УДК 336.339.92.71:681

ЦИМБАЛЮК І.В., науковий співробітник Науково-дослідного інституту інформатики і права НАПрН України

БЕЗПЕКА ЕЛЕКТРОННОЇ ТОРГІВЛІ (ОРГАНІЗАЦІЙНО-ПРАВОВИЙ АСПЕКТ)

Анотація. *Пропонуються до розгляду окремі результати дослідження правовідносин, пов’язаних з організацією безпеки електронної торгівлі. Визначаються підходи щодо подальшого правового регулювання безпеки електронної торгівлі в Україні у складі інформаційного законодавства.*

Ключові слова: *електронна торгівля, безпека, правове регулювання.*

Аннотация. *Предлагаются к рассмотрению отдельные результаты исследования правоотношений, связанных с организацией безопасности электронной торговли. Определяются подходы дальнейшего правового регулирования безопасности электронной торговли в Украине в составе информационного законодательства.*

Ключевые слова: *электронная торговля, безопасность, правовое регулирование.*

Summary. *The separate results of research of legal relationships related to organization of safety of electronic trade are offered to consideration. Approaches of the further legal adjusting of safety of electronic trade are determined in Ukraine in composition of informational legislation.*

Keywords: *electronic trade, security, legal adjusting.*

Постановка проблеми. В умовах розвитку інформаційного суспільства зростає роль такого його рушія як електронна торгівля. За сутністю торгівля із застосуванням Інтернет є важливим компонентом, що зумовлює значну долю фінансового забезпечення подальшого становлення інформаційного суспільства бізнесом.

Електронна торгівля у ідеальному варіанті знаходить вираз у купівлі-продажі із застосуванням Інтернет таких товарів і послуг як: програмне забезпечення комп’ютерів, електронні книжки, музика, кінофільми, банківські операції, операції з цінними паперами, аукціони, реклама, маркетингові дослідження, результати інших інформаційно-аналітичних, а також науково-дослідних і освітніх робіт (послуг) із застосуванням дистанційних технологій комунікації та інші аудіо- і відео продукти в електронній формі. Зазначене, у операційному аспекті, дозволяє оптимально, без великих затрат, пов’язаних із традиційним контактом фізичного переміщення сторін комерційних угод, її реалізовувати з економією часу.

До умