, як це передбачено в статті 10(1) Конвенції про захист основних прав та свобод людини, ратифікованої усіма державами-членами; з цієї причини директиви, що регулюють постачання інформаційних послуг, повинні забезпечувати право вільно

займатись цією діяльністю відповідно до статті 46(1) Договору, на яку поширюються обмеження, що містяться в положеннях пункту 2 тієї статті та в статті 46(1) Договору; ця Директива не має на меті впливати на основоположні норми і принципи національного законодавства, що регулюють свободу самовираження.

10) Відповідно до принципу пропорційності, заходи, передбачені в цій Директиві, суворо обмежені до мінімуму, необхідного для досягнення ефективного функціонування внутрішнього ринку; у випадку, коли необхідні дії на рівні Співтовариства з метою гарантування зони без внутрішніх кордонів, чого і потребує електронна комерція, ця Директива повинна забезпечити високий рівень захисту цілей, які представляють загальний інтерес, зокрема, у сфері захисту неповнолітніх та людської гідності, захисту прав споживача та здоров'я громадян; відповідно до статті 152 Договору захист здоров'я громадян є суттєвим компонентом політики інших держав

Співтовариства.

11) Ця Директива застосовується без перешкод до рівня захисту, зокрема, здоров'я громадян та інтересів, як це передбачено актами Співтовариства; серед інших, Директива Ради 93/13/ЄЕС від 5 квітня 1993 року про нечесні строки в контрактах споживачів (5) та Директива 97/7/ЄС Європейського парламенту та Ради від 20 травня 1997 року про захист прав споживачів по відношенню до контрактів, що укладаються на відстані (6), складають важливий елемент захисту споживачів у сфері укладання контрактів; тіж директиви також застосовуються до інформаційних послуг; те ж базове законодавство держав Співтовариства, яке повною мірою застосовується до інформаційних послуг, також включає в себе, зокрема, Директиву Ради 84/450/ЄЕС від 10 вересня 1984 року про порівняльну рекламу та рекламу, що вводить в оману(7), Директива Ради 87/102/ЄЕС від 22 грудня 1986 року про зближення законів, постанов та адміністративних положень держав-членів в сфері операцій із споживацьким кредитом(8), Директива Ради 93/22/ЄЕС від 10 травня 1993 року про інвестиційні послуги в сфері цінних паперів(9), Директива Ради 90/314/ЄЕС від 13 червня 1990 року про груповий туризм (10), Директива 98/6/ЄС Європейського парламенту і Ради від 16 лютого 1998 року про виробництво, орієнтоване на споживача, при вказівці на ціни на продукти, що пропонуються споживачам(11), Директива Ради 92/59/ЄЕС від 29 червня 1992 року про загальну безпеку продукції(12), Директива 94/47/ЄС Європейського парламенту та Ради від 26 жовтня 1994 року про захист покупців у певних сферах укладення контрактів, що стосуються купівлі права на використання нерухомості на тимчасовій

основі(13), Директива 98/27/ЄС Європейського парламенту та Ради від 19 травня 1998 року про судову заборону захищати інтереси споживачів (14), Директива Ради 85/374/ЄЕС від 25 липня 1985 року про зближення законів, постанов та адміністративних положень стосовно несення відповідальності за дефективні продукти (15), Директива 1999/44/ЄС Європейського парламенту та Ради від 25 травня 1999 року про визначені аспекти продажу товарів споживання та взаємодіючі гарантії (16), майбутня Директива Європейського парламенту та Ради стосовно дистанційного маркетингу споживацьких фінансових послуг та Директива Ради 92/28/ЄЕС від 31 травня 1992 року про рекламування медичної продукції (17); ця Директива має застосовуватись без перешкод до Директиви 98/43/ЄС Європейського парламенту та Ради від 6 липня 1998 року про зближення законів, постанов та адміністративних положень держав-членів стосовно рекламування та спонсорування виробництва тютюнової продукції (18), прийнятих в межах структури внутрішнього ринку; ця Директива доповнює інформаційні вимоги, визначені вищезазначеними директивами, а, зокрема, Директивою 97/7/ЄС.

12) Зі сфери застосування цієї Директиви слід виключити певні види діяльності на підставі того, що свобода надання послуг у цій сфері на цьому етапі не може гарантуватись відповідно до Договору чи існуючого вторинного законодавства; виключення цієї діяльності не усуває ніяких засобів, які можуть бути необхідними для ефективного функціонування внутрішнього ринку; оподаткування, зокрема, податок на додану вартість, накладений на велику кількість послуг, передбачених цією Директивою, має бути виключене зі сфери застосування цієї Директиви.

13) Ця Директива не має на меті встановлювати норми щодо податкових зобов'язань чи визначати засоби, що використовують держави Співтовариства у фіскальній сфері електронної комерції.

14) Захист осіб в сфері переробки особистої інформації регулюється виключно Директивою 95/46/ЄС Європейського парламенту та Ради від 24 жовтня 1995 року про захист осіб в сфері переробки особистої інформації та вільного переміщення такої інформації (19) та Директивою 97/66/ЄС Європейського парламенту та Ради від 15 грудня 1997 року стосовно переробки особистої інформації та захисту таємниці у сфері телекомунікацій (20), які повною мірою можуть бути застосовані до інформаційних послуг; ці директиви вже визначають правову структуру Співтовариства в сфері обробки особистої інформації і, таким чином, немає потреби роз'яснювати цю проблему в даній Директиві з тим, щоб забезпечити ефективне функціонування внутрішнього ринку, зокрема, вільне переміщення особистої інформації між державами-членами; запровадження та застосування цієї Директиви має бути здійснене у повній відповідності із принципами, що стосуються захисту особистих даних, зокрема, стосовно надсилання комерційного повідомлення без згоди одержувача та відповідальності посередників; ця Директива не може перешкоджати анонімному використанню відкритих мереж, таких як Інтернет.

15) Конфіденційність повідомлень гарантується статтею 5 Директиви 97/66/ЄС; згідно із цією Директивою держави-члени повинні заборонити будь-який вид перехоплень чи контролю над такими повідомленнями іншими суб'єктами, відмінними від відправників та одержувачів, окрім випадків законного дозволу на таку діяльність.

16) Виключення азартних ігор зі сфери застосування цієї Директиви поширюється виключно на лотереї та парі, що передбачає ставку із грошовою вартістю; це не передбачає рекламну конкуренцію чи ігри, метою яких є стимулювання продажу товарів чи послуг, і в яких оплата, якщо така буде передбачатись, служить лише для придбання товарів чи послуг, що рекламувались.

17) Визначення поняття "інформаційне суспільство" вже міститься в законодавстві держав Співтовариства у Директиві 98/34/ЄС Європейського парламенту та Ради від 22 червня 1998 року, яка передбачає процедуру для постачання інформації в області технічних стандартів та постанови і правила надання інформаційних послуг (21) та Директиві 98/84/ЄС Європейського парламенту та Ради від 20 листопада 1998 року про правовий захист послуг, що ґрунтуються чи складаються з умовного доступу (22); це визначення включає в себе будь-які послуги, що надаються, як правило, за винагороду на відстані за допомогою електронного обладнання, що використовується для переробки (включаючи цифрове стиснення) та зберігання інформації та за індивідуальним запитом одержувача послуг; ті послуги, про які йдеться у вказівному списку в Додатку V до Директиви 98/34/ЄС, які не передбачають переробки та збереження інформації, не регулюються цим визначенням.

18) Інформаційні послуги охоплюють широкий спектр сфер економічної діяльності, що здійснюється в оперативному режимі; ця діяльність, зокрема, може включати в себе продаж товарів в оперативному режимі; не включаються такі сфери діяльності, як постачання товарів, як таке, або постачання послуг в автономному режимі; інформаційні послуги не обмежуються виключно послугами, які забезпечують інтерактивне укладання договорів, але, оскільки вони є економічною діяльністю, то включають в себе і послуги, надання яких не оплачується їх одержувачами, такими як ті, хто пропонує інтерактивну інформацію чи комерційні повідомлення або ті, хто забезпечує механізми, що дозволяють пошук, доступ та отримання інформації; інформаційні послуги також включають в себе послуги, що складаються з передачі інформації через мережу зв'язку, надання доступу до мережі зв'язку чи послуги по розміщенню інформації, що надається одержувачем послуг; телевізійне мовлення в тому сенсі, в якому воно вживається в Директиві ЄЕС/89/552, та радіомовлення не є інформаційними послугами, оскільки вони надаються не за індивідуальним запитом; послуги, що передаються від одного місця до іншого, такі як надання відео послуг за запитом, або відправлення комерційних повідомлень за допомогою електронної пошти, навпаки, є інформаційними послугами; використання електронної пошти чи еквівалентного індивідуального зв'язку, наприклад, фізичними особами, які діють не з метою здійснення професійної чи комерційної діяльності, в тому числі використання ними вищезазначеного виду пошти та зв'язку для укладення контрактів між такими особами, не є інформаційними послугами; відносини між службовцем та його роботодавцем, засновані на контракті, не є наданням інформаційних послуг; діяльність, яка через саму сутність своєї природи не може здійснюватись на відстані та за допомогою електронних засобів, така як законний

аудит рахунків компаній чи надання консультації лікарем, що вимагає фізичного дослідження пацієнта, не є наданням інформаційних послуг.

19) Місце заснування постачальника послуг має визначатися відповідно до прецедентного права Суду Справедливості, відповідно до якого концепція заснування передбачає фактичне здійснення економічної діяльності через фіксовану установу протягом невизначеного періоду часу; ця вимога також виконується, якщо компанія створюється на певний період; місце заснування компанії, що надає послуги через вебсайт Інтернету, не є місцем розташування технологій, що забезпечують підтримку цьому вебсайту, або місцем, з якого цей вебсайт доступний. Це місце, де компанія здійснює свою економічну діяльність; у випадках, якщо постачальник має декілька місць заснування компанії, важливо визначити, з якого з них надаються відповідні послуги; у тому випадку, якщо важко визначити, з якого із декількох місць заснування надається певна послуга, таким вважається місце знаходження центру діяльності компанії, який має відношення до цієї конкретної послуги.

20) Визначення "одержувач послуг" охоплює усі види використання інформаційних послуг як особами, які надають інформацію всередині відкритих мереж, таких як Інтернет, так і особами, які здійснюють пошук інформації в Інтернет в приватних чи професійних цілях.

21) Сфера координації застосовується без перешкод до майбутньої гармонізації законодавства держав Співтовариства стосовно надання інформаційних послуг та майбутнього законодавства, прийнятого на національному рівні відповідно до законодавства Співтовариства; сфера координації охоплює лише вимоги, що стосуються інтерактивної діяльності, такої як інтерактивна інформація, інтерактивна реклама, інтерактивні покупки, інтерактивне укладання контрактів, і не стосується правових вимог держав-членів щодо товарів, таких як стандарти безпеки, зобов’язання щодо маркування чи відповідальність за товари, або вимог держав-членів стосовно доставки чи перевезення товарів, включаючи розподіл медичних продуктів; сфера координації не охоплює здійснення переважного права купівл державними органами товарів, таких як твори мистецтва.

22) Надання інформаційних послуг контролюється від самого початку діяльності з метою забезпечення ефективного захисту громадських інтересів; з цією метою необхідно забезпечити надання такого захисту з боку компетентного органу не лише для громадян власної держави, але й для громадян всього Співтовариства; з метою посилення взаємної довіри між державами-членами важливо чітко наголосити на відповідальності з боку держави-члена, з території якої надходять послуги; більш того, з метою ефективного гарантування свободи надання послуг та правової визначеності для постачальників та одержувачів послуг, надання таких інформаційних послуг, в принципі, має підпорядковуватись законодавству держави-члена, на території якої знаходиться місце заснування постачальника послуг.

23) Ця Директива не має на меті ні встановлювати додаткові норми стосовно колізійного права у міжнародному приватному праві, ні зачіпає судочинство судів; положення правової норми, що застосовується, утвореної нормами міжнародного приватного права, не повинні обмежувати свободу надання інформаційних послуг, як передбачено цією Директивою.

24) На підставі цієї Директиви, незалежно від норми щодо контролю за джерелами інформаційних послуг, вживання заходів по обмеженню вільного переміщення інформаційних послуг є законним відповідно до умов, визначених у цій Директиві для держав-членів.

25) Національні суди, в тому числі і суди цивільної юрисдикції, які розглядають спори у приватному праві, можуть вживати заходів щодо відступу від свободи надання інформаційних послуг відповідно до умов, передбачених цією Директивою.

26) Держави-члени відповідно до умов, передбачених цією Директивою, можуть застосовувати свої внутрішні норми у кримінальному праві та кримінальному провадженні з метою проведення усіх слідчих та інших заходів, необхідних для затримання та переслідування злочинців без потреби повідомляти Комісію про такі заходи.

27) Ця Директива разом із майбутньою Директивою Європейського парламенту та Ради стосовно дистанційного маркетингу споживацьких фінансових послуг є внеском у створення правової структури для інтерактивного надання фінансових послуг; ця Директива не є поштовхом до майбутніх ініціатив в області фінансових послуг, зокрема, в сфері гармонізації норм поведінки; можливість (передбачена цією Директивою для держав-членів) обмеження свободи надання інформаційних послуг за певних умов з метою захисту споживачів також охоплює заходи в сфері фінансових послуг, зокрема, заходи, спрямовані на захист інвесторів.

28) Зобов'язання держав-членів не ставити умовою доступу до здійснення діяльності постачальником інформаційних послуг отримання попередньої ліцензії не поширюється на поштові послуги, які регулюються положеннями Директиви 97/67/ЄС Європейського парламенту та Ради від 15 грудня 1997 року про спільні правила розвитку внутрішнього ринку поштових послуг держав Співтовариства та вдосконалення якості послуг (23), що складаються з фізичної доставки роздрукованого повідомлення електронної пошти і не впливають на добровільні системи акредитації, зокрема, для постачальників електронних послуг по засвідченню підписів.

29) Комерційні повідомлення важливі для фінансування інформаційних послуг та для розвитку широкого спектру нових безкоштовних послуг; в інтересах захисту споживача та справедливої торгівлі комерційні повідомлення, включаючи повідомлення про знижки, рекламні пропозиції та рекламні змагання чи ігри, повинні задовольняти ряд прозорих умов; ці умови застосовуються без перешкод до Директиви 97/7/ЄС; ця Директива не впливає на положення існуючих Директив про комерційні повідомлення, зокрема, директиву 98/43/ЄС.

30) Розсилка комерційних повідомлень без згоди одержувача електронною поштою може бути небажаною для споживачів та постачальників інформаційних послуг і може завадити стабільному функціонуванню інтерактивних мереж; питання узгодження одержувачем певних форм комерційних повідомлень, що розсилаються без його згоди, не регулюються цією Директивою, але воно передбачалось Директивою 97/7/ЄС та Директивою 97/66/ЄС; в тих державах-членахxs18 т, які дозволяють розсилку комерційних повідомлень без згоди одержувача електронною поштою, має стимулюватись та полегшуватись запровадження відповідної системи фільтрації повідомлень; крім того, в будь-якому випадку комерційні повідомлення, що розсилаються без згоди одержувача, мають чітко ідентифікуватись як такі з метою посилення прозорості та полегшення функціонування такої системи фільтрації; добровільна доставка комерційних повідомлень по електронній пошті не повинна завдавати додаткових витрат для одержувача.

31) Держави-члени, які дозволяють розсилку постачальником послуг, заснованим на їх території, комерційних повідомлень без згоди одержувача електронною поштою, мають забезпечити регулярні консультації постачальників послуг між собою та поважання ними списків відмов, в яких фізичні особи, які не бажають отримувати такі комерційні повідомлення, можуть зареєструватись.

32) З метою усунути перешкоди до розвитку транскордонних послуг в межах Співтовариства, які представники професій, які регулюються законодавством держав ЄС, можуть пропонувати в Інтернет, необхідно гарантувати на рівні Співтовариства відповідність професійним нормам, спрямованим, зокрема, на захист споживачів чи здоров'я громадян; прийняття кодексів поведінки на рівні Співтовариства було б найкращим засобом визначення правил професійної етики в сфері комерційних повідомлень; розробка чи, якщо необхідно, адаптація таких правил має стимулюватись без перешкод до самостійності професійних органів та

об'єднань.

33) Ця Директива доповнює законодавство Співтовариства та національне законодавство в області професій, що регулюються законодавством держав ЄС, формуючи повну систему норм, що застосовуються у цій сфері.

34) Кожна держава-член має доповнити своє законодавство, що містить вимоги, а, зокрема, вимоги до форми, які обмежують використання контрактів за допомогою електронних засобів; вивчення законодавства, що потребує такої адаптації, має бути систематичним та охоплювати усі необхідні етапи та дії процесу укладання контракту, включаючи його зберігання; ці доповнення повинні мати на меті зробити дієвими контракти, укладені за допомогою електронних засобів; законна сила підписів в електронному вигляді регулюється Директивою 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів в межах Співтовариства (24); підтвердження отримання постачальником послуг може прийняти форму інтерактивного надання оплачених послуг.

35) Ця Директива не впливає на можливість для держав-членів формулювати чи встановлювати загальні чи специфічні вимоги для контрактів, які можуть бути задоволені за допомогою електронних засобів, зокрема, вимоги щодо гарантування електронних підписів.

36) Держави-члени можуть встановлювати обмеження на використання контрактів, укладених в електронній формі, які за законом вимагають для свого укладення залучення судів, державних органів чи осіб, які здійснюють державні повноваження; ця можливість також охоплює контракти, що вимагають залучення судів, державних органів чи осіб, які здійснюють державні повноваження, з

метою впливу на треті сторони, а також контракти, які, згідно закону, мають бути засвідчені нотаріусом.

37) Зобов'язання держав-членів усувати перешкоди до використання контрактів, укладених електронним шляхом, поширюються виключно на перешкоди, що випливають з правових вимог, а не на практичні перешкоди, що з'являються внаслідок неможливості використання у певних випадках електронних засобів.

38) Зобов'язання держав-членів усувати перешкоди для використання контрактів, укладених електронним шляхом, мають бути виконані згідно із правовими вимогами до контрактів, які передбачені в законодавстві Співтовариства.

39) Виключення до положень стосовно контрактів, укладених винятково за допомогою електронної пошти чи еквівалентного індивідуального зв'язку, що передбачено цією Директивою, стосовно інформації, що надається, та розміщення запитів не повинні, як наслідок, призводити до ігнорування постачальниками інформаційних послуг цих положень.

40) Як існуючі, так і нові розбіжності в законодавстві держав-членів та прецедентному праві стосовно відповідальності постачальників послуг, що діють як посередники, перешкоджають стабільному функціонуванню внутрішнього ринку, зокрема, шляхом послаблення розвитку транскордонних послуг та створюючи диспропорції в конкуренції; діяльність постачальників послуг за певних умов повинна бути спрямована на попередження чи припинення незаконної діяльності; ця Директива має бути відповідною основою для розвитку швидких та надійних процедур усунення та відключення доступу до незаконної інформації; такі механізми можуть бути розвинені на підставі добровільних угод між усіма зацікавленими сторонами та мають стимулюватись державами-членами; в інтересах усіх сторін, залучених до постачання інформаційних послуг, приймати та запроваджувати ці процедури; положення цієї Директиви стосовно відповідальності не повинні створювати перешкоди з боку різних зацікавлених сторін розвитку та ефективному функціонуванню технічних систем захисту та ідентифікації, засобів технічного контролю, які стали можливі завдяки розвитку цифрових технологій в рамках обмежень, передбачених Директивами 95/46/ЄС та 97/66/ЄС.

41) Ця Директива сприяє встановленню рівноваги між різними інтересами, поставленими на карту, та встановлює принципи, на яких можуть ґрунтуватись угоди та стандарти у цій області.

42) Звільнення від відповідальності, передбачене в цій Директиві, поширюється лише на випадки, коли діяльність постачальників інформаційних послуг обмежена технічним процесом дії та наданням доступу до мережі передачі даних, за допомогою якої інформація, що стає доступною для третіх сторін, передається чи тимчасово зберігається з єдиною метою – зробити передачу більш ефективною; ця діяльність має просту технічну, автоматичну та пасивну сутність, яка передбачає, що постачальник інформаційних послуг не має ні знань, ні може контролювати інформацію, що передається чи зберігається.

43) Постачальник послуг може виграти внаслідок використання каналів передачі інформації чи кешування, якщо він ніяким чином не залучений до передачі інформації; серед іншого, це вимагає незмінності інформації, яку він передає; ця вимога не поширюється на управління операціями технічного характеру, яке має місце в ході передачі, оскільки вони не змінюють цілісність інформації, що міститься при передачі.

44) Постачальник послуг, який цілеспрямовано співробітничає із одним з одержувачів інформації, з метою здійснення незаконних дій, виходить за межі діяльності стосовно каналів передачі інформації чи

кешування і, як наслідок, не може отримати вигоду від звільнення відвідповідальності, що передбачено за таку діяльність.

45) Обмеження відповідальності посередника у постачанні послуг, що передбачено цією Директивою, не впливає на можливість судових заборон різного роду; такі заборони можуть, зокрема, складатись із наказів судів чи адміністративних органів, що вимагають попередження будь-якого порушення, включаючи переміщення незаконної інформації чи відключення доступу до неї.

46) З метою отримання переваг від обмеження відповідальності постачальник інформаційних послуг, які включають в себе зберігання інформації, по отриманню фактичних знань чи обізнаності про незаконну діяльність має терміново вживати певні дії з метою усунення можливості доступу чи відключення доступу до відповідної інформації; усунення можливості доступу чи його відключення має здійснюватись при дотриманні принципу свободи самовираження та процедур, визначених для цих цілей на національному рівні; ця Директива не впливає на здатність держав-членів встановлювати

особливі вимоги, які мають бути терміново задоволені до того як інформація буде знищена чи доступ до неї буде відключений.

47) Державам-членам не дозволяється накладати на постачальників послуг зобов'язання по відслідковуванню виключно стосовно зобов'язань загального характеру; це не стосується зобов'язань по відслідковуванню в особливому випадку та, зокрема, не впливає на розпорядження, видані національними органами влади відповідно до внутрішнього законодавства.

48) Ця Директива не впливає на здатність держав-членів вимагати від постачальників послуг, які розпоряджаються інформацією, наданою одержувачами їхніх послуг, застосовувати засоби безпеки, що логічно було б очікувати з їх боку, та які мають відповідати нормам національного законодавства, з метою виявлення та запобігання певним видам незаконної діяльності.

49) Держави-члени та Комісія мають заохочувати розробку кодексів поведінки; не варто принижувати добровільний характер таких кодексів та можливість вільного вирішення зацікавленими сторонами, чи дотримуватись положень таких кодексів.

50) Важливо, щоб запропонована директива про гармонізацію певних галузей авторського права та суміжних прав в інформаційному суспільстві та ця Директива набирали чинності одночасно з метою встановлення чіткої системи правил стосовно питання відповідальності посередників за порушення в сфері авторського права та суміжних прав на рівні Співтовариства.

51) Від кожної держави-члена у випадку необхідності вимагається доповнити будь-яке законодавство, яке має на меті перешкоджати використанню механізмів вирішення спорів поза межами суду за допомогою електронних каналів; ці доповнення мають на меті зробити функціонування таких механізмів ефективним у законі та на практиці на міжнародному рівні.

52) Ефективна реалізація свобод на внутрішньому ринку потребує гарантувати жертвам ефективний доступ до засобів вирішення спорів; шкода, що може бути нанесена через інформаційні послуги, характеризується як швидкістю нанесення, так і її географічним поширенням; беручи до уваги цей особливий характер шкоди та потребу забезпечити неможливість перешкоджання державними органами влади встановлювати взаємну довіру між собою, ця Директива містить запит до держав-членів про доступність відповідних судових позовів; держави-члени мають вивчити потребу надання доступу до судових процедур за допомогою відповідних електронних засобів.

53) Директива 98/27/ЄС, що застосовується до інформаційних послуг, передбачає механізм подання позовів щодо винесення судової заборони, спрямований на захист колективних інтересів споживачів; цей механізм сприятиме вільному переміщенню інформаційних послуг шляхом забезпечення високого рівня захисту споживача.

54) Санкції, передбачені цією Директивою, застосовуються без перешкод до будь-яких інших санкцій чи засобів, передбачених національним правом; держави-члени не зобов'язані передбачати кримінальні санкції за порушення положень національного законодавства, прийнятих відповідно до цієї Директиви.

55) Ця Директива не впливає на закон, що застосовується до контрактних зобов'язань споживачів; відповідно, ця Директива не може мати наслідком позбавлення споживача захисту, наданого йому обов'язковими правилами стосовно контрактних зобов'язань за законодавством держави-члена, в якій він постійно проживає.

56) Що стосується передбачених в цій Директиві відступів від контрактних зобов'язань стосовно контрактів, укладених споживачами, то ці зобов'язання мають тлумачитись як такі, що містять інформацію про істотні елементи змісту контракту, включаючи права споживача, які мають вирішальний вплив на рішення за контрактом.

57) Європейський Суд неодноразово постановляв, що держава-член зберігає за собою право вживати заходи проти постачальника послуг, заснованого на території іншої держави-члена, але діяльність якого повністю чи переважно спрямована на територію першої держави-члена, у випадку, якщо вибір місця заснування був зроблений з метою ухилення від законодавства, яке застосовувалося б до постачальника у випадку, якби його установа була заснована на території першої держави-члена.

58) Ця Директива не повинна застосовуватись до послуг, наданих постачальником послуг, заснованим в третій державі; беручи до уваги глобальне скорочення обсягу електронної комерції, доречно було б передбачити відповідність норм Співтовариства міжнародним нормам; ця Директива без перешкод застосовується до результатів обговорень в межах міжнародних організацій (серед яких виділяються ВТО, ОЕСР, Комісія ООН з права міжнародної торгівлі) по правовим питанням.

59) Незважаючи на глобальний характер електронного зв'язку, координація національних заходів регуляції на рівні Європейського Союзу необхідна з метою уникнення фрагментації внутрішнього ринку та з метою встановлення відповідної європейської системи регуляції; така координація також має сприяти формуванню спільної та сильної переговорної позиції на міжнародних форумах.

60) З метою безперешкодного розвитку електронної комерції правова система має бути чіткою та простою, передбачливою та узгодженою із нормами, що застосовуються на міжнародному рівні таким чином, щоб їх застосування не справляло негативного впливу на конкурентоспроможність європейської промисловості чи не перешкоджало інноваціям у цій сфері.

61) Якщо ринок фактично функціонуватиме за допомогою електронних засобів в контексті глобалізації, Європейський Союз та основні не європейські зони потребують консультацій одна з одною з метою узгодження законів та процедур.

62) Співробітництво із третіми державами в області електронної комерції має зміцнюватись, а зокрема, це стосується співробітництва із державами, що подали заявку на вступ до ЄС, розвинутими державами та іншими торгівельними партнерами Європейського Союзу.

63) Прийняття цієї Директиви не перешкоджатиме державам- членам брати до уваги різноманітні соціальні та культурні наслідки, характерні для епохи інформаційного суспільства; зокрема, таке прийняття не повинно перешкоджати засобам, які держави-члени можуть приймати відповідно до законодавства держав Співтовариства з метою досягнення соціальних, культурних та демократичних цілей, беручи до уваги як свою

мовну різноманітність, національні та регіональні особливості, так і культурну спадщину, та з метою забезпечити громадський доступ до найширшої мережі інформаційних послуг; в будь-якому випадку розвиток інформаційного суспільства має забезпечити можливість доступу громадян держав Співтовариства до європейської культурної спадщини, представленої в цифровому середовищі.

64) Електронні комунікації пропонують державам-членам надзвичайні засоби постачання громадських послуг в культурній, освітній та мовній сферах.

65) Рада в своїй резолюції від 19 січня 1999 року про споживацький вимір інформаційного суспільства (25) наголосила на тому, що проблема захисту споживачів заслуговує на особливу увагу; Комісія вивчатиме сфери, в яких захист надається в недостатній мірі в контексті розвитку інформаційного суспільства та визначатиме у випадку необхідності недоліки законодавства та ті проблемні питання, які вимагають додаткових заходів; якщо буде необхідно, Комісія має зробити особливі додаткові пропозиції для виправлення цих недоліків, які таким чином будуть виявлені,

ПРИЙНЯЛИ ЦЮ ДИРЕКТИВУ**:**

ГЛАВА I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1
Цілі та сфера застосування

1. Ця Директива має на меті зробити внесок у належне функціонування внутрішнього ринку шляхом забезпечення вільного переміщення інформаційних послуг між державами-членами.

2. Ця Директива зближається до міри, необхідної для досягнення цілей, викладених в пункті 1, із певними положеннями національного законодавства про інформаційні послуги на внутрішньому ринку, заснування постачальників послуг, комерційні повідомлення, контракти, укладені за допомогою електронних засобів, відповідальність посередників, кодекси поведінки, вирішення спорів поза судом, судові позови та співробітництво між державами-членами.

3. Ця Директива доповнює законодавство держав Співтовариства, що застосовується до інформаційних послуг без перешкод до рівня захисту, зокрема, здоров'я громадян та інтересів споживачів, як передбачено актами Співтовариства та внутрішнього законодавства, відповідно до якого вони запроваджуються до тієї міри, до якої це не обмежує свободу забезпечення інформаційних послуг.

4. Ця Директива не вносить додаткові норми до міжнародного приватного права і не впливає на юрисдикцію судів.

5. Ця Директива застосовується до:

a) сфери оподаткування;

b) питань, що стосуються інформаційних послуг, на які поширюються положення директив 95/46/ЄС та 97/66/ЄС;

c) питань, що стосуються угод та практики, які регулюються законами картелю;

d) такої діяльності в сфері інформаційних послуг:

- діяльності нотаріусів тією мірою, до якої вони прямим чи опосередкованим чином здійснюють державні повноваження,

- представництва клієнта та захисту його інтересів перед судом,

- азартних ігор, які передбачають ставки грошової цінності в іграх, включаючи лотереї та угоди про парі.

6. Ця Директива не впливає на акти, прийняті на національному рівні чи на рівні Співтовариства з метою розвитку культурної та мовної різноманітності та забезпечення захисту плюралізму.

Визначення

Відповідно до мети цієї Директиви наступні терміни мають такі значення:

a) термін "інформаційні послуги" означає послуги у тому сенсі, в якому вони використовуються в статті 1(2) Директиви 98/34/ЄС, доповненої Директивою 98/48/ЄС;

b) термін "постачальник послуг" означає будь-яку фізичну чи юридичну особу, яка надає інформаційні послуги;

c) термін "заснований постачальник послуг" означає постачальника послуг, який ефективно займається економічною діяльністю, використовуючи постійну установу протягом невизначеного періоду часу. Наявність та використання технічних засобів та технологій, що вимагаються для постачання послуг, саме по собі не представляє собою установу постачальника;

d) термін "одержувач послуг" означає будь-яку фізичну чи юридичну особу, яка в професійних чи інших цілях, зокрема, в цілях пошуку інформації чи забезпечення її доступності, користується інформаційними послугами;

e) термін "споживач" означає будь-яку особу, яка діє не в цілях своєї комерційної, професійної діяльності;

f) термін "комерційне повідомлення" означає будь-яку форму повідомлення, спрямованого на пряме чи опосередковане просування товарів, послуг чи іміджу компанії, організації чи особи, яка займається комерційною, промисловою чи професійною діяльністю або реалізує професію, що регулюється законодавством держав ЄС. Комерційними повідомленнями не є наступне:

- інформація, що надає прямий доступ до діяльності компанії, організації чи особи, зокрема, ім’я домену чи адреса електронної пошти,

- повідомлення стосовно товарів, послуг чи іміджу компанії, організації чи особи, подане у самостійній формі, зокрема, за відсутності фінансових міркувань;

g) термін "професія, що регулюється законодавством держав ЄС" означає будь-яку професію в сенсі, в якому це поняття використовується в статті 1 (d) Директиви Ради 89/48/ЄЕС від 21 грудня 1998 року про загальну систему визнання дипломів про вищу освіту, які видаються по отриманню професійної освіти та навчання тривалістю щонайменш три роки (26) або в статті 1 (f) Директиви Ради 92/51/ЄЕС від 18 червня 1992 року про другу загальну систему по визнанню професійної освіти та навчання, яка доповнює Директиву 89/48/ЄЕС (27);

h) термін "сфера координації" означає вимоги, закладені в правових системах держав-членів, що застосовуються до постачальників інформаційних послуг чи до самих інформаційних послуг, незалежно від того, загальна їх природа, чи ці вимоги спеціально для них вироблені.

i) Сфера координації стосується вимог, яким постачальник послуг повинен відповідати по відношенню до:

- заняття діяльністю в сфері інформаційних послуг -- такі як вимоги щодо кваліфікації, уповноваження чи повідомлення;

- заняття діяльністю в сфері інформаційних послуг -- такі як вимоги щодо діяльності постачальника послуг, вимоги щодо якості чи сутності послуг, включаючи ті, що застосовуються до реклам і контрактів чи вимоги,

що стосуються відповідальності постачальника послуг;

ii) Сфера координації не поширюється на такі вимоги як:

- вимоги, що застосовуються до товарів, як таких,

- вимоги, що застосовуються до доставки товарів,
- вимоги, що застосовуються до послуг, які надаються відмінним від електронного шляхом.

Стаття 3

Внутрішній ринок

1. Кожна держава-член забезпечує відповідність наданих інформаційних послуг постачальником послуг, заснованим на її території, положенням національного законодавства, що застосовуються на території відповідної держави-члена, і які підпадають під сферу координації.

2. Держави-члени з причин, що знаходяться в межах сфери координації, можуть обмежувати свободу постачання інформаційних послуг з боку іншої держави-члена.

3. Пункти 1 та 2 не застосовуються до положень, передбачених в Додатку.

4. Держави-члени також можуть вживати заходів з метою ухилення від положень пункту 2 щодо наданих інформаційних послуг у випадку, якщо вони задовольняють наступні умови:

a) заходи

i) необхідні для однієї з наступних цілей:

- державної політики, зокрема щодо запобігання, розслідування, затримання та переслідування злочинців, в тому числі, захисту неповнолітніх та боротьби із будь-яким підбурюванням до ненависті на ґрунті раси, статі, релігії чи національності, та порушень людської гідності стосовно окремих осіб,
- захисту здоров'я громадян,
- державної безпеки, в тому числі забезпечення національної безпеки та оборони,
- захисту споживачів, в тому числі інвесторів;

ii) застосовуються до інформаційних послуг, які перешкоджають цілям, про які йдеться у пункті (i) або які представляють серйозний ризик перешкоджання цим цілям;

iii) пропорційні цим цілям;

b) до того як вдаватись до відповідних заходів та без перешкод для судових слухань, включаючи попередні провадження та дії, що здійснюються в рамках кримінального розслідування, держава-член:

- попросила державу-член, про яку йдеться в пункті 1, вжити заходів, а остання їх не вжила або вони були неадекватними,
- повідомила Комісію та державу-члена, про яку йдеться в пункті 1, про свої наміри вжити такі заходи.

5. У випадку крайньої необхідності держави-члени можуть відійти від умов, передбачених в пункті 4(b).

У тому ж випадку Комісія та держава-член, про яку йдеться в пункті 1, повідомляються в найкоротший строк про заходи із вказівкою причин віднесення ситуації до крайньої необхідності.

6. Без нанесення шкоди здатності держави-члена розвивати заходи, що розглядаються, Комісія вивчає сумісність повідомлених заходів із законодавством держав Співтовариства протягом найкоротшого періоду часу; у випадку, якщо буде зроблено висновок про невідповідність законодавства держав Співтовариства, Комісія просить відповідну державу-члена утриматись від будь-яких запропонованих заходів чи терміново завершити відповідні заходи.

ГЛАВА II
ПРИНЦИПИ

Частина 1.
Вимоги щодо заснування та інформації

Стаття 4

Принцип, що виключає отримання попередньої ліцензії

1. Держави-члени забезпечують, що вжиття та здійснення діяльності по постачанню інформаційних послуг може не потребувати отримання попередньої ліцензії чи будь-якої іншої вимоги, яка має таке ж значення.

2. Пункт 1 без перешкод застосовується до механізмів ліцензування, які не спрямовані винятково на інформаційні послуги або які регулюються Директивою 97/13/ЄС Європейського парламенту та Ради від 10 квітня 1997 року про спільну систему загального та індивідуального ліцензування в сфері надання телекомунікаційних послуг (28).

Стаття 5

Загальна інформація, що має бути надана

1. На додаток до інших вимог до постачання інформації, передбачених законодавством держав Співтовариства держави-члени гарантують забезпечення з боку постачальника послуг простого, прямого та стабільного доступу одержувачів послуг та компетентних органів принаймні до наступної інформації:

a) ім'я постачальника послуг;

b) географічна адреса заснованого постачальника послуг;

c) детальна інформація про постачальника послуг, включаючи адресу його електронної пошти, що дозволяє швидко з ним зв'язуватись та безпосередньо й ефективно надсилати йому повідомлення;

d) якщо постачальник послуг зареєстрований в торгівельному чи подібному реєстрі, то інформацію про цей торгівельний реєстр, в який він занесений, та реєстраційний номер або еквівалентні засоби ідентифікації постачальника послуг в цьому реєстрі;

e) якщо діяльність підлягає ліцензуванню, -- особливості відповідного контрольного органу;

f) стосовно професій, що регулюються законодавством ЄС:

- будь-який професійний орган чи подібна установа, в якій зареєстрований постачальник послуг,

- професійне звання та назва держави-члена, де воно було видане,

- посилання на професійні правила, що застосовуються на території держави-члена, де заснована установа, та містяться засоби доступу до них;

g) якщо постачальник послуг займається діяльністю, яка підлягає сплаті ПДВ, ідентифікаційний номер, про який йдеться в статті 22(1) шостої Директиви Ради 77/388/ЄЕС від 17 травня 1977 року про гармонізацію законодавства держав-членів стосовно податку з обігу – Спільна система податку на додану вартість: універсальна основа оцінки (29).

2. На додаток до інших вимог щодо інформації, визначених законодавством Співтовариства, держави-члени принаймні забезпечують, що у випадку, якщо інформаційні послуги містять посилання на ціни, то такі послуги мають бути чітко та однозначно вказані та, зокрема, повинні містити вказівку на те, чи включають вони податкові витрати та витрати на доставку.

Частина 2.
Комерційні повідомлення

Стаття 6

Інформація, що має постачатись

На додаток до інших вимог до інформації, визначених законодавством держав Співтовариства, держави-члени забезпечують відповідність комерційних повідомлень, які є частиною інформаційних послуг, принаймні наступним умовам:

a) комерційні повідомлення чітко ідентифікуються як такі;

b) фізична чи юридична особа, від імені якої надсилається комерційне повідомлення, чітко ідентифікується;

c) рекламні пропозиції, такі як знижки, винагороди та подарунки, якщо такі передбачаються на території держави-члена, де заснований постачальник послуг, чітко ідентифікуються як такі, а умови, що мають бути задоволені для їх кваліфікації, легко доступні та подаються чітко і однозначно;

d) рекламні змагання чи ігри, якщо такі передбачені на території держави-члена, де заснований постачальник послуг, чітко ідентифікуються як такі, а умови участі легко доступні та подаються чітко і однозначно.

Стаття 7

Комерційне повідомлення, що надсилаються без згоди одержувача

1. На додаток до вимог, визначених законодавством Співтовариства, держави-члени, які дозволяють надсилання комерційних повідомлень електронною поштою без згоди одержувача, забезпечують чітку та однозначну ідентифікацію такого комерційного повідомлення, відправленого постачальником послуг, заснованим на її території, як такого, одразу після отримання його одержувачем.

2. Без шкоди Директиві 97/7/ЄС та Директиві 97/66/ЄС держави-члени вживають заходів для забезпечення регулярного консультування та поважання постачальником послуг, який займається надсиланням комерційних повідомлень без згоди одержувача електронною поштою, реєстру відмов, в якому реєструються фізичні особи, які не бажають отримувати такі комерційні повідомлення.

Стаття 8

Професії, що регулюються законодавством ЄС

1. Держави-члени забезпечують відповідність використання комерційних повідомлень, які є складовою інформаційних послуг, що надаються представником професії, що регулюється законодавством ЄС, професійним нормам щодо, зокрема, незалежності, гідності та честі професії, професійної таємниці та справедливого ставлення до клієнтів та інших представників професії.

2. Без нанесення шкоди самостійності професійних органів та об'єднань держави-члени та Комісія заохочують професійні об'єднання та органи до розробки кодексів поведінки на рівні Співтовариства з метою визначити види інформації, яка може надаватись в цілях комерційного повідомлення відповідно до норм, про які йдеться в пункті 1.

3. При розробці пропозиції щодо ініціатив в межах Співтовариства, потреба в яких виникає у зв'язку із необхідністю забезпечити належне функціонування внутрішнього ринку щодо інформації, про яку йдеться в пункті 2, Комісія приділяє належну увагу кодексам поведінки, що застосовуються на рівні Співтовариства та діють у тісному співробітництві із відповідними професійними об'єднаннями та органами.

4. Ця Директива застосовується додатково до директив Співтовариства щодо доступу, реалізації діяльності в межах професій, що регулюються законодавством ЄС.

Частина 3.

Контракти, що укладаються за допомогою електронних засобів

Стаття 9

Режим укладення контрактів

1. Держави-члени гарантують, що їх правова система передбачає укладення контрактів за допомогою електронних засобів.

Держави-члени також, зокрема, забезпечують, що правові вимоги до процессу укладення контрактів ні створюють перешкоди для використання контрактів, укладених в електронному вигляді, ні призводять до позбавлення таких контрактів законної сили через укладення їх в електронній формі.

2. Держави-члени можуть передбачити, що пункт 1 не застосовується до всіх чи визначених контрактів, які підпадають під одну з наступних категорій:

a) контракти, які передбачають появу чи передачу прав на нерухоме майно, окрім прав оренди;

b) контракти, що вимагають відповідно до закону залучення судів, державних органів чи професій, що передбачають реалізацію державних повноважень;

c) контракти про поручительство та майнове забезпечення, що надається особами, які діють в цілях, що лежать поза межами їх комерційної чи професійної діяльності;

d) контракти, що регулюються сімейним правом чи спадковим правом.

3. Держави-члени вказують Комісії на категорії, що містяться в пункті 2, до яких не застосовується пункт 1. Держави-члени кожні п'ять років подають до Комісії звіт про застосування пункту 2 із поясненням причин зберігання в силі категорії, що передбачається в пункті 2(b), до якого не застосовуються положення пункту 1.

Стаття 10

Інформація, що має бути надана

1. На додаток до інших вимог до інформації, що визначені законодавством держав Співтовариства, держави-члени забезпечують , якщо інше не узгоджено сторонами, які не є споживачами, що принаймні наступна інформація надається постачальником послуг чітко, повно та однозначно під першим номером в порядку, визначеному одержувачем послуг:

a) різні технічні заходи на шляху до укладення контракту;

b) чи буде укладений контракт прийнятий постачальником послуг та чи буде він доступним;

c) технічні засоби ідентифікації та виправлення помилок вводу до розміщення запиту;

d) мови, запропоновані для укладення контракту.

2. Держави-члени забезпечують, якщо інше не узгоджено між сторонами, які не є споживачами, повідомлення постачальником послуг про дотримання ним будь-якого відповідного кодексу поведінки та інформацію щодо способу консультації із цими кодексами електронним шляхом.

3. Умови контракту та загальні умови, що висуваються до одержувача, мають бути доступні таким чином, щоб він міг їх зберігати та відновлювати.

Пункти 1 та 2 не застосовуються до контрактів, укладених виключно шляхом обміну електронною поштою чи еквівалентних індивідуальних повідомлень.

Стаття 11

Розміщення запиту

1. Держави-члени забезпечують, якщо інше не узгоджено між сторонами, які не є споживачами, що у випадку, якщо одержувач послуг розміщує свій запит за допомогою технологічних засобів, застосовуються наступні принципи:

- постачальник послуг має безвідкладно та за допомогою електронних засобів підтвердити отримання запиту одержувача,

- вважається, що запит та підтвердження отримання надходять в той момент, коли сторони, якім вони адресовані, здатні отримати доступ до них.

2. Держави-члени гарантують, якщо інше не узгоджене між сторонами, які не є споживачами, надання постачальником послуг одержувачеві цих послуг доступу до ефективних технічних засобів, що дозволять йому виявляти та виправляти помилки вводу до розміщення запиту.

3. Пункт 1.1 та пункт 2 не застосовуються до контрактів,укладених виключно шляхом обміну електронною поштою чи еквівалентних індивідуальних повідомлень.

Частина 4.

Відповідальність проміжкових постачальників послуг

Стаття 12

Канали передачі інформації

1. Якщо надаються інформаційні послуги, які складаються з передачі інформації, що надається одержувачем послуг, всередині мережі зв’язку або надання доступу до мережі зв’язку, держави-члени забезпечують звільнення постачальника послуг від відповідальності за передану інформацію при умові, що постачальник:

a) не є ініціатором передачі;

b) не обирає одержувача передачі; та

c) не обирає чи не змінює інформацію, що міститься в передачі.

2. Акти передачі та забезпечення доступу, про що йдеться в пункті 1,

включають в себе автоматичне, проміжкове тимчасове зберігання переданої інформації, оскільки це робиться з єдиною метою – здійснення передачі в мережі зв’язку та передбачає, що інформація не зберігається довше, ніж це необхідно для передачі.

3. Ця стаття не впливає на можливість для суду чи адміністративного органу, відповідно до правової системи держав-членів, вимагати від постачальника послуг обмеження чи запобігання порушення.

Стаття 13

"Кешування"

1. Якщо надаються інформаційні послуги, які складаються з передачі в мережі зв'язку інформації, що надається одержувачем послуг, держави-члени забезпечують звільнення постачальника послуг від відповідальності за автономне, проміжкове тимчасове зберігання інформації, що здійснюється з єдиною метою – більш ефективної поступальної передачі інформації до інших одержувачів послуг за їх запитом за умови що:

a) постачальник послуг не змінює інформацію;

b) постачальник задовольняє умови доступу до інформації;

c) постачальник задовольняє правила оновлення інформації, які є широко визнаними та використовуються даною індустрією;

d) постачальник не перешкоджає законному використанню технологій, які широко визнані та використовуються індустрією, при отриманні даних про використання інформації; та

e) постачальник вдається до швидких дій з метою усунення можливості доступу чи відключення доступу до інформації, яку він зберігав, після того як він узнає, що інформація на початковій стадії передання булла видалена з мережі або доступ до неї був відключений, чи суд або адміністративний орган наказав здійснити таке усунення чи відключення.

2. Ця стаття не впливає на можливість для суду чи адміністративного органу, відповідно до правової системи держав-членів, вимагати від постачальника послуг обмеження чи запобігання порушення.

Стаття 14

Розміщення інформації

1. Якщо надаються інформаційні послуги, які включають в себе зберігання інформації, що надається одержувачем послуг, держави-члени забезпечують звільнення постачальника послуг від відповідальності за інформацію, що була збережена за запитом одержувача послуг, при умові, що:

a) постачальник послуг не знає про незаконну діяльність чи інформацію, що стосується позовів про відшкодування збитків, не обізнаний із фактами чи обставинами, з яких випливає незаконна діяльність чи інформація; або

b) постачальник за умов обізнаності вдається до швидких дій з метою усунення можливості доступу чи відключення доступу до інформації.

2. Пункт 1 не застосовується, якщо одержувач послуг діє під егідою чи під контролем постачальника.

3. Ця стаття не впливає як на можливість для суду чи адміністративного органу, відповідно до правової системи держав-членів,вимагати від постачальника послуг обмеження чи запобігання порушення, так і на здатність держав-членів встановлювати процедури, що регулюють усунення можливості доступу чи відключення доступу до інформації.

Стаття 15

Відсутність загального обов'язку відслідковувати

1. Держави-члени не накладають на постачальників послуг ні загального обов'язку при наданні послуг, що регулюється статтями 12, 13 та 14, відслідковувати інформацію, яку вони передають чи зберігають, ні загального обов'язку здійснювати активний пошук фактів чи обставин, що вказують на незаконну діяльність.

2. Держави-члени можуть передбачити обов'язки для постачальників інформаційних послуг інформувати компетентні державні органи про підозрілу незаконну діяльність, що здійснюється, чи інформацію, що надається одержувачем послуг, або обов'язки повідомляти компетентні органи за їх запитом про інформацію, яка надає можливість ідентифікувати тих одержувачів послуг, з якими вони мають угоди про зберігання інформації.

ГЛАВА III
ЗАПРОВАДЖЕННЯ

Стаття 16
Кодекси поведінки

1. Держави-члени та Комісія заохочують:

a) розробку кодексів поведінки на рівні Співтовариства торгівельними, професійними та споживацькими об'єднаннями чи організаціями, метою чого є належне запровадження статей 5-15;

b) добровільну передачу проектів кодексів на національному рівні чи на рівні Співтовариства Комісії;

c) доступність цих кодексів поведінки в електронному вигляді на мовах держав Співтовариства;

d) повідомлення держав-членів та Комісії торгівельними, професійними та споживацькими об'єднаннями чи організаціями про їх оцінку своїх кодексів поведінки та їх впливу на практику, звички чи звичаї в сфері електронної комерції;

e) розробку кодексів поведінки в сфері захисту неповнолітніх та людської гідності.

2. Держави-члени та Комісія заохочують залучення об'єднань та організації, що представляють споживачів, до розробки й імплементації кодексів поведінки, які становлять сферу їх інтересів і складені відповідно до пункту 1(a). Якщо необхідно, з метою забезпечення особливих потреб більш слабких об'єднань, з ними мають проводитись консультації.

Стаття 17
Вирішення спорів поза межами суду

1. Держави-члени забезпечують, що в умовах відсутності узгодженості між постачальником інформаційних послуг та одержувачем послуг їх законодавство не перешкоджає використовувати позасудові механізми, доступні згідно національному законодавству, до вирішення спорів, включаючи відповідні електронні засоби.

2. Держави-члени заохочують органи, відповідальні за позасудове вирішення спорів, зокрема, спорів, стороною яких є споживач, діяти у такий спосіб, який передбачає адекватні процесуальні гарантії для зацікавлених сторін.

3. Держави-члени заохочують органи, відповідальні за позасудове вирішення спорів, повідомляти Комісію про важливі рішення, що приймаються ними в сфері інформаційних послуг, та передавати будь-яку іншу інформацію про практику, використання чи звичаї в галузі електронної комерції.

Стаття 18
Судові позови

1. Держави-члени забезпечують, що судові позови, які передбачаються національним законодавством про діяльність в сфері інформаційних послуг, надають можливість швидкого прийняття актів, включаючи тимчасові, метою яких є обмеження будь-якого підозрілого порушення та попередження нанесення будь-якої шкоди інтересам.

2. Додаток до Директиви 98/27/ЄС доповнюється наступним чином:

"11. Директива 2000/31/ЄС Європейського парламенту та Ради від 8 червня 2000 року про визначені правові аспекти надання інформаційнихпослуг, зокрема, в сфері електронної комерції, на внутрішньому ринку (Директива про електронну комерцію) (ОЖ L 178, 17.07.2000, с.1)."

Стаття 19
Співробітництво

1. Держави-члени мають адекватні засоби контролю та розслідування, необхідні для ефективної імплементації цієї Директиви, забезпечують надання постачальником послуг необхідної їм інформації.

2. Держави-члени співробітничають із іншими державами-членами; з цією ж метою вони обирають один чи декілька контактних пунктів, інформацію з яких вони повідомляють іншим державам-членам та Комісії.

3. Держави-члени якомога швидше та згідно із національним законодавством надають допомогу та інформацію, щодо яких надсилають запит інші держави-члени та Комісія, включаючи відповідні електронні засоби.

4. Держави-члени створюють контактні пункти, які доступні принаймні за допомогою електронних засобів та з яких одержувачі послуг та постачальники послуг можуть:

a) отримати загальну інформацію як про контрактні права та обов'язки, так і про механізми подання скарг та відшкодування збитків у випадку спорів, включаючи практичні аспекти, залучені при використанн таких механізмів;

b) отримати детальну інформацію про органи, об'єднання чи організації, з яких вони можуть отримати подальшу інформацію чи практичну допомогу.

5. Держави-члени заохочують повідомлення Комісії про будь-які важливі адміністративні чи судові рішення, прийняті на їх території стосовно спорів в сфері інформаційних послуг, а також про практику, використання та звичаї в сфері електронної комерції. Комісія повідомляє іншим державам-членам про ці рішення.

Стаття 20

Санкції

Держави-члени визначають санкції, що застосовуються до порушень положень національного законодавства, прийнятого відповідно до цієї Директиви, та вживають заходів, необхідних для його реалізації. Санкції, які вони накладають, ефективні, пропорційні до здійсненого порушення.

ГЛАВА IV
ЗАКЛЮЧНІ ПОЛОЖЕННЯ

Стаття 21

Повторне вивчення

1. До 17 липня 2003 року та після цього кожні два роки Комісія подає до Європейського парламенту, Ради та Комітету з економічних та соціальних питань звіт про застосування цієї Директиви разом із пропозиціями про її адаптацію до правового, технічного та економічного розвитку в сфері інформаційних послуг (у випадку необхідності), зокрема, звертаючи увагу на попередження злочинів, захист неповнолітніх, захист прав споживача та ефективне функціонування внутрішнього ринку.

2. При вивченні потреби адаптації цієї Директиви у звіті, зокрема, міститься аналіз необхідності прийняття пропозицій щодо відповідальності постачальників гіперзв'язку та послуг щодо розміщення, процедур повідомлення та розміщення та накладення відповідальності. Звіт також містить аналіз потреби в додаткових умовах щодо звільнення від відповідальності, що передбачається статтями 12 та 13, у зв'язку із технічним розвитком та можливістю застосування принципів внутрішнього ринку до комерційних повідомлень, відправлених електронною поштою без згоди одержувача.

Стаття 22

Впровадження

1. Держави-члени приймають законодавчі, нормативні й адміністративні положення, необхідні для виконання даної Директиви, не пізніше 17 січня 2002 року. Вони негайно сповіщають про це Комісію.

2. Коли держави-члени приймають такі акти, про які йдеться в пункті 1,останні повинні містити посилання на цю Директиву чи супроводжуватися таким посиланням у разі їх офіційної публікації. Методи, за якими робиться таке посилання, встановлюються державами-членами.

Стаття 23

Набрання чинності

Ця Директива набирає чинності в день її публікації в Офіційному журналі Європейських Співтовариств.

Стаття 24

Адресати

Ця Директива адресована державам-членам.

Вчинено в Люксембурзі 8 червня 2000 року.

За Європейський парламент

Президент Н. Фонтен

За Раду

Президент

Ж. Мартінс д'Олівейра

(1) ОЖ С 30, 05.02. 1999, с. 4.

(2) ОЖ С 169, 16.06.1999, с. 36.

(3) Висновки Європейського парламенту від 6 травня 1999 року (ОЖ С 279, 01.10.1999, с. 389), Спільна позиція Ради від 28 лютого 2000 року (ОЖС 128, 08.05.2000 року, с.32) та Рішення Європейського парламенту від 4 травня 2000 року (ще не опубліковане в Офіційному журналі).

(4) ОЖ L 298, 17.10.1989, с. 23. Директива з поправками, внесеними Директивою 7/36/ЄС Європейського парламенту та Ради (ОЖ L 202, 30.07.1997, с.60).

(5) ОЖ L 95, 21.04.1993, с. 29.

(6) ОЖ L 144, 04.06.1999, с.19.

(7) ОЖ L 250, 19.09.1984, с. 17. Директива з поправками, внесеними Директивою 97/55/ЄС Європейського парламенту та Ради (ОЖ L 290, 23.10.1997, с.18).

(8) ОЖ L 42, 12.02.1987, с.48. Директива з поправками, востаннє внесеними Директивою 98/7/ЄС Європейського парламенту та Ради (ОЖ L 101, 01.04.1998, с. 17).

(9) ОЖ L 141, 11.06.1993, с.27. Директива з поправками, востаннє внесеними Директивою 97/9/ЄС Європейського парламенту та Ради (ОЖ L 84, 26.03.1997, с.22).

(10) ОЖ L 158, 23.06.1990, с.59.

(11) ОЖ L 80, 18.03.1998, с.27.

(12) ОЖ L 228, 11.08.1992, с. 24.

(13) ОЖ L 280, 29.10.1994, с.83.

(14) ОЖ L 166, 11.06.1998, с.51. Директива з поправками, внесеними Директивою 1999/44/ЄС (ОЖ L 171, 07.07.1999, с.12).

(15) ОЖ L 210, 07.08.1985, с.29. Директива з поправками, внесеними Директивою 1999/34/ЄС (ОЖ L 141, 04.06.1999, с.20).

(16) ОЖ L 171, 07.07.1999, с.12.

(17) ОЖ L 113, 30.04.1992, с.13.

(18) ОЖ L 213, 30.07.1998, с.9.

(19) ОЖ L 281, 23.11.1995, с.31.

(20) ОЖ L 24, 30.01.1998, с.1.

(21) ОЖ L 204, 21.07.1998, с. 37. Директива з поправками, внесеними Директивою 98/48/ЄС (ОЖ L 217, 05.08.1998, с.18).

(22) ОЖ L 320, 28.11.1998, с.54.

(23) ОЖ L 15, 21.01.1998, с.14.

(24) ОЖ L 13,19.01.2000,с.12.

(25) ОЖ L С 23, 28.01.1999, с.1.

(26) ОЖ L 19, 24.01.1989, с.16.

(27) ОЖ L 209, 24.07.1992, с.25. Директива з поправками, востаннє внесеними Директивою Комісії 97/38/ЄС (ОЖ L 184, 12.07.1997, с.31).

(28) ОЖ L 117, 07.05.1997, с.15.

(29) ОЖ L 145, 13.06.1977, с.1. Директива з поправками, востаннє внесеними Директивою 1999/85/ЄС (ОЖ L 277, 28.10.1999, с.34).

ДОДАТОК

ВІДСТУПИ ВІД СТАТТІ 3

Як передбачено в статті 3(3), стаття 3(1) та (2) не застосовується до:

- авторського права, суміжних прав, прав, про які йдеться в Директиві 87/54/ЄЕС(1) та Директиві 96/9/ЄС(2), а також до прав промислової власності,

- випуску електронних грошей установами, по відношенню до яких держави-члени застосували один з відступів, передбачених в статті 8(1) Директиви 2000/46/ЄС(3),

- статті 44(2) Директиви 85/611/ЄЕС(4),

- статті 30 та Розділу IV Директиви 92/49/ЄЕС(5), Розділу IV

Директиви 92/96/ЄЕС(6), статей 7 та 8 Директиви 88/357/ЄЕС(7) та статті 4 Директиви 90/619/ЄЕС(8),

- свободи сторін обирати закон, що застосовується до їх контракту,

- контрактних зобов'язань стосовно контрактів, укладених споживачами,

- формальної чинності контрактів, які створюють чи передають права на нерухоме майно, якщо на такі контракти поширюються обов'язкові формальні вимоги законодавства держави-члена, на території якого розташоване нерухоме майно,

- дозволу на передання комерційних повідомлень електронною поштою без згоди одержувача.

(1) ОЖ L 24, 27.01.1987, с.36.

(2) ОЖ L 77, 27.03.1996, с.20.

(3) Ще не опублікована в Офіційному журналі.

(4) ОЖ L 375, 31.12.1985, с.3. Директива з поправками, востаннє внесеними Директивою 95/26/ЄС (ОЖ L 168, 18.07.1995, с.7).

(5) ОЖ L 228, 11.08.1992, с.1. Директива, з поправками, востаннє внесеними Директивою 95/26/ЄС.

(6) ОЖ L 360, 09.12.1992, с.2. Директива, з поправками, востаннє внесеними Директивою 95/26/ЄС.

(7) ОЖ L 172, 04.07.1988, с.1. Директива, з поправками, востаннє внесеними Директивою 92/49/ЄС.

(8) ОЖ L 330, 29.11.1990, с.50. Директива, останній раз доповнена Директивою 92/96/ЄС.__

Додаток 2. Комиссия ООН по праву международной торговли

(ЮНСИТРАЛ)

Типовой закон ЮНСИТРАЛ «Об электронной коммерции» 1996 г.

(с дополнительной статьей 5 bis, принятой в 1998 г.)

ЧАСТЬ ПЕРВАЯ.
ЭЛЕКТРОННАЯ КОММЕРЦИЯ В ЦЕЛОМ

Глава I.
Общие положення

Статья 1.
Сфера применения

Настоящий Закон применяется к любому виду информации в форме сообщения данных, используемой в контексте коммерческой деятельности.

Статья 2.
Определения

Для целей настоящего Закона:

(a) «сообщение данных» обозначает информацию, сформированную, отправленную, полученную или хранимую с помощью электронных, оптических или аналогичных средств, включая, но не ограничиваясь, электронный обмен данными (ЭОД), электронную почту, телеграмму, телекс или телефакс;

(b) «электронный обмен данными (ЭОД)» обозначает электронную передачу с одного компьютера на другой информации с использованием согласованного стандарта структуры информации;

(c) «инициатор» сообщения данных обозначает лицо, которым или от имени которого сообщение данных, как предполагается, было отправлено или сформировано до момента хранения,

если таковое имело место, но не включает в себя лицо, действующее в качестве посредника в отношении этого сообщения данных;

(d) «адресат» сообщения данных обозначает лицо, которое, согласно намерению инициатора, должно получить сообщение данных, но не включает в себя лицо, действующее в качестве посредника в отношении этого сообщения данных;

(e) «посредник» в отношении конкретного сообщения данных обозначает лицо, которое от имени другого лица отправляет, получает либо хранит это сообщение данных либо оказывает другие услуги в отношении этого сообщения данных;

Для государств, которые, возможно, пожелают ограничить сферу применения настоящего Закона международными сообщениями данных. Комиссия предлагает следующий текст: «Настоящий Закон применяется к сообщению данных, как оно определено в параграфе (1) статьи 2, в том случае, когда сообщение данных имеет отношение к международной торговле».

Настоящий Закон не имеет преимущественной силы по отношению к любым правовым нормам, предназначенным для защиты прав потребителей.

Для государств, которые, возможно, пожелают расширить сферу применения настоящего Закона, Комиссия предлагает следующий текст: «Настоящий Закон применяется к любому виду информации в форме сообщения данных, за исключением следующих случаев: [...]».

Термин «коммерческая» следует толковать широко, с тем чтобы он охватывал вопросы, вытекающие из всех отношений коммерческого характера, как договорных, так и не договорных. Отношения коммерческого характера включают следующие сделки, но не ограничиваясь ими: любые торговые сделки на поставку или обмен товарами или услугами; дистрибьюторские соглашения; коммерческое представительство и агентские отношения; факторинг; лизинг; строительство промышленных объектов; консалтинг; инжиниринг; лицензионные отношения; инвестирование; финансирование; банковские услуги; страхование; соглашения об эксплуатации или концессии; совместные предприятия и другие формы промышленного или делового сотрудничества; перевозка товаров и пассажиров воздушным, морским, железнодорожным или автомобильным транспортом.

(f) «информационная система» обозначает систему для формирования, отправления, получения, хранения или иной обработки сообщений данных.

Статья 3.

Толкование

1 При толковании настоящего Закона следует учитывать его международное происхождение и необходимость содействовать достижению единообразия в его применении соблюдению добросовестности.

2 Вопросы, которые относятся к предмету регулирования настоящего Закона и которые прямо в нем не разрешены, подлежат разрешению в соответствии с общими принципами, на которых основан настоящий Закон.

Статья 4.

Изменение по соглашению

1) Если не предусмотрено иное, положения главы III могут быть изменены по (соглашению между сторонами, участвующими в формировании, отправлении, получении, хранении или иной обработке сообщений данных.

2) Пункт (1) не затрагивает любое право, которое может существовать, на изменение по соглашению любой правовой нормы, указанной в главе II.

Глава II.

Применение правовых требований вотношении сообщений даннях

Статья 5.

Признание юридической силы сообщений данных

Информация не может быть лишена юридической силы, действительности или исковой силы на том лишь основании, что она имеет форму сообщения данных.

Статья 5 bis.

Включение путем отсылки

Информация не может быть лишена юридической силы, действительности или эй силы на том лишь основании, что она не содержится в сообщении данных, предназначенном для придания такой силы, но к которой просто содержится отсылка в этом сообщении данных.

Статья 6.

Письменная форма

I) Когда законодательство требует, чтобы информация была представлена в Ценной форме, это требование считается выполненным путем представления рения данных, если содержащаяся в нем информация является доступной для последующей ссылки на нее.

(2) Пункт (1) применяется как в тех случаях, когда содержащееся в нем требование выражено в форме обязательства, так и в тех случаях, когда законодательство просто осматривает наступление определенных последствий, если информация представлена в письменной форме.

3) Положения настоящей статьи не применяются в следующих случаях: [...].

Статья 7.

Подпись

1) Если законодательство требует подпись лица, это требование считается выполенным в отношении сообщения данных, если:

.(a) использован какой-либо способ для идентификации этого лица и указания на кие этого лица с информацией, содержащейся в сообщении данных; и

(b) этот способ является как надежным, так и соответствующим цели, для которой сообщение данных было сформировано или передано с учетом всех обстоя-1тв, включая любое соответствующее соглашение.

(2) Пункт (1) применяется как в тех случаях, когда содержащееся в нем требование выражено в форме обязательства, так и в тех случаях, когда законодательство просто предусматривает наступление определенных последствий при отсутствии подписи.

(3) Положения настоящей статьи не применяются в следующих случаях: [...].

Приията Комиссией на своей 31-й сессии в июле 1998 г.

Статья 8.

Оригинал

(1) Если законодательство требует, чтобы информация представлялась или сохранялась в ее оригинальной форме, это требование считается выполненным посредством сообщения данных, если:

(a) имеются надежные доказательства целостности информации с момента, когда она была впервые сформирована в ее окончательной форме в виде сообщения данных или иным образом; и

(b) в том случае, когда требуется представление информации, эта информация может быть продемонстрирована лицу, которому она должна быть представлена.

(2) Пункт (1) применяется как в тех случаях, когда содержащееся в нем требование выражено в форме обязательства, так и в тех случаях, когда законодательство просто предусматривает наступление определенных последствий, если информация не была представлена или сохранена в ее оригинальной форме.

(3) Для целей подпункта (a) пункта (1):

(a) критерием оценки целостности является сохранение информации в полном и неизменном виде, без учета добавления любых индоссаментов и любых изменений, происходящих при нормальном процессе передачи, хранения и представления; и

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

(4) Положения настоящей статьи не применяются в следующих случаях: [...].

Статья 9.

Допустимость и доказательственная сила сообщения данных

(1) При любых процессуальных действиях никакие положения норм доказательственного права не должны применяться таким образом, чтобы отрицалась 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 оригинальной форме.

(2) Информации в форме сообщения данных должна придаваться надлежащая доказательственная сила. При оценке доказательственной силы сообщения данных должна учитываться надежность способа, с помощью которого формировалось, хранилось или передавалось это сообщение данных, надежность способа, с помощью которого обеспечивалась целостность информации, способа, посредством которого идентифицировался его инициатор, и любой другой соответствующий фактор.

Статья 10.

'Сохранение сообщений данных

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

(a) информация, содержащаяся в сообщении данных, доступна для последующей ссылки на нее; и

(b) сообщение данных сохраняется в том формате, в котором оно было сформировано, отправлено или получено, либо в таком формате, в котором может быть представлена точным образом сформированная, отправленная или полученная информация; и

(c) сохраняется такая информация, при ее наличии, 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.

(3) Лицо может выполнить требование, указанное в пункте (1), посредством использования услуг любого другого лица при соблюдении условий, изложенных в подпунктах (a), (Ь) и (c) пункта (1).

Глава III.
Передача сообщений данных

Статья 11.

Заключение и действительность договоров

(1) В контексте заключения договоров, если стороны не договорились об ином, оферта и акцепт оферты могут производиться с использованием сообщений данных. В случае, когда при заключении договора используется сообщение данных, этот договор не может быть лишен действительности или исковой силы на том лишь основании, что для этой цели использовалось сообщение данных.

(2) Положения настоящей статьи не применяются в следующих случаях: [,..].

Статья 12.

Признание сторонами сообщений данных

(1) В отношениях между инициатором и адресатом сообщения данных волеизъявление или другое заявление не может быть лишено юридической силы, действительности или исковой силы на том лишь основании, что оно имеет форму сообщения данных.

(2) Положения настоящей статьи не применяются в следующих случаях: [...].

Статья 13.

Атрибуция (установление авторства) сообщения данных

(1) Сообщение данных считается сообщением данных инициатора, если оно было отправлено самим инициатором.

(2) В отношениях между инициатором и адресатом сообщение данных считается сообщением данных инициатора, если оно было отправлено:

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

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

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

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

(b) сообщение данных, полученное адресатом, явилось результатом действий лица, отношения которого с инициатором или любым агентом инициатора дали такому лицу возможность доступа к способу, используемому инициатором для идентификации сообщений данных как своих собственных.

(4) Пункт (3) не применяется:

(a) с момента, когда адресат получил уведомление инициатора о том, что сообщение данных не является сообщением данных инициатора, и 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 в любую согласованную процедуру, должно было стать известно о том, что сообщение данных не являлось сообщением данных инициатора.

(5) Когда сообщение данных является сообщением данных инициатора или считается сообщением данных инициатора или когда адресат имеет право действовать исходя из этого предположения, в отношениях между инициатором и адресатом, адресат имеет право считать, что полученное сообщение данных является таким, каким инициатор намеревался его отправить, и действовать исходя из этого предположения. Адресат не имеет такого права, когда ему стало известно или, если бы он проявил разумную осмотрительность или использовал любую согласованную процедуру, должно было стать известно, что при передаче в полученном сообщении данных допущена ошибка.

(6) Адресат имеет право рассматривать каждое полученное сообщение данных как отдельное сообщение данных и действовать исходя из этого предположения, за исключением случая, когда это сообщение данных дублирует другое сообщение данных и когда адресату стало известно или, если бы он проявил разумную осмотрительность или использовал любую согласованную процедуру, должно было стать известно, что это сообщение данных было дубликатом.

Статья 14.

Подтверждение получения

(1) Пункты (2)-(4) настоящей статьи применяются в случае, когда при отправке сообщения данных или до его отправки или посредством этого сообщения данных инициатор просит адресата или договаривается с адресатом о подтверждении получения этого сообщения данных.

(2) В случае, когда инициатор не договорился с адресатом о том, что подтверждение будет осуществлено в какой-либо конкретной форме или посредством конкретного способа, подтверждение может быть осуществлено путем:

(a) любого сообщения со стороны адресата, направленного автоматизированным или иным способом, или

(b) любых действий со стороны адресата, достаточных для того, чтобы показать инициатору, что сообщение данных было получено.

(3) В случае, когда инициатор указал, что сообщение данных обусловливается получением такого подтверждения, сообщение данных считается неотправленным до тех пор, пока не будет получено подтверждение.

(4) В случае, когда инициатор 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, инициатор:

(a) может направить адресату уведомление, указав в нем, что подтверждение получено не было, и установив разумный срок, к которому подтверждение должно быть получено; и

(Ь) 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.

(5) В случае, когда инициатор получает от адресата подтверждение получения, считается, что соответствующее сообщение данных было получено адресатом. Такая презумпция не предполагает, что отправленное сообщение данных соответствует полученному сообщению.

(6) Если в полученном подтверждении указывается, что соответствующее сообщение данных отвечает техническим требованиям, согласованным или установленным в применимых стандартах, предполагается, что эти требования были выполнены.

(7) За исключением той степени, в которой она имеет отношение к отправлению или получению сообщения данных, настоящая статья не затрагивает правовых последствий, которые могут вытекать либо из такого сообщения данных, либо из подтверждения его получения.

Статья 15.

Время и место отправления и получения сообщений данных

(1) Если инициатор и адресат не договорились об ином, отправление сообщения данных происходит в момент, когда оно поступает в информационную систему, находящуюся вне контроля инициатора или лица, которое отправило сообщение данных от имени составителя.

(2) Если инициатор и адресат не договорились об ином, момент получения сообщения данных устанавливается следующим образом:

(a) если адресат указал информационную систему для цели получения таких сообщений данных, получение происходит:

(1) в момент, когда сообщение данных поступает в указанную информационную систему; или

(II) если сообщение данных направляется в информационную систему адресата, которая не является указанной информационной системой, в момент, когда сообщение данных извлекается адресатом из системы;

(b) если адресат не указал информационную систему, получение происходит в момент, когда сообщение данных поступает в какую-либо информационную систему адресата.

(3) Пункт (2) применяется независимо от того, что место, в котором находится информационная система, может отличаться от места, в котором сообщение данных считается полученным в соответствии с пунктом (4).

(4) Если инициатор и адресат не договорились об ином, сообщение данных считается отправленным в месте нахождения коммерческого предприятия инициатора и считается полученным в месте нахождения коммерческого предприятия адресата. Для целей настоящего пункта:

(a) если инициатор или адресат имеют несколько коммерческих предприятий, местом нахождения коммерческого предприятия считается такое место, которое имеет наиболее тесное отношение к основной сделке, или - в случае отсутствия основной сделки - место нахождения основного коммерческого предприятия;

(b) если инициатор или адресат не имеют коммерческого предприятия, таковым считается их обычное место жительства.

(5) Положения настоящей статьи не применяются в следующих случаях: [...].

ЧАСТЬ ВТОРАЯ.
ЭЛЕКТРОННАЯ КОММЕРЦИЯ В ОТДЕЛЬНЫХ ОБЛАСТЯХ

Глава 1.
Перевозка грузив

Статья 16.

Действия, связанные с договорами перевозки грузов

Не умаляя положений части первой настоящего Закона, настоящая глава применяется к любому из действий, совершаемых в связи с договором перевозки грузов или во исполнение такого договора, включая, в частности:

(a)(1) указание марок, числа мест и предметов, количества или веса груза;

(ii) указание или декларирование характера или стоимости груза;

(iii) выдачу расписки в получении груза;

(IV) подтверждение погрузки груза;

(b)(1) направление какому-либо лицу уведомления об условиях договора;

(ii) дачу инструкций перевозчику;

(c)(1) предъявление требования о сдаче груза;

(ii) разрешение на выдачу груза;

(III) направление уведомления об утрате или повреждении груза;

(d) направление любого другого уведомления или заявления в связи с исполнением договора;

(e) принятие обязательства сдать груз поименованному лицу или лицу, уполномоченному требовать сдачи груза;

(f) предоставление, приобретение, отклонение, отказ, передачу или переуступку прав на груз;

(g) приобретение или передачу прав и обязательств по договору.

Статья 17.

Транспортные документы

(1) С учетом положений пункта (3), если законодательство требует, чтобы любое действие, упомянутое в статье 16, совершалось в письменной форме или с использованием бумажного документа, это требование считается выполненным, если действие совершается путем использования одного или нескольких сообщений данных.

(2) Пункт (1) применяется как в тех случаях, когда содержащееся в нем требование выражено в форме обязательства, так и в тех случаях, когда законодательство просто предусматривает наступление определенных последствий за не совершение действия в письменной форме или не использование бумажного документа.

(3) Если какое-либо право должно быть предоставлено одному и никакому другому лицу или же какое-либо обязательство должно быть принято перед одним и никаким другим лицом и если законодательство требует, чтобы для достижения этого такое право или обязательство было передано этому лицу путем передачи или использования бумажного документа, это требование считается выполненным, если право или обязательство передается посредством одного или нескольких сообщений данных, при условии использования надежного способа придания такому сообщению или сообщениям данных уникального характера.

(4) Для целей пункта (3) требуемая степень надежности оценивается с учетом цели передачи права или обязательства и всех обстоятельств, включая любое соответствующее соглашение.

(5) Если для осуществления любых действий, упомянутых в подпунктах (f) и (g) статьи 16, используется одно или несколько сообщений данных, любой бумажный документ, использованный для осуществления любых таких действий, не имеет силы, за исключением случаев, когда использование сообщений данных было прекращено или заменено использованием бумажных документов. Бумажный документ, выданный в таких обстоятельствах, должен содержать заявление о таком прекращении. Замена сообщений данных бумажными документами не затрагивает прав или обязательств соответствующих сторон.

(6) Если какая-либо правовая норма в обязательном порядке должна применяться к договору перевозки грузов, который представлен или который подтверждается бумажным документом, эта норма не может не применяться к такому договору перевозки грузов, который подтверждается одним или несколькими сообщениями данных, в силу того факта, что такой договор подтверждается таким сообщением или такими сообщениями данных, а не бумажным документом.

(7) Положения настоящей статьи не применяются в следующих случаях: [...].

Додаток 3.Типовой закон ЮНСИТРАЛ «Об электронных подписях» 2001 г.

Статья 1.
Сфера применения

Настоящий Закон применяется в случаях, когда электронные подписи используются в контексте' коммерческой деятельности/ Закон не имеет преимущественного действия применительно к любой правовой норме, предназначенной для защиты прав потребителей.

Комиссия предлагает следующий текст для государств, которые пожелают расширить применение настоящего Закона: «Настоящий Закон применяется в случаях, когда используются электронные подписи, за исключением следующих ситуаций: [...].»

Термину «коммерческая» должно придаваться широкое толкование, с тем чтобы он охватывал вопросы, вытекающие из всех отношений коммерческого характера, являются ли они договорными или нет. Отношения коммерческого характера включают следующие сделки, но не ограничиваются ими: любые торговые сделки на поставку или обмен товарами или услугами; дистрибьюторское соглашение; коммерческое представительство или агентские отношения; факторинг; лизинг; строительные работы; консалтинг; инжиниринг; лицензионные отношения; инвестирование; финансирование; банковские услуги; страхование; соглашение об эксплуатации или концессия; совместное предприятие и другие формы промышленного или делового сотрудничества; перевозка товаров и пассажиров воздушным, морским, железнодорожным или автомобильным транспортом.

Додаток 4. Типовой закон ЮНСИТРАЛ «Об международных кредитовых переводах» 1992 г.

(Извлечения)

Глава 1.
Общие положения

<...>

Статья 2.

Определения

В целях настоящего закона:

<•••>

1) «Удостоверение подлинности» означает определенную соглашением процедуру для установления того, действительно ли платежное поручение, измененное платежное поручение или отзыв платежного поручения выданы лицом, указанным в качестве отправителя.

Глава 2.
Обязанности сторон

Статья 5.

Обязанности отправителя

(1) Отправитель несет обязанности в связи с платежным поручением, измененным платежным поручением или отзывом платежного поручения, если они были выданы отправителем или другим лицом, которое имело полномочия обязать отправителя.

(2) Когда подлинность платежного поручения, измененного платежного поручения или отзыва платежного поручения должна быть удостоверена каким-либо иным способом помимо простого сопоставления подписей, предполагаемый отправитель, который не несет обязанностей согласно пункту 1, тем не менее несет такие обязанности, если

(a) удостоверение подлинности представляет собой в данных обстоятельствах коммерчески обоснованный метод защиты против несанкционированных платежных поручений;

(b) банк-получатель произвел удостоверение подлинности.

(3) Сторонам не разрешается договариваться о возложении обязанностей на предполагаемого отправителя согласно пункту 2, если удостоверение подлинности не является коммерчески обоснованным в данных обстоятельствах.

(4) Предполагаемый отправитель не несет, однако, ответственности согласно пункту 2, если

он докажет, что платежное поручение, полученное банком-получателем, было результатом действий какого-либо лица, иного, чем:

(a) нынешний или бывший служащий предполагаемого отправителя или

(bb) лицо, отношения которого с предполагаемым отправителем дали такому лицу возможность получить доступ к процедуре удостоверения подлинности.

Предыдущее предложение не применяется, если банк-получатель докажет, что платежное поручение явилось результатом действий лица, которое получило доступ к процедуре удостоверения подлинности по вине предполагаемого отправителя.

(5) Отправитель, несущий обязанности по платежному поручению, несет обязанности в соответствии с условиями поручения, полученного банком-получателем. Однако отправитель не несет ответственности за ошибочные дубликаты платежного поручения, ошибки или несоответствия в платежном поручении, если

(a) отправитель и банк-получатель договорились о процедуре обнаружения ошибочных дубликатов, ошибок или несоответствий в платежном поручении и

(b) использование этой процедуры банком-получателем позволило или могло бы позволить обнаружить ошибочный дубликат, ошибку или несоответствие.

Если ошибка или несоответствие, которое обнаружил бы банк, заключается в том, что отправитель дал указание о платеже в сумме большей, чем это входило в его намерения, то отправитель несет ответственность только в объеме предполагавшейся суммы. Пункт 5 применяется в отношении ошибки или несоответствия в измененном поручении или поручении об отзыве так же, как он применяется в отношении ошибки или несоответствия в платежном поручении.

<...>

Додаток 5.Правовое руководство ЮНСИТРАЛ по электронному переводу средств 1987 г.

(Извлечения)

Предисловие

1. Настоящее Правовое руководство подготовлено для оказания помощи законодателям и юристам, рассматривающим правила для тех или иных систем. Поскольку оно предназначено для практического использования в целом ряде стран, в нем сознательно стремились не использовать и не обсуждать правовые теории и не рассматривать проблемы, возникающие лишь в небольшом числе стран. Напротив, в нем преднамеренно была предпринята попытка найти общие элементы в правовой и банковской практике перевода средств, с тем чтобы облегчить процесс адаптации законодательств, регулирующих перевод средств с применением бумажных документов, в соответствии с требованиями электронных методов перевода средств. Хотя электронные методы перевода средств в настоящее время наиболее широко распространены в экономически развитых странах, данное руководство может иметь исключительно большое значение в развивающихся странах, где ощущается необходимость в модернизации их системы перевода средств как внутри страны, так и в международном плане.

2. Компьютеры впервые появились в бэк-офисах банков как средство более эффективного выполнения всевозрастающего объема операций по переводу средств с применением бумажных документов. Внедрение машинного распознавания нанесенных магнитными чернилами символов (MICR) и, позднее, оптического считывания символов (ОСК) применительно к инструкциям дебетового и кредитового перевода обеспечило возможность автоматизированной обработки стандартизированных бумажных документов. Это повысило эффективность осуществления расчетными палатами и отдельными банками возросшего числа операций по переводу средств и часто приводило к полной реорганизации конторских операций банков. Создание банками компьютерных центров позволило некоторым из них централизовать ведение счетов клиентов в одном компьютерном центре вместо сохранения практики децентрализованного ведения счетов в каждом филиале.

3. После того как многие банки были оборудованы компьютерами для обработки инструкций по переводу средств с применением бумажных документов, стало возможным разработать средства для обмена инструкциями о переводе средств в электронной форме либо путем физического обмена компьютерными запоминающими устройствами, либо по каналам связи. В одних странах стало

возможно осуществить этот шаг, не прибегая к коренному изменению Существующей институциональной структуры. В других странах были созданы новые учреждения по эксплуатации средств межбанковских телекоммуникаций, коммутации сообщений, а также электронных расчетных палат. Компьютерные запоминающие устройства могут представляться банками в автоматизированные расчетные палаты для сортировки содержащихся в них инструкций о переводе средств и пересылки их банкам-получателям.

4. Инструкции о переводе средств уже давно отправляются по телеграфу и телексу. Международная передача инструкций о переводе средств между компьютерами по каналам связи доступна в настоящее время через подключение к Обществу всемирных межбанковских финансовых телекоммуникаций (SWIFT), а также через внутренние телекоммуникационные системы банков, имеющих отделения в других странах. В некоторых ориентированных на потребителей системах дебетовых и кредитных карт разрабатываются международные телекоммуникационные системы для авторизации трансакций, передачи данных о переводе средств и обеспечения связи между пунктами выдачи наличных денег и банкоматами. Предполагается, что в ближайшем будущем возникнут международные системы пунктов продажи. В связи с этим наблюдается тенденция транкации еврочеков в стране депозита с электронным представлением банку плательщика (трассата) в его стране.

Глоссарий

Аутентификация (подтверждение подлинности): идентификация сообщения физическим, электронным или другим образом, позволяющая получателю установить, что сообщение исходит из указанного источника. В целях настоящего руководства не является существенным, позволяет ли аутентификация получателю также определить, что сообщение не было преднамеренно или по небрежности изменено. Аутентификация сообщения необязательно указывает на то, что полученное сообщение было санкционировано или что лицо, направившее сообщение, уполномочено на это.

Коммуникационная услуга: услуга, посредством которой передаются сообщения, включая инструкции перевода средств, между абонентами, но которая не реализует функцию бухгалтерского учета для обеспечения возможности расчета.

Устройство компьютерной памяти: внешнее устройство, на котором могут храниться данные в машиночитаемой форме.

Персональный идентификационный номер (ПИН): секретный код, используемый для авторизации инструкций о переводе средств, инициируемых через инициализируемый клиентский терминал.

Коммутационное устройство: механизм, который получает, сортирует и направляет сообщения, включая инструкции о переводе средств.

Глава 1. Системы электронного перевода средств в целом

A. Расширенная роль системы

<...>

4. Развитие эффективной межкомпьютерной передачи инструкций перевода средств путем физической передачи устройств компьютерной памяти или по каналам связи еще больше расширило активную роль данной системы. Были созданы новые сети замкнутых групп пользователей для электронного перевода средств. Технические требования таких сетей вызвали необходимость более строгих требований в отношении форматов сообщений и используемых оперативных и чрезвычайных процедур. Потенциальная возможность использования систем электронного перевода средств в мошеннических целях привела к разработке обязательных процедур безопасности. В настоящее время качество и безопасность межбанковских переводов средств начинают зависеть от качества проектирования и функционирования упомянутых сетей замкнутых групп пользователей, а также от качества работы самих банков. Далее, банковские стандарты и практика, первоначально разработанные в рамках сетей замкнутых групп пользователей, в настоящее время приспосабливаются национальными и международными органами стандартизации, связанными с банковской деятельностью, к более широким потребностям системы перевода средств в целом.

B. Два типа перевода средств

<...>

6. Электронный перевод средств, как он понимается в данном руководстве, - это перевод

средств, при котором одна и более операций в процессе такого перевода, ранее выполнявшихся с применением бумажных носителей, теперь осуществляются с применением электронных. Наиболее очевидным и важным из упомянутых методов является замена физической транспортировки между банками, участвующими в переводе средств, инструкции дебетового или кредитового перевода в бумажном виде отправлением электронного сообщения между ними и обработкой инструкций дебетового или кредитового перевода компьютером. Путем сочетания различных методов с применением электронных носителей также стало возможным создавать новые электронные системы, которые не являются простыми модификациями предшествующих методов с применением бумажных носителей.

7. Было бы возможно рассмотреть банковские и правовые проблемы, возникающие в случае переводов средств, осуществляемых в чисто электронном окружении, без ссылки на перевод средств с использованием бумажных носителей. Вместе с тем, это не было бы полезным. Многие виды перевода средств содержат элементы [операций] с применением как электронных, так и бумажных носителей. Более того, основные модели перевода средств являются одинаковыми независимо от средств передачи инструкций между банками и способов ведения счетов банками. Настоящая глава описывает основные процедуры осуществления перевода средств в целом с особым акцентом на электронные переводы средств.

1. Кредитовый перевод

<...>

12. Кредитовый перевод особенно хорошо подходит для использования электронных средств связи. При обычном ходе дел ни плательщик, ни получатель не имеет причин возражать против такого использования, и поскольку оборотные документы при кредитовом переводе не применяются, то правовые проблемы, которые должны преодолеваться для электронного инкассирования оборотных документов, не возникают.

Кредитовые переводы в электронной форме широко используются уже на протяжении ста лет в виде телеграфных переводов. Передача платежных инструкций по телексу и через межкомпьютерные соединения является лишь современным видом этого древнего способа. Даже в тех странах, где большинство внутренних межбанковских переводов осуществляется путем дебетового перевода с использованием чеков, электронные кредитовые переводы часто используются при платежах в предпринимательских целях. В некоторых из этих стран средства электронного перевода средств в последние годы значительно усовершенствованы и таким образом производится большинство крупных платежей в предпринимательских целях.

13. В последнее время сложилась практика платежей по таким обязательствам, как зарплата, пенсии и ежемесячные пособия по социальному страхованию на счет в банке получателя - услуга, ставшая доступной только в силу увеличения числа физических лиц, имеющих счета в банках. Такой вид кредитового перевода особенно пригоден для компьютерной обработки. Плательщики крупных сумм, которые обладают оборудованием, сопоставимым с оборудованием банков, могут поощряться к самостоятельной подготовке магнитных лент и других компьютерных устройств памяти с необходимыми данными для перевода средств в целях их использования банками.

2. Дебетовый перевод

<...>

15. В целях устранения проблем, возникающих при инкассации переводных векселей и вызванных не только правовым режимом оборотных документов, но и гербовыми сборами и другими соображениями, растущая доля дебетовых переводов в международной торговле затрагивает применение требования, выставляемого продавцом-получателем без использования переводного векселя. Такие требования пригодны для передачи электронными средствами, если они только не сопровождаются коммерческими документами в бумажной форме. Наиболее сложной проблемой при международном использовании электронных дебетовых переводов является разработка средств выполнения коммерческих аккредитивных сделок и банковского финансирования без обращения к использованию бумажного коносамента.

16. В дополнение к дебетовым переводам, возникающим из конкретных сделок, в практику могут вводиться дебетовые переводы в пользу получателя, перед которым у многочисленных сторон возникает задолженность на регулярной основе. Дебетовые переводы, основанные на постоянном разрешении на дебетование, вполне пригодны для электронной обработки, и крупные клиенты с

собственными компьютерными мощностями могут самостоятельно подготавливать магнитные ленты и иные устройства компьютерной памяти с инструкциями дебетового перевода.

С. Маршрутизация инструкций перевода средств

<...>

20. Прямая передача инструкций перевода средств одним банком другому может сопровождаться физической передачей инструкций перевода средств в бумажной форме или передачей устройств компьютерной памяти, таких как магнитная лента, Прямая передача также предполагается имевшей место, если инструкция перевода средств передается между двумя банками без участия посредников, за исключением коммуникационной службы связи или расчетной палаты.

21. Коммуникационная служба, .при помощи которой передаются инструкции перевода средств, может быть доступна для публичного использования, как это имеет место в случае с почтовой или телексной службой, либо ее функции могут ограничиваться передачей сообщений между членами группы банков, как в случае 8УУ1РТ. В любом случае коммуникационная служба доставляет инструкции, сортирует или перенаправляет их соответствующему адресату. В некоторых электронных расчетных палатах, работающих в режиме онлайн, инструкции перевода средств передаются по общедоступным телекоммуникациям из банков на коммутационный блок, принадлежащий банкам-участникам определенной сети или используемый для их обслуживания.

22. Независимо от наличия публичного доступа к телекоммуникационным мощностям или коммутационному блоку или их принадлежности банкам или использования в их интересах, а также без учета того факта, какая сторона несет убытки в случае задержки или недоставки инструкций, мошенничества или ошибки в содержании инструкций, коммуникационная служба не влияет и не участвует в банковских отношениях. Банковские отношения существуют только между направляющим и получающим банком.

Р. Некоторые характерные черты электронного перевода средств

1. Замена одной или более бумажных операций

<...>

45. Одним из элементарных, но одновременно широко распространенных видов использования методов электронного перевода средств является замена одной или более операций в процессе перевода средств, который остается, преимущественно, основанным на применении бумажных документов. Характерной чертой системы перевода средств с применением бумажных документов является то, что инструкция перевода средств подготавливается и передается в банковскую систему в виде бумажной формы и часто направляется одним банком другому через систему в этой форме. Вместе с тем, для банка, который получает инструкцию в бумажной форме, отсутствует причина, препятствующая передаче информации, содержащейся в данной инструкции, получающему банку в электронной форме. Это наиболее просто реализуемо в национальных системах кредитовых переводов. Обычно плательщик не знает и не интересуется, каким образом инструкция кредитового перевода передается банками, поскольку такой перевод выполняется оперативно и точно. Банки поэтому способны переносить инструкции в бумажной форме на магнитную ленту или другое устройство компьютерной памяти и обмениваться этими устройствами непосредственно между собой или через автоматизированные расчетные палаты либо направлять инструкции кредитового перевода по каналам связи, если это окажется более эффективным.

46. По сути, аналогичный технический процесс может использоваться и для бумажных инструкций дебетового перевода, таких как чеки и переводные векселя. Инструкции могут храниться в банке-получателе (депозитарии), а наиболее важные данные могут направляться банку-плательщику (трассату) путем обмена устройствами компьютерной памяти или по каналам связи, т.е. бумажный чек вводится в сокращенной форме (транкируется) банком-получателем для обеспечения возможности его электронного представления в банк-плательщик. Вместе с тем, законодательство, относящееся к оборотным документам, будет продолжать применяться к инструкциям дебетового перевода средств, выданных в форме чеков, переводных или простых векселей с определенными потенциальными последствиями, если только в законодательство не внесены изменения для

перехода к электронной обработке данных'.

2. Телекоммуникации

47. Несмотря на то, что для банков уже давно стали привычными переводы крупных сумм с применением телеграфа и телекса, до недавнего времени наибольшая часть переводов крупных сумм продолжала совершаться в виде бумажных инструкций перевода средств, отправляемых по почте. В большинстве государств не ощущалась необходимость в кодификации банковского права и практики телеграфных и телексных переводов средств, пока они оставались исключительной формой перевода средств. Ориентированные на потребителей услуги электронного перевода средств, предлагаемые многими почтовыми службами, как правило, игнорировались при обсуждении вопросов электронного перевода средств. Вместе с тем, уже давно существуют подробные правила, регулирующие внутренние и международные телеграфные денежные переводы (когда получатель не имеет счета в почтовой системе жирорасчетов или в банке) и международные жиропереводы (когда получатель имеет такой счет). К интересным особенностям правил относятся предписанный формат инструкции телеграфного перевода средств и требование, что телекс должен быть на французском языке, если иное не согласовано двумя почтовыми службами.

48. Эти две системы электронного перевода средств исторически обслуживали различные рынки и были мало связаны между собой, как и аналогичные системы, основывающиеся на бумажных документах. Вместе с тем их объединяла одна черта. Хотя почтовая жиросистема имела процедуру отправления списков кредитуемых счетов, обе системы могут быть справедливо охарактеризованы как обеспечивающие возможность отправления индивидуальных инструкций перевода средств.

49. Сокращение стоимости услуг связи и повышение стоимости наземных и воздушных перевозок сделали для банков менее обременительной передачу большого числа инструкций перевода средств на крупные и малые суммы пакетным способом по каналам связи, в частности, когда в ночное время предлагаются более низкие тарифы и в иные периоды неполной загрузки каналов связи. В частности, SWIFT подписало соглашения о пакетной передаче подробных данных о некоторых операциях с использованием кредитных карт. Более того, во многих случаях пользователю в настоящее время выгоднее послать индивидуальную инструкцию перевода средств по каналам связи, чем использовать бумажную инструкцию. Возможно классифицировать «телеграфный перевод средств» как перевод, включающий элементы срочности, независимо от того, осуществляется он на крупную сумму через банковскую систему или на небольшую сумму через почтовую систему, и в отдельных случаях разработаны нормы права, отражающие необходимость оперативных действий в ответ на сообщение. Вместе с тем, по мере того, как использование каналов связи для передачи инструкций перевода средств становилось более привычным, оно утрачивает свой особый характер. В настоящее время использование каналов связи может быть описано только как другое средство, посредством которого инструкция перевода средств передается от банка-отправителя банку-получателю.

3. Пакетная передача

50. Ни стоимость, ни срочность большинства бумажных, а также электронных межбанковских инструкций перевода средств не оправдывают расходов по их передаче на индивидуальной основе между банками. Вследствие этого инструкции накапливаются и обмен ими осуществляется пакетами. Пакетная передача инструкций электронного перевода средств обычно осуществляется путем физического обмена устройствами компьютерной памяти. Такие устройства компьютерной памяти, содержащие инструкции перевода средств, обычно подготавливаются самими банками. Основными типами записанных в устройствах компьютерной памяти операций являются бумажные инструкции перевода средств, направляемые в банк, операции клиентов других банков, записанные в офлайновых автоматических пунктах выдачи наличных или банкоматах, постоянные разрешения на дебетование и постоянные кредитовые инструкции.

51. Клиенты банков, обладающие необходимыми мощностями и направляющие большое число инструкций дебетового и кредитового перевода могут самостоятельно подготавливать устройства компьютерной памяти. В большинстве систем банковская клиентура направляет устройства компьютерной памяти своим банкам, В некоторых системах клиентам разрешается направлять устройства компьютерной памяти непосредственно в автоматизированную расчетную

палату. В любом случае банк отвечает перед расчетной палатой за стоимость инструкций перевода средств, содержащихся в устройствах компьютерной памяти, представленных клиентами банка, а также за их техническое качество.

52. Равно как и в случае пакетной передачи бумажных инструкций перевода средств, банки-участники могут непосредственно обмениваться устройствами компьютерной памяти. Если таковая процедура затрудняется слишком большим количеством банков-участников, то обмен инструкциями может осуществляться через автоматизированную расчетную палату. Автоматизированная расчетная палата предоставляет почти такие же услуги, что и расчетная палата для бумажных инструкций. Если банки направляют инструкции, уже отсортированные банками-получателями, и если каждый пакет хранится в отдельном устройстве памяти, то банки могут просто обмениваться такими устройствами памяти. Более часто банки направляют устройства памяти, в которых отдельные инструкции не отсортированы банками-получателями или, если они отсортированы, одно и то же устройство содержит инструкции, адресованные более чем одному банку. В том и другом случае автоматизированная расчетная палата сортирует инструкции с использованием собственных компьютеров и подготавливает новые устройства памяти, содержащие инструкции, адресованные каждому банку-получателю.

53. Пакетная передача также обычно выполняется путем физического обмена устройствами компьютерной памяти, и выше, в пункте 49, уже отмечалось, что с сокращением стоимости передачи данных по каналам связи пакетные данные все больше передаются по этим каналам.

4. Электронный перевод средств, инициируемый клиентом

54. Электронный перевод средств начинается с действий сотрудника банка, получившего указание ответственного должностного лица данного банка (в случае перевода, инициируемого банком), клиента или другого банка. Вместе с тем, все большее число электронных переводов средств инициируется через клиентские терминалы. К таким терминалам относятся пункты выдачи наличных, банкоматы, пункты продаж, домашние банковские терминалы и онлайновые компьютерные терминалы, расположенные в месте ведения бизнеса коммерческих клиентов. К категории электронного перевода средств, исходящего от клиента, можно также отнести подготовку клиентом устройств компьютерной памяти, содержащих инструкции дебетового или кредитового перевода, и передачу их банку или, когда эта допускается, непосредственно автоматической расчетной палате.

55. Большое число переводов средств, инициируемых с использованием клиентских терминалов, проходит через весь процесс перевода средств без человеческого вмешательства со стороны банков. Компьютеры банков проверяют соответствие техническим нормам, требуемым для совершения перевода средств, представление надлежащей аутентификации, а также наличие на счету плательщика достаточного остатка для дебетования счета. В ряде случаев, особенно затрагивающих крупные суммы, со стороны должностного лица отправляющего банка может быть необходима санкция на перевод средств до принятия каких-либо действий на основании инструкции, даже если перевод был инициирован на клиентском терминале.

56. Электронные переводы средств, инициируемые путем использования пластиковой карты с магнитной полосой на обороте, содержащей информацию для идентификации держателя карты и его счета, включая персональный идентификационный номер (ПИН) либо информацию, по которой банковский компьютер может установить ПИН с помощью специального алгоритма, образуют особую подгруппу электронных переводов средств, инициируемых через клиентские терминалы. Использование карт с магнитной полосой в качестве устройств доступа порождает серьезные технические проблемы обеспечения надлежащего уровня безопасности против мошенничества. Это объясняется тем фактом, что подавляющее количество карт с магнитной полосой используется для инициирования потребительских переводов средств, что порождает вопросы о защите прав потребителя.

57. С появлением микропроцессорной технологии на кремниевом чипе стало возможным создание пластиковых карт с микропроцессорными устройствами. Это

обеспечивает дополнительные возможности хранения и обработки информации о держателе карты, обеспечивая, среди прочего, более высокий уровень безопасности. Микропроцессорные карты предполагается использовать в банковских операциях, особенно в сфере электронного перевода средств, инициируемого клиентами. Ожидается, что они найдут самое широкое применение в пунктах продажи, где наиболее важно обеспечение безопасности.

Глава II.
Соглашения о переводе средств и инструкцииперевода средств

С. Инструкции перевода средств

1. Аутентификация (установление подлинности)

<...>

26. Аутентификация документа или сообщения придает ему правовую форму, которая обеспечивает его .достоверность. Официальное установление подлинности заключается в оформлении документа в присутствии нотариуса или другого государственного должностного лица, уполномоченного выполнять такие функции, что, в частности, в странах с системой гражданского права придает документу особый вес при любом последующем судебном разбирательстве. Неофициальное установление подлинности состоит в проставлении на документе или сообщении отметки таким образом, чтобы указать на его источник. Инструкции перевода средств аутентифицируются неофициально.

27. Термин «аутентификация», используемый в настоящем документе, следует отличать от такого же термина, используемого в межкомпьютерных телекоммуникациях, особенно в том смысле, как это определено ISO DIS 7982. В этом контексте, учитывая наличие некоторых методов использования компьютеров, аутентификация сообщения может придавать юридическую силу как полному тексту сообщения, так и его источнику. Это, несомненно, является положительным свойством таких методов. Вместе с тем, поскольку такие методы доступны только при использовании компьютеров, они не применимы ни при электронном переводе средств, который не основан на использовании компьютеров, ни при переводе средств на основе бумажных документов.

28. Относительная редкость электронных переводов средств до внедрения компьютеров может быть отнесена на счет отсутствия законодательных или нормативных положений, которые требуют, чтобы инструкции электронного перевода средств аутентифицировались до получения заинтересованными банками разрешения на их выполнение. Вместе с тем, возможно, что все соглашения между банками и их клиентами требуют того, чтобы аутентификация инструкций перевода средств, выданных клиентом, производилась до получения банком разрешения на их исполнение. Соглашение должно также включать в себя форму аутентификации.

29. Во многих закрытых системах электронного перевода средств внедрены необходимые средства аутентификации проходящих через них инструкций перевода средств. Ориентированные на потребителя системы, такие как сети банкоматов, пунктов выдачи наличных и терминалов пунктов продаж, устанавливают процедуру аутентификации, требуемую от клиента. Сети межбанковских переводов средств устанавливают процедуру аутентификации, требуемую от банков-отправителей.

а) Форма аутентификации

30. Аутентификация инструкции перевода средств в бумажной форме обычно сопровождается подписью уполномоченного лица. Обычно подразумевается, что «подпись» означает собственноручно написанные имя или инициалы лица. Таким образом исполненная подпись считается личной подписью этого лица. Ее наличие в инструкции перевода средств является очевидным указанием на намерение лица выдать такую инструкцию. Более того, возможность ее сравнения с образцом подписи, известной как подлинная, обеспечивает средство проверки того, что подпись в инструкции также является подлинной.

31. Требования современной торговли привели к тому, что многие правовые системы разрешают совершение подписи в виде штампа, символа, факсимиле, перфорации или с использованием других механических или электрических средств'. Это отвечает изменениям и в других сферах торгового права.

Например, все основные многосторонние конвенции, регулирующие международную перевозку грузов, требующие наличия подписи в транспортном документе, разрешают, чтобы подпись была сделана не от руки, а каким-либо иным способом

32. Аутентификация инструкции перевода средств, совершенной электронным способом, должна производиться с использованием средств, соответствующих используемым средствам связи. При телексной и межкомпьютерной связи для проверки источника сообщений часто используются процедуры типа «обратный звонок» и проверочные ключи. Некоторые методы шифрования аутентифицируют как источник сообщения, так и его содержание. При снятии наличных в пункте

выдачи наличных, осуществлении перевода средств со счета с помощью банкомата или электронного перевода средств в пункте продажи с использованием пластиковой карты аутентификация производится в соответствии с наиболее широко используемой современной технологией, путем ввода в терминал персонального идентификационного номера (ПИН), совпадающего с ПИН, присвоенным держателю карты. В целях замены ПИН в экспериментальном режиме используются методы динамического анализа подписи компьютером и другие методы, основанные на характеристиках, присущих только конкретному лицу. Инструкция перевода средств, передаваемая по телефону, может аутентифицироваться с использованием кодов, а банк плательщика может сделать обратный звонок плательщику для проверки источника запроса. Более современные телекоммуникационные системы регистрируют идентичность телефонной линии как часть своих нормальных операций, и эта информация может быть доступна вызываемому терминалу. Нарушителю в системе пришлось бы не только симулировать процедуры аутентификации, но и сделать это с использованием линии, нормально используемой правомочным лицом.

33. Хотя аутентификация в любой форме выполняет основные функции установления источника инструкции и указания на то, что данная инструкция предполагалась быть выданной, существует принципиальная разница между собственноручной подписью и аутентификацией с использованием существующих электронных средств. Даже если собственноручная подпись может быть подделана столь качественно, что подделку трудно обнаружить, тем не менее подпись может быть надлежащим образом совершена только конкретным лицом. Поэтому, если подпись была подделана, то она по своему характеру является недействительной, не имеющим законной силы средством аутентификации, даже если другие соображения могут способствовать возникновению в правовой системе мнения, что в некоторых случаях нести ответственность за последствия должно лицо, чья подпись была подделана, а не лицо, которое добросовестно и без небрежности полагалось на подделанную подпись.

34. Механические формы подписи на бумажных документах и используемые в настоящее время методы аутентификации инструкции электронного перевода средств могут удостоверяться в надлежащей форме неуполномоченным лицом или лицом, превышающим свои полномочия. Если такое лицо располагает доступом к подлинной печати, перфорационному устройству, проверочному ключу, ключу шифрования,

35. Это различие между отдельными методами аутентификации инструкции перевода средств имеет определенные правовые последствия в случае, когда банк исполняет инструкцию перевода средств, в отношении которой проведена несанкционированная аутентификация. Эти правовые последствия обсуждаются в связи с распределением убытков, возникающих в результате мошенничества'. Тем не менее, это различие не следует понимать как означающее, что собственноручная подпись, требующая визуального сравнения, является более безопасной формой аутентификации, чем электронная. Напротив, подпись лица может быть достаточно легко подделана, чтобы быть признанной банком, даже если бы эксперт позднее мог определить с высокой степенью определенности, что она является подделанной. Кроме того, визуальное сравнение подписей является настолько длительной и дорогостоящей процедурой, что во многих странах она не производится в отношении инструкций перевода небольших сумм, даже если применимые нормы права могут предполагать или требовать визуального сравнения всех подписей. С другой стороны, электронная форма аутентификации может применяться с приемлемым уровнем расходов даже в отношении сделок на самые незначительные суммы. Более того, хорошо организованная система аутентификации и неукоснительное следование процедурам, необходимым для обеспечения безопасности системы, могут свести к минимуму вероятность того, что будут выполняться инструкции перевода средств с несанкционированной аутентификацией.

b) Что должно аутентифицироваться

36. Как указывалось выше, в пункте 12, при всех кредитных переводах в бумажной или электронной форме и при некоторых дебетовых переводах в бумажной форме, особенно затрагивающих традиционное инкассирование чека, инструкция перевода средств, выданная плательщиком, передается или представляется в банк плательщика. Поскольку эта инструкция перевода средств служит разрешением на перевод средств и дебетование счета плательщика, она является единственным сообщением, которое должно аутентифицироваться для этой цели. При транкировании инструкции дебетового перевода в бумажной форме банк плательщика дебетует счет

плательщика на основании инструкции перевода средств, выданной представляющим банком. Поэтому в данном случае должны аутентифицироваться как эта последняя инструкция, так и оригинал инструкции дебетового перевода.

<...>

38. При переводе средств в бумажной или электронной форме между двумя банками без участия клиента ни в качестве плательщика, ни в качестве получателя, очевидно, что инструкция перевода средств, передаваемая между двумя банками, должна аутентифицироваться. Если электронный перевод средств должен проходить через банки-посредники, для каждой операции перевода средств должна составляться новая инструкция перевода средств и она должна отдельно аутентифицироваться. Аналогичным образом, если электронный перевод средств инициируется, лицом, не являющимся клиентом банка, то должны аутентифицироваться как инструкция клиента, так и инструкция, передаваемая между каждой парой банков.

39. Когда инструкции перевода средств передаются пакетами, обычно производится единая аутентификация всего пакета. В случае передачи пакета по каналам связи, аутентификация касается заголовка сообщения. В случае передачи инструкций электронного перевода средств, передаваемых посредством физического обмена устройствами компьютерной памяти, аутентификация может затрагивать заголовок, отдельный лист бумаги или оба.

<...>

41. Отсутствуют общие законодательные требования в отношении необходимых элементов данных в необоротной инструкции перевода средств. Вместе с тем, многие электронные расчетные палаты и коммуникационные службы устанавливают необходимые элементы данных для передаваемых через них различных видов инструкций перевода средств. ISO DIS 7982 содержит перечень элементов данных, которые могут использоваться при межкомпьютерной передаче инструкций перевода средств, и приводит примеры того, каким образом они представляются в различных видах инструкций, не делает попытки определить, какие элементы данных могут оказаться необходимыми при данном виде перевода средств. Элементы данных для инструкций перевода средств, используемые в телексных сообщениях и при обмене сообщениями о дебетовых и кредитных картах между финансовыми учреждениями, также стандартизируются Комитетом ISO по банковской деятельности. Когда законодательство о защите прав потребителя предусматривает определенную информацию, которая должна присутствовать в периодической выписке по счету, инструкция перевода средств, направляемая банку-плательщику, должна содержать такую информацию, чтобы этот банк мог включить ее в выписку.

42. В тех случаях, когда транкирование бумажных инструкций дебетового или кредитового перевода осуществляется до их поступления в банк-получатель, электронная инструкция, подготовленная транкирующим банком, может не содержать все элементы данных, которые имелись на бумажной инструкции. Так, не передаются слова об оборотности чека. Дебетуемый или кредитуемый счет может указываться лишь по его номеру, если это возможно, а не по имени владельца. Сумма может указываться только цифрами, даже если бумажная инструкция содержит слова и цифры вместе и даже если применимое право предусматривает приоритет текстовой формы. Может также не включаться дата составления бумажной инструкции.

43. Банк-отправитель обязан удостовериться в том, что отправлены все элементы данных, которые могут быть необходимы банку-получателю, чтобы действовать согласно инструкции. Невыполнение этого требования делает инструкцию неполной. Вместе с тем, получающий банк может не знать о том, что инструкция является неполной, при этом инструкция будет исполнена неправильно. С другой стороны, банк-получатель может быть способен вывести некоторые элементы данных из содержания инструкций перевода средств. Внутренний перевод средств может предполагаться осуществляемым в местной валюте, если не установлено иное. Некоторые из требуемых элементов данных могут быть получены на основании уже указанных элементов данных. При правильном указании фамилии владельца счета обычно может быть установлен номер дебетуемого или кредитуемого счета и соответствующее отделение банка. В других случаях банк-получатель может исправить неполную инструкцию на основании предыдущих операций или другой имеющейся у него информации. Однако поскольку попытка исправить инструкцию банком-получателем может привести к неточности инструкции, ответственным за эту ошибку может стать банк-получатель, а не банк-отправитель. Поэтому, если у банка-получателя имеются какие-либо сомнения, он должен обратиться за разъяснениями.

44. Идентификация счета по фамилии владельца или номеру. Банковские счета обычно открываются на имя определенного физического или юридического лица. Один клиент может иметь несколько различных счетов для различных целей. Эти счета часто открываются на сходные, хотя и не идентичные фамилии. Аналогичным образом различные клиенты могут иметь сходные и даже идентичные фамилии. Более того, клиенты могут не всегда одинаково или абсолютно точно указывать фамилию, которую они используют в своем счете или в своих счетах. Банки обычно стремятся решить эту проблему, присваивая каждому счету уникальный номер, что позволяет им различать счета, открытые на похожие фамилии, или различные счета одного и того же клиента. Если каждому банку также присвоен уникальный номер, то весь процесс сортировки и маршрутизации инструкций перевода средств между банками и внутри банков может осуществляться автоматически с использованием методов машинного распознавания нанесенных магнитными чернилами символов (M1CR.), или оптического считывания символов (OCR.) в случае использования бумажных инструкций перевода средств, или компьютером в случае электронных переводов средств. При полной автоматизации банковских операций счет плательщика мог бы дебетоваться, а счет получателя - кредитоваться исключительно на основе машиночитаемых номеров счетов, что позволит сократить стоимость бухгалтерских операций, а также вероятность дебетования или кредитования неправильного счета.

45. Несмотря на преимущества осуществления перевода средств по номеру счета, а не фамилии его владельца, существует несколько проблем. Банк может присвоить один и тот же номер счета двум различным клиентам, хотя можно надеяться, что такая ошибка вскоре будет исправлена. Клиент может неправильно указать номер своего счета или номер счета другой стороны, или же, если банк должен занести этот номер на кодовую линию бумажной инструкции перевода средств или новую электронную инструкцию, он может сделать это неправильно. В случае переводов средств на основе бумажных документов эта проблема может быть уменьшена за счет использования бланков инструкций перевода средств, содержащих заранее впечатанные и пригодные для машинной обработки номера счетов. Заранее впечатать номера счетов как плательщика, так и получателя можно лишь в том случае, когда между ними регулярно осуществляются переводы средств. Однако, как правило, на бланках инструкций перевода средств заранее впечатать можно лишь номер счета или плательщика или получателя, а другой номер счета должен вноситься на бланк во время перевода средств. Номера дебетуемых и кредитуемых счетов при переводе средств, обрабатываемых компьютером, могут проверяться на предмет их наличия, что позволяет уменьшить возможность ошибки, но все случаи мошенничества при помощи такой проверки не могут быть исключены.

46. Хотя использование машиночитаемых бумажных инструкций перевода средств и использование методов электронного перевода средств привели к тому, что банки полагаются при переводах в основном на номера счетов, сейчас пока еще не ясно, в какой степени в различных правовых системах для банка юридически оправданно полагаться только на номер счета, указанный в инструкции перевода средств для дебетовых и кредитовых проводок, и, в частности, производить это автоматически по кодовой линии бумажной или электронной инструкции перевода средств. Когда перевод средств идентифицируется только по номеру счета, как, например, в случае операции, инициируемой путем использования пластиковой карты с магнитной полосой и ПИН в банкомате, автоматическом пункте выдачи наличных или терминале пункта продажи, банк может идентифицировать дебетуемый счет только по этому номеру, и можно полагать, что в большинстве стран такая практика является юридически оправданной либо в соответствии с общими принципами права, либо в результате договора между банком и клиентом. Однако, если в инструкции перевода средств указаны как фамилия владельца, так и номер дебетуемого или кредитуемого счета, а две стороны не состоят в договорных отношениях, то действующие правовые нормы могут предусматривать приоритет фамилии владельца счета. Правовая система может идти даже дальше и предусматривать, что банк должен расследовать случаи явного наличия ошибки или мошенничества. Однако в той степени, в какой это может отвечать действующим общепринятым в данной юрисдикции нормам, разработка быстрой, надежной и недорогой системы электронного перевода средств, несомненно, должна сопровождаться предоставлением банком возможности полностью полагаться на номер счета в инструкции перевода средств.

<...>

50. В прошлом инструкции электронного перевода средств, направляемые по телеграфу или телексу, не были стандартизованы. Шаг к стандартизации форматов сообщений инструкций

электронного перевода средств, несомненно, был сделан тогда, когда банки, непосредственно или с помощью автоматизированных расчетных палат, начали обмениваться устройствами компьютерной памяти, содержащими инструкции перевода средств. Для того чтобы компьютеры банка-получателя могли обрабатывать такие инструкции, программы компьютеров банков и автоматизированных расчетных палат должны быть совместимыми, а элементы данных должны водиться по стандартному формату.

51. В основном те же соображения касаются и переводов денежных средств, осуществляемых средствами межкомпьютерных коммуникаций. Хотя межкомпьютерная телекоммуникационная сеть не обладает какими-либо свойствами, препятствующими передаче сообщений в свободном формате, поскольку получающий компьютер может выводить сообщение на экран или производить бумажную распечатку, которая затем может использоваться в качестве эквивалента телексного сообщения, использование сообщения свободного формата лишает межкомпьютерную сеть присущих ей преимуществ. Поэтому для различных типов инструкций перевода средств, разрешаемых в каждой сети, были разработаны стандартные форматы. Банк, программирующий свои компьютеры для обеспечения их совместимости со стандартным форматом, используемым для внутренних и международных переводов средств, может производить операции по своим счетам непосредственно на основе получаемых, а также посылаемых инструкций при наличии, в крайнем случае, минимума дополнительно вводимых данных, имеющих отношение только к этому банку.

52. Как только конкретной закрытой сетью пользователей принят стандартный формат в отношении инструкций перевода средств, то использование этого формата должно стать обязательным. Действующий в рамках этой сети банк, не использующий требуемый формат, должен нести ответственность за вызванные этим убытки перед банком-получателем. Вместе с тем, когда банки могут использовать эту сеть также для сообщений, обязательно посылаемых в свободном формате, существуют доказательства того, что операторы компьютеров используют требуемые форматы для типа часто посылаемых сообщений, но пользуются сообщениями свободного формата для передачи сообщений менее распространенного типа. Поскольку несоблюдение требуемого формата может привести к дополнительной работе и задержкам для банка-получателя, даже если при этом может и не возникнуть исчислимый в денежном выражении ущерб, следует рассмотреть вопрос о введении для банка-отправителя стандартного сбора за каждое отклонение от требуемого формата.

53. Стандартные форматы, разработанные для различных закрытых сетей пользователей, не были ни идентичными, ни совместимыми во всех отношениях. Если форматы совместимы, хотя и не идентичны, то для них существует программное обеспечение, позволяющее преобразовывать инструкции перевода средств из одного формата в другой. Если форматы закрытых сетей пользователей для межкомпьютерных переводов средств, в которых банк принимает участие, несовместимы друг с другом, то банк, получающий инструкцию перевода средств из одной закрытой сети пользователей и передающий ее через другую сеть, возможно, должен будет повторно ввести эти данные для исходящей инструкции, что влечет соответствующие задержки, дополнительные расходы и, что самое главное, большую вероятность ошибок. Несовместимость форматов может препятствовать клирингу инструкций перевода средств между банками или же ограничивать доступ некоторых банков к некоторым аспектам рынка перевода средств.

54. Несовместимость форматов носит наиболее серьезный характер в тех случаях, когда формат сообщений в одной сети не содержит элементов данных, необходимых в другой сети. Эта последняя проблема возникла в своей наиболее острой форме применительно к использованию пластиковых карт с магнитной полосой в сетях пунктов продажи. Продавцы в большинстве стран, в которых сети пунктов продажи были созданы или вопрос об их создании активно обсуждается, как правило, настаивают на том, что они могут устанавливать у каждой кассы лишь один терминал пункта продажи. Если в большом числе магазинов будут установлены терминалы пунктов продажи, которые могут принимать лишь одну из нескольких конкурирующих карт с магнитной полосой, можно ожидать отрицательное воздействие на конкурентоспособность банков, принадлежащих к соперничающим системам. В результате этого в нескольких странах со стороны официальных кругов было оказано давление с целью принятия совместимого формата для таких карт. Эту проблему часто называют проблемой совместного использования технических средств.

5. Влияние межфилиальных операций

<-..>

80. Когда записи о счете клиента ведутся в автономном режиме в централизованном центре обработки данных, а образцы подписей для бумажных инструкций перевода средств хранятся в филиале, не совсем ясно, следует ли измерять время принятия банком соответствующих действий, начиная со времени получения бумажной инструкции в центре обработки данных или со времени его получения в том филиале, где может производиться проверка подлинности. В правилах многих расчетных палат время для возвращения неисполненной инструкции дебетового перевода или необрабатываемой инструкции кредитового перевода измеряется с того момента, когда получающий банк забирает ее из расчетной палаты. При этом не учитывается потребность банка получателя в обработке инструкции как в центре обработки данных, так и в филиале. Тем не менее, если по мнению большинства банков, участвующих в данной расчетной палате, это время является слишком незначительным, можно надеяться, что правила расчетной палаты будут изменены, с тем чтобы предоставить дополнительное время для возврата таких инструкций.

81. Поскольку ПИН, пароль или другие виды авторизации клиентом электронных переводов средств в режимах как «офлайн», так и «онлайн» содержатся в компьютере вместе с данными о его счете, то инструкции перевода средств должны направляться только в центр обработки данных, а не в филиал. Кроме того, если филиалы и отделения банка работают в режиме «онлайн», то записи о счете клиента и авторизации электронных переводов средств можно было бы оценивать с терминалов, установленных в любом из этих пунктов. Однако при переводах средств на основе бумажных документов банку плательщика, возможно, необходимо будет направить инструкции в соответствующий филиал для проверки подписи, даже если дебетовые или кредитовые проводки по счету клиента могли бы быть сделаны с работающего в режиме «онлайн» терминала в другом удобном месте. С другой стороны, если банки транки-руют бумажную инструкцию перевода средств, то отсутствует необходимость предоставлять им время на отправление этих инструкций в филиал для проверки подписи.

Глава III.
Обман, ошибки, неправильная обработка инструкций и связанная с этим ответственность

Введение

1. Сам объем электронных переводов средств и размеры сумм, подлежащих переводу, наводят на мысль о том, что возможные убытки при этом могут превышать убытки, имеющие место при переводе средств бумажными документами. В то же самое время клиенты банков озабочены, что переход от перевода средств бумажными документами к электронному переводу средств приведет к распределению между ними еще больших убытков, возникающих в результате ошибок или обмана. Вследствие попыток определить соответствующие основания для определения убытков в многочисленных новых и быстро меняющихся фактических ситуациях положение в области законодательства по этим проблемам стало еще более неясным. Даже если бы речь шла лишь о банковском законодательстве, регулирующем ответственность различных сторон в отношении перевода средств, то и в этом случае проблемы были бы достаточно сложными. Несмотря на то, что такого рода проблемы рассматривались в течение многих лет в связи с переводами средств бумажными документами, все еще существует значительное число вопросов, на которые невозможно найти ответы во многих правовых системах. Более того, изменения в процедурах, вызванные использованием электронного перевода средств, поднимают вопрос относительно того, должны ли распространяться правила об ответственности при переводе средств бумажными документами на электронный перевод средств.

2. Положение усугубляется быстро меняющейся ролью телекоммуникационных операторов и теми трудностями, перед которыми стоят законы, регулирующие вопросы ответственности. Если ранее вследствие общей монополии на средства связи телекоммуникации представляли собою внешнюю сферу по отношению к банкам, то сегодня офисное оборудование во многих банках объединено в локальные сети, отделения банков соединены по выделенным линиям связи, а банки направляют все большее число своих сообщений о переводе средств в другие банки с помощью телекоммуникаций. Телекоммуникации более не являются чем-то внешним по отношению к банкам, они стали насущным операционным средством их деятельности так же, как и во многих других

сферах экономической деятельности. В результате стирания граней между компьютерами и телекоммуникациями монополия телекоммуникационных услуг в некоторых странах уже нарушена или находится под угрозой. В результате такого развития возникают вопросы относительно того, является ли прежнее (и во многих случаях, все еще действующее) освобождение от ответственности, предоставляемое телекоммуникационным операторам, все еще жизнеспособной политикой.

3. В начале этой главы рассматриваются некоторые факторы, которые способствуют появлению ошибок или обмана при электронном переводе средств, и те действия, которые могут быть предприняты, для того чтобы свести подобные явления к минимуму. Во-вторых, рассматривается распределение убытков между различными сторонами перевода средств. Далее, обращается внимание на то, в какой мере и за чей счет клиент банка в качестве плательщика или получателя средств может возместить понесенные убытки в результате неправильной обработки инструкций перевода.

A. **Обман 1. Возможности для обмана**

<...>

4. Обман при электронном переводе средств затрагивает несанкционированные инструкции, изменение счета, по которому должна быть произведена проводка, или изменение суммы проводки. В целях предотвращения убытков от обмана должны предприниматься соответствующие меры той стороной, которая в состоянии не допустить появления несанкционированных инструкций, которые выдаются за санкционированные инструкции.

Ь) Обманное использование инициализируемых клиентами терминалов

<...>

13. Терминалы, расположенные по месту нахождения коммерческого предприятия клиента банка, а также банкоматы, пункты выдачи наличных, терминалы торговых точек и домашние банковские терминалы характеризуются тем, что они инициализируются клиентами. Одна из целей создания инициализируемых клиентами терминалов заключается в исключении необходимости человеческого участия со стороны банка. Это ведет к уменьшению возможности ошибок со стороны банка при обработке инструкций перевода средств. Однако, использование инициализируемых клиентами терминалов также увеличивает возможность *для* обмана.

14. Все компьютерные терминалы, которые санкционируют перевод средств, функционируют в сущности одинаково. До того, как физическое лицо сможет использовать терминал, оно прежде должно получить разрешение на такое использование. Банковский служащий может провести регистрацию один раз для получения разрешения на использование терминала в течение всего дня. Обычно инициализируемый клиентом терминал требует отдельного разрешения для каждой операции, если только он не находится в постоянном использовании клиентами. Отдельно взятый терминал или клиент могут иметь определенные ограничения в отношении типов операций, которые могут быть санкционированы, дебетуемых или кредитуемых счетов, а также в отношении денежных сумм, которые определяются для каждой операции ежедневно или любым другим соответствующим образом.

15. Процедуры регистрации или авторизации, которые должны выполняться до использования инициализируемым клиентом терминала, устанавливаются банком. Принимая решение о выполняемой процедуре, банк (или сеть электронных переводов средств, членом которой является банк) должен учитывать вопросы безопасности, стоимости и приемлемости для клиентов. Обычно чем более безопасна процедура авторизации, тем дороже обходится банку ее внедрение и поддержание и тем труднее для клиентов ее использовать. По маркетинговым соображениям может быть желательно, чтобы инициализируемый клиентом терминал был удобным для пользователя, но такой терминал также является доступным для вторжения. Это деликатный вопрос для банка и он видоизменяется по мере технологического прогресса.

16. Ограничения по видам операций, которые могут быть санкционированы, или счетов, которые могут дебетоваться или кредитоваться, являются эффективным средством уменьшения вероятности обманных операций. Ограничения в отношении размеров денежных сумм дают ограниченный эффект в плане исключения возможности обмана, но они могут быть важным средством ограничения финансовых последствий обмана. Последнее, однако, имеет смысл только в ориентированных на потребителя сетях, так как верхний лимит в коммерчески ориентированных сетях может быть настолько высок, что допускается достаточная возможность для серьезного

обмана.

17. Современные модели пунктов выдачи наличных, банкоматов и терминалов торговых точек требуют соблюдения двух условий для авторизации операции: наличия пластиковой карты с магнитной полосой, содержащей определенную информацию, и введения клиентом банка своего персонального идентификационного номера (ПИН). Новые и более безопасные формы пластиковых карт все еще находятся в экспериментальном использовании. В некоторых предлагаемых домашних банковских системах было бы невозможно предусмотреть использование пластиковых карт в целях авторизации, поэтому процедура авторизации может всецело зависеть от использования ПИН или пароля. В других системах ПИН или пароль, используемый клиентом в течение определенного периода времени, может дополняться уникальным номером сделки. Терминал, расположенный в деловом заведении, может обладать более сложной и, возможно, более надежной процедурой, но все процедуры, в сущности, обычно сводятся к использованию паролей и возможному использованию пластиковой карты.

18. В настоящее время в целях защиты ПИН банки используют два различных подхода. Один метод сводится к исключению возможности того, чтобы служащий банка или системы перевода средств мог узнать ПИН. ПИН формируется компьютером с использованием определенного алгоритма и некоторых основных данных, относящихся к клиенту. Получаемое в результате четырех- или шестизначное число вводится компьютером в запечатываемый конверт и отсылается по почте или каким-либо другим образом доставляется клиенту. Этот метод, при его надлежащем выполнении, может обеспечить безопасный ПИН для каждого клиента. Но поскольку это число является абстрактным и трудным для запоминания, многие клиенты банков считают необходимым иметь при себе этот номер всякий раз, когда они намерены использовать свои пластиковые карты, и, таким образом, серьезно компрометируют безопасность ПИН.

19. При другом подходе делается попытка облегчить клиентам банка запоминание ПИН, разрешая клиентам выбирать собственный номер. Клиент часто выбирает номер, основанный на цифрах его собственного дня рождения или дня рождения его супруги, связанных с домашним адресом, номером телефона или другим уже хорошо известным ему номером. Хотя такой метод выгоден, поскольку делает менее вероятным, что клиент банка будет носить этот номер с собой в письменной форме, тем не менее он имеет недостаток сведения к минимуму возможной комбинации цифр, выбранной данным лицом, и это, в свою очередь, облегчает определение ПИН данного лица. Более того, ПИН известен, по крайней мере, нескольким служащим банка, и поскольку ПИН больше не формируется компьютером, он должен вноситься в досье клиента и открыт любому лицу, имеющему доступ к этому досье.

20. Сохранность в тайне пароля, используемого в терминалах, расположенных в различных организациях и по месту жительства, приводит к той же самой проблеме. Пароль не должен быть настолько очевидным, чтобы его можно было легко угадать, или настолько сложным, чтобы пользователь был вынужден хранить его в письменной форме, если только запись не хранится под строгим контролем. Терминал, с помощью которого может совершаться широкий перечень переводов средств в значительных размерах, должен быть объектом дополнительных мер защиты. Регистрация может потребовать согласия двух различных лиц с различными паролями. Пароли могут меняться в течение относительно коротких интервалов, хотя это создает трудности для передачи их от банка клиенту и наоборот. Банк может автоматически аннулировать пароль, если он не используется в течение определенного периода времени, так как это может означать, что лицо, которому присвоен пароль, отсутствует.

21. Защита против обмана при использовании инициализируемых клиентами терминалов является общей заботой банка и клиентов. Банк должен внедрить и поддерживать настолько эффективную систему безопасности, насколько это практически осуществимо, принимая во внимание расходы и трудности, с которыми это может быть связано. Один из факторов, обеспечивающих качество системы безопасности, зависит от того, в какой степени клиенты банка, часто являющиеся непрофессионалами в использовании компьютеров и переводов средств, следуют тем инструкциям безопасности, которые они получают от банка.

c) Машиночитаемые инструкции, предоставляемые клиентом

22. Нечто подобное существует и в случае, когда клиент предоставляет банку или автоматической расчетной палате инструкции перевода средств пакетами на устройствах компьютерной памяти или в бумажной машиночитаемой форме. Хотя клиент отвечает за

надлежащую подготовку инструкций, включая использование механизмов внутреннего контроля в целях защиты от мошенничества и ошибок при подготовке инструкций, банк или расчетная палата отвечают за проверку того, чтобы количество поручений и их размер совпадали с указанными суммами, что они не выходят за рамки, санкционированные клиентом для таких пакетов, и что, другими словами, пакеты иным образом были свободными от изменений после их подготовки. Эти меры контроля могут быть легко осуществлены банком или расчетной палатой во время проверки устройств до обработки.

(1) Обман со стороны служащих банка

23. Служащие банков и других учреждений в системе перевода средств также имеют доступ к терминалам, с помощью которых они могут осуществить мошеннические операции. Обман со стороны таких лиц особенно трудно обнаружить, если в банке не существует хорошо организованная система. Очень много говорилось о возможности недобросовестного служащего запрограммировать компьютер для кредитования своего счета и после этого уничтожить все записи об этой операции. Это, однако, вряд ли возможно, так как компьютеры банка могут программироваться в целях полного протоколирования всей деятельности, включая команды об уничтожении операции. Чтобы это работало эффективно, механизм протоколирования должен программироваться лицами, отличными от участвующих в подготовке прикладных программ и подлежать независимому аудиту.

c) Обман путем перехвата телекоммуникационных сообщений

24. Сравнительно легко внедриться в любую телекоммуникационную систему, через которую могут направляться инструкции электронного перевода средств. Стоимость полной физической безопасности системы передачи данных настолько высока, что является неприемлемой в коммерческих целях. В силу этого архитектура любой системы электронного перевода средств не должна исключать возможности вмешательства, прочтения сообщений, изменения первоначальных и внедрения ложных сообщений. Первая линия защиты против всякого рода мошенничества - это использование шифрования. Если используемый стандарт шифрования достаточно высок, то не существует опасности вмешательства, изменения или внедрения ложных сообщений. Вместе с тем, стандарт шифрования, являющийся сегодня высоконадежным, через несколько лет может оказаться ненадежным в результате создания более мощных компьютеров, обеспечивающих более широкий поиск ключей шифрования, или, в случае применения криптосистем с открытым ключом, в результате развития новых методов факторизации больших чисел, на которых они основаны. Более того, реализация предложений некоторых стран о том, чтобы все ключи шифрования, используемые для трансграничной передачи данных, находились у какого-либо правительственного ведомства, может создать потенциально слабое звено в системе безопасности, над которым участники не будут иметь контроля. Введение жесткой системы регистрации всех входящих и исходящих инструкций перевода средств и присвоение входящих и исходящих последовательных номеров является средством контроля времени получения и отправления, а также причастности кого-либо к этому сообщению. Эти процедуры увеличивают вероятность того, что ложные инструкции могут быть распознаны, и они являются существенным средством для последующего обнаружения и протоколирования подозрительных инструкций.

2. Когда может быть оправдано дебетование счета на основании мошеннической инструкции

25. Хотя обычно банк вправе дебетовать счет клиента в сумме санкционированной инструкции, он может также дебетовать счет клиента на сумму определенных несанкционированных инструкций, особенно в тех случаях, когда обман стал возможен вследствие недостаточного контроля со стороны клиента. Например, не существует больших сомнений в отношении того, что счет клиента может быть дебетован на сумму мошеннического перевода, инициированного служащими, уполномоченными действовать от имени клиента, если только операция не выглядит столь необычно, что может вызвать подозрения со стороны банка.

26. Вместе с тем, менее ясно, банк или клиент должен нести убытки за обман, совершенный посредством инициализируемого клиентом терминала. Поскольку банк разрабатывает общие процедуры безопасности и авторизации, а клиент выполняет их, то один из подходов заключается в отнесении убытков на основании сравнительной небрежности в каждом случае. Такой подход может быть приемлем лишь в тех случаях, когда очевидно, что обман стал возможным в результате явно неадекватной процедуры безопасности и авторизации или в результате того, что клиент был весьма

небрежен, выполняя эти процедуры. Однако, это не является достаточным средством для распределения убытков, особенно в случаях обмана в ориентированных на потребителей системах, где индивидуальные убытки часто незначительны для поддержки судебного разбирательства.

27. В результате существует тенденция к поиску формул общего действия для большинства случаев. Договоры между банками и их клиентами, обычно являющиеся договорами со стандартной формой, подготавливаемые банками, как правило, разрешают банку дебетовать счет клиента в связи с любым переводом средств, совершенным с помощью определенного типа инициализируемого клиентом терминала, когда использовались надлежащие ПИН или пароль и пластиковая карта, если таковые имеются. В случае применения систем, при которых переводы санкционируются частично путем использования пластиковых карт, ответственность клиента обычно прекращается сразу после извещения клиентом банка об утрате или краже карты, и банк имеет возможность ввода информации в стол-файл. Это может происходить незамедлительно в случае использования онлайновой системы или на следующий банковский день в случае использования офлайновой системы.

28. Альтернативный подход, который был наиболее очевиден в отношении некоторых ориентированных на потребителей систем, заключается в разрешении банкам дебетовать счет клиента в связи с мошенническим переводом в пределах относительно небольшой суммы. Клиент несет значительный риск убытков, что побуждает его сообщать о любой утрате или краже пластиковой карты, компрометации пароля, ПИН или процедуры безопасности, тогда как банк несет риск основных убытков, что побуждает его стремиться к более надежной процедуре авторизации. Такой подход может дополняться правилом, что банк может дебетовать счет клиента на полную сумму, указанную в мошеннических переводах, если они являются результатом определенных действий клиента. Они могут включать в себя временную передачу карты с магнитной полосой третьему лицу и сообщение ему ПИН, написание ПИН на карте, а также иное хранение их вместе, так что утрата или кража одного равносильна утрате или краже обоих.

29. Третий способ отнесения убытков в большинстве случаев заключается в возложении на банк или клиента бремени доказывания того, как произошел обман, так как во многих случаях сторона, которая несет бремя доказывания, обычно проигрывает. Представляется особенно трудным доказать, что обман, совершенный третьим лицом, которое не было задержано, вызван действиями самого клиента, который оставил пароль в ящике письменного стола или написал свой ПИН на пластиковой карте. В обычном случае клиенту еще труднее доказать, что банк разработал недостаточную систему безопасности или не выполнял свои собственные процедуры авторизации и безопасности.

30. Страхование также может использоваться для перенесения убытков от мошенничества с банка на клиента. Вместе с тем, крупные или повторяемые убытки вскоре находят свое отражение в более высоких страховых премиях.

B. Ошибки

1. Общие источники ошибок при использовании компьютеров

31. Когда компьютеры начали впервые широко использоваться в некоторых странах в коммерческих целях, опыт, связанный с большим количеством ошибок, был обескураживающим для фирм, владеющих компьютерами, и разочаровывающим для их клиентов. Речь шла не только о большом количестве ошибок, но для фирм представлялось трудным исправить многие из них. Вместе с тем, ранний отрицательный опыт ошибок многих фирм при использовании компьютеров был отчасти обусловлен контролем качества самих аппаратных средств и неопытностью в разработке программного обеспечения. Эти факторы, однако, более не являются источником постоянного разочарования, каковыми они были первоначально; аппаратные средства являются высоко надежными, а программное обеспечение, все еще создавая проблемы, отличается лучшим качеством, чем прежде. Ошибки, возникающие в результате дефектов аппаратных средств и программного обеспечения, составляют незначительную долю в общем числе операций.

32. Ранний отрицательный опыт объясняется также теми неправильными процедурами, которые приняты во многих фирмах в отношении их вновь приобретаемых компьютерных систем. В целях достижения максимального объема операций, необходимых для поддержки мэйн-фрейма, часто создавался главный центр обработки данных, который организационно и физически был отделен от операционных управлений, которые получали, формировали и использовали данные. Центр обработки данных часто находился в отдельном здании и, в случае организации с филиалами в разных городах, он по необходимости был расположен в другом городе вдали от этих филиалов.

Персонал операционных управлений слишком часто не понимал потребностей управления обработки данных по представлению данных в соответствующей форме; управление обработки данных находилось в ведении специалистов, которые слишком часто не понимали операций и потребностей фирм; процедуры по устранению и исправлению ошибок не всегда требовали такого же уровня поддержки, как установка нового оборудования; и часто для клиентов, поставщиков и служащих в равной степени было трудно найти человека с достаточными полномочиями для решения возникающих проблем.

33. Хотя эти проблемы далеки от разрешения и сегодня, можно сказать с определенной уверенностью, что ошибки, возникавшие в связи с отделением управления обработки данных от операционных секторов фирмы, а также в результате неадекватных внутренних процедур в целом, более не являются причиной для беспокойства, как это было раньше. Операционный персонал лучше знаком с теми процедурами, которые необходимы для функционирования компьютеров, а персонал по обработке данных научился лучше приспосабливать технологические потребности и возможности компьютеров к требованиям коммерческой и административной деятельности, в рамках которой они функционируют.

34. В равной степени децентрализация ввода данных в компьютерные устройства была важна особенно в контексте банковской деятельности. В настоящее время во многих странах мира терминалы, как правило, находятся в различных операционных управлениях. Банковские автоматы, непосредственно взаимодействующие с клиентами банка, могут делать записи о депозитах и изъятиях наличных прямо в компьютере, также как и операционный персонал, получающий инструкции перевода средств и другие банковские инструкции по почте, телефону или другими средствами.

35. Децентрализация ввода данных в банках сократила вероятность ошибок во многих отношениях. Ввод данных в операционных управлениях, ответственных за операции, налагает на персонал, вводящий эти данные, ответственность за всю операцию. Эти лица могут чувствовать большую ответственность за точность данных, они получают ответ от компьютера немедленно и узнают о том, принята ли инструкция; они в большей степени осознают тот контекст, в котором создавались данные, и это дает им возможность осознавать трудности и разрешать их быстро и правильно, при этом данные следует вводить в записи банка только один раз, а не два или более, как это иногда происходило при системе централизованной обработки данных или системе, основанной на бумажных документов.

36 Внедрение инициализируемых клиентами терминалов с возможностями упорядочивания стандартных переводов средств еще в большей степени сокращает вероятность ошибок со стороны банка, так как инструкция перевода средств обычно обрабатывается автоматически без вмешательства со стороны персонала банка. Меньшая вероятность ошибок существует в полностью автоматизированной системе электронного перевода средств по сравнению с полуавтоматической системой или основанной на применении бумажных документов. Вместе с тем, ошибки в полностью автоматизированной системе гораздо труднее доказать, особенно в том случае, если они повлияли лишь на одну операцию. Соответственно, вопрос о распределении ответственности за любые убытки, возникающие в результате этого, сам по себе является для клиента серьезной проблемой. Другие виды ошибок могут затрагивать многих клиентов в связи с чрезвычайно большим числом операций, обрабатываемых компьютером. Более того, в силу растущей сложности компьютерных систем, используемых в настоящем или планируемых в будущем, фактически невозможно полностью обеспечить отсутствие ошибок. В результате этого существует возможность крупных сбоев, выходящих за пределы предыдущего опыта, и необходимо, чтобы банки предусмотрели аварийные меры для учета этой возможности.

2. Текущие источники ошибок, присущих электронному переводу средств

а) Нестандартизированные сообщения

37. В связи с отсутствием общепризнанного стандартного формата инструкций электронного перевода средств увеличивается возможность ошибки при составлении сообщения отправителем или его восприятии получателем. Более того, если поля сообщения в двух межкомпьютерных сетях перевода средств полностью не совпадают, допуская автоматическое преобразование из одного формата сообщений в другой посредством интерфейсного программного обеспечения, то инструкция перевода средств, полученная из одной сети, должна быть полностью или частично перекодирована для отправления через вторую сеть.

b) Воссоздание сообщений

38. Перекодирование сообщения о переводе создает возможность ошибок. Эта возможность в некоторой степени неизбежна при любом электронном переводе средств. В отличие от переводов средств бумажными документами, когда первоначальный документ, заполненный клиентом, обычно можно направить через банковскую систему, препятствуя изменению платежной инструкции, за исключением обмана, сообщение электронного перевода средств воссоздается на каждом этапе обработки. Платежные инструкции, поступающие в банк в бумажной форме, преобразуются в электронные сообщения, которые после этого снова могут воспроизводиться на бумаге при получении. Для перевода по телетайпу через банк-корреспондент необходимо, чтобы банк-корреспондент послал новые сообщения с несколько иным содержанием данных. Сообщения, направляемые через сети пакетной коммутации, разбиваются на элементы одинаковой длины, которые передаются по отдельным каналам и вновь собираются в пункте назначения. Инструкции о переводе, подаваемые на магнитных лентах в автоматическую расчетную палату, сортируются и записываются на новые магнитные ленты, прежде чем их посылают банку-получателю.

39. Каждый из этих процессов создает возможность непроизвольного изменения содержания платежной инструкции вследствие ошибки человека, неправильной компьютерной программы, сбоя или поломки оборудования. Однако эти ошибки можно выявить, прежде чем они попадут в систему, если в системе, а также в операциях каждого банка предусмотрены необходимые контрольные меры и они строго выполняются. (]) Компьютерные сбои и ошибки в программном обеспечении 42. Один из источников ошибок при электронном переводе средств, который не существует при переводах средств бумажными документами, связан с самим электронным оборудованием. Оно включает в себя компьютерные аппаратные средства банков, телекоммуникационных операторов расчетных палат или других коммутаторов сообщений и программное обеспечение для их функционирования. Хотя ошибки из этих источников относительно немногочисленны по сравнению с ошибками, имевшими место всего несколько лет назад, они тем не менее особенно серьезны. Ошибка, возникающая в результате неправильного ввода инструкции перевода средств в систему, затрагивает только это одно сообщение. Однако дефект компьютерных аппаратных средств или программного обеспечения может отрицательно сказаться на всей серии инструкций. Более того, сам характер проблем в аппаратных средствах или программном обеспечении может вызвать ошибку, приводящую к обходу процедур проверки достоверности, предусмотренных в большинстве компьютерных программ. Самое важное, с юридической точки зрения, заключается в том, что ошибки, возникающие в результате дефектов аппаратных средств и программного обеспечения, ставят серьезные вопросы в отношении ответственности за возникающие в результате убытки.

3. Возможные методы предотвращения ошибок

43. К счастью, каждый банк самостоятельно может принять большинство мер, которые необходимы для сокращения числа ошибок, возникающих при электронном переводе средств. Некоторые другие меры, однако, могут быть приняты только банковским сообществом в целом. В частности, следует установить стандартизированные форматы сообщений и банковских процедур как для внутренних, так и для международных переводов средств. Соглашение на международном уровне может быть в некоторых отношениях более важным и более трудным. Крупные суммы переводятся по международным оптовым сетям, а международные системы электронного перевода средств, связанные с потребителями, приобретают все большую важность. Более того, соглашение на международном уровне должно заложить твердую основу для соглашений на национальном уровне.

44. Международное банковское сообщество в настоящее время участвует в нескольких проектах в рамках Банковского комитета (ТС 68), Международной организации по стандартизации (ISO), что должно привести к выработке общепризнанных форматов для наиболее типичных сообщений при международном переводе средств. Проект международного стандарта ISO (DIS) 7982, часть 1, содержит словарь и элементы данных, используемые при описании, обработке и форматировании инструкций перевода средств. ISO/DIS 7746 предусматривает стандартные телексные форматы для инструкций межбанковского перевода средств. Эти стандартные форматы, основанные на форматах сообщений SWIFT, предназначены 1) для исключения неправильного толкования со стороны банка-получателя инструкции банка-отправителя, и 2) обеспечения основы для разработки системы для автоматической обработки телексных инструкций перевода средств. Другая работа ISO TC 68 по таким вопросам, как проверочные ключи, технические характеристики магнитной

полосы карт и спецификация обмена сообщениями по дебетовым и кредитным картам, будет также способствовать более эффективному, безошибочному и безопасному электронному переводу средств.

45. Постепенное принятие стандартных форматов ISO для телексных инструкций перевода средств, находящихся в полном соответствии с форматами сообщений SWIFT и согласующихся со словарем, используемым при передаче инструкций перевода средств, а также их принятие и использование во всем мире для внутренних и международных переводов средств, уменьшит вероятность ошибок, возникающих вследствие необходимости перекодировки инструкций перевода средств. Стандартный формат телекса с числовыми полями признаков, а также идентификаторы полей позволят банку-получателю вводить инструкции в свою компьютерную систему для внесения в записи банка и для повторной передачи, в случае необходимости, без интерпретации инструкции. Это имеет особую ценность в тех случаях, когда банк-получатель и банк-отправитель принадлежат к различным языковым зонам.

46. Можно также надеяться и ожидать, что с течением времени международное банковское сообщество через соответствующие институты сможет договориться в отношении процедур, выполняемых получающим перевод банком, особенно когда он не является банком получателя средств. Следует признать, однако, что когда получающий банк должен передать инструкцию о переводе средств через внутреннюю систему перевода средств, то соглашение о действиях, которые он должен предпринимать, потребует значительной степени гармонизации технических средств, с помощью которых обрабатываются переводы средств на национальном уровне в различных странах, а также соответствующих банковских законов и процедур. В качестве временной меры для создания основы для будущих усилий по гармонизации может послужить более четкое определение действий, которые предпринимает получающий банк в различных странах в стандартных ситуациях, и времени, которое требуется для осуществления этих различных действий.

E. Допустимость оговорки об освобоиедении от ответственности

62. Степень, в которой условия об освобождении от ответственности в договорах, регулирующих электронный перевод средств, будут принудительно осуществляться [судом], зависит отчасти от общего подхода правовой системы в отношении такого рода оговорок и отчасти от степени, в которой законодательство, регулирующее переводы средств, рассматривается в качестве обязательного или необязательного. Можно ожидать, что условия об освобождении от ответственности, непосредственно затрагивающие права и обязанности в отношении оборотных документов, не будут принудительно осуществляться, в то время как условия, относящиеся к их инкассированию или электронному переводу средств, ни одно из которых не отражено во всеобъемлющих законах в большинстве стран, с большей вероятностью могут принудительно осуществляться. Там, где принят закон о защите прав потребителей при электронном переводе средств, как это имеет место в США, такие права могут быть изменены лишь в ограниченной степени договорными условиями.

63. Договорное освобождение от ответственности в договорах между банками, между банками и другими организациями при осуществлении электронного перевода средств и между банками и поставщиками компьютеров и программного обеспечения, не имеет никакой официальной силы в отношениях между банками и его клиентами. Клиент как сторона-инициатор может предъявить свой иск организации, чьи действия или бездействие вызвали убытки, безотносительно к условиям об освобождении от ответственности в договорах, стороной которых он не являлся.

1. Технические недостатки компьютерных аппаратных средств и программного обеспечения

64. Многие договоры между банком и клиентами прямо или косвенно предусматривают, что банк освобождается от ответственности за свою неспособность выполнить инструкцию перевода средств надлежащим образом, если он может доказать технические недостатки компьютерных аппаратных средств и программного обеспечения. Вместе с тем, такое освобождение от ответственности по указанным причинам должно быть в значительной степени ограниченным.

65. Хотя компьютеры стали значительно более надежными по сравнению с прошлым, простои компьютеров случаются достаточно часто. Банки, использующие компьютеры для перевода средств, а также в других целях, должны иметь и обычно имеют достаточное дополнительное оборудование, находящееся либо в их собственном помещении; либо в помещении других организаций (поставщика компьютеров, сервисного бюро, другого банка или другой фирмы, имеющих соответствующее

оборудование), чтобы осуществлять операции в тот период, когда их собственные компьютеры бездействуют, возможно, с некоторым ущербом для дела. Именно поэтому простои компьютеров предполагаемой длительности, которые должны быть компенсированы за счет использования дополнительных возможностей, не должны с готовностью приниматься в качестве оправдания неспособности выполнить инструкцию по переводу средств в иной приемлемый период времени. С другой стороны, некоторая задержка является допустимой. Кроме того, простои компьютеров, выходящие за рамки ожидаемого периода, особенно если они связаны с общей аварией или нехваткой электроэнергии в месте, где расположен банк, или *они* связаны с крупной аварией, относящейся к банку, как, например, пожар, могут служить основанием для освобождения банка от ответственности.

66. Банки, которые не имеют достаточного числа дополнительных компьютеров; должны сохранять существующие у них возможности для получения и отправления инструкций перевода средств с использованием других приемлемых каналов.

2. Служба передачи данных

68. Большинство межбанковских и внутрибанковских электронных переводов средств должны использовать службу передачи данных. Традиционно телекоммуникационные операторы часто были освобождены от ответственности за ущерб, причиненный в результате задержки или недоставки сообщений или за любое изменение содержания самого сообщения.

69. Тот аргумент в пользу освобождения от ответственности, что телекоммуникационный оператор не мог предвидеть последствий задержки или недоставки сообщения либо изменения его содержания, поэтому он не знал содержания, не всегда являлся удовлетворительным в отношении телеграфной и телексной служб, когда клиент вручает сообщение оператору для его передачи. Во многих случаях персонал поставщика услуг полностью осознает значение посылаемого сообщения. В любом случае, когда ущерб нельзя было предвидеть, вид и размеры ущерба могли бы быть максимально ограничены, но это не оправдывает полное освобождение от ответственности.

70. Межкомпьютерные телекоммуникации, осуществляемые обычными операторами связи, на первый взгляд, представляются типичным примером случая, когда оператор не знает содержания сообщения, особенно если сообщение зашифровано. Если внедрены цифровые сети интегрированных услуг (ISDN), оператор может даже не знать, передает ли он данные, письменные сообщения, голос или образы; все это передается в виде цифровых строк. В то же самое время операторы более не ограничивают себя лишь предоставлением основных телекоммуникационных услуг. По мере стирания различий между компьютерными услугами и телекоммуникациями операторы предлагают более совершенные услуги, а поставщики компьютеров и офисного оборудования объединяют свое оборудование в сети. Во многих случаях банк или иной пользователь может получить одинаковые или эквивалентные услуги от оператора сети с добавленной стоимостью (VAN) или телекоммуникационного оператора. Способность переадресовывать сообщения входит в число услуг, доступных во многих странах, и это более не является исключительной привилегией телекоммуникационных операторов. По этой причине, даже если освобождение от ответственности оператора остается здравой политикой общества в отношении основных внешних телекоммуникационных услуг, освобождение от ответственности за эти основные услуги должно ограничиваться теми услугами, которые невозможно получить из других источников, не обладающих таким же правом на освобождение от ответственности.

71. Во многих странах телекоммуникационные услуги предоставлялись государством, часто через те же министерства, которые оказывают почтовый услуги. В результате телекоммуникационные службы получили преимущества от общего освобождения государства от ответственности. Когда это необходимо, общее освобождение от ответственности сопровождалось специальными правилами, защищающими телекоммуникационные услуги. В странах, где телекоммуникационные услуги предоставлялись частными компаниями, регулятивная структура, в рамках которой действовали эти компании, позволяла ограничивать ответственность в части, касающейся тарифов.

72. Однако прежнее монопольное положение телекоммуникационных операторов более не является самоочевидным и возникает вопрос в отношении того, следует ли и впредь сохранять освобождение от ответственности. Дерегулирование деятельности национальных операторов в США уже устранило прежнюю правовую основу для освобождения от ответственности в этой стране. Все еще не ясно, будут ли суды учитывать оговорки, включаемые в договоры операторами,

предполагающие ограничение ответственности в случаях их собственной небрежности.

73. Вопросы ответственности представляют собой второстепенную проблему в рамках более широкого обсуждения будущей сферы публичных телекоммуникационных услуг. Однако по мере того, как основные частные пользователи, такие как банки, организуют частные сети, в рамках которых они осуществляют контроль над техническими средствами и принимают риск в случаях задержки, недоставки сообщений или их изменения при передаче, на государственных телекоммуникационных операторов будет оказываться все большее давление, чтобы они принимали на себя аналогичный риск.

3. Должен ли инициирующий банк освобождаться от ответственности за задержку или недоставку инструкции перевода средств после ее отправки

74. Поскольку невозможно привлекать телекоммуникационного оператора к ответственности за убытки, причиненные в результате недоставки сообщения надлежащим образом, то стороны, использующие телекоммуникации, действуют таким образом, чтобы распределить между собой возникающие убытки. В контексте телеграфного или телексного перевода средств для банков является нормальным предусматривать в договорах с клиентами, что банк не несет ответственности за такие убытки. В результате клиенты банков несли полный риск того, что сообщение перевода средств не было получено или получено в измененном виде. Разумность такого договорного условия основывалась на неспособности банка осуществлять контроль над сообщением, после того как оно было отправлено телекоммуникационному оператору для передачи.

75. Разумность такого договорного условия представляется менее очевидной в том случае, если сообщение отправлено банком с использованием своего собственного телекса непосредственно на телекс банка-получателя. Оператор предоставляет только линию связи и коммутатор для соединения двух телексных устройств. Банк, направляющий сообщение, может потребовать ответ, чтобы проверить надлежащее соединение, и направить проверочный ключ, чтобы установить подлинность отправителя и проверить, что части сообщения этого ключа не были изменены по ошибке. При наличии сомнений в правильности получения сообщения или в случаях, когда сообщение является особенно важным, за счет повторной передачи банк-отправитель может потребовать, чтобы банк-получатель повторил полностью сообщение.

Глава IV.
Окончательность перевода средств

<...>

C. Технологические изменения, затрагивающие окончательность

<...>

2. Пакетная обработка

33. Использование методов пакетной обработки изменяет ряд фактических предпосылок, на которых часто основываются традиционные правила об окончательности:

а) в целях достижения операционной эффективности при пакетной обработке значительного числа операций были созданы централизованные механизмы обработки данных. При этом записи о счетах уже больше не ведутся отдельными отделениями банка. Осуществление соответствующих действий, ведущих к выполнению или к отказу в выполнении инструкции, часто распределяется между центром обработке данных и отделениями.

Ь) для создания однородных пакетов с необходимыми характеристиками инструкции могут периодически собираться и передаваться в механизм обработки данных, причем в некоторых случаях только в конце дня. Инструкции перевода средств, исполняемые в определенный день, могут заранее направляться до даты совершения проводок в автоматическую расчетную палату или банк получателя для предварительной обработки. Уже больше не существует установленной взаимосвязи между моментом, когда определенная инструкция перевода средств получена банком, когда прямо или косвенно принимается решение его исполнить, когда делаются проводки в записях по счету к когда перевод средств вступает в силу. Правила окончательности,, основывающиеся на этой фиксированной взаимосвязи, становится трудно применять на практике.

с) пакетная обработка предназначена для экономичной обработки большого числа операций, а не для ускорения обработки. Перевод средств, осуществляемый в определенный день, может заранее обрабатываться банком плательщика, автоматической расчетной палатой или банком получателя, часто за много дней до установленной даты. Инструкция перевода средств, полученная

для исполнения текущим днем:

может обрабатываться вечером того же дня. Только на следующий день банковские служащие, ответственные за счета клиентов, получат распечатки, показывающие запись операций и новое сальдо по счетам. Правила о завершении, предусматривающие осуществление всех действий в течение дня получения, может оказаться трудно применить при пакетной обработке. 3. Онлайновая обработка данных

34. Внедрение онлайновой обработки данных вновь затрагивает некоторые аспекты ранее применявшейся процедуры, при которой инструкции обрабатывались индивидуально. Когда банк обрабатывает переводы средств в режиме онлайн, его компьютер проверяет подлинность инструкции, состояние затрагиваемых счетов и одновременно проводит дебетование и кредитование счета, независимо от того, условное или нет. В результате онлайновой обработки данных:

а) онлайновые дебетовые и кредитовые проводки по счетам в многочисленных отделениях банка, а также внешних офисов снимает с правил окончательности (и сроков) предыдущие ограничения, связанные с физическим нахождением записей о счетах;

Ь) индивидуальные переводы средств обрабатываются в банке и проводки делаются на индивидуальной основе без ожидания формирования пакетов с соответствующими характеристиками или физической доставки инструкций в центр обработки данных. Записи счетов постоянно отражают порядок, в котором производились онлайновые операции, включая точное время, если это желательно.

4. Инициализируемые клиентами терминалы

<...>

38. Офлайновые инициализируемые клиентами терминалы хранят данные об операциях в устройствах компьютерной памяти для дальнейшей пакетной обработки. В большинстве случаев уместны обычные правила об окончательности, применимые к пакетной обработке инструкций перевода средств. Вместе с тем выдача наличных в пункте выдачи наличных, в онлайне или офлайне, вероятно, будет считаться окончательной в момент снятия наличных. В этом случае дебетование счета клиента будет представлять собой только реализацию акта ведения записей. Это будет соответствовать правилам, регулирующим момент окончательности по чекам, или инструкциям кредитового перевода, платеж по которым производится наличными.

<...>

6. Микропроцессорные карты <...>

44. Поскольку микропроцессорные карты еще не получили широкого распространения при переводе средств, влияние этой новой технологии на правила окончательности можно только предполагать. Вместе с тем, складывается впечатление, что если микропроцессорная карта используется только как более безопасное, по сравнению с существующими, средство идентификации плательщика, непосредственного влияния на законы, регулирующие перевод средств, включая правила окончательности, она не оказывает. Это справедливо независимо от того, осуществлялся ли перевод средств в режиме онлайн или офлайн. Аналогично, если используется офлайновая система и карта запрограммирована на авторизацию определенного числа покупок (безусловно при гарантии платежа банком плательщика), но дебетование счета плательщика и кредитование счета получателя производятся только после осуществления покупки, представляется, что правила окончательности будут теми же, которые применяются в случае гарантии платежа.

45. Третья процедура перевода средств с использованием микропроцессорных карт порождает более сложные вопросы в отношении соответствующих правил окончательности. При этой процедуре микропроцессорные карты загружаются на определенную сумму банком плательщика. Плательщик может перевести наличные в банк плательщика, но обычно его счет дебетуется на эту сумму в момент загрузки карточки. По мере использования карты в терминалах для покупки товаров или услуг сумма стоимости, доступная на карте, сокращается. Счет получателя (продавца) кредитуется банком получателя в режиме онлайн либо, что более вероятно, офлайн на сумму покупки. При этой процедуре весь процесс перевода средств состоит из двух этапов: загрузки карты стоимостью и использования стоимости для покупки товаров и услуг. Эти два этапа можно рассматривать как две отдельные операции или как одну операцию, происходящую в два различных момента времени. При любом из этих подходов кредитование счета получателя становится окончательным в одно и тоже время, то есть только в момент покупки товаров и услуг или позднее. Однако дебетование счета плательщика можно считать окончательным либо в момент загрузки карты

стоимостью и дебетования счета, либо в момент использования карты для покупки товаров и услуг.

46. С одной стороны, дебетование счета плательщика можно считать окончательным, не принимая во внимание использование карты, если загрузку карты банком плательщика и соответствующее дебетование счета плательщика рассматривать как операцию, эквивалентную снятию плательщиком со счета наличных или продажу дорожных чеков или не денежных жетонов для использования в общественном транспорте или общественной телефонной сети. Хотя у плательщика сохраняется тот же размер денежной стоимости, она приобретает отличную форму.

47. С другой стороны, карта может рассматриваться как особая форма счета плательщика в банке плательщика. Если принимается эта точка зрения на операцию, карту можно рассматривать в качестве отдельного счета, либо особой формы первоначального счета. Если карта образует отдельный счет, дебетование первоначального счета будет окончательным после загрузки карты. Дебетование счета, содержащегося на карте, осуществляемое в связи с покупкой товаров и услуг, вероятно, будет окончательным в момент покупки, когда сохраняющаяся на карте стоимость доступна для использования плательщиком путем сокращения терминалом пункта продажи. Если карта является особой формой первоначального счета, дебетование первоначального счета будет окончательным в момент покупки. В любом случае неиспользованная стоимость карты будет представлять собой требование клиента к банку. Представляется, что банк может осуществить зачет своего требования против этой стоимости. Более того, на эту стоимость, вероятно, распространяется любое обременение требований клиента к банку, и, таким образом, банк обязан принять меры по предотвращению дальнейшего использования карты.

Глава V. Правовые вопросы, связанные с электронным переводом средств

Введение

1. В предшествующих главах настоящего правового руководства говорится о связи между развитием электронного перевода средств и развитием систем перевода средств с помощью бумажных документов с учетом правового режима, регулирующего перевод средств. В настоящей главе излагается ряд правовых проблем, вытекающих из развития таких систем переводов, которые следует рассматривать в качестве вопросов для рассмотрения при разработке новых правил, необходимых в связи с введением в практику электронного перевода средств. Большинство этих проблем затрагивает конкретные вопросы, связанные с соответствующими правовыми нормами, и основано на обсуждении, изложенном в предшествующих главах. Некоторые из проблем затрагивают вопросы общей политики. После каждого вопроса приводится краткий комментарий, указывающий на некоторые факторы, которые могут оказать влияние на принятие решения по поставленному вопросу.

Вопрос 1

Влечет ли развитие электронного перевода средств существенное изменение законодательства?

Комментарий

1. Поскольку основополагающие процедуры перевода средств остаются неизменными независимо от того, является ли носитель информации бумажным или электронным, можно было бы ожидать, что законодательство, регулирующее перевод средств с помощью бумажных документов, будет в основном соответствовать электронному переводу средств. Вместе с тем, поскольку электронный перевод средств осуществляется отличным от перевода средств бумажными документами образом, возникает необходимость в изменении законодательства для приведения его в соответствие с новыми процедурами. В следующих пунктах приводятся некоторые основные элементы, которые влияют на степень необходимой адаптации законодательства, предусмотренного для перевода средств с помощью бумажных документов, к электронному переводу средств.

<...>

4. Даже в странах с достаточно развитой правовой структурой для кредитовых переводов с помощью бумажных документов новая технология требует уточнения законодательства по таким вопросам, как сроки, в течение которых должны осуществляться те или иные операции, наличие или отсутствие ответственности в связи с компьютерным сбоем в одном из банков, расчетных палатах или коммуникационных сетях, время, когда перевод средств считается окончательным, и последствия окончательности перевода. Модификация такого рода существующих правовых норм не затрагивает их структуры, но может в значительной степени изменить их содержание.

5. Несмотря на то, что отсутствие оборотности в электронном переводе средств позволяет упростить законодательство путем гармонизации правовых норм, регулирующих дебетовый и кредитовый переводы, техническое развитие альтернативных способов совершения переводов средств и постоянное изменение технологии может привести к возникновению новых отраслей права. Полезно различать переводы средств, обрабатываемые пакетами, индивидуальные переводы средств, направляемые по каналам связи, операции с использованием дебетовых карт и кредитных карт, переводы, совершаемые с инициализируемых клиентами терминалов и когда обмен сообщениями инициируется в банке. В определенной степени такие различия могут быть достаточно точно отражены в договорах между банками и их клиентами и в межбанковских правилах, регулирующих различные типы сетей перевода средств. Однако в отдельных случаях целесообразно отразить эти различия в законодательных нормах, регулирующих переводы средств. Если число специальных правил, являющихся результатом этих различий, невелико, то вопрос о них можно рассматривать в рамках общего законодательства о переводе средств. Если же число специальных правил значительно, то может быть предпочтительнее принять специальное законодательство, подобное тому, которое в настоящее время применяется в отношении дебетового и кредитового переводов. В любом случае сохранится потребность в правилах, регулирующих перевод средств с помощью бумажных документов и, в частности, распространяющихся на чеки и векселя.

6. Некоторые вопросы, возникающие в связи с электронным переводом средств, являются общими для всех форм автоматической обработки данных; соответственно, правовые нормы также могут быть общими для всех подобных операций. Важным среди этих вопросов является вопрос о доказательной силе компьютерных записей инструкций перевода средств, отправляемых и получаемых в форме, пригодной для компьютерной обработки, и данных о состоянии счетов, хранящихся в .таком виде. Особый вопрос - это приемлемость средств аутентификации, используемых при электронном переводе средств. В некоторых случаях правила, относящиеся к этим вопросам, могут быть скорее обнаружены в законодательстве, регулирующем перевод средств, чем в законах общего применения.

7. Рост электронного перевода средств наряду с ростом международных переводов крупных и малых сумм ведет к международной стандартизации процедур перевода средств и повышению интереса к международной унификации и гармонизации применяемых правовых норм. Настоящее правовое руководство является важным шагом в этом направлении. Следующим шагом будет разработка правил, регулирующих различные аспекты международного перевода средств. Затем будет проведена унификация или гармонизация некоторых аспектов национального законодательства, в частности, в отношении тех аспектов перевода средств, которые являются национальным продолжением международного перевода средств.

<...>

Вопрос 7

Придают ли доказательственные правила записям о переводе средств, ведущимся в машиночитаемой форме, ту же правовую ценность, что и записям, ведущимся на бумаге?

Комментарий

1. Хотя доказательственные правила не являются частью права электронного перевода средств, чтобы внутренние или международные электронные переводы средств осуществлялись с Правовыми гарантиями, доказательственные правила должны предоставлять банковским записям, ведущимся в машиночитаемой форме или представляемым на основе компьютерных проводок по счетам, ту же степень правовой ценности, что и записям, ведущимся или представляемым в бумажной форме, Поэтому значительная часть многих национальных исследований по правовым аспектам электронного перевода средств посвящена вопросу о доказательствах.

2. Результаты обзора, проведенного секретариатом Комиссии ООН по праву международной торговли, показывают, что в большинстве стран записи, ведущиеся в компьютерах, могут быть использованы в качестве доказательства в случае судебного разбирательства. В странах общего права компьютерные записи обычно принимаются в качестве доказательства только в тех случаях, когда сторона, представляющая запись, устанавливает определенные факты в отношении записи и компьютерной системы. Самое важное заключается в том, чтобы эта система была надлежащим образом организованной и достаточно легко управляемой, чтобы свести к минимуму вероятность того, что данные, хранимые в записи, являются неточными. В некоторых странах общего права записи финансовых учреждений допустимы в качестве доказательств с меньшими формальностями.

В других правовых системах для того, чтобы компьютерная запись была принята в качестве доказательства, не обязательно устанавливать, что данная система надлежащим образом организована и легко управляема. Однако во всех правовых системах можно оспаривать точность компьютерной записи, в частности, на том основании, что компьютерная система не организована надлежащим образом или плохо управляема.

3. В ряде стран с исчерпывающим перечнем видов допустимых доказательств компьютерные записи допустимы в коммерческих спорах, но могут не рассматриваться в качестве доказательств в некоммерческих спорах. Поскольку последняя категория может включать в себя большинство операций, производимых через пункты выдачи наличных, банкоматы и терминалы пунктов продаж, в этих странах могут быть значительны проблемы, связанные с электронным переводом средств. В частности, если некоммерческий клиент отрицает факт использования инициализируемого клиентом терминала, для банка может быть трудно или даже невозможно доказать противное только на основании компьютерной записи данной операции (см. вопрос 21). В некоторых странах с законодательными требованиями о предоставлении суду вспомогательной информации, на основании которой суд мог бы определить, следует ли принимать компьютерную запись в качестве доказательства, законодательные требования разработаны

с учетом обработки данных в пакетном режиме, и поэтому могут возникнуть трудности при использовании компьютерных записей, посредством которых инструкция перевода средств составлялась на одном компьютере и передавалась на другой путем передачи устройства компьютерной памяти либо по телекоммуникациям.

4. По-видимому, до сих пор отсутствует опыт использования компьютерных записей, созданных в одной стране, в качестве доказательства в судах другой страны на тех же условиях, что и использование компьютерных записей, созданных во втором государстве. Любые связанные с этим трудности могут создать серьезную проблему для международных электронных переводов средств.

5. Транкация бумажных инструкций дебетового или кредитового переводов и направление основных данных с помощью электронных средств могут породить вопросы о доказательственной ценности компьютерных записей в транкирующем банке или получающем банке по сравнению с доказательственной ценностью бумажных инструкций. Многие государства могут требовать твердую копию оригинала бумажных инструкций, но могут допускать, чтобы твердая копия хранилась в виде микрофильма.

<...>

Вопрос 9

Требует ли развитие методов электронного перевода средств изменения в законодательстве, регулирующем банковскую тайну?

Комментарий

1. Банковская тайна является одним из наиболее важных аспектов продолжающихся публичных дебатов о вторжении в тайну частной жизни, которым способствуют хранение данных в компьютерах, соединение компьютеров по телекоммуникациям и возможность удаленного доступа к этим данным. Кроме того, вызывает беспокойство то обстоятельство, что данные, относящиеся к банковским операциям, могут раскрывать скрытые мотивы экономической деятельности. Поэтому некоторые государства стремятся ограничить трансграничные потоки данных, посредством которых информация передается в другие государства для последующей обработки или использования.

2. Во многих странах в профессиональные обязанности банков входит сохранение тайны дел своих клиентов, за исключением случаев, когда раскрытие информации разрешено клиентом или требуется государством в соответствии с нормами закона. Нарушение банком своих профессиональных обязанностей может повлечь уголовную ответственность или ответственность перед клиентом за причиненный ущерб. В прошлом несанкционированное разглашение обычно представляло собой преднамеренное действие банка или одного из его служащих. В настоящее время, когда несанкционированное разглашение может быть следствием доступа к компьютеру банка неуполномоченного лица или перехвата инструкции перевода средств, передаваемой по каналам связи, следует, вероятно, поставить вопрос о том, обладают ли банки более широкими обязанностями по созданию системы безопасности при передаче инструкций перевода средств и их хранении, которая ограничивала бы возможность такого доступа.

Вопрос 10

Следует ли банкам заключать со своими клиентами письменные договоры, охватывающие

права и обязанности клиентов и банков в связи с электронным переводом средств?

Комментарий

1. В отношении необходимости письменных договоров в разных странах существуют различные традиции. В странах, где письменные договоры не распространены, содержание соглашений между сторонами диктуется обычно банковскими традициями и практикой.

2. Однако, в отношении новых методов перевода средств, и особенно электронного перевода средств, в банковских традициях и практике могут быть не предусмотрены необходимые аспекты многих возникающих вопросов. Представляется, что банки всегда требуют письменных соглашений до выдачи кредитных или дебетовых карт. Письменные договоры, видимо, не всегда требуются до того, как клиенты допускаются к участию в программах управления активами и других переводах крупных сумм, хотя это может оказаться особенно полезным, поскольку некоторые аспекты соглашения между банком и клиентом могут быть различными, в зависимости от клиента.

3. За исключением некоторых аспектов договоров, заключаемых для переводов крупных сумм, соглашения между банками и клиентами разрабатываются банками и представляются своим клиентам в качестве условия открытия счета. В разных странах существуют различные методы ограничения потенциальных злоупотреблений При заключении таких договоров.

<...>

Вопрос 12

Должно ли быть правовое требование в отношении формы аутентификации при электронном переводе средств?

Комментарий

1. По-видимому, ни одна из стран не требует представлять инструкции перевода средств в письменной форме. Именно по этой причине банки использовали различные методы электронного перевода средств, включая телекс, межкомпьютерные телекоммуникации, передачу устройств компьютерной памяти и в некоторых странах -устные инструкции по телефону без необходимости прямой авторизации в силу закона. В отсутствие законодательства, разрешающего совершение перевода средств электронным способом, видимо, не существует общего требования об аутентификации инструкции перевода средств.

2. Может быть признано желательным предусмотреть в праве требование, что все инструкции перевода средств, включая [переводы] в электронной форме, должны аутентифицироваться. Вместе с тем, может быть признано, что такое требование не является обязательным, поскольку банк не станет делать дебетовую проводку по счету, если только он не обладает инструкцией перевода средств в форме, на которую он мог бы полагаться в случае последующего спора. Последнее должно быть достаточным сдерживающим фактором для банков, чтобы они с осторожностью использовали такие методы перевода средств, при которых аутентификация является сложной или она невозможна. Далее, во многих странах органы банковского надзора считают необоснованной банковскую практику перевода средств на основании инструкций, подлинность которых надлежащим образом не установлена.

3. Может быть признано желательным установить в праве требования об аутентификации инструкций электронного перевода средств, а также указать юридически признаваемый тип аутентификации. Это не только ограничит способы установления подлинности теми, которые законодатель считает достаточно безопасными, но также обеспечит возможность полагаться на аутентификацию требуемого типа в целях разрешения на дебетование счета плательщика в случае каких-либо сомнений.

4. Вместе с тем, может быть признано практически нецелесообразным устанавливать законом любой значимый способ аутентификации инструкций электронного перевода средств. В отличие от аутентификации бумажных документов, когда при необходимости можно представить довольно исчерпывающий перечень средств аутентификации, включая сравнение подписей, существует неисчислимое множество способов аутентифицировать сообщение, отправляемое по телекоммуникациям. С учетом быстрого развития технологий можно предположить, что некоторые современные методы аутентификации окажутся со временем не столь надежными и вместе с тем появятся новые и более безопасные способы аутентификации.

4. В результате может быть сделан вывод, что любое законодательное положение, касающееся аутентификации инструкций электронного перевода средств, должно предусматривать больше, чем просто разрешение использовать средства, соответствующие виду инструкции. Отдельно могут быть рассмотрены вопросы ответственности за убытки, вызванные мошеннической или ошибочной аутентификацией, а также вопросы о том, какая из сторон несет бремя доказывания того, являлась ли аутентификация подлинной.

Вопрос 13

Следует ли требовать от направляющего банка соблюдения стандартных форматов при отправлении инструкций перевода средств?

Комментарий

1. Направляющий банк может не придерживаться стандартного формата в двух случаях. Он может не использовать надлежащий тип сообщения при наличии более чем одного типа сообщений и он не может включить необходимую для автоматической обработки информацию, в том числе при использовании ненадлежащих сокращений или прочих стандартных обозначений, помещении информации в ненадлежащее поле или поле для дополнительной информации, когда ее следовало помещать в конкретное поле данных. Не является нарушением правил использования форматов включение неправильной информации, например, неверная сумма перевода, если неправильная информация помещена в правильное поле данных.

2. Правила SWIFT и других аналогичных сетей устанавливают формат, соблюдаемый для каждого типа сообщений. Неясным остается лишь вопрос о последствиях несоблюдения направляющим банком этого формата. Напротив, даже когда правила использования форматов для инструкций перевода средств по телексу, которые в настоящее время находятся на завершающей стадии разработки и приближены к правилам использования форматов SWIFT, станут международным стандартом, они тем самым не приобретут юридической силы. За исключением случаев, когда такие правила использования форматов приобретают характер норм надлежащей банковской практики, они могут приобрести юридическую силу только при условии введения законодательных или нормативных требований об их соблюдении или наличия соглашения сторон.

3. Правовые последствия невыполнения направляющим банком надлежащих правил использования форматов могут быть двоякими. Банк может нести ответственность за все ошибки со стороны последующих банков, вызванные нарушением формата. Может допускаться оправдывающее основание, что последующий банк сам допустил небрежность и что он должен был понимать данное сообщение правильно, но следует признать, что оправдания по этой причине должны быть редкими. Другим последствием невыполнения правил использования форматов может быть взимание стандартного сбора,с направляющего банка в пользу получающего банка для возмещения его усилий по исправлению ошибки направляющего банка. Если получающие банки будут регулярно требовать уплаты таких сборов, это правило может иметь благотворное последствие для направляющих банков ~ быть более добросовестными при соблюдении правил использования форматов, что послужит на пользу всем заинтересованным сторонам.

Вопрос 18

Должны ли государственные телекоммуникационные операторы, частные службы передачи данных, сети электронного перевода средств и электронные расчетные палаты нести ответственность за убытки, возникающие из-за ошибок или обмана в связи с инструкцией перевода средств?

Комментарий

1. Вопрос о том, должны ли государственные телекоммуникационные операторы продолжать освобождаться от любой ответственности за убытки, возникающие в связи с утратой или задержкой сообщения или в результате изменений содержания сообщений, вновь возник в связи с изменением характера предлагаемых услуг, дерегулированием или приватизацией услуг в ряде государств. Однако в случае отсутствия такой ответственности следует рассмотреть вопрос о том, несет ли убытки плательщик или один из банков. В пользу того, чтобы убытки нес плательщик, свидетельствует тот факт, что перевод средств осуществляется в его интересах, а убытки возникают не по вине любой из сторон, могущих нести ответственность. В пользу того, чтобы убытки нес один из банков, свидетельствует тот факт, что банки наилучшим образом в состоянии разработать систему перевода средств с использованием услуг государственных операторов, в результате чего задержки или ошибки доводятся до сведения направляющего или получающего банка, обеспечивая возможность быстрого исправления. Среди банков, которые могли бы относиться к числу несущих убытки, находится банк плательщика, в особенности, если банк плательщика несет ответственность за правильное исполнение всего перевода средств, и банк, направивший инструкцию, которая была утрачена, задержана или содержание которой было изменено.

2. Частные службы передачи данных, сети электронного перевода средств, электронные расчетные палаты могут заключать договоры с банками-участниками в целях ограничения или освобождения их от ответственности за утрату, задержку или изменение инструкций перевода средств. Предполагается, что договорное распределение убытков между этими организациями и банками-участниками не должно нарушать публичного порядка. Однако необходимо иметь в виду, что целью этих договорных условий является возложение убытков на плательщика. Предполагается, что

у плательщика меньше оснований нести убытки, когда они причинены по вине государственного оператора, поскольку сети и расчетные палаты являются неотъемлемой частью банковской индустрии, и банки могут выбирать использование частных служб передачи данных для направления инструкций перевода средств.

3. Предполагается, что телекоммуникационный оператор, служба передачи данных, сеть электронного перевода средств или электронная расчетная палата должны нести ответственность за убытки, причиненные в результате мошенничества их служащих. Вместе с тем, можно также предположить наличие определенных пределов ответственности работодателя за действия служащих, в особенности когда эти действия являются незаконными. Необходимо проводить разграничение между убытками от мошенничества, которое стало возможным благодаря доступу к записям о счетах и оборудованию, что является частью трудовых отношений, за что работодатель несет ответственность, и между убытками от мошенничества, которое стало возможным благодаря получению служащими соответствующих сведений в процессе своей работы, за что работодатель не несет ответственности.,

Вопрос 19

Следует ли освобождать банк от ответственности за ошибки или задержку перевода средств, вызванные сбоями аппаратных средств или программного обеспечения?

Комментарий

1. Хотя банковские компьютерные аппаратные средства и программное обеспечение достигли высокой степени надежности по сравнению с прошлыми годами, по причине компьютерных сбоев происходят ошибки, утраты, задержки или изменения при переводе средств. С одной стороны, предполагается, что технические проблемы такого характера находятся вне контроля банка и он освобождается от ответственности за любые убытки, причиненные клиентам в результате этого. Если банки обладают таким правом, они часто включают подобное условие в договоры, которые они заключают со своими клиентами.

2. С другой стороны, предполагается, что степень надежности компьютеров такова, что позволяет к ним относиться так же, как и к другим видам оборудования, используемого банками. Компьютерные сбои могут быть результатом ненадлежащей работы оборудования, программного обеспечения или обслуживания, а последствия компьютерного сбоя могут быть уменьшены посредством предварительного планирования, которое может включать наличие резервного оборудования, источников энергии, планов использования альтернативных средств осуществления перевода средств и в целом принятия банком безотлагательных мер. В результате предполагается, что общее освобождение от ответственности было бы неоправданным, однако освобождение от ответственности в результате компьютерных сбоев могло бы быть оправданным в случае, когда банк не мог предотвратить такие сбои или уменьшить их последствия.

<...>

Вопрос 22

Должны ли клиент или соответствующие банки представлять доказательства источника ошибки или обмана, вызвавших ущерб при переводе средств?

Комментарий

1. Этот вопрос может возникнуть в двух случаях. Во-первых, когда клиент утверждает, что он инициировал инструкцию перевода средств, а банк не зафиксировал ее. Хотя наиболее частые случаи, вызывающие убытки, будут, несомненно, связаны с инструкциями, которые якобы были направлены через инициализируемый клиентом терминал в его коммерческом предприятии, как только переводы средств с помощью банкоматов или домашних банковских терминалов станут обычными, могут возникнуть случаи, касающиеся таких вопросов, как прекращение страховых договоров, по которым должны быть, но не уплачены страховые премии. Можно ожидать, что в большинстве случаев, когда инструкция направляется через инициализируемый клиентом терминал по месту нахождения коммерческого предприятия клиента, его компьютер должен сохранить запись этой передачи. Часто может возникать вопрос о том, какая из сторон несет риск утраты сообщения - клиент или банк. В случае использования банкомата или домашнего банковского терминала у клиента часто отсутствует квитанция или компьютерная запись, позволяющие клиенту доказать факт передачи. Без такой квитанции или записи, а также при отсутствии обычных деловых процедур со стороны некоммерческого клиента, подтверждающих его требование, предполагается, что такой клиент должен нести бремя доказывания.

2. Во-вторых, такой вопрос может возникнуть, когда эта инструкция была утрачена, передана с задержкой или содержала ошибку при поступлении в банк получателя, но источник проблем не выяснен. Если избранная норма возлагает ответственность на банк плательщика за надлежащее исполнение всего перевода средств, можно ожидать, что он несет бремя доказывания того, что утрата, задержка или ошибка произошли при таких обстоятельствах, которые освобождают банк от

ответственности (см. вопрос 16). Если избранная норма не возлагает на банк плательщика такой ответственности, то можно ожидать, что плательщик несет бремя доказывания того, какой банк несет ответственность за утрату, задержку или ошибку. Обычно для выяснения банка, в котором возникли проблемы, достаточно наличия контрольного следа. Вместе с тем, записи, создающие контрольный след, полностью контролируются банками, а в случае международного перевода средств некоторые из этих банков могут быть иностранными, вследствие чего возрастает трудность обеспечения информации. Если записи банка вызывают разногласия, плательщик не имеет независимых средств доказывания. Кроме того, от плательщика могут потребоваться доказательства того, что утрата, задержка или ошибка произошли в силу небрежности или иной вины соответствующего банка; и в этом случае считается, что он должен нести бремя доказывания источника проблемы.

Додаток 6. Рекомендация ЮНСИТРАЛ о правовой ценности компьютерных записей 1985 г.

Комиссия ООН по праву международной торговли,

отмечая, что использование автоматической обработки данных (АОД) уже прочно внедряется во всем мире во многих сферах внутренней и международной торговли, а также в административных службах,

отмечая также, что правовые нормы, основанные на предшествующих АОД средствах документирования международной торговли, могут создать препятствие такому использованию АОД и привести к правовой незащищенности или осложнить эффективное использование АОД там, где оно иначе было бы оправданно,

отмечая далее с признательностью усилия Совета Европы, Совета таможенного сотрудничества и Европейской экономической комиссии ООН, направленные на преодоление препятствий для использования АОД в международной торговле, вызываемых этими правовыми нормами,

считая в то же самое время, что отсутствует необходимость в унификации доказательственных правил в отношении использования компьютерных записей в международной торговле, поскольку существующий опыт свидетельствуете том, что значительные расхождения в доказательственных правилах, применяющихся в системе бумажной документации, до сих пор не нанесли заметного ущерба развитию международной торговли,

считая также, что достижения в использовании АОД порождают желательность приспособления для ряда правовых систем существующих правовых норм к этим достижениям, уделяя, однако, должное внимание необходимости поощрения использования таких средств АОД, которые могли бы обеспечить такую же или еще большую надежность по сравнению с бумажной документацией,

1. Рекомендует правительствам:

(а) проанализировать правовые нормы, затрагивающие использование компьютерных записей в качестве доказательства при судебных разбирательствах в целях устранения ненужных препятствий для их допустимости, удостоверяться в соответствии этих норм достижениям в области технологии и предоставлять суду надлежащие средства для оценки достоверности данных, содержащихся в этих записях;

(Ь) проанализировать правовые требования о письменной форме определенных торговых сделок или торговых документов, независимо от того, является ли эта форма условием, обеспечивающим исковую силу или действительность сделки или документа, чтобы допускать, когда это уместно, возможность записи сделок или документов и их передачи в машиночитаемой форме;

(с) проанализировать правовые требования собственноручной подписи или других способов установления подлинности торговых документов, основанных на использовании бумажного носителя, чтобы допускать, когда это уместно, использование электронных средств установления подлинности;

(и) проанализировать правовые требования о письменной форме и собственноручной подписи документов, представляемых правительственным органам, чтобы разрешать, когда это уместно, представлять такие документы в машиночитаемой форме тем административным службам, которые приобрели необходимое оборудование и установили необходимые процедуры.

2. *Рекомендует* международным организациям, разрабатывающим ' правовые тексты, относящиеся к торговле, принимать во внимание настоящую Рекомендацию при принятии таких текстов и, когда это уместно, рассматривать возможность изменения существующих правовых текстов в соответствии с настоящей Рекомендацией.

Додаток 7. Дополнительный протокол к Конвенции о защите физических лиц в отношении автоматической обработки персональных данных, касающийся надзорных органов и трансграничных потоков данных от 8 ноября 2001 г.

(Страсбург)

Преамбула

Стороны настоящего Дополнительного протокола к Конвенции о защите физических лиц в отношении автоматической обработки персональных данных, открытой для подписания в Страсбурге 28 января 1981 г. (в дальнейшем именуемая «Конвенция»),

убежденные, что надзорные органы, реализующие свои функции полностью независимо, являются элементом эффективной защиты физических лиц в отношении обработки персональных данных;

принимая во внимание важность информационных потоков между людьми; принимая во внимание, что с увеличением обмена персональными данными через национальные границы необходимо гарантировать эффективную защиту прав и основных свобод человека и в особенности права на тайну частной жизни применительно к таким обменам персональными данными, согласились о нижеследующем:

Статья 1
Надзорные органы

1. Каждая Сторона обеспечивает, чтобы один или несколько органов являлись ответственными за обеспечение соблюдения норм в своем внутреннем праве, реализующих принципы, изложенные в главах II и III Конвенции и настоящем Протоколе.

2. a. С этой целью указанные органы должны обладать, в частности, полномочиями по расследованию и вмешательству, а равно по участию в судебном производстве или обращению внимания компетентных судебных органов на нарушения положений внутреннего права, реализующих принципы, изложенные в пункте 1 статьи 1 настоящего Протокола.

Ь. Каждый надзорный орган должен заслушивать в пределах своей компетенции требования, заявленные любым лицом, заинтересованным в защите его/ее прав и основных свобод в отношении обработки персональных данных.

3. Надзорный орган должен реализовывать свои функции полностью независимо.

4. Решения надзорных органов, дающие основание для исков, могут быть обжалованы в суде.

5. В соответствии с положениями главы IV и без ущерба для положений статьи 13 Конвенции надзорные органы должны сотрудничать друг с другом в степени, необходимой для выполнения своих обязанностей, в частности, путем обмена всей пригодной информации.

Статья 2
Трансграничные потоки персональных данных получателю, который не подпадает под юрисдикцию Стороны Конвенции

1. Каждая Сторона обеспечивает передачу персональных данных получателю, который подпадает под юрисдикцию Государства или организации, не являющейся Стороной Конвенции, только если это Государство или организация гарантируют адекватный уровень защиты предполагаемой передачи данных.

2. Путем изъятия из пункта 1 статьи 2 настоящего Протокола каждая Сторона может допускать передачу персональных данных: a. если внутреннее право предусматривает это в силу:

- особых интересов субъекта данных, или

-законах превалирующих интересов, особо важных общественных интересов, или

b. если контролером, ответственным за передачу, обеспечиваются гарантии, которые могут следовать, в частности, из договорных условий, и они признаются адекватными компетентными органами согласно внутреннему праву.

Статья 3
Заключительные положения

1. Положения статей 1 и 2 настоящего Протокола рассматриваются Сторонами как дополнительные статьи Конвенции и все положения Конвенции должны применяться соответственно.

2. Настоящий Протокол открыт для подписания Государствами, подписавшими Конвенцию.

После присоединения к Конвенции согласно предусмотренным в ней условиям Европейские сообщества могут подписать настоящий Протокол. Настоящий Протокол подлежит ратификации, утверждению или одобрению. Государство, подписавшее настоящий Протокол, может его не ратифицировать, не утверждать или не одобрять, если только оно предварительно или в последующем ратифицирует, утверждает или одобряет Конвенцию или присоединяется к ней. Документы о ратификации, утверждении или одобрении настоящего Протокола депонируются у Генерального секретаря Совета Европы.

3. a. Настоящий Протокол вступает в силу в первый день месяца, следующего за окончанием трехмесячного периода после даты, когда пять Государств, подписавших Протокол, выразят согласие быть связанными обязательствами, вытекающими из Протокола, в соответствии с положениями пункта 2 статьи 3.

b. В отношении любого Государства, подписавшего настоящий Протокол, которое в последующем выразит свое согласие быть связанным обязательствами, вытекающими из Протокола, он вступает в силу в первый день месяца, следующего за окончанием трехмесячного периода после даты депонирования документа о ратификации, принятии или одобрении.

4. a. После вступления в силу настоящего Протокола любое Государство, присоединившееся к Конвенции, также может присоединиться к Протоколу.

b. Присоединение осуществляется путем депонирования у Генерального секретаря Совета Европы документа о присоединении, который вступает в силу в первый день месяца, следующего за окончанием трехмесячного периода после даты депонирования.

5. a. Каждая Сторона может в любое время денонсировать настоящий Протокол посредством уведомления, направленного в адрес Генерального секретаря Совета Европы.

b. Такая денонсация начинает действовать с первого дня месяца, следующего за истечением трехмесячного периода после даты получения уведомления Генеральным секретарем.

6. Генеральный секретарь Совета Европы извещает Государства, входящие в Совет Европы, Европейские сообщества, и любое другое Государство, присоединившееся к настоящему Протоколу: о каждом подписании;

b. о депонировании каждого документа о ратификации, утверждении, одобрении; о каждой дате вступления настоящего Протокола в силу в соответствии со статьей 3;

ii) о любых других актах, уведомлениях или сообщениях, касающихся Протокола. В удостоверение этого нижеподписавшиеся, будучи должным образом для этого уполномочены, подписали настоящий Протокол.

Совершено в Страсбурге 8 ноября 2001 г. на английском и французском языках, оба текста являются равно аутентичными, в единственном экземпляре, который подлежит , передаче на хранение в архивы Совета Европы. Генеральный секретарь Совета Европы направляет заверенные копии каждому Государству - члену Совета Европы, Европейским сообществам и каждому Государству, приглашенному присоединиться к Конвенции.

Додаток 8. Конвенция об информационном и правовом сотрудничестве, касающемся «услуг информационного общества» от 4 октября 2001 г.

(Извлечения) .

Преамбула

Стороны настоящей Конвенции, ее подписавшие, принимая во внимание, что целью Совета Европы является достижение большего единства между его членами в целях защиты и реализации идеалов и принципов, 1 которые являются их общим наследием;

отмечая продолжающееся развитие информационных и коммуникационных технологий, многочисленные инициативы и их влияние на европейском и международном уровне;

признавая трансграничный характер интерактивных услуг, которые распространяются в режиме «онлайн» с использованием новых средств электронных коммуникаций, и их растущую важность для содействия экономическому, социальному и культурному прогрессу государств - членов Совета Европы;

вспоминая систему, установленную законодательством Европейского сообщества, об обмене текстами проектов национальных правовых актов, касающихся «услуг

Информационного общества»;

отмечая необходимость регулярного информирования всех государств - членов Совета Европы о законодательных тенденциях в сфере «услуг информационного общества» на паневропейском уровне и, где это необходимо, возможности обсуждать и обмениваться информацией и идеями, относящимися к этим тенденциям;

соглашаясь с желательностью предусмотреть правовые основы для обеспечения возможности государствам - членам Совета Европы обмениваться, где это практически возможно, с использованием электронных средств текстами проектов национальных правовых актов, специально направленных на «услуги информационного общества»,

согласились о нижеследующем:

Статья 1
Предмет и сфера применения

1. В соответствии с положениями настоящей Конвенции Стороны обмениваются текстами, где это практически возможно, с использованием электронных средств, проектов национальных правовых актов, специально направленных на «услуги информационного общества», и сотрудничают в части функционирования системы информационного и правового сотрудничества, установленной согласно Конвенции.

2. Настоящая Конвенция не применяется:

a. к национальным правовым актам, изъятым из предварительного уведомления в силу законодательства Европейского сообщества (здесь и далее именуется «право сообщества»), или

b. когда уведомление должно быть сделано в целях соблюдения других международных соглашений. 3. Настоящая Конвенция не применяется: a. к радиовещательным услугам;

b. к услугам телевизионных программ, охватываемым Европейской Конвенцией о трансграничном телевидении, открытой для подписания в Страсбурге 5 мая 1989 г. (ETS № 132) с изменениями, внесенными Протоколом от 1 октября 1998 г. (ETS № 171);

c. к национальным правовым актам, касающихся вопросов, которые не охватываются законодательством Европейского сообщества или международными соглашениями в сфере телекоммуникационных услуг и финансовых услуг.

Статья 2
Определения

Для целей настоящей Конвенции

a. «услуги информационного общества» означают любые услуги, обычно предоставляемые за вознаграждение, дистанционно, с использованием электронных средств и по индивидуальному запросу получателя услуг;

b. «национальные правовые акты» означают правовые тексты, касающиеся соблюдения требований общего характера к занятию и осуществлению деятельностью по оказанию услуг в значении пункта a настоящей статьи, в частности, положений, касающихся сервис-провайдеров, услуг и тюлучателей услуг, исключая любые правила, которые специально не направлены на услуги информационного общества.

Статья 3
Получающие и передающие органы

Каждая Сторона назначает орган, ответственный за передачу и получение, когда это практически возможно, с использованием электронных средств, проектов национальных нормативных актов, специально направленных на «услуги информационного общества», а также любых других документов, относящихся к действию настоящей Конвенции.

Статья 4
Процедура

1. Каждая Сторона передает, когда это практически возможно, с использованием электронных средств Генеральному секретарю Совета Европы тексты проектов национальных нормативных актов, специально направленных на «услуги информационного общества» и находящихся на стадии подготовки, в которые все еще возможно внесение существенных изменений, а также краткие извлечения из этих текстов на английском и французском языках. Стороны снова направляют проекты на вышеуказанных условиях, если они вносят в проект изменения, влекущие существенное

изменение сферы, сокращение временных сроков, первоначально предусмотренных для выполнения, добавление деталей или требований либо придание им ограничительного характера.

2. После получения текстов проектов национальных правовых актов и кратких извлечений согласно части 1 выше или части 6 ниже, Генеральный секретарь Совета Европы направляет их, когда это практически возможно, с использованием электронных средств органам каждой Стороны.

3. После получения текстов и кратких извлечений согласно части 2 выше, каждая Сторона может направить, когда это практически возможно, с использованием электронных средств свои замечания по текстам проектов национальных правовых актов на английском или французском языках Генеральному секретарю Совета Европы и заинтересованной Стороне.

4. Сторона, получающая замечания согласно части 3 выше, должна, стараться учитывать их, насколько это возможно, при подготовке новых национальных правовых актов.

5. Части 1-4 выше не применяются:

a. в случаях, когда по чрезвычайным причинам, вызванным серьезными и непредвиденными обстоятельствами, касающимися защиты общественного здоровья, безопасности, защиты животных или сохранения растений и публичного порядка, особенно защиты несовершеннолетних, Сторона обязана за очень короткое время подготовить технические нормативные акты для их незамедлительного принятия и внесения без возможности проведения любых консультаций;

b. в случаях, когда по чрезвычайным причинам, вызванным серьезными обстоятельствами, касающимися защиты безопасности и целостности финансовой системы, особенно защиты вкладчиков, инвесторов и застрахованных лиц, Сторона обязана незамедлительно принять и реализовать правила о финансовых услугах;

в случаях, упомянутых в пунктах a и b Сторона сообщает о причинах чрезвычайности рассматриваемых мер Генеральному секретарю Совета Европы;

c. к национальным правовым актам, принятым на регулируемых или иных рынках, для регулируемых или иных рынков, либо органами, осуществляющими клиринговые или расчетные функции для этих рынков.

6. Каждая Сторона, которая завершает принятие любых национальных правовых актов, специально направленных на «услуги информационного общества», передает без задержки окончательный текст Генеральному секретарю Совета Европы и, когда это практически возможно, с использованием электронных средств.

7. После получения текстов принятых национальных правовых актов согласно части 6 выше Генеральный секретарь Совета Европы делает их доступными, когда это практически возможно, с использованием электронных средств и хранит данную информацию в единой базе данных в Совете Европы.

Статья 5

Декларации

Органы, указанные в статье 3, назначаются посредством декларации, адресованной Генеральному секретарю Совета Европы, когда заинтересованное государство или Европейское сообщество становятся Стороной настоящей Конвенции в соответствии с положениями статей 8 и 9. О любом изменении должно аналогичным образом заявляться Генеральному секретарю Совета Европы.

Статья 6

Отношение к другим документам и соглашениям

1. Настоящая Конвенция не затрагивает любых международных документов, которые обязывают Стороны и содержат положения по вопросам, регулируемым настоящей Конвенцией.

2. Европейское сообщество равным образом выполняет обязательства по уведомлению о текстах, переданных своими государствами - членами во исполнение положений части 1 статьи 4, а также передает им полученные замечания других Сторон во исполнение положения части 3 статьи 4.

Статья 7

Изменения статьи 1 Конвенции, касающейся исключаемых вопросов

1. О любом изменении к части 3 статьи 1 настоящей Конвенции, предлагаемом Стороной, сообщается Генеральному секретарю Совета Европы, который направляет сообщение Европейскому комитету по правовому сотрудничеству (CDC}).

2. Предложенное изменение должно быть изучено Сторонами, которые могут его принять

большинством голосов в две трети. Принятый текст должен быть направлен Сторонам. Европейское сообщество должно иметь то же число голосов, что и число его государств - членов.

3. В первый день месяца, следующего за окончанием четырехмесячного срока после своего принятия Сторонами, если только Стороны не заявили возражения одной третью голосов, любое изменение вступает в силу для тех Сторон, которые не заявили о возражении.

4. Сторона, которая заявила о возражении согласно положениям части 3 статьи 7, может впоследствии отозвать его полностью или частично. Такой отзыв должен быть сделан посредством уведомления, адресованного Генеральному секретарю Совета Европы и вступает в силу с даты своего получения.

Додаток 9. Всемирная торговая организация (ВТО) Генеральное соглашение по торговле услугами от 15 апреля 1994 г. (Приложение по телекоммуникациям)

1. Цели

Признавая специфику сектора телекоммуникационных услуг, в особенности его двоякую роль как особого сектора экономической деятельности и как основного средства передачи информации для других видов экономической деятельности, участники договариваются о следующем Приложении с целью дальнейшей разработки положений Соглашения в отношении мер, затрагивающих доступ к телекоммуникационным сетям и услугам общего пользования и их использование. Соответственно настоящее Приложение содержит замечания и дополняющие положения к настоящему Соглашению.

2. Сфера действия

(a) Настоящее Приложение применяется ко всем мерам участника, затрагивающим доступ к телекоммуникационным сетям и услугам общего пользования, а также их использование.

(b) Настоящее Приложение не применяется к мерам, затрагивающим кабельное или вещательное распределение радио- или телепрограмм.

(c) Ничто в настоящем Соглашении не должно истолковываться:

(1) как требующее от участника уполномочивать поставщика услуг какого-либо другого участника устанавливать, создавать, приобретать, арендовать, эксплуатировать или поставлять телекоммуникационные передающие сети или услуги иначе, чем ^ предусмотрено в его Перечне; или

(1)как требующее от участника (или требующее от участника обязать поставщиков услуг, находящихся под его юрисдикцией) устанавливать, создавать, приобретать, арендовать, эксплуатировать или поставлять телекоммуникационные передающие сети или услуги, которые обычно не предлагаются широкому кругу лиц.

3. Определения

Для целей настоящего Приложения:

(a) «Телекоммуникации» означают передачу или прием сигналов любым электромагнитным способом.

(b) «Телекоммуникационная услуга общего пользования» означает любую телекоммуникационную услугу, которую участник требует открыто или фактически предоставлять широкому кругу лиц. Такие услуги могут включать, inter alia, телеграф, телефон, телекс и передачу данных, как правило, включающие передачу в реальном и времени потребителям информации между двумя или более пунктами без каких-либо изменений формы или содержания этой информации между начальным и конечным пунктом передачи.

(c) «Телекоммуникационная сеть общего пользования» означает телекоммуникационную инфраструктуру общего пользования, которая позволяет осуществлять телекоммуникационные связи между сетью определенных конечных пунктов или внутри них.

(1) «Внутрикорпоративные коммуникации» означают телекоммуникации, по-1средством которых компания поддерживает связь внутри компании или с ее дочерними компаниями, филиалами, отделениями или между ними в соответствии с национальными законами и правилами участника. Для этих целей термины «дочерние компании», «филиалы» и, где это применимо, «отделения» должны быть определены каждым участником. «Внутрикорпоративные коммуникации» в настоящем Приложении исключают коммерческие или некоммерческие услуги, поставляемые компаниям, которые не являются зависимыми дочерними компаниями, филиалами или отделениями

или которые предлагаются потребителям или потенциальным потребителям.

(e) Любая ссылка на пункт или подпункт настоящего Приложения включает все его подразделы.

4. Гласность

При применении статьи 3 Соглашения каждый участник обеспечивает, чтобы соответствующая информация об условиях доступа к телекоммуникационным сетям и услугам общего пользования и их использования являлась общедоступной, включая: тарифы и другие условия предоставления услуг; спецификации технических соединений с такими сетями и услугами; информацию об органах, ответственных за подготовку и принятие стандартов, затрагивающих такой доступ и использование; условия, касающиеся подсоединения терминалов или другой аппаратуры, а также требования к уведомлениям, регистрации или лицензированию, если таковые необходимы.

5. Доступ к телекоммуникационным сетям и услугам общего пользования и их использование

(a) Каждый участник обеспечивает, чтобы любой поставщик услуг любого другого участника имел доступ к телекоммуникационным сетям и услугам общего пользования и к их использованию на основе разумных и недискриминационных условий для поставки услуг, включенных в его Перечень. Это обязательство применяется, inter alia, в соответствии с нижеприведенными пунктами

(b) Каждый участник обеспечивает, чтобы поставщики услуг любого другого участника имели доступ к общественным телекоммуникационным сетям и услугам общего пользования и к их использованию в пределах его территории или через границу этого участника, включая частные арендованные линии связи, и в этих целях должен обеспечить в соответствии с пунктами (e), чтобы таким поставщикам разрешалось:

(1) приобретать или арендовать и подсоединять терминалы или другую аппаратуру, которые могут быть соединены с сетью и которые необходимы поставщику для поставки услуг;

(ii) подключать частные арендованные или приобретенные линии связи к телекоммуникационным сетям или услугам общего пользования или к арендованным или приобретенным линиям связи другим поставщиком услуг; и

(i) использовать правила эксплуатации по выбору поставщика услуг при поставке любой услуги иные, чем необходимы для того, чтобы обеспечить обычную доступность телекоммуникационных сетей и услуг.

(c) Каждый участник должен обеспечить, чтобы поставщики услуг любого другого участника могли использовать телекоммуникационные сети и услуги общего пользования для передачи информации в пределах его территории или через границу, включая внутрикорпоративные коммуникации таких поставщиков услуг, и для доступа к информации, содержащейся в базах данных или хранящейся иным образом в машиночитаемой форме с территории любого участника. Любые новые или измененные меры участника, существенно затрагивающие такое использование, подлежат уведомлению и становятся предметом консультаций согласно соответствующим положениям настоящего Соглашения.

(ss) Несмотря на предыдущий пункт, любой член может принимать такие меры, которые необходимы для обеспечения безопасности и конфиденциальности сообщеий при условии соблюдения требования, что такие меры не применяются способом, который бы создавал произвольную или необоснованную дискриминацию или скрытое ограничение в торговле услугами.

(e) Каждый участник обеспечивает, чтобы не навязывались никакие условия доступа к телекоммуникационным сетям и услугам общего пользования и их использования, кроме необходимых для того, чтобы:

(1) гарантировать обязанности поставщиков услуг телекоммуникационных сетей : и услуг общего пользования, в особенности их способности делать их сети или услуги доступными для широкого круга лиц;

(ii) защитить техническую целостность телекоммуникационных сетей и услуг общего пользования; или

(iii)обеспечить, чтобы поставщики услуг любого участника не поставляли услуги до получения разрешения в соответствии с обязательствами в Перечне члена.

(O) При условии, что они удовлетворяют критерию, установленному в пункте (e), условия доступа к телекоммуникационным сетям л услугам общего пользования могут включать:

(1) ограничения на перепродажу или раздельное использование таких услуг;

(ii) требование использовать определенные технические соединения, включая правила

соединения, для подключения к таким сетям и услугам;

(iii) при необходимости, требования взаимодействия таких услуг и содействия достижению целей, установленных в пункте 7(a);

(IV) Одобрение типа терминала или другого оборудования, которые соединяются ; сетью, и технические требования, относящиеся к присоединению такой аппаратуры к таким сетям;

(V) Ограничения на подключение частной, арендованной или приобретенной линии связи к таким сетям или услугам или линиям связи, арендованным или приобретенным другим поставщиком услуг; или

(VI) Уведомление, регистрацию и лицензирование.

(g) Несмотря на предыдущий пункт настоящего раздела, развивающаяся страна-участник может, сообразно с ее уровнем развития, устанавливать разумные условия доступа к телекоммуникационным сетям и услугам общего пользования и к их использованию, необходимые, чтобы усилить ее национальную телекоммуникационную инфраструктуру и потенциал сектора услуг и активизировать ее участие в международной торговле телекоммуникационными услугами. Такие условия указываются в Списке участника.

6. Техническое сотрудничество

(a) Участники признают, что эффективная, развитая телекоммуникационная инфраструктура в странах, особенно развивающихся странах, важна для расширения их торговли услугами. С этой целью участники одобряют и поощряют максимально возможное участие развитых и развивающихся стран и их поставщиков телекоммуникационных сетей и услуг общего пользования и Других структур в программах развития международных и региональных организаций, включая Международный союз электросвязи, Программу развития ООН и Международный банк реконструкции и развития.

(b) Участники поощряют и поддерживают телекоммуникационное сотрудничество среди развивающихся стран на международном, региональном и субрегиональном уровнях.

(c) В сотрудничестве с соответствующими международными организациями члены обеспечивают доступ, где это практически возможно, развивающихся стран к информации в отношении телекоммуникационных услуг и развития в области телекоммуникационной и информационной технологии, в целях содействия усилению их национального телекоммуникационного сектора услуг.

(Д) Участники уделяют особое внимание возможностям наименее развитых стран поощрять иностранных поставщиков телекоммуникационных услуг оказывать содействие в передаче технологии, в обучении и других видах деятельности, которые помогают развитию их телекоммуникационной инфраструктуры и расширению торговли телекоммуникационными услугами.

7. Отношение к международным организациям и соглашениям

(a) Участники признают важность международных стандартов для глобальной совместимости и взаимодействия телекоммуникационных сетей и услуг и берут на себя обязательство содействовать распространению таких стандартов посредством работы соответствующих международных органов, включая Международный союз электросвязи и Международную организацию по стандартизации.

(b) Участники признают роль, которую играют межправительственные и неправительственные организации и соглашения в обеспечении эффективности функционирования национальных и глобальных телекоммуникационных услуг, в особенности роль Международного союза электросвязи. Участники при необходимости добиваются соответствующих договоренностей для проведения консультаций с такими организациями по вопросам, возникающим при применении настоящего Приложения.

Додаток 10. Соглашение по торговым аспектам прав интеллектуальной собственности 1994 г.

(Извлечение)

<...>

Статья 10.
Компьютерные программы и компиляции данных

1. Компьютерные программы, как исходный текст, так и объектный код, охраняются как литературные произведения в соответствии с Бернской Конвенцией (1971 г.).

2. Компиляции данных или другая информация в машиночитаемой или в другой форме, которые по причине отбора или классификации своего содержания составляют результат творчества, должны охраняться как таковые. Такая охрана, которая не распространяется на сами данные или информацию, не затрагивает авторское право, существующее в самих данных или информации.

Статья 11.
Права на прокат

В отношении по меньшей мере компьютерных программ и кинематографических произведений участник предоставляет авторам или их правопреемникам право разрешать или запрещать публичный коммерческий прокат оригиналов или копий их произведений, охраняемых авторским правом. В отношении компьютерных программ это обязательство не применяется к сдаче в коммерческий прокат, если сама программа не является существенной частью объекта проката.

Додаток 11. Международная торговая палата (МТП) Общие обычаи для удостоверенной цифровым способ международной коммерции 1997

<->

КЛЮЧЕВЫЕ ПРИНЦИПЫ

VI. Глоссарий терминов

1. Удостоверять

Ставить или применять цифровой знак или символ, связанный с сообщением, с явным намерением идентифицировать себя как составителя сообщения.

Пояснение:

«Удостоверять»: в американском употреблении термин «подтверждать подлинность» часто используется для обозначения акта идентификации лица с сообщением, но в европейском употреблении термин «подтверждать подлинность» больше ассоциируется с проверкой подписи (см. ниже). Кроме того, главное затруднение в Концепции «цифрового подписания» сообщения заключается в том, что существуют значительные различия между физической подписью и подписью, используемой с применением электронных средств. Самое важное различие при этом, что большинство электронных подписей основано на применении смарт-карты или иного устройства хранения данных в целях воспроизведения алгоритма, необходимого для неразрывного присоединения «подписи» к сообщению, с которым она связывается. Если впоследствии происходит так, что к данному устройству хранения данных получает доступ кто-либо иной, чем лицо, которому принадлежит это устройство, сообщение может быть «подписано» и будет иметь вид составленного собственником устройства 1 вне зависимости от наличия или отсутствия его согласия. Именно по этой причине использован термин «удостоверять», который определяется в «Webster's Universal College Dictionary» как: «1) защищать или гарантировать; 2) делать достоверным или , определенным; 3) делать безопасным или сохранным от вреда» И это именно то, чего добиваются от электронного сообщения - сделать его защищенным от последующих : .изменений.

«Сообщение»: означает только сообщение, которое удостоверено. Если сообще ние изменено (за исключением изменения с одобрения удостоверителя), в этом случае отсутствует намерение удостоверяющего лица идентифицировать себя в качестве составителя сообщения, а удостоверение такого сообщения не распространяется на . изменение.

«Намерение идентифицировать себя в качестве составителя сообщения»: действие по удостоверению может иметь основанием не только минимально необходимую идентификацию удостоверителя в качестве состовителя сообщения. Часто это действие указывает на согласие удостоверителя с сообщения или его намерение быть юридически связанным с сообщением. Основываясь на выражении этих различных намерений посредством удостоверения, право и/или коммерческие обычаи придают сообщению определенную силу формально-признанного акта удостоверителя (см. ниже: «юридическая значимость удостоверения сообщения»). Сертификация рассматривает необходимость гарантирования действительности удостоверения и некоторые правовые системы требуют этого в отношении определенных сообщений, в частности, когда требуется или допускается публичная регистрация либо когда риски ложной идентификациии затрагивают иные интересы, защищаемые в соответствии с принципами правовой системы,

Смотри ст. 6 (критерии удовлетворения требований к подписи) и ст. II (установление подлинности сообщения) Типового закона ЮНСИТРАЛ; ст. 5() Конвенции ООН по международным простым и переводным векселям 1998 г. («Подпись» означает собственноручную подпись, ее факсимиле или иной эквивалентный способ идентификации...»).

Комментарий

(1) В целом и как минимум удостоверение сообщения представляет доказательство того, что:

a) удостоверитель имел контакт с сообщением, и

b) сообщение сохранялось неповрежденным с момента своего удостоверения. Удостоверение может также указывать на большее в зависимости от обстоятельств или иметь юридическую значимость, проистекающую из соглашения или закона. Кроме того, большинство средств подтверждения подлинности предоставляет лишь неполное доказательство контакта удостоверителя с сообщением и его целостность, они также неустойчивы к подделке и подлогу.

(2) Удостоверенное фальшивое сообщение, измененное без согласия удостоверителя, не создает для него связывающего обязательства. Оно является недействительным или признается таковым по требованию заинтересованного удостоверителя. В некоторых правовых системах искаженное соглашение, будучи измененным без согласия удостоверителя, традиционно рассматривается как недействительное и не может быть исполнено принудительно в соответствии с его первоначальным содержанием. В рамках других юрисдикций фальсификация сообщения преимущественно игнорируется, а сообщение может быть исполнено принудительно в том виде, в каком оно было удостоверено первоначально.

2. Сертификат

Сообщение, удостоверенное лицом, чье сообщение свидетельствует о точности фактов, имеющих существенное значение для юридической силы действия другого лица.

Пояснение:

«удостоверенное сообщение»: сертификат, сам по себе представляет сообщение, и удостоверение его подлинности является обычно важным фактом. Для того чтобы сертификат был в рамках коммерции очевидно надежным, сертифицирующее лицо, создающее сертификат, должно проявлять степень заботливости, превышающую степень заботливости для обычных удостоверенных сообщений;

«факт, имеющий существенное значение для юридической силы действия другого лица»: примеры фактов, которые могут подлежать сертификации, включают идентичность лица, совершающего действие, такое, как удостоверение сообщения, обстоятельства, затрагивающих такое существование лица в качестве правоспособного юридического лица и/или полномочия лица, выполняющего спорное действие. Отдельно взятый сертификат может удостоверять один или более таких фактов.

Комментарий

(1) Признается множество различных типов сертификатов. Нотариусы различных правовых систем выдают сертификаты, различающиеся по форме и силе, такие как публичные или свидетельствующие подлинность, а также частные формы сертификатов в рамках гражданско-правовой традиции и менее строгие «подтверждения» североамериканских нотариусов. Технические компьютерные стандарты, как правило, описывают сертификаты, чья действительность определяется в соответствии с определенным периодом времени, тогда как традиционные сертификаты действительны в рамках конкретной сделки. Сертификаты открытого ключа, как они определены ниже, являются сертификатами особого типа, но несмотря на это подпадают под общее определение. В том определении часто признаются глубокие различия в концепции «сертификата», но несмотря на это сосредоточивается внимание на общей сути.

(2) Сертификат по определению не включает указание на сферу его предполагаемого действия. Сертификат, который является действительным только для одного сообщения или сделки, подпадает под это определение, так же как и сертификат, который является действительным в рамках нескольких сделок в течение определенного времени. Если сертификат является действительным только для одного сообщения или сделки, он должен указывать на это и быть явным образом связан с данным сообщением или сделкой. Если сертификат ограничен в действии в течение определенного периода времени, этот период времени должен быть, как правило, указан в сертификате.

(3) Содержание сертификата зависит от его типа и цели, а также часто предписывается законом или обычаем делового оборота.

3. Заявление о практике сертификации

Заявление о практике, которое делает сертифицирующее лицо при выдаче сертификатов в целом или при выдаче конкретных сертификатов.

Пояснение:

«заявление»: заявление может включать в себя технический стандарт, правила профессионального поведения, законы, применимые к деятельности сертифицирующего лица, товарный знак или марку, представляющие иные правила, в соответствии с которыми действует сертифицирующее лицо.

Комментарий

(1) Если заявление о практике сертификации не является уже хорошо известным или согласованным сторонами в отношении конкретной сделки, широко допускаемым обычаем делового оборота и общеизвестным в торговле или не является предметом широко известного обыкновения и/или соответствующего национального права, форма заявления должна быть приспособлена для представления извещения полагающимся на сертификат сторонам, а также для эффективной ссылки на него и использования. Заявление о практике сертификации не обязательно требует документарности формы, однако его внешнее представление должно обеспечивать разумно высокую степень человекочитаемости, доступности и эффективности. Оно должно также благоприятствовать использованию электронных средств доставки и представления, если электронные средства предполагаются к использованию при совершении сделки или имеют для нее существенное значение, чтобы разумно способствовать автоматизированной обработке и/или компьютеризированному просмотру важных условий. Заявление о практике сертификации главным образом выполняет функцию извещения о практике сертифицирующего лица при выдаче сертификата, и сертифицирующее лицо действует недобросовестно и может быть даже умышленно, если важная часть заявления о практике сертификации необоснованно скрывается.

(2) Данный документ может служить руководством в отношении содержания и формы заявления о практике сертификации.

4. Сертифицирующее лицо

Лицо, которое выдает сертификат и тем самым свидетельствует о точности фактов, имеющих существенное значение для юридической силы действия другого лица. ***Пояснение***

«лицо»: определяется в настоящей публикации с целью включить любое физическое или юридическое лицо, способное удостоверить сообщение, и поэтому должно включать корпорации, партнерства, правительственные агентства и иные юридические лица. Вместе с тем эти не имеющие физической сущности лица могут понимать ; определенные факты только через своих агентов - людей. В конечном счете поэтому процесс сертификации может осуществляться только людьми, несмотря на то, что нематериальные юридические лица могут оказывать помощь в представлении технических средств, услуг и содействия.

Комментарий

(1) Например, сертифицирующими лицами являются нотариусы, органы сертификации открытых ключей (которые могут также включать нотариусов и иных доверенных лиц), а также правительственные служащие и другие лица.

5. Хранилище

Компьютерная система для хранения и извлечения сертификатов и иных сообщений, соответствующих удостоверяемому сообщению.

Комментарий

Цифровое хранилище сертификатов может представляться фирмой, специализирующейся на такой деятельности, в связи с услугами в качестве сертифицирующего лица или иного лица, участвующего в электронной коммерции. Цифровое хранилище является отличным от архива бумажных документов.

6. Цифровая подпись

Преобразование сообщения с использованием асимметричной криптосистемы таким образом, что лицо, обладающее удостоверенным сообщением и открытым ключом удостоверителя может точно установить:

(а) было ли преобразование результатом использования закрытого ключа, который соответствует открытому ключу подписавшего лица, и

(Ь) было ли подписанное сообщение изменено с момента преобразования. ***Пояснение:***

«криптосистема»: данный термин означает информационную систему с применением в ней криптографических средств в целях обеспечения безопасности данных при их передаче по коммуникационным каналам, которые могут быть не безопасными, Безопасность данных, обеспечиваемая таким образом, включает в себя способность соотнесения отдельно взятого сообщения с конкретным криптографическим ключом, а также одну или более операций по установлению того, является ли данное сообщение точно тем же самым, что и в момент предшествующего выполнения операции;

«асимметричная криптосистема»: асимметричная криптосистема, также часто определяемая как «криптосистема с открытым ключом», является информационной системой, использующей алгоритм или ряд алгоритмов, которые обеспечивают пару криптографических ключей, состоящих из закрытого ключа и соответствующего ему открытого ключа. Пара ключей имеет такие свойства, что: (1) открытый ключ способен подтвердить правильность цифровой подписи, создаваемой с использованием закрытого ключа, и

(2) физически невозможно путем вычислений выделить или воспроизвести закрытый ключ из открытого ключа. Открытый ключ, поэтому, может раскрываться без значительного риска разглашения закрытого ключа;

«удостоверитель»: удостоверителем является лицо, применяющее алгоритм в целях быть связанным с содержанием сообщения. Данное определение предполагает, что пара криптографических ключей сама по себе связана с идентифицируемым лицом таким образом, что цифровые подписи, созданные этим лицом, могут быть достоверно отнесены к нему другими лицами. Установление связи лица с парой ключей может сопровождаться сертификатом, идентифицирующим лицо и включающим открытый ключ лица. Такой сертификат определяется в настоящем документе как «сертификат открытого ключа»;

«соответствовать»: в настоящем определении применительно к криптографическим ключам означает принадлежность к одной паре ключей;

«закрытый ключ»: в асимметричной криптосистеме криптографические ключи являются парными, как это указано выше. Закрытый ключ является одним из пары, используемым для создания цифровой подписи. Он должен, поэтому, быть доступным только удостоверителю, и удостоверитель соответственно обязан сохранять исключительный контроль над закрытым ключом (см. обеспечение сохранности средства удостоверения);

«открытый ключ»: в асимметричной криптосистеме как минимум один крипто-рафический ключ из пары может быть раскрыт без возможности обнаружения закрытого ключа. Ключ, который может быть таким образом раскрыт, обычно именуются «открытым ключом».

Комментарий

(1) Некоторые методы аутентификации электронных сообщений не используют Несимметричную криптосистему. Результаты таких методов не подпадают под вышеуказанное определение «цифровой подписи». Таким образом, для удостоверения сообщения могут быть использованы цифровым способом отсканированный образ собственноручной подписи, подпись, проставляемая с использованием стилуса и оцифровывающей таблетки, имя, проставляемое с использованием клавиатуры, пароли или иные механизмы контроля доступа, а также иные процедуры, но они не являются цифровыми подписями», как этот термин используется в настоящем документе. .

(2) Цифровая подпись должна быть защищенным и недвусмысленным образом связанной со своим сообщением. Настолько, насколько долго такая связь поддержиается, неважно, хранится ли цифровая подпись вместе с сообщением, присоединена в начало или конец сообщения либо сохраняется в отдельном электронном файле или информационной системе.

7. Владеть закрытым ключом

Использовать или быть способным использовать закрытый ключ.

Пояснение:

«использовать или быть способным использовать»: основным принципом, лежащим в основе данного определения, является наличие или доступ как вопрос факта, более чем вопрос права или юридического полномочия. Лицо, которое получает ключ путем кражи, обладает доступом или использует ключ, преимущественное право использования которого принадлежит другому лицу, тем не менее «владеет ключом», как это здесь определено.

Комментарий

(1) Поскольку закрытый ключ по своей природе является устройством, способным создавать цифровую подпись при его использовании в информационной системе для этой цели и поскольку цифровая подпись может рассматриваться в качестве удостоверения сообщения, юридическая способность использовать закрытый ключ в целях создания цифровой подписи должна ограничиваться только в пользу удостоверителя. Владение закрытым ключом должно, поэтому, юридически являться исключи тельным правом удостоверителя.

(3) Владение закрытым ключом может включать в себя трудовые или иные агентские отношения, а также иные юридически признанные отношения, в которых право ответственного хранения или контроля (или право собственности, если затрагивается «имущество») распределяется или разделяется способом, признаваемым в соответствии с применимым правом. Например, корпоративный работодатель может предназначить закрытый ключ для использования работником от имени корпоративного работодателя. Посредством этого закрытого ключа цифровые подписи могут быть относимы к корпоративному работодателю путем использования принципов агентских отношений или уполномочия, цифровые подписи позволяют следить за действиями работника. См. также «удостоверение сообщения агентом».

(3) Как правило, закрытый ключ должен иметь минимум одного держателя, если владение ключом намеренно не распределяется или разделяется. В том случае, если асимметричная криптосистема разработана, применяется и поддерживается надлежащим образом, дублирование закрытых ключей возникает крайне редко или не возникает совсем, если только дублирование не производится неправомерно. Если обнаруживается несанкционированное дублирование, держатель должен незамедлительно « приостановить сертификат на время расследования и, в зависимости от результата, отозвать сертификат.

8. Человекочитаемая форма

Представление цифрового сообщения таким образом, чтобы оно могло восприниматься людьми.

Пояснение:

«цифровое сообщение»; информация, обрабатываемая практически всеми компьютерными информационными системами, имеет существенные различия в напряжении, переменных магнитных полярностях, ямках травления на пластике и иных подходах к представлению цифровых битов физическим образом и в виде электрической энергии. Будучи практическим вопросом, представление битов таким образом делает их невоспринимаемыми и нечитаемыми людьми, если только информационная система не представляет их в виде символов, таких как буквы, цифры, знаки пунктуации и форматирования.

Комментарий

(1)Человекочитаемое представление по определению ни обеспечивается технологически надежной информационной системой, ни удостоверяется, иными словами, данное определение не включает в себя гарантию того, что информационная система точно преобразовала сообщение из его базовой цифровой формы в человекочитаемую или что человекочитаемая форма является той же самой, что и форма, воспринимавшаяся удостоверителем сообщения. Является ли представленное сообщение тем же самым, чем оно являлось для удостоверителя, главным образом, зависит от того, включил ли удостоверитель в него параметры, достаточным образом определяющие человекочитаемое представление удостоверенного сообщения. См. ниже, «при установлении сферы использования удостоверенного сообщения изменения в его форме могут быть или не быть существенными».

9. Выдача сертификата

Процесс, посредством которого сертифицирующее лицо создает сертификат и направляет извещение абоненту, указанному в сертификате, о его содержании. ***Пояснение:***

«создает»: создание нового сертификата не подразумевает формирование новых отношений с абонентом по обслуживанию его в качестве клиента. В отношении сертификатов, чья действительность ограничена в течение определенного периода времени, новый сертификат может заменять собой или «обновлять» выданный ранее сертификат с истекшим сроком или отозванный

или с истекающим сроком или отзываемый;

«извещение» и «абонент» см. ниже. Выдача сертификата не обязательно гарантирует его действительную передачу.

Комментарий

(1) Некоторые правовые системы гражданского права или национальные обычаи могут предписывать способ, в котором может быть выдан сертификат, в частности, в отношении отдельных сделок. Правовые системы гражданского права, как правило, требуют официального участия нотариуса в определенных видах сделок, в рамках которых выдаются сертификаты. Нотариальная практика гражданского права часто включает в себя детальное изучение намерения сторон и аспектов сделки в целях получения определенности в том, что стороны в полной мере информированы о последствиях своей сделки.

10. Извещение

Сообщать информацию другому лицу способом, который с учетом обстоятельств вероятнее всего сделает другое лицо осведомленным об информации.

Пояснение:

«информация»: извещение может вызвать иск о введении в умышленное или неосторожное заблуждение, если будет доказана неточность информации. Достаточной предупредительной мерой может являться проявление извещающим лицом заботливости при составлении окончательных выводов. Извещающее лицо может сообщать ' получателю соответствующие обоснованные сведения или вероятные события, оставляя получателю возможность самостоятельного установления степени достоверности извещения. Получатель часто способен лучше оценить все признаки и степень неопределенности с точки зрения своих рисков;

«с учетом обстоятельств вероятнее всего сделает другое лицо осведомленным об информации»: обязанность по извещению может считаться исполненной даже в том случае, когда предполагаемый получатель извещения оказывается неспособен ознакомиться с его содержанием, при условии, что извещающее лицо действует добросовестно и предпринимает действия, которые при обычном ходе ведения дел должны быть достаточными для доведения извещения до предполагаемого получателя и при-- влечения его внимания. Принципы Международного института унификации частного права (UNIDROIT) для международных коммерческих договоров отмечают:

(1) Когда требуется извещение, оно может быть направлено с использованием любых средств, соответствующих обстоятельствам.

(2) Извещение приобретает силу, когда оно достигает лица, которому было направлено.

(2) Для целей параграфа

(2) извещение «достигает» лица, когда делается ему устно или доставляется по месту нахождения коммерческого предприятия либо по почтовому адресу.

(4) Для целей настоящей статьи термин «извещение» включает в себя заявление, требование, запрос или иное изъявление намерения».

Принципы UNIDROIT для международных коммерческих договоров, ст. 1.9(1994). Комментарий 4 к этой же самой статье указывает при определении термина «достигает», что извещение достигает адресата тогда, когда оно доставлено по месту ведения адресатом предпринимательской деятельности либо по его почтовому адресу. Конкретное сообщение, являющееся предметом рассмотрения, не обязательно должно физически попадать к адресату. Достаточно, чтобы оно было получено по факсу, телексу или через компьютер адресата.

В электронной среде доставка надежно удостоверенного сообщения, адресованного предполагаемому получателю, с использованием технологически надежной системы без очевидных ошибок должна быть достаточной с точки зрения средств извещения, если стороны не договорятся об ином.

Комментарий

(1) Если стороны заключили договор, то он сам или общая договорная обязанность добросовестности могут включать в себя также требование извещения, и, может быть, согласованная формулировка лучше применима к взаимоотношениям сторон. Вместе с тем стороны также могут находиться в преддоговорном состоянии, и удостоверение сообщения или сертификация, подлежащие извещению, являются частью усилий по заключению договора и удовлетворяют требованиям к форме договора. В таком преддоговорном окружении обязанность воздерживаться от

введения в заблуждение, соблюдать добросовестность при заключении сделки или доктрина culpa in contrahendo составляют и определяют общие требования к извещению.

11. Лицо

Физическое или юридическое лицо, которое либо:

(а) признано в соответствии с применимым правом способным к удостоверению сообщения, либо

(Ь) способно к удостоверению сообщения в силу фактических обстоятельств. ***Пояснение:***

«юридическое лицо»: информационные системы и иные устройства не являются «юридическими лицами» в значении, употребляемом в данном определении. Скорее такие системы и устройства являются инструментами лиц, которым они принадлежат и которыми они используются.

12. Сертификат открытого ключа

Сертификат, свидетельствующий о принадлежности открытого ключа своему абоненту, соответствующий закрытому ключу, которым обладает этот абонент. ***Пояснение:***

«открытый ключ»: открытые ключи могут использоваться лицом, имеющим цифровую подпись, для установления того, с использованием какого закрытого ключа создана цифровая подпись и подвергалось ли изменению подписанное сообщение с момента своего подписания. См. выше - «цифровая подпись» и ниже - «проверять цифровую подпись»;

«свидетельствующий»: процесс, посредством которого сертифицирующее лицо удостоверяется в точности сведений, указанных в сертификате.

13. Отзыв сертификата открытого ключа

Действие, которым сертифицирующее лицо объявляет сертификат открытого ключа постоянно недействующим, начиная с определенного периода времени.

Пояснение:

«объявляет»: отзыв является очевидным заявлением и не включает в себя уничтожение утрачивающего силу сертификата. Утрачивающий силу сертификат остается доступным для проверки цифровых подписей, вступивших в силу в течение того времени, когда сертификат был еще действителен;

«время»: данное определение предполагает, что действительность сертификата открытого ключа ограничена определенным периодом времени, который прекращается с отзывом сертификата. Сертификаты открытого ключа, чья действительность ограничена рамками конкретной сделки или по иным критериям, могут быть, наверное, объявлены недействительными после выдачи, но настоящий документ не определяет такую утрату действительности как «отзыв».

Комментарий

Несмотря на то, что извещение не является составной частью данного определения (определение см, выше), оно требует отзыва.

14. Абонент

Лицо, которое является субъектом, указанным в сертификате.

Пояснение:

«субъект сертификата»: не каждый удостоверитель является абонентом, так же как не каждое удостоверенное сообщение имеет взаимосвязанный сертификат. «Абонент» вполне может иметь отношение к удостоверителю, но скорее в качестве субъекта сертификата, чем удостоверителя как такового.

Комментарий

(1) Например, если сертификат открытого ключа указывает явным образом или какой-либо форме отсылки:

Настоящим я свидетельствую 4 августа 1997 г., что Джон Вильям Томпсон, проживающий по адресу: 38 Cours A1bert 1er, 75008 Paris, France лично присутствовал и был идентифицирован ... Далее, тот же самый Джон Вильям Томпсон продемонстрировал мне, что он обладает закрытым ключом, соответствующим следующему открытому ключу... и, таким образом, Джон Вильям Томпсон является абонентом данного сертификата.

(2) В некоторых случаях в качестве абонента может выступать лицо, действующее по

поручению другого лица. Так, нижеприведенный пример может включать следующее:

Тот же самый Джон Вильям Томпсон также представил решение корпорации XYZ Corporation 5A, подлинность которого я удостоверил... Названное решение, копия которого прилагается, уполномочивает названного Джона Вильяма Томпсона. действовать по определенным вопросам от имени корпорации XYZ Corporation SA в качестве ее уполномоченного представителя.

Удостоверения сообщение закрытым ключом, соответствующим открытому ключу, указанному в сертификате, может быть, в силу национального законодательства об агентских отношениях, признано в качестве удостоверения сообщения принципалом посредством действия агента.

. (3) Абонент, как правило, также является клиентом или состоит в договорных отношениях с сертифицирующим лицом.

15. Приостанавливать сертификат открытого ключа

Действие, которым сертифицирующее лицо объявляет сертификат открытого ключа временно недействительным на определенный период времени.

Пояснение:

«недействительный»; если сертификат является недействительным, то в этом случае третьи лица не могут на него полагаться, хотя это не исключает действие правового принципа, что если полагающаяся на сертификат сторона действовала разумно (см. пояснение ниже) или добросовестно, то факт приостановления не препятствует такому доверию;

«время»: данное определение предполагает, что действительность сертификата открытого ключа ограничена определенным периодом времени, который прекращается с отзывом сертификата. Сертификаты открытого ключа, чья действительность ограничена рамками конкретной сделки или по иным критериям, могут быть, наверное, объявлены недействительными после выдачи, но настоящий документ не определяет такую утрату действительности, как «приостановление».

16. Технологически надежный

Обладающий качествами:

(a) разумной защиты от вмешательства и злоупотреблений;

(b) обеспечения разумного уровня доступности, надежности и правильности и функционирования.

Пояснение:

«разумно .... разумный»: стандарт разумности в данном определении отражает и тот факт, что безопасность существует в различной степени и должна, обычно, оцениваться с точки зрения фактических обстоятельств. Большая или меньшая степень и •безопасности возможна практически при всех ситуациях, подобно тому как улицы или аэропорты всегда могут становиться более безопасными. При рассмотрении дела в суде, поэтому, основным должен быть не вопрос о том, мог ли ответчик сделать больше, но проявил ли ответчик достаточную степень заботливости при разработке, поддержании работоспособности и эксплуатации рассматриваемой системы, принимая во внимание экономическую целесообразность и стоимость дополнительных мероприятий, а также преимуществ, которые они могли бы предоставить при соответствующих обстоятельствах. Следует отметить, что использование принципа «разумности» может быть проблематичным в юрисдикциях стран гражданского права, несмотря на то, что могут использоваться стандарты заботливого отца семейства или добропорядочного предпринимателя для большего приближения к данному принципу;

«правильное функционирование»: какой тип функционирования является «правильным» для системы, зависит от ее проектировочных особенностей. Ожидания пользователя системы должны рассматриваться с точки зрения того, что разумно можно ожидать от системы, учитывая пределы ее организации и функционирования в той степени, в которой с ними был ознакомлен пользователь.

Комментарий

(1) Цели технологической надежности являются, по существу, следующими:

Конфиденциальность: защита информации в целях недопущения ее раскрытия неуполномоченным лицам или обнаружения ими.

Целостность: защита логической структуры данных, в частности от несанкционированного создания, изменения или уничтожения данных

Доступность: защита доступа к информации и ресурсам в целях, чтобы правомочные пользователи не могли недобросовестно отрицать факты доступа.

Правомерное использование: защита ресурсов в целях их использования только уполномоченными лицами разрешенными способами.

17. Надежный

Осуществление предпринимательской деятельности таким образом, который гарантирует доверие действующего разумным образом в области коммерции лица, имеющего возможности, деловые навыки и иные ресурсы, которые являются достаточными для обеспечения исполнения этим лицом юридических обязанностей, а также гарантируют беспристрастное судебное разбирательство.

Пояснение:

«достаточный»: достаточность возможностей, деловых навыков и ресурсов лица, а также степень не заинтересованности лица должны исследоваться в соответствии со стандартами ответственности. В любом случае возможны большие усилия и финансовые вложения, но вопросом является то, могло ли действующего разумным образом лицо с учетом обстоятельств прилагать дополнительные усилия и делать дополнительные финансовые вложения в целях получения больших возможностей, деловых навыков или отсутствия предвзятости.

Комментарий

(1) Надежность является центральным принципом всех деловых отношений и не является принципом, который может быть строго определен. Оценка коммерческого риска, присущего определенной сделке, будет всегда играть центральную роль. Конечно, существуют профессии, такие как нотариусы, которые устраняют значительную долю риска, создавая презумпцию добросовестности в отношении подписи путем выдачи свидетельств, которыми они принимают на себя ответственность за точность содержащихся в них фактов, в пользу получающей стороны. Действительно, нотариус остается ответственным за любое заявление, сделанное в свидетельстве, вне зависимости от отсутствия договорных отношений между ним и стороной, полагающейся на сделанное заявление.

(2) Вопросом оценки коммерческого риска будет являться, могло бы или нет полагаться лицо на сертификат в случае, если удостоверитель, абонент и даже сертифицирующее лицо относятся к одинаковой группе. Примеры бумажной технологии, такие как индустрия кредитных карт, исторически представляют образцы непредвзятого исполнения юридических обязанностей, несмотря на выполнение определенной роли в сделке.

18. Действительный сертификат

Сертификат, который сертифицирующее лицо выдало или предоставило другому лицу при обстоятельствах, когда доверие этого лица к сертификату является предвидимым, если только сертифицирующее лицо своевременно не направляет извещение ; о том, что на сертификат нельзя полагаться или сертификат не является сертификатом ′ открытого ключа, который был отозван или на момент рассмотрения вопроса приостановлен.

Пояснение:

«направляет извещение»: извещение должно доводиться до всех лиц, которые способны полагаться на сертификат.

Комментарий

(1) Сертифицирующее лицо может желать усиления ответственности за содержание выданного сертификата посредством вступления в договорные отношения абонентом, оговорки об отказе от прав в заявлении либо даже в самом сертификате Вместе с тем должно уделяться внимание таким оговоркам об отказе от прав, которые некоторые юрисдикции рассматривают в качестве недобросовестных или недействительных договорных условий. В частности, это является правилом для сделок которые рассматриваются «потребительскими».

19. Проверять цифровую подпись

Применительно к удостоверению отдельно взятого сообщения (цифровая подпись, сообщение и открытый ключ) точно устанавливать, что: &

(a) цифровая подпись создана с использованием закрытого ключа, соответствующего открытому ключу; и

(b) сообщение не было изменено с момента создания цифровой подписи. :. ***Пояснение:***

«проверять»: если получатель не проверяет указанную информацию, то не может быть

доверия к инфраструктурным механизмам, которые были созданы специально для этой цели, а также к обеспечению безопасности сообщения.

Комментарий

Конечно, это является центральным вопросом в доверии к удостоверенному сообщению с цифровой подписью.

НАИЛУЧШАЯ ПРАКТИКА
VII. Удостоверение сообщения

1. Удостоверение сообщения как вопрос факта

Сообщение является удостоверенным как вопрос факта, если приемлемые доказательства указывают:

(a) на идентичность удостоверителя; и

(b) что сообщение не было изменено с момента удостоверения.

Пояснение:

«как вопрос факта»: в отличие от юридической значимости или значения, фактиче-ский вопрос удостоверения сообщения касается только идентификации удостоверителя . и удостоверенного сообщения, исходя из доступных и допустимых доказательств. Таким вопросом стремятся только установить факты того, кто что удостоверил.

Комментарий

(1) Удостоверение сообщения в доказательственных целях в рамках судопроизводства перед судебным заседанием, как правило, служит целью удостоверения сообщения в качестве вопроса факта. Центральным вопросом судебного исследования является подлинность предлагаемого доказательства и его фактическая связь с вовлеченным в спор лицом. (Для примера см.: Федеральные правила доказывания США № 901, предусматривающие, что требования к доказательствам считаются соблюденными представлением «доказательств, достаточных для поддержания вывода о правомерности требования защиты по спорному вопросу», и приводящие ряд примеров).

(2) Удостоверение сообщения может также служить для указания на источник события, часто в доказательственном аспекте, в том случае, когда вопрос является фактом причинности, более чем любое другое юридическое последствие использования подписи.

2. Установление авторства (атрибуция) и юридическая значимость сообщения

Лицо должно проводить атрибуцию удостоверенного сообщения с лицом, которое действительно удостоверило сообщение.

Пояснение:

«должен»: следует ли любое последствие из неспособности установить связь удостоверенного сообщения с лицом, зависит от подразумеваемого смысла сообщения. Если сообщение может быть безболезненно игнорировано, в этом случае неспособность установить связь сообщения с лицом не влечет за собой последствий;

«приписывать»: лицо, обладающее удостоверенным сообщением, должно рассматривать его в качестве связанного с удостоверителем различными способами, которые часто являются очевидными, исходя из сопутствующего выражения намерения удостоверителя, фактов и обстоятельств сделки, хода дел или торговых обычаев;

«удостоверенное сообщение»: с точки зрения определения «удостоверять» (см. выше), термин «удостоверенное сообщение» здесь означает сообщение, которое:

(1) не повреждено и не изменено с момента удостоверения, и

(2) идентифицирует удостоверителя;

«действительно удостоверил»: в случае подлога мошенник является действительным удостоверителем более, чем предполагаемое подписавшее лицо.

В этой связи см. также ст. 11 (Атрибуция сообщения данных) Типового закона ЮНСИТРАЛ 1995.

Комментарий

(1) Обязанность по атрибуции удостоверенного сообщения его удостоверителю предполагает, что лицо, обладающее удостоверенным сообщением, действует добросовестно, проявляет разумную

заботу при оценке удостоверенного сообщения, а также своевременно не осведомлено или не извещено о том, что удостоверенное сообщение является фальшивым или существенно оспоримым.

(2) При выяснении того, кто действительно удостоверил сообщение, лицо вправе получать дальнейшие разумные заверения, что удостоверитель удостоверил сообщение надлежащим образом. При установлении того, что является разумным на самом деле, суд должен рассматривать указания на надежность удостоверенного сообщения или ее отсутствие, доступность этих указаний для лица, обладающего сообщением, а равно ресурсов, требуемых для обретения доступности к дальнейшей информации.

(3) Если лицо ошибочно проводит установление авторства подложного или неправомерно измененного сообщения и, таким образом, несет убытки, а подлог или неправомерное изменение происходят вследствие неспособности подразумеваемого удостоверителя обеспечить сохранность аутентифицирующего устройства или иным образом по вине подразумеваемого удостоверителя, в этом случае он обязан предоставить возмещение или компенсацию убытков лицу, проводящему атрибуцию.

(4) Сила атрибуции в отношении удостоверителя зависит от содержания удостоверенного сообщения, иных фактов и обстоятельств сделки, применимого права, обычного ведения дел между сторонами и/или торговых обычаев. Например, удостоверение письменного волеизъявления по договору обычно принимается в целях указания на согласие с договором и может отвечать формальным требованиям к удостоверению сообщения, достаточных, чтобы придать договору юридическую или исковую силу. Удостоверение письма обычно указывает на авторство. Удостоверение оборотного документа способом, аналогичным индоссаменту, имеет силу индоссамента.

(4) Атрибуция или принудительная сила сообщения, в отношении которого иным образом проведена атрибуция, могут быть ограничены формальными требованиями к удостоверению и сертификации.

3. Удостоверение сообщения агентом

Если агент удостоверяет сообщение и представляет себя действующим на основании полномочия принципала, удостоверенное сообщение является действительным в качестве сообщения принципала, если в соответствии с применимым правом агент обладал достаточными полномочиями для удостоверения сообщения.

Пояснение:

«достаточные полномочия для удостоверения»: правовые системы различаются порядком, обычно используемым для предоставления полномочий и, в частности, степенью, в которой признаются подразумеваемые или явные полномочия, и предоставляемой юридической силой (см. комментарий (2) ниже). Если в соответствии с применимым правом существование достаточных предполагаемых агентских полномочий находится под сомнением, получатель удостоверенного сообщения может обоснованно добиваться дальнейших гарантий.

Комментарий

(1) Лицо, как правило, действует на свой риск, полагаясь на представление агентом своих полномочий. Вместо того, чтобы принимать на веру слова предполагаемого агента о действительности, и сфере действия агентских отношений, лицо, обладающее удостоверенным сообщением, должно требовать сертификат или иное, более 1 достоверное, доказательство агентских отношений.

(2) Правовые системы различаются степенью, в которой лицо может полагаться на заверения об агентских отношениях предполагаемого принципала, которые недостаточны, чтобы обладать силой действительной доверенности в случаях, когда принципал позднее оспаривает наличие агентских отношений. В общем праве «явные полномочия» могут возникать почти из любого проявления агентских отношений со стороны принципала к третьим лицам. Правовые системы гражданского права традиционно избегают признания явных полномочий, несмотря на то, что юриспруденция отчасти разработала сопоставимые доктрины в случаях, когда принципал оказывается неспособным опровергнуть представление, что агент обладал агентскими полномочиями, или удержать агента от действий от имени принципала. 4. Приемлемая практика для удостоверения сообщений .Удостоверитель должен удостоверять сообщение с использованием средств; приемлемых с учетом обстоятельств.

Пояснение:

«должен»: следствием неспособности удостоверить сообщение надлежащим образом может быть право не принимать его во внимание. В рамках общей коммерческой или иным образом согласованной практики сообщение может не приниматься во внимание, если способ его удостоверения либо противоречит соглашению сторон, являясь неприемлемым для придания юридических последствий, предполагаемых р. сторонами в отношении соглашения, либо если доверие к соглашению в том виде, как оно было удостоверено, не могло бы быть разумным с учетом обстоятельств; «приемлемых с учетом обстоятельств»: как поясняет нижеприведенный комментарий, средства должны реализовывать намерение сторон или, как минимум, разумно в отвечать контексту сделки. По крайней мере требования к подписи оказывали бы благотворное воздействие, требуя от лица использовать минимальные способы удостоверения. Вместе с тем наложение санкций за неспособность соответствовать требованиям к форме может оказаться проблематичным. В общем праве прецеденты обладают тенденцией к ослаблению формальных требований, может быть, в силу трудности в определении соответствующей санкции за неисполнение. В гражданском праве существуют более строгие формы, которых следует придерживаться, в частности в тех 1 сферах, где государство может иметь интерес, таких как законодательство о недвижимости, наследование или коммерческая регистрация компаний. Такие случаи требуют вмешательства нотариуса в качестве сертифицирующего лица. Типовой закон ЮНСИТРАЛ (ст. 6) не касается формальных требований и оставляет получателю доказывание авторства сообщения. Несмотря на разумность, такой подход сохраняет одну острую проблему: получатель несет бремя доказывания в отношении вопросов авторства, но только отправитель сообщения может удостоверить , свое сообщение. Получатель может действовать на свой риск при отказе в приеме сообщения, которое, с учетом различных формулировок, понятия «подпись», могло бы рассматриваться как подлинное. Настоящая статья стремится рассматривать эту проблему путем предоставления получателю права требовать разумные гарантии подлинности удостоверенного сообщения.

Комментарий

(1) Получатель удостоверенного сообщения может требовать больших гарантий и его действительности, таких как действительный сертификат, свидетельствующий существенный факт, а также замены или дополнения удостоверенного сообщения с использованием более технологически надежного метода, если удостоверение сообщения либо не осуществлялось согласованным сторонами способом, либо является неприемлемым для придания юридических последствий, предполагаемых сторонами в отношении соглашения. При отсутствии явно выраженного соглашения предполагается, что стороны намеревались достичь разумного результата и поэтому использовать только такую практику удостоверения, которая является разумной с учетом обстоятельств.

(2) При установлении того, что является разумным с учетом обстоятельств, получатель должен оценивать:

факты, о которых получатель знает или о которых он был извещен, включая все факты, приведенные в сертификате; ценность или важность удостоверенного сообщения;

в рамках спорной сделки - ход исполнения обязательств между полагающимся на сертификат лицом и его абонентом, а также доступные показатели надежности или ненадежности, подтверждающие удостоверенное сообщение;

в предшествующих сделках - ход ведения деловых отношений между полагающимся на сертификат лицом и его абонентом, а также доступные показатели надежности или ненадежности, подтверждающие удостоверенное сообщение;

обычаи торговли, которыми руководствуются в технологически надежных информационных системах.

Факторы перечислены приблизительно в порядке их значимости.

5. Сфера использования удостоверенного сообщения

Составитель удостоверенного сообщения должен ясно указывать, что оно является удостоверенным.

Пояснение:

«ясно указывать»; удостоверитель должен равно установить, что является сообщением в целях отграничения его от других предметов, а также создать явную связь между действием по удостоверению сообщения и самим удостоверенным сообщением.

Комментарий

(1) Поскольку удостоверение сообщения не затрагивает изменений сообщения, получающее сообщение лицо должно установить, доходит ли его сообщение незатронутым. Такое установление только тогда возможно, когда сообщение было четко определено и увязано со временем его удостоверения. На бумаге установление сопровождается пространственными ограничениями, условиями форматирования и обычаем проставления подписи в конце сообщения. Связь между подписью и сообщением часто сопровождается включением их обоих в один и тот же бумажный документ с подписью, следующей за сообщением.

(2) Определение сообщения осложнено тем фактом, что различные системы могут представлять сообщение в различных человекочитаемых формах. Например, один принтер или факс-аппарат может использовать иные размеры бумаги, чем другой. Различия в представлении подписанного материала могут быть или не быть значимыми. В электронных сообщениях различия являются обычными, даже когда все соответствующие информационные системы технологически надежны, просто в силу различия возможностей и предпочтений информационных систем. Удостоверитель должен оформлять удостоверенное сообщение способом, который позволяет получающей информационной системе представлять его надлежащим образом, либо способом, требуемым законодательством или согласованным между удостоверителем и получателем или в соответствии с торговым обычаем, применимыми техническими стандартами и/или общей практикой для сообщений такого типа. Стороны должны согласовать при установлении формы своих сообщений, какие отклонения будут рассматриваться в качестве значительных. При отсутствии такого соглашения удостоверитель может сам установить отклонения, которые будут рассматриваться в качестве значительных изменений сообщения. Обычно небольшие отклонения в размере, шрифте, разбивке, отступах и аналогичных деталях не являются существенными, вместе с тем изменение, существенно затрагивающее смысловое содержание, включая изменение логической структуры сообщения, должно, как правило, рассматриваться в качестве значительного изменения.

6. Обеспечение сохранности средства удостоверения Если лицо удостоверяет сообщение посредством устройства, лицо должно про-. являть, как минимум, разумную заботливость в целях предотвращения его несанкционированного использования.

Пояснение:

«устройство»: если устройство состоит из системы взаимосвязанных элементов, не обязательно должна обеспечиваться сохранность всей системы. Более удовлетворительным является обеспечение сохранности одного или более ключевых элементов системы, достаточных, чтобы воспрепятствовать появлению фальшивого удостоверенного сообщения;

«разумная заботливость»: является степенью осторожности и осмотрительности, которую разумный человек проявил бы с учетом обстоятельств (комментарий к понятию «разумный» см. выше).

Комментарий

(1) Удостоверяющее устройство должно физически содержаться в месте, где доступ к нему ограничен или надежно контролируется. Право доступа должно предоставляться только заслуживающим доверия лицам и, как правило, быть основано на их потребности в использовании удостоверяющих средств. Лица, которым предоставляется право доступа, должны идентифицироваться путем ввода пароля или парольных фраз, по биометрической информации или с использованием иных защищенных средств.

(2) В том случае, если возможно исправляющее действие вслед за утратой контроля за удостоверяющим устройством, оно должно предприниматься без задержки. . В случае, когда утрачивается закрытый ключ, сертификат открытого ключа должен быть отозван или незамедлительно приостановлен до того времени, пока он не сможет быть отозван.

7. Заверения сертифицирующему лицу

Абонент должен точно представлять сертифицирующему лицу все факты, существенные для сертификата.

Пояснение:

«представлять»: может приобретать многие формы. Может быть просто заявлением абонента, или сертифицирующее лицо может получить внешние доказательства по вопросам,

содержащимся в сертификате. Поскольку сертифицирующее лицо будут нести ответственность за заявления, сделанные в сертификате, в нем рекомендуется пояснить, каким образом достигаются заявления о фактах.

Комментарий (1) См. ниже определение «сертификация».

VIII. Сертификация

1. Юридическая сила действительного сертификата

Лицо может полагаться на действительный сертификат как на точно представляющий изложенные в нем факт или факты, если лицо не получило извещения о том, что сертифицирующее лицо оказалось неспособным выполнить существенные требования к практике удостоверения сообщений.

Пояснение:

«полагаться»: степень, в которой лицо может надлежащим образом полагаться [на факты], ограничивается тем что является разумным с учетом обстоятельств. Иными словами, лицо не вправе полагаться [на факты], если предприниматель с обычной осмотрительностью не сделал бы этого, находясь в существенно сходном информационном и ситуационном положении. Это подразумеваемое ограничение в отношении доверия находит свое выражение в материальном праве при ограничении возможностей для обмана со стороны истцов, которые не являются чрезмерно доверчивыми или пострадавшими; см. например: Второй свод законов США о деликтах, § 548A (1977) («злонамеренное введение в заблуждение является юридическим основанием денежных убытков, возникающих вследствие действия или бездействия, совершаемого в результате доверия, если и только если убытки могли быть разумно ожидаемы в результате такого доверия»);

«извещение»; Принципы UNIDROIT для международных коммерческих договоров (1994) отмечают в ст. 1.9, что «извещение включает в себя заявление, требование, запрос или иное сообщение о намерении».

Комментарий

(1) По существу сертификат является только доказательством факта или фактов, которые он представляет. Как таковой он является настолько надежным, насколько заслуживает доверия сертифицирующее лицо. Для того, чтобы коммерция функционировала надлежащим образом, общество должно предоставить надежные средства для установления важнейших фактов, таких как идентичность удостоверителя. Сертифицирующие лица предоставляют такие средства, но только если сертифицирующие лица сами заслуживают доверия.

(2) Когда общеизвестно, что соблюдается заслуживающая доверия практика в отношении сертификатов, сертификаты, как правило, рассматриваются как устанавливающие представленные в них факты. Для каждой сделки стороны обычно могут установить, является ли приемлемым конкретный сертификат или тип сертификата. При определенных обстоятельствах и, в частности, при отсутствии соглашения между сторонами, применимое материальное право часто может предусматривать норму для установления действительности наряду с поддерживающей ролью сертификации. Такие материальные нормы могут относиться к надзору правовой системы за деятельностью сертифицирующих лиц.

(3) Несмотря на то, что сертификат является принципиальным доказательством, допустим ли он в судебном или арбитражном процессе, устанавливается в соответствии с правилами суда.

(5) Все вышеуказанное предполагает, что стороны действуют добросовестно и без обмана или небрежности при ведении своего бизнеса.

2. Точность заверений в сертификате

Сертифицирующее лицо должно подтвердить точность всех фактов, изложенных в действительном сертификате, если только из самого сертификата не ясно, что какая-то информация не была проверена.

Пояснение:

«изложенных»: применяется, равно к фактам, явно указанным в сертификате, и к фактам, на которых основаны выводы в сертификате;

«какая-то информация не была проверена»: было озаглавлено как «непроверенная информация абонента». См. комментарий ниже.

Комментарий

(1) Одна из правовых школ придерживается точки зрения, что вся информация, изложенная в сертификате, должна проверяться сертифицирующим лицом. Это могло бы оказаться излишним ограничением для коммерческой практики при наличии обстоятельств, когда требуется удостоверить сообщение, но удостоверитель не способен представить достаточные доказательства, например, его корпоративных полномочий для выполнения каких-либо действий. Поэтому должно быть возможным включение в сертификат заявления о факте, что удостоверитель предполагается действующим от имени конкретной корпорации, но это не было подтверждено. Получающая сторона тогда способна произвести оценку коммерческого риска на предмет того, принимать ли удостоверенное сообщение в его текущем состоянии или требовать дальнейших доказательств.

3. Надежность сертифицирующего лица

Сертифицирующее лицо должно:

(а) использовать только технологически надежные информационные системы и процессы, а также заслуживающий доверия персонал при выдаче сертификата, приостановлении или отзыве сертификата открытого ключа и для обеспечения сохранности своего закрытого ключа, если таковой есть;

(Ь) не иметь конфликта интересов, которые могли бы лишить сертифицирующее лицо доверия при выдаче, приостановлении и отзыве сертификата;

(с) воздерживаться от содействия абоненту в нарушении обязанностей;

(с1) воздерживаться от действий или упущений, которые значительно ослабят разумное и предвидимое доверие к действительному сертификату;

(е) действовать заслуживающим доверия образом в отношении абонента и лиц, которые полагаются на действительный сертификат.

Пояснение:

«заслуживающий доверия персонал»: сертифицирующее лицо должно принимать разумные меры, чтобы контролировать, обучать, управлять и обеспечивать лояльность всех работников, осуществляющих функции, значительно затрагивающие процесс сертификации;

«конфликт интересов»: будучи доверенным лицом сторон по сделке и выполняя функции доверенного, проверяющего факты лица в случае возникновения спора, сертифицирующее лицо не должно иметь в сделке интересов, которые могли бы скомпрометировать доверия к сертифицирующему лицу;

«абонент»: сертифицирующее лицо несет обязанность перед абонентом, которому сертифицирующее лицо выдало сертификат, а также перед правопреемниками абонента, права которых зависят от сертификации.

Комментарий

(1) Надежность сертифицирующего лица является ключевым элементом во всей концепции сертификации. Это доверие, в свою очередь, в общем основано на

ответственности за свои заявления, которую согласно принять сертифицирующее лицо. Сертифицирующее лицо может стремиться ограничить свою ответственность

определенным уровнем посредством «заявления о практике сертификации» (см. 1 выше), но при этом оно должно проявлять осторожность в том, что такое ограничение ответственности было допустимо в рамках юрисдикции сертифицирующего лица. В дальнейшем сама природа электронной коммерции как международного средства осложняет данный вопрос по мере того, как сертифицирующее лицо обнаруживает, что на его сертификацию полагаются за пределами собственных границ. По аналогичному признаку лицо, полагающееся на сертификат, должно установить уровень доверия, который сертифицирующее лицо ожидает от него при внесении записей в сертификат.

4. Извещение о практике и проблемах

Сертифицирующее лицо должно принимать разумные меры, чтобы извещать заинтересованное лицо:

(а) о любом существенном заявлении о практике сертификации, и

(Ь) любом факте, существенном либо для надежности сертификата, который выдан сертифицирующим лицом, либо длящего способности оказывать свои услуги.

Пояснение:

«заинтересованное лицо»: чтобы гарантировать, что сертифицирующее лицо предвидит правовой результат, лицо, которое считает затронутыми свои права, может (известить сертифицирующее лицо о своей позиции и интересах, а также потребовать предоставления заявления о практике сертификации или прочую информацию.

Комментарий

(1) Предвидимость является сложной концепцией, особенно когда сертификат может свободно обращаться, хотя, конечно, это является составной частью оценки коммерческого риска.

5. Финансовые ресурсы

Сертифицирующее лицо должно обладать финансовыми ресурсами, достаточными, чтобы осуществлять свою деятельность и нести разумные риски, возникающие в результате выдачи им сертификата.

Пояснение:

«достаточные»: как между сертифицирующим лицом и его клиентом, абонентом, достаточность финансового положения сертифицирующего лица является очевидной из их готовности вести дела друг с другом в рамках обстановки, при которой абонент мог бы сохранить услуги другой стороны. По отношению к третьим лицам, однако, достаточность финансового положения сертифицирующего лица должна оцениваться в соответствии со стандартом разумности;

«разумные риски»: разумность риска должна оцениваться с точки зрения того, что является предвидимым, исходя из состояния информированности сертифицирующего лица, и что является вероятным.

Комментарий

(1) В рамках данного раздела мы должны рассматривать влияние страхования, поручительного либо гарантийного. От профессиональных сертифицирующих лиц, таких как нотариусы, требуется осуществлять достаточное страхование на случай возмещения ущерба в целях покрытия таких убытков, которые вероятно могут наступить в результате того, что другие лица полагаются на их сертификацию. Такое страхование может рассматриваться как дополнительное к имеющимся в распоряжении финансовым ресурсам сертифицирующего лица, хотя очевидно, что оно не будет обладать доступом к таким ресурсам, если только и пока к нему не предъявлен иск.

б. Записи

Сертифицирующее лицо должно сохранять записи всех фактов, имеющих существенное значение для сертификата, который выдан на разумный период времени. ***Пояснение:***

«факты, имеющие существенное значение для сертификата»: требуемые записи включают в себя доказательства, поддерживающие все представления, сделанные в сертификате;

«разумный период времени»: продолжительность периода сохранения записей является трудным вопросом с точки зрения ее точного определения и требует оценки необходимости в обращении к записям по сравнению с издержками по их хранению. Записи могут потребоваться, как минимум, в течение времени, пока может быть оспорена сделка, основанная на действительном сертификате. В отношении большинства сделок законодательство об исковой давности окончательно делает сделку бесспорной. Вместе с тем в отношении некоторых сделок, таких как передача прав на недвижимое имущество, юридическая чистота не может быть достигнута до истечения удлиненного периода времени.

Комментарий

(1) Представители большинства профессий уже приняли правила хранения записей в зависимости от их характера. Не существует причины для того, чтобы эти правила были отличными в электронном мире, хотя дополнительная заботливость должна проявляться для обеспечения возможности поиска хранимой информации, особенно с точки зрения быстрого развития технологий.

7. Прекращение деятельности сертифицирующего лица

В случае прекращения своей деятельности сертифицирующее лицо должно:

(а) действовать таким образом, который влечет минимальную вредоносность для держателей и лиц, полагающихся на выданные действительные, работоспособные сертификаты; и

(В) передавать свои записи компетентному правопреемнику.

Пояснение:

«компетентный правопреемник»: другое сертифицирующее лицо является, по общему правилу, компетентным в целях правопреемства ликвидируемого сертифицирующего лица. Подотчетная, высококвалифицированная архивная служба, профессиональная ассоциация или регулирующий орган также могут соответствовать этому требованию. Правопреемник не обязан выдавать новые сертификаты, но должен, как минимум, продолжать обеспечивать услуги по приостановлению, отзыву и возврату сертификатов.

Комментарий

(1) В том случае, если нет правопреемника, готового принять бизнес сертифицирующего лица, может быть необходим отзыв всех остающихся действительными сертификатов с того момента, когда сертифицирующее лицо окажется не способным поддерживать их в будущем.

8. Приостановление сертификата открытого ключа по запросу

Сертифицирующее лицо, которое выдало сертификат, должно незамедлительно приостановить его по запросу лица, идентифицирующего себя в качестве абонента, поименованного в сертификате открытого ключа, или в качестве лица, которое вероятно может быть способно знать о нарушении безопасности закрытого ключа абонента, такого, как агент, работник, партнер по бизнесу или ближайший член семьи абонента.

Пояснение:

«сертифицирующее лицо, которое выдало»: хотя сертифицирующее лицо не обязано подтверждать идентичность или наличие агентских полномочий у лица, делающего запрос, сертифицирующее лицо, которое выдало сертификат, обычно должно быть лицом приостанавливающим его, поскольку сертифицирующее лицо в наилучшей степени способно производить проверку и отказывать в исполнении запросов, очевидно противоречащих интересам абонента, таких как запросы, предназначенные для использования в хулиганских, оскорбительных целях или для неправомерного вмешательства в частную жизнь;

«приостановить»: поскольку по своему определению приостановление прерывает в ином случае применимый период времени, оно касается только сертификатов, чья действительность определяется этим периодом времени. Если действительность определяется согласно иному критерию, такому как предмет идентифицируемой сделки, настоящий параграф не может применяться в полной мере;

«по запросу»: сертифицирующее лицо должно действовать добросовестно при ответе на запрос, но не обязано достоверно подтверждать идентичность или наличие ' агентских полномочий у лица, просящего о приостановлении сертификата. Сертифицирующее лицо может полагаться на представления лица, просящего о приостановлении сертификата, хотя при этом должен присутствовать элемент проверки идентичности лица, проводимой сертифицирующим лицом.

Комментарий

(1) Поскольку приостановление сертификата делает временно недействительным сертификат открытого ключа, он, по существу, временно разрывает взаимосвязь абонента с открытым ключом, указанным в сертификате. При отсутствии такой взаимосвязи цифровые подписи, проверяемые с использованием данного открытого ключа, не могут приписываться абоненту. Абонент, таким образом, действительно умаляет свою способность использовать цифровую подпись.

(2) Хотя от сертифицирующего лица и не требуется идентифицировать полномочия лица, делающего запрос, оно должно обладать какой-либо процедурой для незамедлительного подтверждения такого запроса. При неспособности сделать это сертифицирующее лицо может нарушить свои обязательств перед абонентом и нести ответственность за любые убытки, возникающие вследствие неспособности абонента использовать свою цифровую подпись.

(3) Способность временно препятствовать установлению принадлежности цифровой подписи через приостановление сертификата открытого ключа является одним из главных средств управления рисками владения закрытым ключом для абонента.

(3) Договор между сертифицирующим лицом и абонентом может ограничивать или препятствовать приостановлению сертификата пока лицо, способное полагаться на сертификацию, не получит извещение об ограничении или препятствии в приостановлении сертификата. Такие ограничения или препятствия могут быть включены в заявление о практике сертификации.

9. Отзыв сертификата открытого ключа по запросу

Сертифицирующее лицо, которое выдало сертификат открытого ключа, должно незамедлительно его отозвать после:

(a) получения запроса на отзыв абонента, поименованного в сертификате, или его уполномоченного агента, и

(b) подтверждения того, что лицо, просящее об отзыве, является этим абонентом или его агентом с полномочиями просить об отзыве сертификата.

Пояснение:

«сертифицирующее лицо, которое выдало»: сертифицирующее лицо, которое выдало сертификат, должно быть лицом, которое его приостанавливает, поскольку выдающее сертификат сертифицирующее лицо способно подтвердить идентичность и наличие агентских полномочий лица, просящего отозвать сертификат;

«отзывать»: поскольку по своему определению отзыв прерывает в ином случае применимый период времени, он касается только сертификатов, чья действительность определяется этим периодом времени. Если действительность определяется согласно иному критерию, такому как предмет идентифицируемой сделки, настоящий параграф не может применяться в полной мере.

Комментарий

(1) Аналогичный комментарий, что приводится в «Приостановлении сертификата открытого ключа по запросу», применим к отзыву, хотя очевидно, что отзыв носит постоянный характер и может рассматриваться в качестве окончательного шага.

10. Приостановление или отзыв сертификата открытого ключа без согласия

Сертифицирующее лицо, которое выдало сертификат открытого ключа, должно отозвать его, если:

(a) сертифицирующее лицо подтвердит, что существенные факты, представленные в сертификате, являются ложными;

(b) сертифицирующее лицо подтвердит, что степень доверия к информационной системе сертифицирующего лица компрометирована способом, существенно затрагивающим надежность сертификата.

Сертифицирующее лицо может приостановить разумно оспариваемый сертификат в течение времени, необходимого для проведения расследования, достаточного для подтверждения оснований отзыва в соответствии с настоящей статьей.

Пояснение:

«должен отозвать»: если сертифицирующее лицо не отзовет сертификат или, как минимум, не приостановит его на время проведения расследования и может быть доказано, что оно получило извещение по любому из вышеуказанных оснований до их наступления, сертифицирующее лицо может быть признано ответственным за любые вытекающие из этого убытки. Такая неспособность к действию даже может поставить под вопрос надежность сертифицирующего лица по отношению к третьим лицам;

«компрометирована»: тот факт, что информация, которая должна быть секретной в целях обеспечения безопасного использования удостоверенного сообщения, разглашена сторонам, которые не имеют права доступа к такой информации.

Комментарий

(1) Ожидается, что точные характеристики, посредством которых сертифицирующее лицо могло быть уполномочено приостанавливать или отзывать сертификат без .согласия, будут устанавливаться в договоре между сертифицирующим лицом и абонентом. При отсутствии таких договорных условий, судебное разбирательство, начатое в результате возникших убытков, должно установить, было ли уполномочено сертифицирующее лицо действовать таким образом.

11. Извещение о приостановлении или отзыве сертификата открытого ключа

Незамедлительно после приостановления или отзыва сертификата открытого ключа сертифицирующим лицом последнее должно направить соответствующее извещение об отзыве или приостановлении.

Пояснение:

«направить соответствующее извещение»: при установлении того, что является соответствующим, сертифицирующее лицо должно оценивать обстоятельства и прилагать разумные усилия по доставке извещения лицам, вероятно, затрагиваемым приостановлением или отзывом. По общему правилу в отношении сертификата, размещенного в хранилище цифровых сертификатов, сертифицирующее лицо должно аналогичным образом разместить извещение о приостановлении в этом же самом хранилище способом, установленным стандартом, принятым хранилищем, или в заявлении о процедурах, с использованием которых был размещен сертификат. Для сертификата, который не размещен в хранилище, извещение должно попадать к лицам, чье доверие к сертификату предвидимо с позиции сертифицирующего лица, а также лиц, просящих о приостановлении или отзыве.

Комментарий

Если сертифицирующее лицо оказывается не способным направить извещение, это может привести его, как минимум, к нарушению договора с абонентом или, в худшем случае, к ответственности за убытки, возникающие из последующего добросовестного использования абонентом любого утратившего силу ключа.

Додаток 12. Общие принципы рекламы и маркетинга в Интернете 1998 г.

Принципы ответственной рекламы и маркетинга через Интернет, World Wide Web, онлайновые услуги и электронные сети

Введение

Глобальные надежды на новые коммуникационные технологии становятся объектом широкого общественного интереса, поскольку бизнес и правительства обсуждают наилучшие пути внедрения этих технологий и разделения с потребителями преимуществ, которые они предлагают. Сочетая дружелюбие для пользователей экрана компьютера/телевизора с мгновенной передачей сообщений, эти технологии предоставляют новые средства доставки информации, развлечений и деловых услуг, соединяя потребителей и бизнес. Потребители приобретают больше прав, чем когда-либо ранее, вести диалог с производителями и точно выражать свои специфические потребности и желания.

Рекламодатели и маркетинговые службы помогают развивать новые средства информации, так же как они помогали развитию традиционных средств информации в прошлом. Сегодня реклама представляет главный источник доходов для традиционных средств информации. Аналогично реклама и маркетинг будут вносить свой жизненный вклад в новые интерактивные средства информации, позволяя им предлагать более доступные товары и услуги более широкой по охвату аудитории. Международная торговая палата (МТП) - крупнейший в мире разработчик кодексов саморегулирования этической маркетинговой и рекламной практики. МТП „ полагает, что реклама и маркетинг в Интернете, ***World Wide Web*** и при онлайновых услугах должны отражать самые высокие стандарты этического поведения, изложенные в Международном кодексе рекламной практики МТП и других соответствующих , кодексах саморегулирования МТП.

Глобальный характер и технологические свойства новых средств информации создают уникальное бизнес-окружение. Владельцев средств информации в традиционном смысле не существует, что ведет к обходу традиционных посредников, таких как издатели и вещательные организации. Ответственные рекламодатели и маркетинговые службы (под которыми в этом новом контексте подразумевается любое лицо или компания, размещающие электронное коммерческое сообщение) должны признать, что в их собственных интересах соблюдать самодисциплинирующие принципы, специально адаптированные к электронным или интерактивным рекламе и маркетингу. Рекламодатели и маркетинговые службы должны стремиться создавать электронное окружение, которому могут полностью доверять потребители по всему миру.

Потребители и маркетинговые службы должны стремиться сотрудничать, чтобы минимизировать потенциальные расходы и увеличивать эффективность выгод, получаемых от использования электронных сетей. Выбирая распределение существенных данных между собой, потребители могут обеспечиваться соответствующей информацией о продуктах, эффективными и экономичными услугами. Это позволит потребителям выбирать товары и услуги, лучше адаптированные к их потребностям и вкусам.

МТП признает, что реклама и маркетинг в интерактивных средствах информации находятся на ранней стадии развития, и подтверждает, что соответствующие принципы и руководства могут претерпеть изменения и эволюцию по мере того, как мы больше узнаем о новых технологиях и их специфических направлениях использования. Таким образом, в свете приобретенного опыта МТП представляет обновленную версию Общих принципов 1996 г. МТП обязуется регулярно пересматривать эти Общие принципы, чтобы гарантировать их длительную жизнеспособность.

Учитывая вышеуказанное, МТП рекомендует публикацию на международном уровне приведенного ниже руководства, которое предназначено для решения следующих задач:

- повысить доверие общественности к рекламе и маркетингу, обеспечиваемым через новые интерактивные системы;
- сохранить оптимум свободы выражения для рекламодателей и маркетинговых служб;

- минимизировать потребность в правительственном и/или межправительственном законодательстве или правилах
- отвечать разумным ожиданиям потребителей в отношении тайны частной жизни.

Сфера Общих принципов

Настоящие Общие принципы применяются ко всей маркетинговой и рекламной деятельности через Интернет по продвижению на рынок любой формы товаров или услуг. Общие принципы содержат стандарты этического поведения, соблюдаемые всеми участвующими в маркетинговой и рекламной деятельности через Интернет. **Определения** Для целей настоящего Руководства:

- термин «Интернет» относится к публичной компьютерной сети, обеспечивающей передачу информации между пользователями или между пользователями и местом в сети, а также ко всем интерактивным средствам информации и электронным сетям, таким как ***World Wide Web*** и онлайновые услуги;
- термин «содержание (контент)» означает все формы рекламной и маркетингевой информации и охватывает текст, рисунки, анимацию, видео и аудио, а также может включать в себя программное обеспечение;
- термин «***World Wide Web*** » относится к сети ресурсов, доступных через Интернет с использованием протокола передачи гипертекста («http»).

Общие принципы

Вся реклама и весь маркетинг в Интернете должны соответствовать духу и букве принципов, изложенных в Кодексах МТП по рекламной практике, содействию продажам, прямому маркетингу, экологической рекламе и спонсорству, а также в Кодексе рпактики маркетинга и социальных исследований МТП-ESOMAR.

Вся реклама и весь маркетинг должны быть законными, пристойными, честными цдостоверными. «Законный» в контексте настоящих Общих принципов предполагается означающим, что рекламные и маркетинговые сообщения должны быть законными в стране их происхождения.

Рекламные и маркетинговые сообщения должны быть чувствительными к вопросам социальной ответственности и, дополнительно, соответствовать общепризнанным принципам в отношении этического маркетинга.

Рекламные и маркетинговые сообщения не должны предназначаться или передаваться таким образом, чтобы наносить ущерб всеобщему общественному доверию к Интернету как к информационной среде и месту ведения бизнеса.

ПРАВИЛА

Раскрытие сведений о личности

Статья 2

Рекламодатели и маркетинговые службы, которые размещают коммерческие сообщения через Интернет, всегда должны раскрывать информацию о собственной личности и своем соответствующем подразделении, если это применимо, таким образом, чтобы пользователь мог без затруднений связываться с рекламодателем и маркетинговой службой.

Расходы и обязательства, связанные с электронными продажами и маркетингом

Статья 3

Рекламодатели и маркетинговые службы должны ясно информировать пользователей о расходах по доступу к сообщению или услуге, когда расходы выше, чем базовый телекоммуникационный тариф. Такое уведомление должно предоставляться пользователям о расходах во время их доступа к сообщению или услуге. Данный механизм уведомления должен обеспечивать пользователям разумное время, как оно установлено маркетинговой службой или предписано применимым правом, для отключения от услуги без несения расходов.

Уважение общественных групп

Статья 4

Рекламодатели и маркетинговые службы должны уважать роль отдельных электронных

новостных групп, форумов или информационных досок объявлений как мест публичных встреч, которые могут иметь правила и стандарты приемлемого коммерческого поведения. Рекламные и маркетинговые сообщения, размещаемые на публичных сайтах, являются надлежащими:

- когда форум или сайт, получающий сообщение, имеет существенно коммерческие характер или деятельность;
- когда предмет или тема Информационной доски или группы новостей являются близкими к содержанию рекламного или маркетингового сообщения;
- когда форум или сайт иным образом косвенно или прямо указал на согласие с получением рекламных или маркетинговых сообщений.

Права пользователей
Статья 5

1. Сбор и использование данных.

Рекламодатели и маркетинговые службы должны раскрывать цель(и) сбора и использования персональных данных пользователям и не должны их использовать образом, несовместимым с данными целями. Файлы данных должны быть точными, полными и вестись в актуальном состоянии. 2. Тайна данных.

Рекламодатели и маркетинговые службы должны принимать разумные меры предосторожности по защите своих файлов данных. 3. Раскрытие данных.

Пользователю должна предоставляться возможность отказаться от передачи данных другому рекламодателю или маркетинговой службе. Персональные данные не должны раскрываться, когда пользователь возражает против этого, за исключением раскрытия в силу закона. В сети должны размещаться онлайновые механизмы, чтобы позволять пользователям реализовывать свое право «активного отказа» с использованием электронных средств. 4. Исправление и блокирование данных.

Рекламодатели и маркетинговые службы должны предоставлять пользователю право получать касающиеся его данные и, когда это приемлемо, возможность исправлять, завершать или блокировать такие данные. 5. Заявления о политике защиты тайны частной жизни.

Рекламодателям и рекламным службам рекомендуется размещать свои заявления о политике защиты тайны частной жизни на своем онлайновом сайте. Когда существуют такие заявления о политике защиты тайны частной жизни, они должны быть легко обнаруживаемы, удобны в использовании и понятны. 6. Инициативные коммерческие сообщения.

Рекламодатели и маркетинговые службы не должны отправлять в режиме он-лайн инициативные коммерческие сообщения пользователям, которые указали, что они не желают получать такие сообщения. Рекламодатели и маркетинговые службы должны делать доступным для пользователей онлайновый механизм, с использованием которого пользователи могут ставить в известность рекламодателей и маркетинговые службы, что они не желают получать будущие онлайновые запросы. Инициативные онлайновые рекламные или маркетинговые коммерческие сообщения должны быть ясно идентифицированы как таковые и должны способствовать идентификации рекламодателя или маркетинговой службы.

Реклама для детей
Статья 6

Рекламодатели и маркетинговые службы, предлагающие в режиме онлайн товары или услуги для детей, должны:

не использовать естественную детскую доверчивость или отсутствие опыта у
молодых людей и не испытывать их чувство лояльности;
не включать любое содержание, которое могло бы причинить вред детям;
идентифицировать материалы, предназначенные только для взрослых;
поощрять родителей и/или опекунов участвовать в онлайновой деятельности
своих детей и/или ее контролировать;
поощрять маленьких детей получать разрешение своего родителя и/или опекуна до предоставления детям информации в режиме онлайн и предпринимать разумные усилия для обеспечения предоставления родительского согласия; предоставлять информацию родителям и/или опекунам в отношении способов защиты тайны частной жизни детей в онлайне.

Уважение потенциальной чувствительности глобальной аудитории
Статья 7

Учитывая глобальную досягаемость электронных сетей, множественность и разнообразие возможных получателей электронных сообщений, рекламодатели и маркетинговые службы должны быть особенно чувствительны к вероятности того, что отдельное сообщение может восприниматься как порнографическое, насильственное, расистское или дискриминирующее по половому признаку.

Додаток 13. Унифицированные правила поведения при обмене торговыми данными путем телетрансмиссии (UN-C1D) 1987 г.

Статья 1.
Цель принятия

Настоящие правила призваны содействовать обмену торговыми данными, осуществляемому путем телетрансмиссии, путем установления согласованных правил поведения сторон, осуществляющих такой обмен. За исключением случаев, предусмотренных настоящими правилами, они не применяются к существу передач данных..

Статья 2.
Определения

Для целей настоящих правил следующие используемые в них выражения будут иметь приведенное ниже значение:

а) торговая сделка: договор купли-продажи или поставки товаров и/или услуг и/или на иное исполнение между сторонами, определяемый как сделка, к которой относится сообщение торговых данных;

Ь) сообщение Торговых данных: торговая информация, обмен которой производится между сторонами с целью заключения или исполнения торговой сделки;

с) передача торговой информации (в дальнейшем именуется «передача»): одно или несколько сообщений торговых данных, отправленные вместе в качестве одной единицы пересылки, которые включают в себя заголовок и заключительные данные;

и) прикладной протокол обмена торговыми данными' (ППО): принятый метод для обмена сообщениями торговых данных, основанный на международных стандартах представления и структурирования торговых данных при передаче, осуществляемой путем телетрансмиссии;

е) журнал регистрации торговых данных: совокупность передач торговых данных, которая представляет полную хронологическую запись обмена торговыми данными.

Статья 3.
Применение

Настоящие правила применяются в отношении обмена торговыми данными между сторонами, использующими ППО. Правила могут также применяться, когда это приемлемо, при использовании иных методов обмена торговыми данными путем телетрансмиссии.

Статья 4.
Стандарты обмена

Элементы торговых данных, структура сообщений и аналогичные правила и коммуникационные стандарты, используемые для обмена, должны соответствовать изложенным в используемом ППО.

Статья 5.
Заботливость

а) Стороны, использующие ППО, обязаны гарантировать, что их передачи будут правильными, целостными по форме и безопасными в соответствии с ППО, а также проявлять заботливость для обеспечения своих возможностей получать такие передачи.

b) Посредники в передаче должны получать указания обеспечивать недопущение несанкционированных изменений в передачи, подлежащие переадресации, а также раскрытия содержания данных такой передачи любому неуполномоченному лицу.

Статья 6.
Сообщения и передачи

a) Сообщение торговых данных может иметь отношение к одной или нескольким торговым сделкам и должно содержать соответствующий идентификатор такой сделки и средства проверки того, что сообщение является полным и правильным в соответствии с задействованным ППО.

b) При передаче должны быть идентифицированы отправитель и получатель: это включает средства проверки через методы, используемые при самой передаче, либо иные, предусмотренные задействованным ППО, формальной целостности и аутентичности передачи,

Статья 7.
Подтверждение передачи

a) Отправитель передачи может предусмотреть, что получатель должен подтвердить ее получение. Подтверждение может быть сделано с использованием телетрансмиссионных либо иных средств, предусмотренных задействованным ППО. Получатель не вправе действовать на основании передачи, пока не выполнит требование отправителя о подтверждении.

b) Если отправитель не получил предусмотренного подтверждения в течение установленного или разумного времени, он должен предпринять действия по его получению. Если, несмотря на такие действия, подтверждение не получено в течение последующего разумного времени, то отправитель обязан известить об этом получателя, соответственно с использованием тех же средств, что и при первой передаче, либо с использованием иных необходимых средств, и если "отправитель совершает указанные действия, то он вправе считать первоначальную передачу неполученной.

c) Если полученная передача не представляется надлежащей, правильной или полной по форме, получатель обязан проинформировать об этом отправителя в максимально короткий срок.

u) Если получатель устанавливает, что передача предназначалась не ему, он обязан предпринять разумные действия по незамедлительному извещению отправителя и обязан уничтожить в своей системе всю информацию, содержащуюся в такой передаче, за исключением журнала регистрации торговых данных.

Статья 8.
Подтверждение содержания

a) Отправитель передачи может просить получателя сообщить ему, является ли содержание одного или нескольких идентифицированных сообщений в передаче правильным по существу, без ущерба для любого последующего вывода или действия получателя, вызванного содержанием сообщения. Получатель не вправе действовать на основании передачи до выполнения запроса отправителя

b) Если отправитель в течение разумного времени не получил запрашиваемого извещения, он обязан предпринять действия для его получения. Если, несмотря на такие действия, извещение не было получено в течение последующего разумного времени, отправитель обязан соответствующим образом уведомить получателя и, если отправитель совершает указанные действия, он вправе считать данное сообщение не принятым получателем как правильное по существу.

Статья 9.
Защита торговых данных

a) Стороны могут договориться, где это возможно, о применении специальной защиты путем шифрования или с использованием иных средств в отношении к некоторым или всем данным, обмен которыми осуществляется между ними.

b) Получатель передачи, защищенной таким образом, должен обеспечить, как минимум, аналогичный уровень защиты при любой последующей передаче.

Статья 10.
Хранение данных

a) Каждая сторона должна обеспечить ведение полного-журнала регистрации торговых Данных, содержащего все передачи в той форме, как они были отправлены и получены, без любых изменений.

b) Такой журнал регистрации торговых данных может вестись с использованием компьютерных средств, при условии, что когда это требуется, данные могли бы извлекаться и представляться в доступной для чтения форме.

c) Указанный в пункте (a) настоящей статьи журнал регистрации торговых данных должен храниться неизменным в течение срока, требуемого национальным правом стороны, ведущей такой журнал, либо в течение более длительного срока, который может быть согласован между сторонами, либо, при отсутствии требований национального права или соглашения сторон, в течение трех лет.

(1) Каждая сторона несет ответственность за заключение соглашений, которые могут быть необходимы, чтобы указанные в пункте (Ь) настоящей статьи данные подготавливались в виде точной записи передач, как они были отправлены и получены Данной стороной в соответствии с пунктом (a) настоящей статьи.

e) Каждая сторона обязана контролировать, чтобы лицо, ответственное за систему обработки данных соответствующей стороны, или такая третья сторона, которая может быть согласована сторонами или требоваться законом, удостоверяли, при необходимости, правильность журнала регистрации торговых данных и любого полученного из него воспроизведения.

Статья 11.
Толкование

Вопросы, касающиеся правильного значения правил, должны направляться Международной торговой палате, Париж.

Додаток 14. Международный морской комітет

Правила для электронных коносаментов от 29 июня 1990 г.

1. Сфера применения

Настоящие Правила применяются всякий раз, Когда стороны об этом договорились.

2. Определения

a. «Договор перевозки» означает любое соглашение о перевозке товаров полностью или частично морем.

b. «ЭОД (E01)» означает электронный обмен данными, т.е. обмен коммерческими данными, осуществляемый посредством их передачи по телекоммуникациям.

c. «UN/EDIFACT» означает Правила Организации Объединенных Наций по электронному обмену данными в сфере управления, торговли и транспорта.

d. «Передача» означает одно или более сообщений, передаваемых электронным способом вместе в одном отправлении, которое включает в себя заголовок и завершающие данные.

e. «Подтверждение» означает передачу, извещающую, что ее содержание представляется полным и правильным, без ущерба для любого последующего рассмотрения или иска, которые может подтверждать содержание.

f. «Закрытый ключ» означает любую технически приемлемую форму, такую как сочетание номеров и/или букв, которую стороны могут согласовать для обеспечения подлинности и целостности передачи.

g. «Держатель» означает сторону, которая обладает правами, описанными в статье 7(a), в силу владения действительным закрытым ключом.

h. «Система электронного мониторинга» означает устройство, посредством которого может быть исследована компьютерная система с точки зрения фиксируемых ею сделок, например система регистрации коммерческих данных или ведения контрольных записей.

i. «Электронное хранение» означает любое временное, промежуточное или постоянное хранение электронных данных, включая основное и резервное хранение таких данных.

3. Процедурные правила

a. При отсутствии коллизии с настоящими Правилами поведение сторон будет регулироваться Унифицированными правилами поведения при обмене торговыми данными путем телетрансмиссии 1987 г. (UN-CID).

b. Осуществляемый в соответствии с настоящими Правилами ЭОД должен соответствовать стандартам «UN/EDIFACT». Вместе с тем стороны могут использовать любой иной способ обмена коммерческими данными, приемлемый для всех пользователей.

c. Если иное не согласовано, формат документа для договора перевозки должен соответствовать схеме кодирования ООН или совместимому национальному стандарту для коносаментов.

d. Если иное не согласовано, получатель передачи не вправе действовать на ее основании, если только он не направил подтверждение.

e. В случае спора, возникающего между сторонами в отношении того, передавались ли действительно данные, может использоваться система электронного мониторинга для проверки полученных данных. Данные, касающиеся других сделок, не относящихся к оспариваемым данным, считаются коммерческими секретами и являются недоступными для изучения. Если такие данные неизбежно обнаруживаются при изучении системой электронного мониторинга, они должны рассматриваться как конфиденциальные и не передаваться любой третьей стороне или не использоваться для любой иной цели.

f. Любая передача прав на товары должна рассматриваться как информация приватного характера и не передаваться любой третьей стороне, не связанной с перевозкой или таможенной очисткой товаров.

4. Форма и содержание сообщения о получении товаров

a. Перевозчик по получении товара от грузоотправителя обязан направить ему извещение о получении товаров в виде сообщения по электронному адресу, указанному грузоотправителем.

b. Данное сообщение о получении должно включать:

(i) наименование грузоотправителя;

(ii) описание товаров со всеми заявлениями и оговорками, с тем же содержанием, как это требовалось бы при выдаче бумажного коносамента;

(iii) дату и место получения товаров;

(IV) ОТСылку к определяемым перевозчиком условиям перевозки;

(V) ЗАкрытый ключ, используемый при последующих передачах. Грузоотправитель должен подтвердить это сообщение о получении перевозчику, после чего грузоотправитель становится держателем.

c. По требованию держателя в сообщении о получении проставляются дата и место отгрузки, как только товары погружены на борт.

d Информация, содержащаяся в пунктах (ii), (iii) и (IV) вышеуказанного параграфа (b), включая дату и место отгрузки, если они проставляются в соответствии с параграфом (c) настоящих Правил, имеет аналогичную силу и действие, как если бы сообщение о получении содержалось в бумажном коносаменте.

5. Условия договора перевозки

a. Согласовано и понимается, что всякий раз) когда перевозчик делает ссылку на условия перевозки, они составляют часть договора перевозки.

b Такие условия должны быть легко доступны сторонам договора перевозки.

c. В случае любой коллизии или несоответствия между такими условиями И на-1 Стоящими Правилами последние имеют преимущественную силу.

6. Применимое право

Договор перевозки подчинен любой международной конвенции или национальному праву, которые бы обязательно применялись в случае выдачи бумажного коносамента.

7. Право контроля и передачи

a. Держатель является единственной стороной, которая вправе в отношении перевозчика:

(1) требовать доставки товаров;

(2) назначать грузополучателя или заменить назначенного грузополучателя любой другой стороной, включая себя;

(3) передавать право контроля и передачи другой стороне;

(4) инструктировать перевозчика по любым другим вопросам, касающимся товаров, в соответствии с условиями договора перевозки, как если бы он был держателем бумажного коносамента.

b Передача права контроля и передачи осуществляется: (i) путем уведомления перевозчика настоящим держателем о своем намерении передавать право контроля и передачи предполагаемому новому держателю; и (ii) подтверждения перевозчиком такого уведомительного сообщения, после чего (iii) перевозчик передает информацию, указанную в статье 4 (за исключением закрытого ключа), предполагаемому новому держателю, и тогда (IV) предполагаемый новый держатель уведомляет перевозчика о принятии им права контроля и передачи, после чего (V) перевозчик аннулирует закрытый ключ и выдает новый закрытый ключ новому держателю.

c. Если предполагаемый новый держатель извещает перевозчика, что он не принимает права контроля и передачи, или оказывается не в состоянии известить перевозчика о таком принятии в течение разумного времени, предполагаемая передача права контроля и передачи не должна иметь место. Соответственно перевозчик должен уведомить об этом настоящего держателя, а закрытый ключ сохраняет свою действительность.

и. Передача права контроля и передачи вышеуказанным способом имеет те же последствия, что и передача такого права по бумажному коносаменту/

8. Закрытый ключ

a. Закрытый ключ является уникальным для каждого последующего держателя. Перевозчик и держатель обязаны обеспечивать безопасность закрытого ключа.

Ь. Перевозчик обязан только направить подтверждение электронного сообщения последнему держателю, которому он выдал закрытый ключ, в то время как такой держатель обеспечивает безопасность передачи, содержащей данное электронное сообщение, использованием закрытого ключа.

c. Закрытый ключ должен быть индивидуальным и отличным от любых средств, используемых для идентификации договора перевозки, а также любого пароля безопасности или идентификации, используемого для доступа к компьютерной сети.

9. Доставка

a. Перевозчик должен уведомить держателя о месте и дате предполагаемой доставки товаров. По получении такого уведомления держатель обязан назначить грузополучателя и направить перевозчику необходимые инструкции по доставке с проверкой закрытым ключом. При отсутствии такого назначения держатель будет считаться грузополучателем.

Ь. Перевозчик обязан доставить товары грузополучателю после проведения надлежащей идентификации в соответствии с инструкциями по доставке, вышеуказанными в параграфе (а); такая доставка автоматически аннулирует закрытый ключ.

c. Перевозчик не несет ответственности за неправильную доставку товара, если он докажет, что им была проявлена разумная заботливость по удостоверению того. что именующая себя в качестве грузополучателя сторона в действительности является таковой.

10. Право на получение бумажного документа

a. В любое время до доставки товаров держатель вправе потребовать от перевозчика бумажный коносамент. Такой документ должен делаться доступным в месте, определяемом держателем, при условии, что никакой перевозчик не обязан делать такой документ доступным в месте, в котором у него отсутствуют средства обслуживания, и в этом случае перевозчик обязан сделать документ доступным в месте нахождения средств обслуживания, ближайшем к определенному держателем. Перевозчик не отвечает за задержку в доставке товаров вследствие осуществления держателем вышеуказанного права.

Ь. В любое время до доставки товаров перевозчик вправе выдать держателю бумажный коносамент, если только реализация такого права не повлечет за собой ненадлежащую задержку или срыв доставки товаров.

c. Коносамент, выдаваемый в соответствии с пунктами (а) или (Ь) Правила 10, должен включать: (1) информацию, изложенную в сообщении о получении, указанном в Правиле 4 (за исключении закрытого ключа); и (Я) заявление о том, что коносамент выдан по окончании процедур

ЭОД согласно Правилам ММК для электронных коносаментов. Вышеуказанный коносамент выдается по выбору держателя либо по приказу держателя, чье имя с этой целью должно быть проставлено в коносаменте, или «предъявителю».

d. Выдача бумажного коносамента согласно пунктам (a) или (b) Правила 10 аннулирует закрытый ключ и завершает процедуры ЭОД в соответствии с настоящими Правилами. Завершение указанных процедур держателем или перевозчиком не лишает стороны договора перевозки их прав и не освобождает от обязательств или ответственности ни в отношении исполнения согласно настоящим Правилам, ни в отношеии и исполнения по договору перевозки.

е. В любое время держатель вправе потребовать выдачи ему распечатки сообщения о получении, указанного в Правиле 4 (за исключением закрытого ключа), помечаемой как «необоротная копия». Выдача такой распечатки не аннулирует закрытый ключ : и не прекращает процедур ЭОД.

11. Электронные данные эквивалентны письменной форме

Перевозчик, грузоотправитель и все последующие стороны, осуществляющие указанные процедуры, соглашаются, что требования любого национального или местного законодательства, обычая или практики, чтобы договор перевозки свидетельствовался в письменной форме и подписывался, выполняются передаваемыми и подтверждаемыми электронными данными, находящимися на средствах хранения компьютерных данных, представляемыми на естественном языке на видео экране или распечатываемыми компьютером. Выражая согласие на применение данных Правил, стороны считаются согласившимися не выдвигать в качестве защиты довод о заключении Договора не в письменной форме.

Додаток 15. Организация экономического сотрудничества и развития (ОЭСР). Общие принципы защиты прав потребителей в контексте электронной коммерции 2000 г.

ЧАСТЬ ПЕРВАЯ
СФЕРА ПРИМЕНЕНИЯ

Настоящие принципы применяются только в рамках электронной коммерции типа «коммерческое предприятие-потребитель» и не применяются к сделкам типа «коммерческое предприятие - коммерческое предприятие».

ЧАСТЬ ВТОРАЯ
ОБЩИЕ ПРИНЦИПЫ

I. Транспарентная и эффективная защита

Потребителям, которые участвуют в электронной коммерции, должна предоставляться транспарентная и эффективная защита их прав, не меньшая, чем уровень защиты, предоставляемой при других формах коммерции.

Правительства, коммерческие предприятия, потребители и их представители должны работать вместе в целях достижения такой защиты и определять, какие изменения могут быть необходимы при обращении к конкретным обстоятельствам электронной коммерции.

II. Добросовестная практика бизнеса, рекламы и маркетинга

Коммерческим предприятиям, участвующим в электронной коммерции, необходимо уделять должное внимание интересам потребителей и действовать в соответствии с добросовестной практикой бизнеса, рекламы и маркетинга.

Коммерческие предприятия не должны допускать какое-либо заверение, упущение или участвовать в любой практике, которая может быть вводящей в заблуждение, дезориентирующей, мошеннической или недобросовестной.

Коммерческие предприятия, реализующие, продвигающие или предлагающие путем маркетинга товары или услуги потребителям, не должны участвовать в практике, которая может причинить необоснованный риск вреда потребителям.

Всякий раз, когда коммерческие предприятия делают доступной информацию о себе или

предоставляемых товарах или услугах, они должны предоставлять такую информацию ясным, очевидным, точным и легко доступным образом.

Коммерческие предприятия должны соблюдать любые заверения, которые они делают в отношении принципов или практики, касающихся их сделок -с потребителями.

Коммерческие предприятия должны принимать во внимание глобальный характер электронной коммерции и всегда, когда это возможно, рассматривать различные регулятивные характеристики рынков, на которые они нацелены.

Коммерческие предприятия не должны использовать особые характеристики электронной коммерции, чтобы скрывать свою истинную личность или место нахождение либо избегать соблюдения стандартов защиты прав потребителей и/или механизмов правоприменения.

Коммерческие предприятия не должны использовать несправедливые условия договора. Реклама и маркетинг должны быть ясно идентифицируемы как таковые.

Реклама и маркетинг должны способствовать идентификации коммерческого предприятия, от чьего имени они осуществляются, в случаях, когда неспособность вделать это может вводить в заблуждение.

Коммерческие предприятия должны быть в состоянии подтверждать любые явно выраженные или подразумеваемые заверения, пока они поддерживаются и в течение разумного времени после этого.

Коммерческие предприятия должны разрабатывать и внедрять эффективные и удобные в использовании процедуры, которые позволяют потребителям выбирать, желают ли они получать инициативные коммерческие сообщения по электронной почте.

В случае, когда потребители указывают, что они не хотят получать инициативные коммерческие сообщения по электронной почте, такой выбор должен уважаться.

В ряде стран передача инициативных коммерческих сообщений по электронной почте подчинена определенным правовым требованиям или требованиям саморегулирования.

Коммерческие предприятия должны проявлять особую осторожность при рек ламе или маркетинге, которые адресуются детям, пожилым, серьезно больным и , иным, кто не обладает способностью полностью понимать информацию, которая им предоставляется.

III. Онлайновое раскрытие информации

A. Информация о коммерческом предприятии

Коммерческие предприятия, участвующие в электронной коммерции с потребителями, должны предоставлять точную, ясную и легко доступную информацию о себе, достаточную, чтобы обеспечивать, как минимум:

i) идентификацию коммерческого предприятия, включая юридическое наименование коммерческого предприятия и наименование, под которым данное коммерческое предприятие осуществляет торговлю; основной географический адрес коммерческого предприятия; адрес электронной почты или другие электронные средства связи или номера телефона; и, когда это применимо, адрес в регистрационных целях и соответствующие номера любой правительственной регистрации или лицензии;

ii) незамедлительную, легкую и эффективную связь потребителя с коммерческим предприятием;

iii) соответствующее и эффективное разрешение споров;

IV) вручение процессуальных извещений;

V) место нахождения коммерческого предприятия в целях правоприменения и отношений с официальными должностными лицами.

В случае, когда коммерческое предприятие публикует сведения о своем членстве в любой соответствующей системе саморегулирования, предпринимательской ассоциации, организации по разрешению споров или ином органе сертификации, коммерческое предприятие должно обеспечивать потребителям соответствующие контактные данные и легкий способ проверки такого членства, а также доступ к соответствующим кодексам и практике органа сертификации. B. Информация о товарах и услугах

Коммерческие предприятия, участвующие в электронной коммерции с потребителями, должны предоставлять точную и легко доступную информацию, описывающую предлагаемые товары или услуги, достаточную для обеспечения потребителпи возможности принятия

квалифицированного решения о том, совершать ли сделку, и способом, который делает возможным для потребителей вести полную запись такой информации в достаточном объеме.

C. Информация о сделке

Коммерческие предприятия, участвующие в электронной коммерции, должны предоставлять достаточную информацию об условиях сделки и связанных смей издержках для обеспечения потребителям возможности принятия квалифицированного решения о том, совершать ли сделку.

Такая информация должна быть ясной, точной, легко доступной и предоставляться способом, дающим потребителям достаточную возможность для изучения до совершения сделки.

При возможности использования нескольких языков для совершения сделки коммерческие предприятия должны делать доступной на этих же самых языках всю информацию, необходимую потребителям для принятия квалифицированного решения относительно сделки.

Коммерческие предприятия должны предоставлять потребителям ясный и полный текст соответствующих условий сделки способом, который делает возможным для потребителей доступ и ведение необходимой записи такой информации в достаточном объеме.

Когда это применимо и является приемлемым в отношении данной сделки, такая информация должна включать в себя следующее:

i) детализацию совокупных издержек, взимаемых с коммерческого предприятия и/или возлагаемых на него;

ii) уведомление о наличии других обычно применяемых издержек в отношении потребителя, которые не взимаются с коммерческого предприятия и/или возлагаются на него;

iii) условия доставки или исполнения;

IV) УСловия и способы платежа;

V) внутренние и внешние ограничения или условия покупки, такие как требования родительского/опекунского одобрения, географические или временные ограничения;

VI) инструкции по надлежащему использованию, включая безопасность и предупреждение для здоровья;

УП) информацию, касающуюся доступных послепродажных услуг; УШ) детали и условия, касающиеся информации о принципах отмены, прекращения, возврата, обмена, расторжения и/или возмещения; 1x) доступные договорные и иные гарантии. Вся информация об издержках должна указывать на применимую валюту.

IV. Процесс подтверждения

В целях избежания двусмысленности в отношении намерения потребителя совершить покупку, потребитель должен быть в состоянии до завершения покупки точно идентифицировать товары или услуги, которые он или она желает приобрести; идентифицировать и исправить любые ошибки или изменить заказ; выразить квалифицированное и взвешенное согласие на покупку и сохранять полную и точную запись сделки.

Потребитель должен быть в состоянии расторгнуть сделку до завершения покупки.

V. Платеж

Потребители должны обеспечиваться удобными в использовании, безопасными способами платежа и информацией об уровне их безопасности, который такие способы предоставляет.

Механизмы ограничения ответственности вследствие несанкционированного или мошеннического использования платежных систем и опротестования платежей предлагают мощные средства повышения доверия потребителей, и их развитие и использование должны поощряться в контексте электронной коммерции.

VI. Разрешение споров и обжалование

A. Применимое право и юрисдикция

Трансграничные сделки типа «коммерческое предприятие — потребитель», независимо от того, осуществляются ли электронным или иным образом, подчиняются существующей правовой основе установления применимого права и юрисдикции.

Электронная коммерция ставит вопросы перед этой существующей правовой основой. Поэтому должно проводиться рассмотрение на предмет того, должна ли изменяться или применяться

отличным образом существующая правовая основа установления применимого права и юрисдикции, чтобы гарантировать эффективную и транспарентную защиту прав потребителей с учетом продолжающегося роста электронной коммерции.

При рассмотрении того, изменять ли существующую правовую основу, правительства должны стремиться гарантировать, чтобы данная правовая основа обеспечивала добросовестность для потребителей и коммерческих предприятий, облегчала электронную коммерцию, приводила к предоставлению потребителям уровня защиты прав, не меньшего, чем при других формах коммерции, а также предоставляла потребителям значимый [с точки зрения последствий] доступ к справедливому и своевременному разрешению споров и обжалованию без ненадлежащих издержек или обременений.

B. Альтернативное разрешение споров и обжалование

Потребителям должен предоставляться значимый [с точки зрения последствий] доступ к справедливому и своевременному альтернативному разрешению споров и обжалованию без ненадлежащих издержек или бремени.

Коммерческие предприятия, представители потребителей и правительства должны совместно работать в целях продолжения использования и разработки справедливых, эффективных и транспарентных саморегулирующихся и иных основных принципов и процедур, включая альтернативные механизмы разрешения споров, для рассмотрения жалоб потребителей и разрешения споров с участием потребителей, возникающих при осуществлении электронной коммерции типа «коммерческое предприятие - потребитель», с особым вниманием к трансграничным сделкам:

i) коммерческие предприятия и представители потребителей должны продолжать устанавливать справедливые, эффективные и транспарентные внутренние механизмы рассмотрения жалоб и трудностей потребителей и реагирования на них добросовестным и своевременным образом без ненадлежащих издержек или обременений для потребителя. Потребители должны поощряться к использованию преимуществ таких механизмов;

ii) коммерческие предприятия и представители потребителей должны продолжать создавать совместные саморегулирующиеся программы рассмотрения жалоб потребителей и содействия потребителям в разрешении споров, возникающих при осуществлении электронной коммерции типа «коммерческое предприятие - потребитель»;

iii) коммерческие предприятия, представители потребителей и правительства должны совместно работать, чтобы продолжать предоставлять потребителям варианты выбора механизмов альтернативного разрешения споров, которые обеспечивают эффективное разрешение споров добросовестным и своевременным образом без ненадлежащих издержек или обременений для потребителя;

IV) при реализации вышеуказанного, коммерческие предприятия, представители потребителей и правительства должны инновационным образом применять информационные технологии и использовать их для повышения осведомленности потребителей и свободы выбора. Дополнительно требуется дальнейшее изучение для достижения целей Раздела VI на международном уровне.

VII. Тайна частной жизни

Электронная коммерция типа «коммерческое предприятие - потребитель» должна осуществляться в соответствии с признанными принципами охраны тайны частной жизни, изложенными в Принципах ОЭСР, регулирующих защиту тайны частной жизни и трансграничные потоки персональных данных (1980), и принимая во внимание Правительственную декларацию ОЭСР по защите тайны частной жизни в глобальных сетях (1998) для обеспечения надлежащей и эффективной защиты прав потребителей.

VIII. Образование и информированность

Правительства, коммерческие предприятия и представители потребителей должны совместно работать, чтобы обучать потребителей вопросам электронной коммерции, содействовать принятию потребителями, участвующими в электронной коммерции, квалифицированных решений и увеличивать информированность коммерческих предприятий и потребителей о правовой основе защиты прав потребителей, которая применяется к их

онлайновой деятельности.

Правительства, коммерческие предприятия, средства информации, образовательные учреждения и представители потребителей должны обеспечить использование всех эффективных средств, доступных посредством глобальных сетей, для обучения потребителей и коммерческих предприятий, включая инновационные методики.

Правительства, представители потребителей и коммерческие предприятия должны совместно работать в целях предоставления информации потребителям и коммерческим предприятиям по всему миру о соответствующем законодательстве по защите прав потребителей и средствах правовой защиты в легко доступной и понятной форме.

ЧАСТЬ ТРЕТЬЯ
ИМПЛЕМЕНТАЦИЯ

Для достижения целей настоящей Рекомендации государства - участники должны на национальном и международном уровне и в сотрудничестве с коммерческими предприятиями, потребителями и их представителями:

1) изучать и, если необходимо, внедрять практику саморегулирования и/или принимать и адаптировать законодательство и практику, чтобы сделать их применимыми к электронной коммерции, имея в виду принципы технологической нейтральности и нейтральности к носителям информации;

ii) поощрять продолжающееся лидерство частного сектора, включающее в себя участие представителей потребителей в развитии эффективных механизмов саморегулирования, которые содержат специальные материальные правила разрешения споров и механизмы их выполнения;

iii) поощрять продолжающееся лидерство частного сектора в развитии технологий как инструмента защиты потребителей и наделения их полномочиями;

IV) как можно более широко продвигать Принципы, их цели, содержание и поощрять их использование;

V) ОБлегчать потребителям возможность доступа к образовательной информации и консультациям, а также предъявления жалоб, связанных с электронной коммерцией,

ЧАСТЬ ЧЕТВЕРТАЯ
ГЛОБАЛЬНОЕ СОТРУДНИЧЕСТВО

В целях обеспечения эффективной защиты прав потребителей в контексте глобальной электронной коммерции, государства -участники должны:

i) содействовать контактам, сотрудничеству и, где это приемлемо, разработке и претворению совместных инициатив на международном уровне среди коммерческих предприятий, представителей потребителей и правительств;

ii) через свои судебные, регулирующие и правоохранительные органы сотрудничать на международном уровне, когда это приемлемо, посредством обмена информацией, осуществлять координацию, контакты и совместные действия в целях борьбы с трансграничным мошенническим, вводящим в заблуждение и недобросовестным коммерческим поведением;

iii) использовать существующие международные сети и заключать двусторонни' и/или многосторонние соглашения или, по необходимости, достигать других договоренностей и, когда это приемлемо, совершенствовать такое сотрудничество;

IV) работать над созданием консенсуса на национальном и международном уровне по коренным вопросам защиты прав потребителей к дальнейшим целям по усилении) доверия потребителей, гарантиям предсказуемости для коммерческих предприятий и защиты прав потребителей;

V) СОТрудничать в деле развития соглашений или других договоренностей по вопросам взаимного признания и приведения в исполнение судебных решений по спора между потребителями и коммерческими предприятиями, а также судебных решений правоприменительным искам, предъявленным в целях борьбы с мошенническим, вводящим в заблуждение или недобросовестным коммерческим поведением.

Додаток 16. Европейская экономическая комиссия ООН

Типовое соглашение обмена при международном коммерческом использовании электронного обмена данными (Приложение к Рекомендации № 26 «Коммерческое использование соглашений обмена при электронном обмене данными», принятой Рабочей группой по содействию международным торговым процедурам Европейской экономической комиссии ООН от 23 июня 1995 г.)

Настоящее Соглашение обмена (Соглашение) заключено между {указать имена и адреса сторон} (далее именуемые Стороны) «_>> _____ 19__г.

Настоящим Соглашением Стороны, имея намерение быть связанными обязательствами по настоящему Соглашению, договорились о нижеследующем:

Статья 1.
Сфера действия и структура

1.1. Сфера действия

Настоящее Соглашение регулирует любую электронную передачу сообщений между Сторонами. Если иное прямо не предусмотрено, Соглашение не регулирует любые другие отношения, договорные или нет, в рамках которых производится обмен сообщениями. Сообщение означает данные, имеющие структуру в соответствии со стандартами UN/EDIFACT, как это предусмотрено в статье 2.

1.2. Техническое приложение

В прилагаемом Техническом приложении изложено описание согласованных Сторонами некоторых технических и процедурных требований. В случае несоответствия между условиями Соглашения и Техническим приложением условия настоящего Соглашения будут иметь высшую юридическую силу.

Статья 2.
Связь и операции

Стороны осуществляют обмен сообщениями в соответствии со следующими правилами:

2.1. Стандарты

Стандартами UN/EDIFACT являются стандарты, установленные для электронного обмена данными (включая соответствующие рекомендации), одобренные и опубликованные в Руководстве ООН по обмену торговыми данными (UN\TDID). Стороны обязаны использовать версии стандартов UN/EDIFACT, приведенные в Техническом приложении.

2.2. Операции системы

Каждая Сторона обязана проверять и поддерживать в работоспособном состоянии соответствующее оборудование, программное обеспечение и иные средства, необходимые для эффективного и надежного приема и передачи сообщений.

2.3. Изменение системы

Ни одна из Сторон не имеет права вносить любые изменения операций системы, которые могут воздействовать на взаимные способности Сторон по поддержанию связи друг с другом в соответствии с настоящим Соглашением, без предварительного уведомления другой Стороны о планируемых изменениях.

2.4. Связь

Стороны обязаны указать в Техническом приложении используемые способы связи, включая требования к системам телекоммуникации или использование услуг независимых провайдеров.

2.5. Правила и меры безопасности

Каждая Сторона обязана принять к использованию и обеспечивать соблюдение процедур и мер безопасности, включая приведенные в Техническом приложении, в целях защиты сообщений и своих записей от возникновения непредвиденных ситуаций и Недопущения злоупотреблений, включая ненадлежащий доступ, изменение или утрату.

2.6. Хранение записей

.Стороны обязаны хранить записи и сообщения, передаваемые в соответствии с 1настбящим Соглашением, в том порядке, как он может быть установлен в Техническом приложении.

Статья 3.
Обработка сообщений

3.1. Получение

Любое сообщение, переданное в соответствии с настоящим Соглашением, считается полученным, если становится доступным для получающей стороны способом, определенном в техническом приложении. До такого получения ни одно переданное сообщение не будет иметь юридическую силу, если только она не придается такому сообщению в соответствии с применимым правом с момента передачи, независимо от его получения.

3.2. Подтверждение

3.2.1. Если иное не предусмотрено в Техническом приложении, получение сообщения не обязательно должно подтверждаться получающей стороной. Требования подтверждения в Техническом приложении должны включать способы и виды подтверждений (включая любые сообщения и процедуры), а также сроки подтверждения, }если они устанавливаются, в течение которых подтверждение должно быть получено.

3.2.2. Подтверждение должно рассматриваться в качестве безусловного доказательства того, что соответствующее сообщение было получено. Сторона, получающая сообщение, требующее подтверждения, не вправе совершать по нему какие-либо действия до отправления подтверждения. Если получающая сторона не способна отправить подтверждение, она не вправе совершать по нему какие-либо действия до указаний со стороны отправителя сообщения. Неспособность получающей стороны подтвердить сообщение не влияет на его юридическую силу, за исключением тех случаев, когда отправитель не может быть идентифицирован на основании сообщения.

3.2.3. В случае, когда отправитель переданного надлежащим образом сообщения не получил требуемого подтверждения о его получении и не направил дальнейших указаний получателю, он вправе объявить сообщение утратившим юридическую силу, уведомив об этом получающую сторону.

3.3. Технические ошибки

Получающая сторона обязана уведомить отправителя о' возникновении обстоятельств, включая технические ошибки в полученном сообщении, препятствующих дальнейшей обработке сообщения.

Статья 4.
Действительность и принудительное исполнение

4.1. Действительность

Стороны соглашаются, что передача сообщений в соответствии с настоящим Соглашением может создавать юридически действительные и подлежащие принудительному исполнению обязательства. Стороны однозначно отказываются от права оспаривать действительность операции единственно на том основании, что связь между сторонами осуществлялась с использованием электронного обмена данными.

4.2. Доказательства

Безотносительно к отсутствию каких-либо письменных документов и собственноручных подписей, в той степени, в какой это допускается правом, записи сообщений, находящиеся у Сторон, должны рассматриваться как допустимые и могут использоваться в качестве доказательства содержащейся в них информации.

4.3. Заключение договора

Договор, заключаемый с использованием электронного обмена данными в соответствии с настоящим Соглашением, считается заключенным, когда сообщение, переданное в качестве акцепта оферты, было получено в соответствии с п. 3.1.

Статья 5.
Требования к содержанию данных

5.1. Конфиденциальный статус

Никакая информация, содержащаяся в любом сообщении, передаваемом в соответствии с настоящим Соглашением, не должна рассматриваться как конфиденциальная, если иное не вытекает из закона, условий Технического приложения или сообщения.

5.2. Соответствие требованиям законодательства

5.2.1. Каждая Сторона обязана обеспечить, чтобы содержание любого переданного, полученного или хранимого сообщения соответствовало всем требованиям, предъявляемым к такой Стороне законодательством.

5.2.2. В случае, если получение или хранение какого-либо элемента сообщения могут привести к нарушению применимого законодательства, получатель обязан незамедлительно сообщить о таком несоответствии.

5.2.3. До того момента, пока получатель не узнает о таком несоответствии сообщения законодательству, его права и обязанности по настоящему Соглашению не будут затронуты.

5.2.4. После направления уведомления о несоответствии сообщения праву получатель не обязан отвечать на последующие сообщения отправителя, не соответствующие законодательству. После получения уведомления отправитель обязан воздержаться от передачи в дальнейшем каких-либо сообщений, не соответствующих законодательству.

Статья 6.
Ответственность

6.1. Форс-мажор

Ни одна из Сторон не будет нести ответственности за любую просрочку исполнения или иную неспособность исполнения своих обязательств по настоящему Соглашению, если такие просрочка или неспособность вызваны любым событием вне контроля сторон, (а) которое нельзя было разумно предвидеть и принять во внимание в момент подписания настоящего Соглашения или (Ь) последствия которого нельзя; было избежать или устранить.

6.2. Убытки, не подлежащие возмещению

Ни одна из Сторон не будет нести ответственности за любые особенные, косвенные или штрафные убытки, возникающие из любого нарушения настоящего Соглашения.
.

6.3. Ответственность провайдера

6.3.1. Сторона, использующая услуги независимого провайдера для передачи или обработки сообщений, несет ответственность по настоящему Соглашению за любые) действия, бездействие или упущения данного провайдера в отношении указанных услуг.)

6.3.2. Сторона, отдающая распоряжение другой Стороне воспользоваться услугами конкретного независимого провайдера, несет ответственность по настоящему Соглашению за любые действия, бездействие или упущения данного провайдера.

Статья 7.
Общие положения

7.1. Регулирующее право Настоящее Соглашение подчинено национальному праву. В случае противоречия между правом, применимым к операции, и правом, применимым к Соглашению, право, применимое к Соглашению, будет иметь высшую юридическую силу.

7.2. Раздельность положений Соглашения

Если какое-либо положение настоящего Соглашения станет недействительным или не будет подлежать принудительному исполнению по любой причине, все остальные положения настоящего Соглашения будут сохранять полную юридическую силу.

7.3. Расторжение Соглашения

Каждая из Сторон вправе расторгнуть настоящее Соглашение с предварительным письменным уведомлением другой Стороны не позднее [30] дней до расторжения. Расторжение Соглашения не влияет на обмен сообщениями, имевший место до расторжения Соглашения, или совершение соответствующих операций. Положения пунктов 2.5, 2.6, 4,5.1,6,7.1 и 7.5 сохраняют свою силу после расторжения Соглашения и являются обязательными для Сторон.

7.4. Цельность Соглашения

Настоящее Соглашение, включая Техническое приложение, образует полное Соглашение между Сторонами по вопросам, являющимся предметом настоящего Соглашения, и вступает в силу с момента подписания Сторонами. Техническое приложение может быть изменено Сторонами либо лицом, уполномоченным Стороной подписывать Соглашение от ее имени. Каждая Сторона обязана предоставить другой Стороне письменную запись любого согласованного изменения за своей

подписью. Каждое изменение вступает в силу после обмена письменными и подписанными записями. Техническое приложение и каждое вступившее в силу изменение образуют соглашение между Сторонами.

7.5. Заголовки и подзаголовки

Заголовки и подзаголовки настоящего Соглашения следует считать частью раздела или подраздела, к которым они относятся.

7.6. Уведомление

За исключением случаев направления подтверждений и уведомлений в соответствии со статьей 3, каждое уведомление, которое должно быть сделано в соответствии с настоящим Соглашением или Техническим приложением, будет считаться совершенным, если направлено другой Стороне в письменной форме и подписано уполномоченным Стороной, направляющей уведомление, лицом либо когда может быть представлен электронный эквивалент такой записи. Каждое уведомление вступает в силу со дня, следующего за днем его получения по вышеуказанному адресу другой Стороны.

7.7. **Разрешение споров**

Вариант 1: Арбитражная оговорка

Любой спор, возникающий в связи с настоящим Соглашением, включая вопросы его наличия, действительности или расторжения, подлежит рассмотрению и окончательному разрешению третейским судом в составе {трех} арбитров, согласованных Сторонами, а при невозможности соглашения - назначаемые в соответствии с процедурными правилами и действующие на основании этих правил.

Вариант 2: Оговорка о юрисдикции

Любой спор, возникающий в связи с настоящим Соглашением, подлежит передаче в суд , который будет иметь исключительную юрисдикцию.

Стороны подписали настоящее Соглашение в вышеуказанную дату.

Наименование Стороны: Уполномоченное должностное лицо: Подпись:

Наименование Стороны: Уполномоченное должностное лицо: Подпись:

Додаток 17. Центр ООН содействия торговле и электронному бизнесу. Соглашение об электронной коммерции

(Рекомендация № 31, принята Центром ООН содействия торговле и электронному бизнесу (UN/CEFACT), март 2000 г., Женева)

ВВЕДЕНИЕ

Электронная коммерция предлагает новые возможности для повышения эффективности деловых операций и Снижения издержек, связанных с торговыми процедурами, предоставляя повышенные конкурентные преимущества субъектам коммерческой деятельности, готовым воспринять новые методы работы и торговли.

Возникающие решения для электронной коммерции и использование Интернета предоставляют пользователям комбинацию технологий для передачи данных в целях заключения договоров электронным способом, а равно управления новыми бизнес-процессами, ведущими к новым бизнес-моделям.

Правовое окружение, традиционно ориентированное на деловые процедуры и требования, подразумевающие использование бумажных носителей, таких как собственноручные подписи, находится в процессе приспособления к таким новым технологиям. На международном уровне наличие Типового закона Комиссии ООН по праву международной торговли (ЮНСИТРАЛ) об электронной коммерции, принятого в 1996 г., обеспечивает правовые основы для принятия законодательства. Международные организации, такие как Всемирная торговая организация (ВТО), ЮНСИТРАЛ, Организация экономического сотрудничества и развития (ОЭСР), Конференция ООН по торговле и развитию (ЮНКТАД), а также Международная торговая палата (МТП) активно участвуют в дискуссиях с правительствами и предпринимателями по разрешению ряда ключевых правовых вопросов, возникающих *при* становлении глобального рыночного пространства для электронной коммерции. На региональном или местном уровне предлагаются или принимаются новые законы в целях разрешения ряда этих вопросов.

Хотя возникающее правовое окружение глобального рыночного пространства для

электронной коммерции и будет способствовать, при его окончательном становлении, установлению доверия, необходимого для его дальнейшего развития, использование электронной коммерции все еще порождает ряд вопросов, которые могут 1 быть более успешно решены в рамках договорного процесса.

ЦЕЛИ

В целях содействия установлению доверия между коммерческими предприятиями и использования преимуществ опыта, приобретенного в рамках Соглашения об обмене; данными (Рекомендация №26 Европейской экономической комиссии ООН), UN/CEFACT принял следующую Рекомендацию на своей шестой сессии в марте 2000 г. UN/CEFACT предлагает в настоящей Рекомендации модель договорного подхда для операций электронной коммерции. Данный подход принимает во внимание) необходимость рамочного подхода к основным условиям, определяемым по соглашеник» между коммерческими предприятиями, в сочетании с гибкостью, требуемой для;) совершения коммерческих сделок на повседневной основе. Соглашение об электронной коммерции, далее именуемое «Электронное соглашение», предназначено для удовлетворения деловых требований партнеров, осуществляющих электронную коммерцию типа «коммерческое предприятие – коммерческое предприятие». Оно содержит базовый перечень условий, способных обеспечить, чтобы одна или более электронных коммерческих сделок, далее именуемых «Электронные сделки», могли впоследствии заключаться коммерческими партнерами в устойчивом правовом окружении.

Электронное соглашение стремится к рассмотрению всех форм электронных коммуникаций, доступных для заключения Электронных сделок. Коммерческим партнерам, участвующим в договорных отношениях, основанных на использовании сочетания технологий электронной коммерции, включая электронный обмен данными, рекомендуется использовать Электронное соглашение и, в необходимой степени, заменять им использование Соглашение об обмене данными.

ОГРАНИЧЕНИЯ

Хотя Электронное соглашение может использоваться в отношениях между коммерческими предприятиями и потребителями, оно не включает в себя условия, касающиеся защиты прав потребителей. Законодательство о защите прав потребителей является общеобязательным, и в большинстве случаев будет применимым национальное и местное законодательство о защите прав потребителей при заключении сделки с потребителем. Коммерческие предприятия, желающие использовать Электронное соглашение для вступления в договорные отношения с потребителями, по-1 этому должны учитывать необходимость соблюдения национального и местного законодательства о защите прав потребителей. Кроме того, потребуются соответствующие изменения, если Электронное соглашение используется во взаимоотношениях с административными и официальными органами.

ДЕЙСТВИЯ, ПРЕДПРИНИМАЕМЫЕ СТОРОНАМИ

Электронное соглашение устанавливает рамочные принципы для совершения последующих Электронных сделок. В некоторых случаях Электронное соглашение предоставляет сторонам выбор между альтернативными вариантами. Сторонам рекомендуется проявлять тщательность при рассмотрении возможных вариантов выбора и решении вопроса о принятии варианта по умолчании или другого варианта. Кроме того, сторонам рекомендуется предпринимать следующие шаги в связи с завершением работы над Электронным соглашением:

установить, какие формы коммуникаций и сообщений будут использоваться, указать их в Главе 2;

установить, какие условия будут применяться в 'отношении принятия обязательств по Электронным сделкам, и указать их в Главе 2.

Стороны должны быть также осведомлены о том, что могут существовать национальные или местные ограничения, которые применяются к отдельным условиям или ведут к ограничениям, которые, в целом, следует принимать во внимание. Каждая Сторона, поэтому, должна в дополнение к заключению Электронного соглашения предпринимать соответствующие шаги для обеспечения соблюдения своего собственного национального и местного законодательства, в частности, в отношении:

хранения сообщений;

НДС и другого налогового регулирования;

защиты данных, включая правила Директивы ЕС № 95/46/ЕЕС о защите данных, если одна из Сторон является резидентом Европейского союза.

Стороны также должны обеспечить, чтобы уровень безопасности, который они используют, соответствовал Электронным сделкам. Например, Стороны могут рас- смотреть использование криптографии с открытым ключом или иных способов в целях увеличения степени защиты против ошибок при передаче и перехвата сообщений, а также в целях повышения доказательственной ценности записей при электронном обмене информацией между Сторонами.

Многие юрисдикции требуют строгого доказательства того, что условия, принятые Сторонами путем отсылки, были согласованы обеими сторонами. В целях минимизации проблем доказывания, Сторонам рекомендуется согласовать способ указания на Электронное соглашение при совершении Электронных сделок и включения такого указания при всех случаях обмена информацией, в отношении которых распространяется Электронное соглашение. Это может делаться путем включения специального кода или указания слов «Электронное соглашение» в пункте 2.1 и путем использования такого кода или указания при последующем обмене информацией.

Следует также напомнить коммерческим партнерам, что во многих случаях электронная коммерция включает в себя международные сделки, и правовые сложности не могут быть разрешены в стандартном соглашении. В силу этого может оказаться необходимым получение дополнительных консультаций.

КАК ИСПОЛЬЗОВАТЬ ЭЛЕКТРОННОЕ СОГЛАШЕНИЕ

Электронное соглашение может использоваться для совершения одной сделки либо нескольких сделок. Электронное соглашение должно заключаться до совершения Электронной сделки, включая случай, когда оно используется только для совершения одной сделки.

Электронное соглашение должно в таком случае установить общие правила, применимые к сделке и, если в Электронное соглашение включается глава 2, к ее исполнению. В том случае, если заключается Электронное соглашение, при последующем обмене информацией, касающемся коммерческой сделки(ок), должно делаться указание на Электронное соглашение и таким образом распространяться принципы регулирования, установленные Электронным соглашением.

Акцептант может избрать один или более способов связи, предлагаемых Предлагающим лицом. Если Акцептант избирает меньшее количество способов коммуникаций, чем предложены. Предлагающее лицо и Акцептант используют только те способы, которые избраны Акцептантом.

Электронное соглашение состоит из двух частей:

А. Документ оферты, посредством которого Сторона делает предложение о вступлении в коммерческие договорные отношения с использованием электронных средств и направляет другой Стороне или делает доступными для другой Стороны условия, на которых она готова это сделать.

Данный документ также может быть использован кем-либо, кто не находит первоначальные условия приемлемыми и направляет первоначальному отправителю новый документ оферты, включающий предлагаемые изменения.

В. Документом акцепта Акцептант подтверждает условия, предлагаемые в Документе оферты, если они являются приемлемыми.

Стороны могут, в качестве альтернативы, вступить в переговоры о содержании Электронного соглашения до направления Документа оферты в форме, приемлемой для обеих Сторон, которая сохраняет согласованные условия.

Электронное соглашение заключается путем обмена/объединения Документов акцепта и оферты и не требует соблюдения дальнейших формальностей. Подпись не является обязательной с того момента, когда ясны условия соглашения между Сторонами путем обмена двумя Документами.

Вместе с тем некоторые предосторожности должны быть соблюдены в отношении записи информации о Документах. Оба Документа должны записываться и храниться каждой Стороной. В некоторых странах доказательства и арбитражные оговорки могут требоваться в письменной форме и в виде подписанного документа. Поэтому должна проявляться заботливость в отношении этих условий.

Сторона, направляющая Документ оферты, далее именуется «Предлагающее лицо», а

Сторона, направляющая Документ, именуется «Акцептант». Предлагающее лицо и Акцептант вместе именуются «Стороны».

В том случае, если Стороны заключают Электронное соглашение, они могут в последующем совершать Электронные сделки способом, изложенном в Электронном соглашении, т.е. обычно путем направления или представления оферты отправителем (который может быть Предлагающим лицом либо Акцептантом) и направления акцепта другой Стороной.

В электронной версии настоящего Соглашения документ акцепта включает только средства связи, избранные Предлагающим лицом.

Электронное соглашение содержит ряд условий, которые Стороны должны избрать из двух или более альтернативных вариантов. Данные возможности выбора отмены квадратными скобками [ ], а варианты - наклонной чертой /. Если Стороны делают выбор между альтернативными вариантами, подчеркнутый текст применяется по умолчанию, в то время как неподчеркнутый текст не будет приниматься во внимание.

А. Документ оферты

Настоящим Предлагающее лицо делает оферту Акцептанту о заключении соглашения, как оно определено ниже. Любой последующий обмен информацией между Сторонами, который Стороны намереваются подчинить настоящему Соглашению, должен содержать указание на настоящее Соглашение путем включения [слов «Электронное соглашение»/указать иной идентификационный код или средства отсылки как настоящему Соглашению].

Существенным условием настоящей оферты является то, что акцепт и заключение Электронного соглашения не рассматриваются как подразумевающие любое обязательство любой из Сторон вступать в дальнейшие договорные отношения.

Документ оферты должен быть акцептован Акцептантом путем направления Документа акцепта надлежащим образом составленного и полученного (как это определено в пункте 2.3.1) Предлагающим лицом не позднее [24 часов после получения Акцептантом Документа оферты / указать другое время получения]. Если Документ оферты акцептуется в течение данного периода времени, то это образует соглашение между Сторонами.

Глава 1 - Электронное соглашение

1. Идентификация Предлагающего лица

Любой договор, заключаемый путем обмена сообщениями, направляемыми с - использованием электронных средств, указанных ниже в пункте 2.1, между Предлагающим лицом и Акцептантом, заключается со следующим юридическим лицом:

[Указать полные и точные данные Предлагающего лица:

Наименование.

Юридический адрес.

Идентификационный номер/Номер торгового реестра/Профессиональный регистрационный номер (если применимо).

Номер НДС или иной налоговый номер.

Телефон, номер факса, адрес электронной почты или веб-сайта.

2. Связь

2.1 Способ связи

[ПОЯСНИТЕЛЬНОЕ ЗАМЕЧАНИЕ: СТОРОНАМ НАСТОЯТЕЛЬНО РЕКОМЕНДУЕТСЯ ОПРЕДЕЛИТЬ СПОСОБ СВЯЗИ].

Предлагающее лицо предлагает, что стороны будут поддерживать связь с использованием следующих способов связи:

[Любой электронный способ связи / специально согласованные способы связи:]

Образцы типов сообщений	Способ связи			
	Веб-сайт	EDI	e-mail	Иные {указать)
Приглашение делать оферты/ вести переговоры				
Оферта				
Акцепт				
Отзыв				
Подтверждение				
Уведомление				
(добавить иные приемлемые виды сообщений)				

В Документе акцепта Акцептант должен указать, какой способ связи может применять Акцептант. Любой обмен информацией с использованием средств, принятых Предлагающим лицом и Акцептантом, далее именуется «Сообщение».

2.2. Коммуникационные стандарты, программное обеспечение и независимый провайдер

Предлагающее лицо предлагает, чтобы Стороны использовали следующие коммуникационные стандарты, программное обеспечение и независимого провайдера(ов) (в случае, если требуется использовать):

Наименование коммуникационных стандартов.

Продукты программного обеспечения/номера версий.

Независимый провайдер(ы).

Каждая Сторона обязана уведомлять другую Сторону до внесения любых изменений в операции системы, аппаратные средства и программное обеспечение, которые могут затронуть обмен информацией между Сторонами или изменить информацию, указанную в пунктах 2.1 и 2.2. В связи с таким уведомлением направляющая уведомление Сторона обязана просить другую Сторону проинформировать направляющую уведомление Сторону о приемлемости изменений. Изменения приобретают силу только в случае, когда их принимает другая Сторона.

2.3 Получение и подтверждение получения

2.3.1 Определение получения

Получение имеет место в то время, когда Сообщение [становится доступным получающей Стороне по электронному адресу, используемому получающей Стороной / другое определение получения].

2.3.2 Подтверждение получения

Получающая Сторона [обязана/не обязана] подтверждать получение Сообщения [если только отправитель не запрашивает подтверждения].

Подтверждение может производиться [указать тип Сообщения/ любым способом связи получающей Стороны, автоматизированным либо иным, или в форме любого поведения получающей Стороны, достаточного для указания отправителю на то, что Сообщение было получено].

В том случае, когда отправитель указал или закон предписывает, что Сообщение является условным до получения подтверждения, Сообщение рассматривается как никогда не отправлявшееся до получения подтверждения.

В случае, когда получающая Сторона обязана представить подтверждение получения и отправитель не указал, что Сообщение является условным до получения подтверждения, и подтверждение не были получено отправителем в течение [указать время для подтверждения / разумное время], отправитель:

(a) вправе направить получателю уведомление, указывающее, что подтверждение не было получено, и устанавливающее разумное время, до истечения которого должно быть получено подтверждение; и

(b) если подтверждение не получено в течении времени, установленного в вышеуказанном пункте (a), вправе после напрпвления уведомления адресату, рассматривать Сообщение как никогда не отправлявшееся или использовать любые другие права, которыми может обладать отправитель.

В том случае, когда отправитель получает подтверждение получения от получающей

Стороны, предполагается, что Сообщение получено получающей Стороной. Такая презумпция не подразумевает, что данное Сообщение соответствует полученному Сообщению. Если подтверждением делается заявление касающееся полученного Сообщения, такое заявление предполагается правильным.

2.4.0шибки связи

Сторона [должна/ не обязана] направлять уведомление другой Стороне об обстоятельствах, включая технические ошибки при передаче, которые препятствуют дальнейшей обработке Сообщения. Такое уведомление должно направляться (как можно скорее в разумно возможное время / указать период времени).

Получатель вправе рассматривать каждое Сообщение как отдельное Сообщение и действовать, исходя из этого предположения, за исключением той степени, в которой оно дублирует другое Сообщение, и получатель знал или должен был знать, если бы он проявил разумную заботливость или использовал любую согласованную процедуру, что Сообщение являлось дубликатом.

Получатель вправе рассматривать Сообщение как полученное в качестве того которое предполагал направить отправитель, и действовать исходя из этого предположения. Получатель не вправе действовать таким образом если он знал или должен был знать, если бы он проявил разумную заботливость или использовал любую согласованную процедуру, что передача привела к ошиbке или задержке.

3. Действительность и заключение Электронных сделок

3.1 Действительность

[ПОЯСНИТЕЛЬНОЕ ЗАМЕЧАНИЕ:

МНОГИЕ ЮРИСДИКЦИИ ТРЕБУЮТ ПИСЬМЕННОЙ ФОРМЫ ДАННОГО УСЛОВИЯ И/ИЛИ ЗА ПОДПИСЬЮ

Стороны соглашаются, что путем обмена Сообщениями мотут создаваться действительные и подлежащие принудительному исполнению обязательства Стороны прямо выражают отказ от любого права отрицать действительность и \или допустимость Электронного соглашения и любой Электронной сделки исключительности по той причине, что обмен информацией между Сторонами осуществлялся с использованием электронного обмена информацией.

3.2 Заключение Электронной сделки

Электронная сделка совершается, когда Сообщение, направляемое в качестве акцепта оферты, акцептуется в соответствии с пунктом 3.2.4

3.2.1 Определение оферты

Сообщение образует оферту, если оно включает предложение о заключении договора, адресуемое одному или более конкретным лицам, которое сформулировано с достаточной степенью определенности и указывает на намерение отправителя оферты быть связанным [обязательствами] в случае акцепта.

Сообщение, доступ к которому в целом осуществляется электронным способом не образует оферту, если иное не указано в сообщении.

3.2.2 Отзыв

Любая оферта, если иное не согласовано или явным образом не указано в оферте, [является / не является] отзывной. В случае отзывности оферта может быть отозвана только в случае, если уведомление об отзыве [получено получателем/направлено получателю] оферты до того момента, когда акцепт [получен отправителем/ направлен отправителю.

Любой акцепт [может быть / не может быть] отменен. При возможности отмены акцепта, она приобретает силу в случае, когда уведомление об отмене получено до получения акцепта, подлежащего отмене.

3.2.3 Срок акцепта

Срок любой оферты истекает [в 24 часа / указать иной период времени], следующих за получением такой оферты, если иное не указано в оферте или оферта не была акцептована в течение данного периода времени. Если акцепт получен позднее, получатель может рассматривать акцепт в качестве новой оферты.

3.2.4 Акцепт

Оферта (как она определена выше, в пункте 3.2.1) акцептуется в тот момент, когда отправитель такой оферты получает безусловный акцепт данной оферты в течение указанного периода времени.

4. Прочие условия

4.1 Выбор права

Настоящее Электронное соглашение регулируется национальным правом [указать страну / места учреждения Предлагающего лица / правом, применимым в соответствии с применимыми правилами международного частного права], исключая нормы коллизионного права.

Электронные сделки регулируются национальным правом [указать страну / места учреждения Предлагающего лица, исключая нормы коллизионного права / страны, чье право применимо в соответствии с правилами международного частного права или избрано для каждой сделки], исключая нормы коллизионного права.

4.2 Раздельность

Если какое-либо положение настоящего Электронного соглашения по любой причине станет недействительным или не будет подлежать принудительному исполнению, все остальные положения настоящего Электронного соглашения будут сохранять полную юридическую силу и действие.

4.3 Расторжение

Каждая из Сторон вправе расторгнуть настоящее Электронное соглашение с предварительным уведомлением о расторжении [не позднее 30 дней / иной период времени]. Расторжение Электронного соглашения не влияет на обмен информацией, имевший место до расторжения, или совершение соответствующих сделок. Положения, которые по своей природе представляют собой длящиеся обязательства, сохраняют свою силу после расторжения Электронного соглашения и являются обязательными для Сторон.

4.4 Цельность Электронного соглашения.

Настоящее Электронное соглашение образует полное соглашение между Сторонами по вопросам, являющимися предметом настоящего Электронного соглашения.

4.5 Выбор суда

[ПОЯСНИТЕЛЬНОЕ ЗАМЕЧАНИЕ: МНОГИЕ ЮРИСДИКЦИИ ТРЕБУЮТ ПИСЬМЕННОЙ ФОРМЫ ДАННОГО УСЛОВИЯ И/ИЛИ ЗА ПОДПИСЬЮ. СТОРОНЫ МОГУТ ИЗБРАТЬ ДЛЯ ВКЛЮЧЕНИЯ СООТВЕТСТВУЮЩУЮ МЕСТНУЮ АЛЬТЕРНАТИВНУЮ ПРОЦЕДУРУ РАЗРЕШЕНИЯ СПОРОВ]

[Вариант 1: Оговорка о юрисдикции: Любой спор, возникающий в связи с настоящим Электронным соглашением, подлежит передаче в суд в месте, вышеуказан» ном в пункте 4.1/ включить страну и муниципалитет или округ]. Вместе с тем Сторона в дополнение к этому вправе предъявить иск другой Стороне в суды по месту постоянного нахождения другой Стороны.

[Вариант 2: Арбитражная оговорка: Любой спор, возникающий в связи с настоящим Электронным соглашением, включая любые вопросы его наличия, действи-тельноста или расторжения, подлежит рассмотрению и окончательному разрешению третейским судом в составе одного/трех арбитров, согласованных Сторонами, а при невозможности соглашения - назначаемые в соответствии с процедурными правилами и действующие на основании этих правил].

Любой спор, возникающий в связи с любой Электронной сделкой, подлежат передаче в [суды, компетентные согласно соответствующим правилам международного Д1 частного права/ вышеуказанный суд или арбитраж/ суды: указать страну и муниципалитет.

Стороны используют максимально возможные усилия в течение 30 дневного II срока после возникновения спора для разрешения любого такого спора.

Глава 2 - Электронная(ые) сделка(и)

Электронная(ые) сделка(и) подчинены следующим условиям:

[При желании включить любые специальные положения об условиях, применимых к Электронной(ым) сделке(ам), включая условия поставки, вид и условия платежа, право собственности и владения, переход риска случайной гибели, прав и т.д. в соответствии с типами

Электронных сделок, по которым принимаются обязательства / Включить указание на применимые условия].

Условия, применимые к Электронным сделкам, формулируются в соответствии с настоящим Соглашением. В случае коллизий, условия [главы 1 настоящего Соглашения] / условия главы 2 настоящего Соглашения, включая общие условия] будут Д1' иметь преимущество.

В. Документ акцепта

Электронное соглашение [указать иной идентификационный код, определенный в Документе оферты],

Настоящим Акцептант акцептует Документ оферты, датированный [указать дату], полученный от [указать наименование Предлагающего лица].

1. Идентификация Акцептанта

Последующие Электронные сделки между Предлагающим лицом и Акцептантом» совершаются со следующим юридическим лицом: (Указать полные и точные данные Акцептанта:

Наименование.

Юридический адрес .

Идентификационный номер/Номер торгового реестра/Профессиональный регистрационный номер (если применимо).

Номер НДС или иной налоговый номер.

Телефон, номер факса, адрес электронной почты или веб-сайта].

2. Связь.

2.1 Форма связи.

[ПОЯСНИТЕЛЬНОЕ ЗАМЕЧАНИЕ: СТОРОНАМ НАСТОЯТЕЛЬНО РЕКОМЕНДУЕТСЯ ОПРЕДЕЛИТЬ ФОРМУ СВЯЗИ].

Акцептант соглашается осуществлять обмен информацией с использованием следующего(их) способа(ов) связи (всех или некоторых способов, указанных в пункте 2.1. Документа оферты):

Любая электронная форма связи / специально согласованные формы связи:

Додаток 18. Регламент № 733/2002 Европейского парламента и Совета от 22 апреля 2002 г. о введении домена верхнего уровня «.eu»

ЕВРОПЕЙСКИЙ ПАРЛАМЕНТ И СОВЕТ ЕВРОПЕЙСКОГО СОЮЗА,

принимая во внимание Договор, учреждающий Европейское сообщество, и, в частности его статью 156,

принимая во внимание предложение Комиссии, принимая во внимание мнение Экономического и социального комитета, следуя консультациям с Комитетом регионов, действуя в соответствии с процедурой, изложенной в статье 251 Договора,

(ТЕКСТ ПРЕАМБУЛЫ)'

ПРИНЯЛИ НАСТОЯЩИЙ РЕГЛАМЕНТ:

Статья 1.
Цель и сфера

1. Целью настоящего Регламента является ввести в Сообществе код страны «.ей» домена высшего уровня (ксДВУ). Регламент устанавливает условия для такого введения, включая назначение Реестра, и определяет основы общей политики, в рамках которых будет функционировать Регистратор.

2. Настоящий Регламент применяется без ущерба для договоренностей в государствах - участниках, касающихся национальных ксДВУ.

Статья 2.
Определения

В целях настоящего Регламента:

(а) «Реестр» означает юридическое лицо, на которое возложены организация,

администрирование и управление ДВУ «.ей», включая поддержание соответствующих баз данных и связанных услуг публичных запросов, регистрация доменных имен, ведение реестра доменных имен, реестра серверов доменных имен высшего уровня и распространение файлов зоны ДВУ;

(b) «Регистратор» означает физическое или юридическое лицо, которое по договору с Реестром предоставляет услуги по регистрации доменных имен регистрантам.

Статья 3.
Свойства Реестра

1. Комиссия:

(a) определяет критерии и процедуру для назначения Реестра в соответствии с процедурой, указанной в статье 6 (3);

(b) назначает Реестр в соответствии с процедурой, указанной в статье 6 (2), после опубликования предложения о выражении интереса в Официальном журнале Европейских сообществ и после того, как была завершена процедура для такого предложения;

(c) заключает договор в соответствии с процедурой, указанной в статье 6 (2), который определяет условия, в соответствии с которыми Комиссия надзирает за организацией, администрированием и управлением ДВУ «.ей». Договор между Комиссией и Реестром должен быть ограничен по времени и возобновляем. Реестр не может принимать заявки на регистрацию до тех пор, пока не утверждена регистрационная политика.

2. Реестр должен быть некоммерческой организацией, образованной в соответствии с правом государства - участника и имеющей в Сообществе свой зарегистрированный офис, центральную администрацию и основное коммерческое предприятие.

3. Получив предварительное согласие Комиссии, Реестр заключает соответствующие договоры, предусматривающие делегирование кода ксДВУ «.eu». С этой целью должны учитываться соответствующие принципы, принятые Правительственным консультативным комитетом.

4. Реестр ДВУ «.eu» не будет сам действовать в качестве Регистратора.

Статья 4.
Обязательства Реестра

1. Реестр обязан соблюдать правила, общие принципы и процедуры, изложенные в настоящем Регламенте и договорах, указанных в статье 3. Реестр обязан соблюдать прозрачные и недискриминационные процедуры.

2. Реестр обязан:

(a) организовывать, администрировать и управлять ДВУ «.eu» в общем интересе и на основе принципов качества, эффективности, надежности и доступности;

(b) регистрировать доменные имена ДВУ «.eu» через любого аккредитованного Регистратора зоны «.eu», запрашиваемого любым:

(1) предприятием, имеющим в Сообществе свой зарегистрированный офис, центральную администрацию или основное коммерческое предприятие, или

(ii) организацией, учрежденной в Сообществе без ущерба для применения национального права, или

(iii) физического лица - резидента Сообщества;

(c) взимать сборы, непосредственно связанные с понесенными издержками;

(d) реализовывать политику внесудебного урегулирования конфликтов, основанную на возмещении издержек, и процедуру быстрого разрешения споров между владельцами доменных имен в отношении прав, касающихся имен, включая права интеллектуальной собственности, а также споров в отношении индивидуальных решений Реестра. Эта политика должна приниматься в соответствии со статьей 5(1)и учитывать рекомендации Всемирной организации интеллектуальной собственности. Политика должна обеспечивать заинтересованным сторонам адекватные процедурные гарантии и применяться без ущерба для любого судебного производства;

(e) принимать процедуры, осуществлять аккредитацию Регистраторов зоны «.eu» и гарантировать эффективные и справедливые условия конкуренции между Регистраторами зоны «.eu»;

(f) гарантировать целостность баз данных доменных имен.

Статья 5.
Основы политики

1. После консультаций с Реестром и следуя процедуре, указанной в статье 6 (3), Комиссия принимает правила публичной политики, касающиеся реализации и функций ДВУ «.eu» и принципов публичной политики по регистрации. Публичная политика включает:

(a) политику внесудебного урегулирования конфликтов;

(b) публичную политику по спекулятивной и злоупотребляющей регистрации доменных имен, включая возможность поэтапной регистрации доменных имен с тем, чтобы гарантировать владельцам предшествующих прав, признанных или установленных национальным правом и/или правом Сообщества и государственным органам соответствующие временные возможности по регистрации своих имен;

(c) политику возможного аннулирования доменных имен, включая вопрос оставленных имен (bona vacantia);

(d) языковые вопросы и географические концепции;

(e) режим интеллектуальной собственности и других прав.

2. В течение трех месяцев с вступления в силу настоящего Регламента, государства - участники могут сообщить Комиссии и другим государствам - участникам ограниченный перечень широко признанных имен в отношении географических и/или геополитических концепций, которые затрагивают их политическую или территориальную организацию, и:

(a) не могут быть зарегистрированы, или

(b) могут быть зарегистрированы только как домен второго уровня согласно правилам публичной политики.

Комиссия без промедления уведомляет Реестр о перечне сообщенных имен, к которым применяются такие критерии. Комиссия публикует данный перечень в то же время, когда уведомляет Реестр.

В случае, когда государство - участник или Комиссия в течение 30 дней со дня публикации заявляют возражение по позиции, включенной в сообщенный перечень, Комиссия предпринимает меры по исправлению ситуации в соответствии с процедурой, указанной в статье 6 (3).

3. До начала регистрационных операций Реестр принимает первоначальную регистрационную политику для ДВУ «.eu» в консультациях с Комиссией и другими заинтересованными сторонами. Реестр реализует в регистрационной политике правила публичной политики, принятые в соответствии с пунктом 1, принимая во внимание перечни исключений, указанные в пункте 2.

4. Комиссия периодически информирует Комитет, указанный в статье 6, о действиях, указанных в пункте 3 настоящей статьи.

Статья 6.
Комитет

1. Комиссии содействует в работе Комитет по коммуникациям, образованный Статьей 22 (1) Директивы 2002/21/ЕС Европейского парламента и Совета от 7 марта 2002 г. об общей регулятивной основе для сетей и услуг электронных коммуникаций (Директива о регулятивной основе). До образования Комитета по коммуникациям в соответствии с Решением 1999/468/ЕС, Комиссии содействует в работе Комитет, образованный статьей 9 Директивы Совета 90/387/ЕЕС от 28 июня 1990 г. об образовании внутреннего рынка телекоммуникационных услуг через реализацию условий открытой сети.

2. В случае, когда делается ссылка на настоящий пункт, статьи 3 и 7 Решения 1999/468/ЕС применяются, учитывая положения его статьи 8.

3. В случае, когда делается ссылка на настоящий пункт, статьи 5 и 7 Решения 1999/468/ЕС применяются, учитывая положения его статьи 8.

Период, изложенный в статье 5(6) Решения 1999/468/ЕС, устанавливается в три месяца. 4. Комиссия принимает правила своей процедуры.

Статья 7.
Сохранение прав

Сообщество сохраняет все права, касающиеся ДВУ».eu», включая, в частности права

интеллектуальной собственности и другие права на базы данных Реестра, требуемые, чтобы гарантировать реализацию настоящего Регламента, а также право повторно назначать Реестр.

Статья 8.
Отчет по реализации

Комиссия представляет Европейскому парламенту и Совету отчет о реализации эффективности и функционированию ДВУ «.eu» через один год после принятия настоящего Регламента и каждые два года после этого.

Статья 9.
Вступление в силу

Настоящий Регламент вступает в силу в день своего опубликования в Официальном журнале Европейских сообществ.

Настоящий Регламент имеет обязательный характер в своей полноте и непосредственно применим во всех государствах - участниках.

Додаток 19. Директива 95/46/ЕС Европейского парламента и Совета от 24 октября 1995 г. о защите физических лиц в отношении обработки персональных данных и свободном движении таких данных

ЕВРОПЕЙСКИЙ ПАРЛАМЕНТ И СОВЕТ ЕВРОПЕЙСКОГО СОЮЗА,
принимая во внимание Договор, учреждающий Европейское сообщество, и, в Частности, его статью 100a,
принимая во внимание предложение Комиссии,
принимая во внимание мнение Экономического и социального комитета,
действуя в соответствии с процедурой, изложенной в ст. 189Ь Договора,
(ТЕКСТ ПРЕАМБУЛЫ)
ПРИНЯЛИ НАСТОЯЩУЮ ДИРЕКТИВУ

Глава 1.
Общие положения

Статья 1.
Цель Директивы

1. В соответствии с настоящей Директивой государства - участники защищают основные права и свободы физических лиц и, в частности, их право на тайну частной жизни в отношении обработки персональных данных.

2. Государства -участники не должны ни ограничивать, ни запрещать свободное . Движение персональных данных между государствами - участниками по причинам, связанным с защитой, предоставляемой согласно части.

Статья 2.
Определения

В целях настоящей Директивы:

(a) «персональные данные» означают любую информацию, касающуюся иден-1тифицированного или идентифицируемого физического лица («субъекта данных»); идентифицируемым является лицо, которое может быть идентифицировано прямо или косвенно, в частности, путем указания на идентификационный номер либо один и более факторов, присущих его физической, физиологической, умственной, экономической, культурной или социальной идентичности;

(b) «обработка персональных данных» («обработка») означает любую операцию или набор операций, которые осуществляются с персональными данными, независимо от использования автоматических средств, такие как сбор, запись, организация, хранение, адаптация или изменение, извлечение, консультирование, использование, раскрытие путем передачи, распространения или

иное предоставление доступа, группировка или объединение, блокирование, стирание или уничтожение;

(c) «система регистрации персональных данных» («система регистрации») означает любой структурированный набор персональных данных, доступный в соответствии со специальными критериями, независимо от того, являются ли данные централизованными, децентрализованными или распределенными на функциональной или географической основе;

(d) «контролер» означает физическое или юридическое лицо, государственный орган, ведомство или иную организацию, которая самостоятельно или совместно с другими лицами определяет цели и средства обработки персональных данных; в случае, когда цели и средства обработки определяются национальным правом или правом Сообщества либо иными правовыми актами, то национальным правом или правом Сообщества может назначаться контролер или определяться специальные критерии его назначения;

(e) «оператор» означает физическое или юридическое лицо, государственный орган, ведомство или иную организацию, которая обрабатывает персональные данные от имени контролера;

(f) «третье лицо» означает любое физическое или юридическое лицо, государственный орган, ведомство или иную организацию, отличную от субъекта данных, контролера, оператора и лиц, которым в силу прямых указаний контролера или оператора разрешено обрабатывать данные;

(g) «получатель» означает физическое или юридическое лицо, государственный орган, ведомство или иную организацию, которой предоставляются данные, независимо от того, является ли она третьим лицом; вместе с тем, органы, которые могут получать данные в рамках конкретного расследования, не рассматриваются в качестве получателей;

(h) «согласие субъекта данных» означает любое свободно данное, конкретное и осведомленное изъявление своего желания, которым субъект данных сообщает о своем согласии с обработкой касающихся его персональных данных.

Статья 3.
Сфера действия

1. Настоящая Директива применяется к обработке персональных данных, осуществляемой полностью или частично с использованием автоматических средств, а также к обработке персональных данных, осуществляемой иным образом, чем с использованием автоматических средств, которая образует часть системы регистрации или предназначена для этого.

2. Настоящая Директива не применяется к обработке персональных данных: - в ходе деятельности, выходящей за пределы сферы регулирования права Сообщества, например предусмотренной разделами V и VI Договора о Европейском союзе, и в любом случае к обработке операций, касающихся общественной безопасности, обороны, безопасности государства (включая экономическое благосостояние государства при обработке операций, касающихся вопросов безопасности государства) и деятельности государства в сфере уголовного права; физическим лицом в ходе исключительно личной или домашней деятельности.

Статья 4.
Применимое национальное право

1. Каждое государство-участник применяет национальные правовые нормы, которые оно примет в соответствии с настоящей Директивой, к обработке персональных данных, когда:

(a) обработка осуществляется в рамках деятельности предприятия контролерами территории государства - участника; если один и тот же контролер имеет предприятия на территории нескольких государств - участников, он должен предпринять необходимые меры по обеспечению того, чтобы каждое из предприятий соответствовало обязанностям, предусмотренным применимым национальным правом;

(b) контролер учрежден не на территории государства - участника, но в месте, где применяется его национальное право в силу действия норм международного публичного права;

(c) контролер учрежден не на территории государства - участника и в целях 061 работки персональных данных использует оборудование, автоматизированное или иное, расположенное на территории указанного государства - участника, если такое оборудование не используется только в

целях транзитной передачи через территории Сообщества.

2. При обстоятельствах, указанных в части 1(c), контролер должен назначит представителя, образованного на территории такого государства - участника, без ущерба для исковых требований, которые могут быть предъявлены против самого контролера.

Глава II. Общие правила правомерности обработки персональных данных

Статья 5.

Государства — участники в рамках положений настоящей главы устанавливают более подробно условия, при которых обработка персональных данных является правомерной.

Раздел 1.
Принципы, касающиеся качества данных

Статья 6

1. Государства - участники обеспечивают, что персональные данные должны:

(a) обрабатываться добросовестно и правомерно;

(b) собираться в установленных, явных и законных целях и не обрабатываться в дальнейшем образом, несовместимым с этими целями. Дальнейшая обработка данных в исторических, статистических и научных целях не будет рассматриваться в качестве несовместимой, при условии, что государства - участники предусмотрят достаточные защитные меры;

(c) быть достаточными, соответствующими и не избыточными в отношении целей, для которых они собирались и/или в дальнейшем обрабатываются;

(d) точными и, когда это необходимо, поддерживаться в актуальном состоянии; должен быть предпринят любой разумный шаг для гарантии того, что неточные или неполные данные, имеющие отношение к целям, для которых они собирались или в дальнейшем обрабатываются, уничтожались либо исправлялись;

(e) поддерживаться в форме, позволяющей идентификацию субъекта данных не дольше, чем это необходимо в целях, для которых они собирались или в дальнейшем обрабатываются. Государства - участники обязаны предусмотреть соответствующие меры защиты для персональных данных, хранимых в течение более позднего времени [для исторического, статистического или научного использования.

2. Контролер гарантирует соблюдение требований части 1.

Раздел II.
Критерии придания законности обработке даннях

Статья 7

Государства - участники обеспечивают, что персональные данные могут обрабатываться, только если:

(a) субъект данных недвусмысленно дал свое согласие; или

(b) обработка необходима в целях исполнения договора, стороной которого является субъект данных, или для выполнения действий по просьбе субъекта данных до заключения договора; или

(c) обработка необходима в целях соблюдения юридического обязательства, субъектом которого является контролер; или

(d) обработка необходима в целях защиты жизненных интересов субъекта данных; или

(e) обработка необходима для решения задачи в государственных интересах или для осуществления официальных полномочий, принадлежащих контролеру или

третьему лицу, которому раскрываются данные; или

(f) обработка необходима в законных интересах, достигаемых контролером либо третьим лицом или лицами, которым раскрываются данные, за исключением случаев, когда над такими интересами преобладают фундаментальные права и свободы субъекта данных, которые требуют защиты согласно статье 1 (1).

Раздел III.
Специальные категории обработки

Статья 8.
Обработка специальных категорий данных

1. Государства - участники запрещают обработку персональных данных, показывающих расовое или этническое происхождение, политические мнения, религиозные или философские убеждения, профсоюзное членство) и обработку данных, касающихся здоровья или половой жизни.

2. Часть 1 не применяется, когда:

(a) субъект данных дает свое прямое согласие на обработку этих данных, за исключением случаев, когда право государств - участников предусматривает, что запрет, указанный в части 1, не может быть снят путем предоставления субъектом данных своего согласия; или

(b) обработка необходима в целях выполнения обязанностей и реализации определенных прав контролера в сфере трудового законодательства в той степени, в которой это разрешается национальным правом при условии достаточных защитных мер; или

(c) обработка необходима в целях защиты жизненно важных интересов субъекта данных или иного лица, когда субъект данных физически или юридически не способен дать свое согласие; или

(d) обработка осуществляется В ходе правомерной деятельности с надлежащими гарантиями фонда, ассоциации или иной некоммерческой организации с политическими, философскими, религиозными и профсоюзными задачами, при условии, что обработка касается исключительно членов этой организации или лиц, имеющих с ней регулярные контакты в связи с целями организации и данные Не раскрываются третьему лицу без согласия субъектов данных; или

(e) обработка касается данных, которые явным образом делаются публичными самим субъектом данных или необходимы для выдвижения, реализации или защиты исковых требований.

3. Часть 1 не применяется в случаях, когда обработка данных требуется в целях превентивной медицины, медицинских диагнозов, ухода, лечения или управления в сфере услуг здравоохранения, а также в случаях, когда указанные данные обрабатываются профессиональным специалистом в области здравоохранения с учетом национального права или правил, установленных национальными компетентными органами в отношении обязательств профессиональной тайны, или другим лицом, в отношении которого применяются аналогичные обязательства.

4. С учетом надлежащих защитных мер, государства - участники вправе, в целях обеспечения существенных публичных интересов, предусмотреть национальным правом либо решением надзорного органа изъятия в дополнение к изложенным в части 2,

5. Обработка данных, касающихся правонарушений, уголовных приговоров или мер безопасности, может осуществляться только под контролем официального органа или в случае, если национальным правом установлены соответствующие специальные защитные меры, с учетом изъятий, которые могут быть предоставлены государством - участником в соответствии с национальными нормами, предусматривающими подобные меры. Вместе с тем полный реестр уголовных приговоров может вестись только под контролем официального органа.

Государства - участники вправе установить, что данные, касающиеся административных санкций или судебных решений по гражданским делам, также обрабатываются под контролем официального органа.

6. Об изъятиях из части 1, предусмотренных в части 4 и 5, должна уведомляться Комиссия.

7. Государства - участники должны определить условия, при которых может обрабатываться национальный идентификационный номер или любой другой идентификатор общего применения.

Статья 9.
Обработка персональных данных и свобода выражения

Государства - участники обязаны установить исключения или изъятия из норм настоящего раздела, раздела IV и раздела VI в отношении обработки персональных данных, осуществляемой исключительно в журналистских целях или в целях артистического либо литературного выражения, только в том случае, если они необходимы для согласования права на неприкосновенность частной жизни с правилами, регулирующими свободу выражения.

Раздел IV.
Информация, предоставляемая субъекту данных

Статья 10.
Информация в случаях сбора данных от субъекта данных:

Государства - участники обеспечивают, чтобы контролер или его представитель предоставляли субъекту данных, от которого собираются касающиеся его данные, как минимум, следующую информацию, за исключением случаев, когда он ей уже обладает:

(a) о личности контролера и, при наличии, его представителя;

(b) о цели обработки, для которой предназначаются данные;

(c) любую дополнительную информацию, такую как

- получатели или категории получателей данных;

- .являются ли ответы на вопросы обязательными или добровольными, а также возможные последствия неспособности дать ответ,

- наличие права доступа и права исправления касающихся его данных, в той степени, насколько такая дополнительная информация является необходимой, принимая во внимание особые обстоятельства, при которых собираются данные, гарантии добросовестной обработки в отношении субъекта данных.

Статья 11.
Информация, когда данные не были получены от субъекта данных

1. В случае, когда данные не были получены от субъекта данных, государства-участники обеспечивают, чтобы контролер или его представитель были должны во время осуществления записи персональных данных или, если предусмотрено раскрытие Данных третьему лицу, не позже времени, когда данные раскрываются первоначально, предоставлять субъекту данных, как минимум, следующую информацию, за исключением случаев, когда он ей уже обладает:

(a) о личности контролера и, при наличии, его представителя;

(b) о целях обработки;

(c) любуй дополнительную информацию, такую как

-категории данных,

- получатели или категории получателей,

- наличие права доступа и права внесения исправления в касающиеся его данные настолько, насколько такая дополнительная информация является необходимой, Принимая во внимание особые обстоятельства, при которых обрабатываются данные; в целях гарантии добросовестности обработки в отношении субъекта данных.

2. Часть 1 не применяется в случаях, в частности при обработке для статистических целей или целей исторического или научного исследования, когда предоставление такой информации оказывается невозможным или требует непропорциональных усилий, или если запись или раскрытие данных прямо предусмотрены законом. В этих случаях государства - участники предусматривают соответствующие меры защиты.

Раздел V.
Право субъекта данных на доступ к данным

Статья 12.
Право доступа

Государства - участники гарантируют каждому субъекту данных право получать от контролера:

(a) без ограничений, в разумные сроки, без излишней задержки или расходов:

- подтверждение в отношении того, обрабатывались или нет касающиеся его данные, и информацию, как минимум, о целях обработки, категориях данных и получателях или категориях получателей, которым раскрываются данные,

- сообщение в понятной для него форме данных, проходящих обработку, и любой доступной информации относительно их источника,

- ознакомление с логической схемой, задействованной при любой автоматической обработке

касающихся его данных, как минимум, в случае автоматических решений, указанных в статье 15(1);

(b) насколько это приемлемо, исправление, стирание или блокирование данных, обработка которых не соответствует положениям настоящей Директивы, в частности, вследствие неполного или неточного характера данных;

(c) уведомление третьего лица, которому были раскрыты данные, о любом исправлении, стирании или блокировании, осуществленном согласно пункту (Ь), если только это не оказывается невозможным или не требует непропорциональных усилий.

Раздел VI.
Исключения и ограничения

Статья 13.
Исключения и ограничения

1. Государства - участники вправе принимать законодательные меры, чтобы ограничить сферу обязанностей и прав, предусмотренных в статьях 6 (1), 10, II (1), 12 и 21 в случае, когда такое ограничение образует необходимые меры для гарантии:

(a) национальной безопасности;

(Ь) обороны;

(c) общественной безопасности;

(d) предотвращения, расследования, выявления и преследования уголовных правонарушений или нарушения этических норм регулируемых профессий;

(e) важных экономических или финансовых интересов государства - участника; или Европейского союза, включая монетарные, бюджетные и налоговые вопросы;

(f) мониторинга, инспектирования или связанных с этим регулирующих функций, осуществляемых даже на разовой основе, при выполнении официальных полномочий в случаях, указанных в пунктах (c), (d) и (e);

(g) защиты субъекта данных или прав и свобод других лиц.

2. С учетом адекватных правовых гарантий, в частности того, что данные не используются для принятия мер или решений в отношении любого конкретного физического лица, государства - участники вправе в случае, когда явно отсутствует риск нарушения тайны частной жизни субъекта данных, ограничивать путем законодательных мер права, предусмотренные в статье 12, когда данные обрабатываются исключительно в целях научных исследований или хранятся в персональной форме в течение срока, который не превышает срок, необходимый исключительно с целью формирования статистики.

Раздел VII.
Право субъекта данных заявлять возражения

Статья 14.
Право субъекта данных возражать

Государства - участники предоставят субъекту данных право:

(a) как минимум, в случаях, указанных в статье 7 (e) и (f), возражать в любое время по неопровержимым законным основаниям, относящимся к его ситуации, против касающейся его обработки данных, за исключением случаев, когда иное предусмотрев национальным законодательством. В случаях, когда имеются оправданные возражения вызванная контролером обработка больше не может вовлекать эти данные;

(b) возражать, по своему запросу и безвозмездно, против обработки касающихся; его персональных данных, которые, как этого ожидает контролер, обрабатываются целях прямого маркетинга, или быть проинформированным до того, как персональных данные впервые раскрываются третьим лицам или используются от их имени в целях прямого маркетинга, а также получать на безвозмездной основе прямое предложение права возражать против такого раскрытия персональных данных или их использования.

Государства - участники предпримут необходимые меры для гарантии того, чтобы субъекты данных осведомлялись о наличии права, указанного в первом абзаце пункта (b).

Статья 15.
Автоматические индивидуальные решения

1. Государства - участники предоставят каждому лицу право не быть подчиненным решению, которое порождает касающиеся его правовые последствия или существенно его затрагивает, основанному исключительно на автоматической обработке данных, предназначенной для оценки некоторых касающихся его персональных аспектов, например выполнения работы, кредитоспособности, надежности, поведения и т.д.

2. С учетом других статей настоящей Директивы, государства - участники предусматривают, что на лицо может распространяться решение указанного в части 1 типа, если это решение:

(a) принимается в ходе заключения или исполнения договора, при условии, что запрос о заключении или исполнении договора, направленный субъектом данных, был удовлетворен, или что существуют приемлемые меры для защиты его законных интересов, такие как соглашения, позволяющие ему выражать свою точку зрения; или

(b) санкционируется законом, который также предусматривает меры по защите законных интересов субъекта данных.

Раздел VIII.
Конфиденциальность и безопасность обработки

Статья 16.
Конфиденциальность обработки.

Любое лицо, действующее в соответствии с полномочиями контролера или оператора, включая самого оператора, которое имеет доступ к персональным данным, не должно их обрабатывать иначе, чем по инструкциям контролера, если только это не требуется от него законом.

Статья 17.
Безопасность обработки

1. Государства — участники обеспечивают, что контролер должен реализовать соответствующие технические и организационные меры по защите персональных данных от случайного или незаконного разрушения или случайных утраты, изменения, несанкционированного разглашения или доступа, в частности, когда обработка вовлекает передачу данных по сети, а также от всех других незаконных форм обработки.

Принимая во внимание уровень технической мысли и стоимость реализации, такие технические и организационные меры должны гарантировать уровень безопасности, соответствующий рискам, создаваемым обработкой и характером защищаемых данных.

2. Государства - участники обеспечивают, что контролер в случае осуществления обработки от своего имени должен избирать оператора, предоставляющего достаточные гарантии в отношении мер технической безопасности и организационных мер, регулирующих осуществление обработки, а также должен обеспечить соблюдения таких мер.

3. Осуществление обработки силами оператора должно регулироваться договором или правовым актом, обязывающим оператора в отношении контролера и предусматривающим, в частности, что:

- оператор действует только согласно инструкциям контролера,
- обязательства, изложенные в части 1, как это определено правом государства -участника, в котором образован оператор, должны также лежать на операторе.

4. В целях сохранения доказательств, части договора или юридического акта, катающегося защиты данных и требований, касающихся мер, указанных в части 1, должны быть в письменной форме или в другой аналогичной форме.

Раздел IX.
Уведомление

Статья 18.
Обязательства уведомлять надзорный орган

1. Государства- участники обеспечивают, что контролер или, при наличии, его представитель, должен уведомлять надзорный орган, указанный в статье 28, до осуществления в целом или части любой автоматической операции по обработке или серии таких операций, предназначенных служить единственной цели или нескольким связанным целям.

2. Государства - участники вправе предусмотреть возможность упрощения уведомления или его исключение только в следующих случаях и на следующих условиях:

- когда в отношении категории операций обработки, которые, принимая во внимание обрабатываемые данные, вероятно не затронут негативным образом права и свободы субъекта данных, государства - участники предусматривают цели обработки, данные или категории данных, подвергающиеся обработке, категорию или категории субъектов данных, получателей или категории получателей, которым раскрываются данные и продолжительность времени, в течение которого хранятся данные, и/или

- когда контролер, в соответствии с регулирующим его национальным правом назначает должностное лицо по защите персональных данных, ответственное, в частности:

- за обеспечение, на независимой основе, внутреннего применения национальных норм, принятых в соответствии с настоящей Директивой,

- за ведение реестра операций обработки, осуществляемых контролером, содержащего статьи информации, указанной в статье 21 (2),

таким образом обеспечивая, что права и свободы субъектов данных вероятно не будут затронуты негативным образом операциями обработки.

3. Государства - участники вправе предусмотреть то, что часть 1 не применяется к обработке, чьей единственной целью является ведение реестра, который согласно законам или правовым актам предназначен для публичного предоставления информации и открытым для публичного обращения в целом или обращения любым лицом, демонстрирующим законный интерес.

4. Государства - участники вправе предусмотреть исключение из обязательства по уведомлению или упрощение уведомления в случае операций обработки, указанных в статье 8 (2) (1).

5. Государства - участники вправе предусмотреть то, что об определенных или всех неавтоматических операциях обработки, вовлекающих персональные данные, должно направляться уведомление, или предусмотреть то, что эти операции обработки в качестве подлежащих упрощенному уведомлению.

Статья 19.
Содержание уведомления

1. Государства — участники устанавливают требования к информации, представляемой в уведомлении. Она должна включать в себя, как минимум:

(a) наименование и адрес контролера и, при наличии, его представителя;

(b) цель или цели обработки;

(c) описание категории или категорий субъектов данных и касающихся их данных или категорий данных;

(d) получатели или категории получателей, которым могут раскрываться данные;

(e) предполагаемая передача данных третьим странам;

(f) общее описание, обеспечивающее возможность предварительной оценки, проводимой на предмет приемлемости мер, принимаемых в соответствии со статьей 17 в целях обеспечения безопасности обработки.

2. Государства - участники устанавливают процедуры, с использованием которых о любом изменении, затрагивающем информацию, указанную в части 1, должен уведомляться надзорный орган.

Статья 20.
Предварительная проверка

1. Государства - участники определяют операции обработки, которые вероятно представляют определенные риски правам и свободам субъектов данных, и проверяют, чтобы эти операции обработки изучались до их начала.

2. Такие предварительные проверки должны осуществляться надзорным органом после получения уведомления от контролера или должностным лицом по защите данных, который, в случае сомнения, должен консультироваться с надзорным органом.

3. Государства - участники также могут осуществлять такие проверки в контексте подготовки мер национального парламента либо мер, основанных на таких законодательных мерах, которые определяют характер обработки и устанавливают соответствующие гарантии.

Статья 21.
Предание публичности операциям обработки

1. Государства - участники предпринимают меры с тем, чтобы гарантировать публичность операций обработки.

2. Государства - участники предусматривают, что надзорным органом ведется реестр операций обработки, в отношении которых направлены уведомления в соответствии со статьей 18.

Реестр должен содержать, как минимум, информацию, перечисленную в статье 19(1) (a) -(e).

Реестр может изучаться любым лицом.

3. Государства - участники обеспечивают в отношении операций обработки, не подлежащих уведомлению, чтобы контролеры или иные организации, назначенные государствами - участниками, делали доступной, как минимум, информацию, указанную в статье 19(1) (a)- (e), в приемлемой форме любому лицу по его запросу.

Государства - участники вправе предусмотреть то, что это положение не применяется к обработке, чьей единственной целью является ведение реестра, который согласно законам или правовым актам предназначен для публичного предоставления информации и является открытым для публичного обращения в целом или любым лицом, которое может предоставить доказательство законного интереса.

Глава III.
Судебная защита, ответственность и санкции

Статья 22.
Средства правовой защиты

Без ущерба для любых административных средств, в отношении которых могут быть приняты правовые нормы, *inter alia*, в отношении надзорных органов, указанных в статье 28, при обращении к ним до судебных органов, государства - участники предусматривают право каждого лица на судебную защиту от любого нарушения прав, гарантированных ему национальным правом, применимым к рассматриваемой обработке.

Статья 23.
Ответственность

1. Государства - участники предусматривают то, что любое лицо, которое понесло ущерб в результате незаконной операции обработки или любого действия, несовместимого с национальными нормами, принятыми в соответствии с настоящей Директивой, имеет право на получение компенсации от контролера за понесенный ущерб.

2. Контролер может быть освобожден от ответственности полностью или частично, если докажет, что он не отвечает за случай, вызвавший ущерб.

Статья 24.
Санкции

Государства - участники принимают соответствующие меры, чтобы обеспечить полное выполнение положений настоящей Директивы и, в частности, устанавливают санкции, которые налагаются в случае нарушения норм, принятых в соответствии с настоящей Директивой.

Глава IV.
Передача персональных данных третьим странам

Статья 25.
Принципы

1. Государства - участники обязаны предусмотреть, что передача третьим странам персональных данных, проходящих обработку или предназначаемых к обработке после передачи, может иметь место, без ущерба для соблюдения национальных норм, принятых в соответствии с другими положениями настоящей Директивы, только если данная третья страна обеспечивает достаточный уровень защиты.

2. Достаточность уровня защиты, предоставляемой третьей страной, должна оцениваться в свете всех обстоятельств, сопровождающих операцию передачи данных или их серию; особому рассмотрению должны подвергаться характер данных, цели и продолжительность предполагаемой операции или операций обработки, страна начала операции и страна окончательного назначения, правовые нормы, общие и специальные, действующие в рассматриваемой третьей стране, а также профессиональные правила и меры безопасности, соблюдаемые в этой стране. :

3. Государства - участники и Комиссия информируют друг друга о случаях, при которых, как они полагают, третья страна не обеспечивает достаточный уровень защиты в значении части 2. 4. В случае, когда Комиссия решает в соответствии с процедурой, предусмотренной в статье 31(2), что третья страна не обеспечивает достаточный уровень защиты в значении части 2 настоящей статьи, государства - участники предпринимают меры, необходимые для предотвращения любой передачи данных того же типа, что передаются рассматриваемой третьей стране. , 5. В надлежащее время Комиссия вступает в переговоры с целью исправления ситуации, возникшей в результате решения, принятого в соответствии с частью 4.

6. Комиссия вправе решить в соответствии с процедурой, указанной в статье 31(2), что третья страна обеспечивает достаточный уровень защиты в значении части 2 настоящей статьи в силу ее внутреннего права или международных обязательств, которые она приняла, в частности, после завершения переговоров, указанных в части 5, о защите частной жизни, основных свобод и прав физических лиц.

Государства - участники предпринимают меры, необходимые для выполнения решения Комиссии.

Статья 26.
Изъятия

1. Путем изъятия из статьи 25 и за исключением случаев, иным образом предусмотренных внутренним правом, регулирующим конкретные случаи, государства-участники обязаны предусмотреть то, что передача или серия передач персональных данных в третью страну, которая не обеспечивает достаточный уровень защиты персональных данных в значении статьи 25(2), может иметь место при условии, что:

(a) субъект данных недвусмысленно дал свое согласие на предполагаемую передачу; или

(b) передача необходима для исполнения договора между субъектом данных и контролером либо реализации преддоговорных мер, предпринимаемых в ответ на запроса субъекта данных; или (c) передача необходима для заключения или исполнения договора, заключаемого в интересах субъекта данных между контролером и третьим лицом; или

(d) передача необходима или юридически требуется по причине важности публичных интересов или возбуждения, реализации или защиты исковых требований; или

(e) передача необходима в целях защиты жизненных интересов субъекта данных или передача осуществляется из реестра, который в соответствии с законами или правовыми актами предназначен для публичного предоставления информации и открыт для публичного обращения в целом либо для обращения любым лицом, которое может продемонстрировать законный интерес, в той степени, в которой в конкретном случае выполняются условия, предусмотренные законом.

2. Без ущерба для части 1, государство-участник вправе разрешить передачу или серию передач персональных данных в третью страну, которая не обеспечивает достаточный уровень защиты в значении статьи 25(1), в случае, когда контролер демонстрирует достаточные гарантии в

отношении защиты неприкосновенности частной жизни и основных прав и свобод физических лиц, а также в отношении реализации соответствующих прав; гарантии могут, в частности, вытекать из соответствующих договорных условий.

3. Государства - участники информируют Комиссию и другие государства-участники о разрешениях, которые они представляют согласно части 2.

Если государство-участник или Комиссия возражают против оправдывающих разрешение причин, затрагивающих вопросы защиты неприкосновенности частной жизни и основных прав и свобод физических лиц, Комиссия должна предпринять соответствующие меры в соответствии с процедурами, изложенными в статье 31(2).

Государства - участники должны предпринимать необходимые меры в целях соответствия решениям Комиссии.

4. В случае, если Комиссия решит, в соответствии с процедурами, указанными в статье 31 (2), что определенные договорные условия предлагают достаточные гарантии, требуемые частью 2, государства — участники должны предпринять необходимые меры в целях выполнения решений Комиссии.

Глава V.
Кодексы поведения

Статья 27

1. Государства - участники и Комиссия должны поощрять разработку кодексов поведения, предназначенных для содействия надлежащей имплементации национальных норм, принятых государствами-участниками в соответствии с настоящей Директивой, принимая во внимание специфические признаки различных секторов.

2. Государства - участники должны принимать нормы для торговых ассоциаций и других организаций, представляющих другие категории контролеров, которые разрабатывают национальные кодексы или которые намереваются изменять или дополнять существующие национальные кодексы, в целях обеспечения возможности их представления для получения мнения национальных органов.

Государства - участники должны принимать нормы для данных органов в целях удостоверения того, среди прочего, представляются ли проекты кодексов в соответствии с национальными нормами, принятыми согласно настоящей Директивы. Если это представляется приемлемым, органы должны стремиться знакомиться со взглядами субъектов данных или их представителей.

3. Проекты кодексов Сообщества, изменения или дополнения существующих кодексов Сообщества, могут представляться Рабочей группе, указанной в статье 29. Данная Рабочая группа должна установить, среди прочего, соответствуют ли представленные ей проекты кодексов национальным нормам, принятым согласно настоящей Директиве. Если это представляется приемлемым, данный орган должен стремиться знакомиться со взглядами субъектов данных или их представителей. Комиссия может обеспечивать соответствующую публичность для кодексов, одобренных Рабочей группой.

Глава VI.
Надзорный орган и рабочая группа по защите, физических лиц в отношении обработки персональных данных

Статья 28.
Надзорный орган

1. Каждое государство-участник обеспечивает, чтобы один или более публичных органов отвечали за контроль применения на своей территории норм, принятых государствами - участниками согласно настоящей Директиве.

Данные органы действуют на основе принципа полной независимости при выполнении возложенных на них функций.

2. Каждое государство-участник обеспечивает, чтобы надзорные органы проводили консультации при подготовке административных мер или разработке правовых актов, касающихся защиты прав и свобод физических лиц в отношении обработки персональных данных.

3. Каждый орган должен, в частности, быть наделен:

- полномочиями по расследованию, такими, как право доступа к данным, образующим предмет операций обработки, и полномочиями по сбору всей информации, необходимой для выполнения своих надзорных обязанностей;

- эффективными полномочиями по вмешательству, такими, как, например, право предоставления мнения до начала осуществления операций обработки данных согласно статье 20 и обеспечения соответствующей публикации такого мнения, право давать указания блокировать, стирать или уничтожать данные, право введения временного или окончательного запрета на обработку, право предупреждения или предостережения контролера либо право постановки вопроса перед национальными парламентами или иными политическими учреждениями;

- полномочиями возбуждать судебное производство в случае, когда были нарушены нормы, принятые в соответствии с настоящей Директивой, или передавать данные нарушения на рассмотрение судебным органам.

На решения надзорного органа, которые вызывают жалобы, может подаваться апелляция в судебном порядке.

4. Каждый надзорный орган должен рассматривать требования, заявленные любым лицом или ассоциацией, представляющей данное лицо, касающиеся защиты их и свобод в отношении обработки персональных данных. Заинтересованное лицо должно быть проинформировано о результатах рассмотрения требования.

Каждый надзорный орган должен, в частности, рассматривать требования о проверке законности обработки данных, заявленные любым лицом в случае, когда применяются национальные правовые нормы, принятые в соответствии со статьей 13 настоящей Директивы. Данное лицо, во всяком случае, должно быть проинформировано о том, что проверка имела место.

5. Каждый надзорный орган должен готовить отчет о своей деятельности на регулярной основе. Отчет должен быть публично доступным.

6. Каждый надзорный орган является компетентным, что бы ни предусматривало национальное законодательство, применимое к рассматриваемой обработке данных, реализовывать на территории своего собственного государства - участника полномочия, возлагаемые на него в соответствии с частью 3. Каждый орган может запрашиваться о реализации своих полномочий органом другого государства - участника.

Надзорные органы должны сотрудничать друг с другом в размере, необходимом для выполнения своих обязанностей, в частности, путем обмена всей полезной информацией.

7. Государства — участники обязаны предусмотреть, что на членов и персонал надзорного органа, даже после прекращения ими трудовых отношений, распространяется обязанность профессиональной тайны в отношении конфиденциальной информации, к которой они имеют доступ.

Статья 29.

Рабочая группа по защите физических лиц в отношении обработки персональных данных

1. Настоящим учреждается Рабочая группа по защите физических лиц в отношении обработки персональных данных, далее именуемая «Рабочая группа». Она будет иметь совещательный статус и действовать независимо.

2. Рабочая группа образуется из представителя надзорного органа или органов, назначенных каждым государством-участником, и представителя органа или органов, созданных учреждениями и органами, а также представителя Комиссии.

Каждый член Рабочей группы назначается учреждением, органом или органами, которые он представляет. В случае, когда государства - участники назначают более одного надзорного органа, эти органы делегируют совместного представителя. Аналогичное применяется к органам, созданным учреждениями и организациями Сообщества.

3. Рабочая группа принимает решения простым большинством голосов представителей надзорных органов.

4. Рабочая группа избирает своего председателя. Срок полномочий председателя составляет два года. Его назначение должно возобновляться.

5. Секретариат Рабочей группы обеспечивается Комиссией.

6. Рабочая группа утверждает собственные процедурные правила.

7. Рабочая группа рассматривает вопросы, включенные в повестку председателем, либо по

собственной инициативе или по просьбе представителя надзорных органов либо по просьбе Комиссии.

Статья 30

1. Рабочая группа должна:

(a) изучать любые вопросы, охватывающие проведение национальных мероприятий, утвержденных согласно настоящей Директивы, в целях способствовать единообразному проведению таких мероприятий;

(b) направлять Комиссии мнение об уровне защиты в Сообществе и третьих странах;

(c) консультировать Комиссию по любым предлагаемым изменениям настоящей Директивы, любым дополнительным или специальным мероприятиям в целях охраны прав и свобод физических лиц в отношении обработки персональных данных, а также любым другим предлагаемым мероприятиям Сообщества, затрагивающим такие права и свободы;

(d) направлять мнение по кодексам поведения, разработанным на уровне Сообщества.

2. Если Рабочая группа обнаружит, что эти отклонения, которые вероятно затронут равенство в защите лиц в отношении обработки персональных данных в Сообществе, возникают между законодательством или практикой государств - участников, она должна, соответственно, информировать об этом Комиссию.

3. Рабочая группа имеет право, по своей инициативе, принимать рекомендации по всем вопросам, касающимся защиты лиц в отношении обработки персональных данных в Сообществе.

4. Мнения и рекомендации Рабочей группы направляются Комиссии и комитету, указанному в статье 31.

5. Комиссия информирует Рабочую группу о действиях, которые она предпримет в ответ на ее мнение и рекомендации. Комиссия делает это в отчете, который также направляется Европейскому Парламенту и Совету. Отчет должен делаться публично доступным.

6. Рабочая группа готовит ежегодный отчет о ситуации в области защиты физических лиц в отношении обработки персональных данных в Сообществе и третьих странах, который передается Комиссии, Европейскому Парламенту и Совету. Отчет должен быть публично доступным.

Глава VII.
Имплементационные меры Сообщества
Статья 31.
Комитет

1, Комиссии должно оказываться содействие комитетом, формируемым из представителей государств — участников и возглавляемым представителем Комиссии.

2. Представитель Комиссии представляет комитету проект мер, подлежащих 1 принятию. Комитет предоставляет свое мнение по данному проекту в течение периода времени, который может установить председатель в соответствии со степенью важности вопросов.

Мнение предоставляется большинством голосов, указанным в статье 148 (2) Договора. Голоса представителей государств - участников в комитете учитываются способом, указанным в данной статье. Председатель права голоса не имеет.

Комиссия утверждает меры, которые применяются незамедлительно. Вместе с тем, если данные меры противоречат мнению комитета. Комиссия незамедлительно сообщает о них Совету. В этом случае:

- Комиссия должна отложить применение мер, в отношении которых она приняла решение, на период в три месяца, начиная с даты сообщения;

- Совет квалифицированным большинством голосов вправе принять отличное решение в течение времени, указанного в первом абзаце.

Заключительные положения
Статья 32

1. Государства - участники должны ввести в действие законы, правовые акты и административные нормы, необходимые для того, чтобы соответствовать требованиям настоящей Директивы, как минимум, по истечении трехлетнего срока с даты её принятия.

В случае принятия государствами - участниками данных документов, они должны содержать

ссылку на настоящую Директиву или сопровождаться такой ссылкой. при их официальной публикации. Способы выполнения таких ссылок устанавливаются государствами-участниками.

2. Государства - участники гарантируют, что обработка данных, которая уже; осуществляется на дату вступления в силу национальных правовых норм, принятых в соответствии с настоящей Директивой, приводится в соответствие с данными правовыми нормами в течение трех лет с даты их вступления в силу.

Путем изъятия из предшествующей части государства - участники вправе предусмотреть, что обработка данных, которая уже осуществляется в системах с ручной . регистрацией на дату вступления в силу национальных правовых норм, принятых в: целях имплементации настоящей Директивы, должны быть приведены в соответствие ; со статьями 6, 7 и 8 настоящей Директивы в течение 12 лет с даты их принятия. Вместе с тем государства - участники должны представлять субъектам данных по их запросу и, в частности, во время реализации права доступа к данным, право на исправление, стирание или блокирование данных, которые являются неполными, неточными или хранятся способом, несовместимым с правомерными целями, преследуемыми контролером.

3. Путем отступления от части 2, государства - участники вправе предусмотреть, при условии приемлемых гарантий, что данные, которые хранятся исключительное целях исторических исследований, не обязаны приводиться в соответствие со статьями 6, 7 и 8 настоящей Директивы.

4. Государства - участники сообщают Комиссии тексты норм национального законодательства, которое они примут в сфере, охватываемой настоящей Директивой.

Статья 33

Комиссия должна с регулярной периодичностью отчитываться перед Советом и Европейским парламентом, начиная не позднее чем через три года с даты, указанной в статье 32 (1), об имплементации настоящей Директивы, прилагая к своему отчету, при необходимости, уместные предложения об изменениях. Отчет должен делаться публично доступным.

Комиссия изучает, в частности, применение настоящей Директивы к обработке данных в форме звуков и образов, имеющих отношение к физическим лицам, и представлять любые уместные предложения, которые оказываются необходимыми, принимая во внимание развитие информационных технологий, а также в свете состояния прогресса информационного общества.

Статья 34

Настоящая Директива адресуется государствам - участникам.

Додаток 20. Директива 97/5/ЕС Европейского парламента и Совета от 27 января 1997 г. о трансграничных кредитовых переводах

(Извлечения)

Раздел I.
Прозрачность условий трансграничных кредитовых переводов

Статья 3.
Предварительная информация об условиях трансграничных кредитовых переводов

Учреждения обязаны предоставлять, включая, если возможно, посредством электронных средств, своим действительным и потенциальным клиентам информацию об условиях трансграничных кредитовых переводов в письменной и легко доступной для понимания форме. Данная информация должна включать в себя, как минимум:

- указание времени, необходимого для исполнения поручения трансграничного кредитового перевода, направленного учреждению, времени, необходимого для кредитования денежных средств на счет учреждения бенефициара; начало данного периода должно быть четко указано;

-указание времени, необходимого после получения трансграничного кредитового перевода для кредитования денежных средств, зачисленных на счет учреждения, Насчет бенефициара;

- способ определения любого комиссионного вознаграждения и сборов, подлежащих уплате клиентом учреждению, включая, если возможно, проценты;

- дату валютирования, если таковая есть, применяемую учреждением,

- подробное описание процедур обжалования и восстановления прав, предоставляемых клиенту и соглашения для доступа к ним;

- указание используемых базовых обменных курсов.

Статья 4.

Информация, предоставляемая после совершения трансграничного кредитового перевода

Учреждения обязаны предоставлять, включая, если возможно, посредством электронных средств, своим клиентам, если только последние явным образом не отказываются от этого, четкую информацию после совершения или получения трансграничного кредитового перевода в письменной и легко доступной для понимания форме. Данная информация должна включать в себя, как минимум:

- данные, позволяющие клиенту идентифицировать трансграничный кредитовый перевод;
- первоначальный размер трансграничного кредитового перевода;
- размер всех сборов и комиссионных вознаграждений, подлежащих уплате клиентом;
- дату валютирования, если таковая есть, применяемую учреждением.

В том случае, если инициатором установлено, что сборы за трансграничный кредитовый перевод полностью или частично относятся на счет бенефициара, последний должен быть об этом проинформирован его собственным учреждением.

В том случае, если любая сумма конвертировалась, учреждение, которое осуществляло конверсию, обязано проинформировать своего клиента об использованном обменном курсе.

Додаток 21. Директива 97/7/ЕС Европейского парламента и Совета от 20 мая 1997 г. о защите потребителей в отношении дистанционных договоров (дистанционная продажа)

ЕВРОПЕЙСКИЙ ПАРЛАМЕНТ И СОВЕТ,

принимая во внимание Договор, учреждающий Европейское сообщество и, в частности, статью 100 a,

принимая во внимание предложение Комиссии, принимая во внимание мнение Экономического и социального комитета, действуя в соответствии с процедурой, изложенной в ст. 189b Договора, в свете совместного текста, одобренного Согласительным комитетом 27 ноября 1996 г.,

(ТЕКСТ ПРЕАМБУЛЫ)

ПРИНЯЛИ НАСТОЯЩУЮ ДИРЕКТИВУ

Статья 1.

Цель

Целью настоящей Директивы является сблизить законы, правила и административные нормы государств - участников, касающиеся дистанционных договоров между потребителями и поставщиками.

Статья 2.

Определения

В целях настоящей Директивы:

(1) «дистанционный договор» означает любой, договор, касающийся товаров или услуг, заключаемый между поставщиком и потребителем в рамках схемы организованной дистанционной продажи или оказания услуг, управляемой поставщиком, который, в целях договора, осуществляет исключительное использование одного или более средств дистанционных коммуникаций до и включая момент, в который заключается договор;

(2) «потребитель» означает любое физическое лицо, которое в договоре, охватываемом настоящей Директивой, действует в целях, которые не связаны с его торговлей, бизнесом или профессией;

(3) «поставщик» означает любое физическое или юридическое лицо, которое в договоре, охватываемом настоящей Директивой, действует в рамках своей коммерческой или профессиональной правоспособности;

(4) «средства дистанционных коммуникаций» - любые средства, которые без одновременного физического присутствия поставщика и потребителя, могут быть использованы для заключения договора между этими сторонами. Примерный перечень средств, охватываемых настоящей Директивой, содержится в приложении ;

(5) «оператор средств коммуникаций» означает любое государственное или частное юридическое или физическое лицо, чьи торговля, бизнес или профессия предполагают предоставление поставщикам одного или более средств дистанционных коммуникаций.

Статья 3.
Изъятия

1. Настоящая Директива не применяется к договорам:

- касающимся финансовых услуг, открытый перечень которых приведен в приложении II;
- заключаемым с использованием автоматических торговых машин или автоматизированных коммерческих мест;
- заключаемым с телекоммуникационными операторами посредством использования публичных платных телефонов;
- заключаемым на строительство и продажу недвижимого имущества или касающимся иных прав на недвижимое имущество, исключая аренду;
- заключаемых на аукционе.

2. Статьи 4, 5,6 и 7(1) не применяются:

- к договорам на поставку продуктов питания, напитков или иных товаров, предназначенных для ежедневного потребления, поставляемых потребителю на дом, по его месту жительства или на его рабочее место постоянным торговым агентом;
- к договорам об оказании жилищных, транспортных услуг, услуг общественного питания и сферы досуга, в том случае, когда поставщик обязуется при заключении договора оказывать такие услуги на определенную дату или в течение определенного срока; за исключением случая проведения уличных развлекательных мероприятий, когда поставщик может сохранить за собой право не применять статью 7(2) при определенных обстоятельствах.

Статья 4.
Предварительная информация

1. Заблаговременно до заключения любого дистанционного договора, потребителю должна быть предоставлена следующая информация:

(a) о личности поставщика и, в случае договоров, требующих авансового платежа, его адрес;

(b) об основных характеристиках товаров или услуг;

(c) о цене товаров или услуг, включая все налоги;

(d) о стоимости доставки, когда это приемлемо;

(e) об условиях платежа, доставки или исполнения;

(f) о наличии права отказа от исполнения, за исключением случаев, указанных в статье 6(3);

(g) о стоимости использования средств дистанционных коммуникаций, когда она рассчитывается иначе, чем по базовой ставке;

(h) о сроке, в течение которого оферта или цена остаются действительными;

(i) когда это приемлемо, о минимальной продолжительности договора - в случае договоров на поставку продуктов или услуг, исполняемых постоянно или на возобновляющейся основе.

2. Информация, указанная в части 1, коммерческая щель которой должна четко, определяться, должна предоставляться ясным и понятным способом, в любом случае соответствующим используемым средствам дистанционных коммуникаций с должным вниманием, в частности, к принципам добросовестности в коммерческих сделках и принципам, регулирующим защиту недееспособных в соответствии с законодательством государств - участников, таких как несовершеннолетние, для получения их 1 согласия.

3. Кроме того, в случае телефонной связи личность поставщика и коммерческая цель звонка должны четко определяться явно выраженным образом в начале любого разговора с потребителем.

Статья 5.
Письменное подтверждение информации

1. Потребитель должен получать письменное подтверждение или подтверждение с использованием иных имеющихся у него и доступных средств длительного применения в отношении

информации, указанной в статье 4(1) (a) -(f), заблаговременно в течение исполнения договора и, самое позднее, во время доставки, когда товары не предназначаются для поставки заинтересованным третьим лицам, если только формация не была уже передана потребителю до заключения договора в письменной форме или с использованием иных имеющихся у него и доступных средств длительного применения.

В любом случае должно предоставляться следующее:

- письменная информация об условиях и процедурах реализации права отказа от исполнения в значении статьи 6, включая случаи, указанные в первом абзаце статьи 6(3);

-географический адрес коммерческого предприятия-поставщика, по которому потребитель может адресовать любые жалобы;

- информация о существующем послепродажном обслуживании и гарантиях;

- положение о прекращении договора в случае, когда он заключен на неопределенный срок или на срок, превышающий один год.

2. Часть 1 не применяется к услугам, исполнение которых производится с использованием средств дистанционных коммуникаций в случае, когда они оказываются только на разовой основе и счета по ним выставляются оператором средств дистанционных коммуникаций. Несмотря на это, потребитель должен во всех случаях быть способен получать географический адрес коммерческого предприятия поставщика, по которому он может адресовать любые жалобы.

Статья 6.

Право отказа от исполнения

1. В отношении любого дистанционного договора у потребителя должен иметься срок, как минимум, в семь рабочих дней, в течение которого он вправе отказаться от исполнения договора без штрафа и объяснения любых причин. Только непосредственная стоимость возврата товаров может взиматься с потребителя за реализацию своего права отказа от исполнения. Срок реализации данного права начинается:

- в случае товаров - со дня получения потребителем, когда были исполнены обязательства, изложенные в статье 5;

- в случае услуг - со дня заключения договора или со дня, в который были исполнены обязательства, изложенные в статье 5, и если они исполняются после заключения договора, при условии, что этот период не превышает трехмесячного срока, указанного в следующем абзаце данной части.

Если поставщик не исполняет обязательства, изложенные в статье 5, срок составляет три месяца. Срок начинается:

- в случае товаров - со дня получения потребителем;

- в случае услуг - со дня заключения договора. Если информация, указанная в статье 5, предоставляется в течение этого трехмесячного срока, то семь рабочих дней, указанных в первом абзаце данной части, начинаются, считая с этого момента.

2. В случае, когда потребителем в соответствии с настоящей статьей реализуется. право отказа от исполнения, поставщик обязан возместить суммы, уплаченные потребителям, без расходов со стороны последнего. Только непосредственная стоимость возврата товаров может взиматься с потребителя за реализацию своего права отказа от исполнения. Такое возмещение должно производиться как можно скорее и, в любом случае, в течение 30 дней.

3. Если стороны не договорились об ином, потребитель не может реализовывать право отказа от исполнения, предусмотренное в части 1, в отношении договоров:

- оказания услуг, если исполнение началось по соглашению с потребителем до истечения срока в семь рабочих дней, указанного в части 1;

- поставки товаров или услуг, цены которых зависят от колебаний на финансовом рынке, который не может контролироваться поставщиком;

- поставки товаров, произведенных по спецификации потребителя или явно для него персонализированных, которые по причине своей природы не могут быть возвращены или являются скоропортящимися или имеют ограниченный срок использования;

- поставки аудио, видеозаписей или компьютерного программного обеспечения, упаковка которых была нарушена потребителем;

- поставки газет, периодических изданий и журналов;

- оказания игорных и лотерейных услуг.

4. Государства - участники предусматривают в своем законодательстве нормы в делях обеспечения того, чтобы:

- в случае, если цена товаров или услуг полностью или частично покрывается кредитом, предоставленным поставщиком, или

- в случае, если цена полностью или частично покрывается кредитом, предоставляемым потребителю третьим лицом на основании соглашения между третьим лицом и поставщиком,

кредитное соглашение расторгалось без любого штрафа, если потребитель реализует свое право отказа от исполнения в соответствии с частью 1.

Государства - участники устанавливают подробные правила для расторжения кредитного соглашения.

Статья 7.
Исполнение

1. Если стороны не договорились об ином, поставщик должен исполнить заказ, максимум, в течение 30 дней, начиная со дня, следующего за днем, в который потребитель направил свой заказ поставщику.

2. В случае, когда поставщик со своей стороны не исполняет договор по причине недоступности заказанных товаров и услуг, потребитель должен быть информирован 106 этой ситуации и вправе получить возмещение любых сумм, которые он уплатил, как можно скорее, но, в любом случае, в течение 30 дней.

3. Несмотря на это государства - участники могут предусмотреть, что постав-1щик может предоставить потребителю товары или услуги равного качества и по равной цене, при условии, что такая возможность была предоставлена до заключения договора или в договоре. Потребитель должен быть проинформирован об этой возможности ясным и понятным образом. Расходы по возврату товаров, следующего за реализацией права на отказ от исполнения, должны в этом случае относиться на счет поставщика и потребитель должен быть проинформирован об этом. В таких случаях поставка товаров или услуг не может рассматриваться как образующая инерционную продажу в значении статьи 9.

Статья 8.
Платеж картой

Государства - участники обеспечивают наличие достаточных мер, позволяющих потребителю:

-требовать аннулирования платежа в случае, если производилось мошенническое использование его платежной карты в связи с дистанционными договорами, охватываемыми настоящей Директивой;

- в случае мошеннического использования - восстановления или возврата уплаченных сумм.

Статья 9.
Инерционные продажи

Государства - участники должны принимать меры, необходимые для того, чтобы:

- запретить поставку товаров или услуг потребителю без того, чтобы они были предварительно заказаны потребителем, в случае, когда такая поставка включает требование платежа;

- изъять потребителей из действия норм о любом встречном удовлетворении в случаях инициативной поставки, при этом отсутствие ответа не образует согласия.

Статья 10.
Ограничения на использование определенных средств дистанционных коммуникаций

1. Использование поставщиком следующих средств требует предварительного согласия потребителя:

- автоматических вызывающих систем без человеческого вмешательства (автоматических вызывающих машин);

- факсимильных машин (факсов).

2. Государства - участники обеспечивают, чтобы средства дистанционных коммуникаций, за

исключением указанных в части 1, которые позволяют индивидуальную связь, могли использоваться только при отсутствии явного возражения со стороны потребителя.

Статья 11.
Судебное или административное восстановление прав

1. Государства - участники обеспечивают наличие достаточных и эффективных средств, чтобы гарантировать соблюдение настоящей Директивы в интересах потребителей.

2. Средства, указанные в части 1, включают нормы, согласно которым один или более из следующих органов, как это установлено национальным правом, могут предъявлять согласно национальному праву иски в суды или уполномоченные административные органы для обеспечения того, чтобы национальные нормы, требуемые для имплементации настоящей Директивы, применялись:

(a) государственными органами или их представителями;

(b) потребительскими организациями, имеющими законные интересы по защите прав потребителей;

(c) профессиональными организациями, имеющими законные интересы для такого действия.

3. (a) Государства - участники могут предусмотреть, что бремя доказывания, касающееся наличия предварительной информации, письменного подтверждения, соответствия с временными рамками и согласия потребителя, может быть возложено на поставщика.

(b) Государства - участники должны принять меры, необходимые для обеспечения того, чтобы поставщики и операторы средств дистанционных коммуникаций, в случае, если они способны это сделать, прекратили практику, которая не соответствует мерам, принятым в соответствии с настоящей Директивой;

4. Государства - участники могут предусмотреть добровольный надзор со стороны саморегулируемых органов на предмет соответствия положениям настоящей Директивы и обращение к таким органам за помощью в разрешении споров, допол- 1 нительно к средствам, которые могут предусмотреть государства - участники с тем, ' чтобы обеспечить соответствие положениям настоящей Директивы.

Статья 12.
Обязательный характер

1. Потребитель не может отказаться от прав, предоставляемых ему путем включения настоящей Директивы в национальное законодательство.

2. Государства - участники должны принимать меры, необходимые для обеспечения того, чтобы потребители не утрачивали защиту, предоставляемую настоящей Директивой в силу выбора права государства, не являющегося участником, в качестве права, применимого к договору, если последний имеет тесную связь с территорией одного или более государств - участников.

Статья 13.
Правила Сообщества

1. Положения настоящей Директивы применяются постольку, поскольку отсутствуют специальные нормы в правилах права Сообщества, регулирующие отдельные типы дистанционных договоров в их целостности.

2. В случае, когда специальные правила Сообщества содержат нормы, регулирующие только отдельные аспекты поставки товаров или услуг, такие нормы применяются вместо положений настоящей Директивы к таким частным аспектам дистанционных договоров.

Статья 14.
Оговорка о минимальном уровне защиты.

Государства - участники могут принимать или поддерживать в сфере, охватываемой настоящей Директивой, более строгие нормы, совместимые с Договором, чтобы обеспечивать более высокий уровень защиты прав потребителей. Такие нормы должны, когда это приемлемо, включать, с должным вниманием к Договору, запрет с точки зрения общих интересов на маркетинг определенных товаров или услуг, в частности, медицинских продуктов на своей территории посредством дистанционных договоров.

Статья 15.
Имплементация

1. Государства - участники должны принять законы, правила и административные нормы, необходимые для того, чтобы соответствовать настоящей Директиве, не позднее трех лет после ее вступления в силу. Они должны незамедлительно информировать об этом Комиссию.

2. Когда государства - участники принимают документы, указанные в части 1, они должны содержать ссылку на настоящую Директиву или сопровождаться такой ссылкой в случае их официальной публикации. Процедура для таких ссылок должна определяться государствами - участниками.

3. Государства - участники должны сообщать Комиссии тексты основных норм национального законодательства, которое они принимают в сфере, регулируемой настоящей Директивой.

4. Не позднее четырех лет с вступления в силу настоящей Директивы Комиссия должна предоставить Европейскому парламенту и Совету отчет о применении настоящей Директивы, сопровождающийся, если необходимо, предложениями по ее пересмотру.

Статья 16.
Потребительская информация

Государства - участники должны принимать соответствующие меры для того, чтобы информировать потребителей о национальном законодательстве при включении настоящей Директивы в свое законодательство и поощрять, когда это приемлемо, профессиональные организации информировать потребителей о своих кодексах поведения.

Статья 17.
Системы обжалования

Комиссия должна изучить возможность создания эффективных средств работы с жалобами потребителей в отношении дистанционной продажи. В течение двух лет после вступления в силу настоящей Директивы Комиссия должна предоставить Европейскому парламенту и Совету отчет о результатах исследования, сопровождаемый, когда это приемлемо, предложениями.

Статья 18

Настоящая Директива вступает в силу со дня своей публикации в Официальном журнале Европейских сообществ.

Статья 19

Настоящая Директива адресуется государствам - участникам.

ПРИЛОЖЕНИЕ I

Средства коммуникаций, охватываемые статьей 2 (4):

- Безадресные печатные материалы
- Адресные печатные материалы
- Стандартное письмо
- Реклама в прессе с формой для заказа и
- Каталог
- Телефон с человеческим вмешательством
- Телефон без человеческого вмешательства (автоматические вызывающие машины, аудиотекст)
- Радио
- Видеофон (телефон с экраном)
- Видеотекст (экран микрокомпьютера и телевизора) с клавиатурой или тактильным экраном
- Электронная почта
- Факсимильная машина (факс)
- Телевидение (телепокупки).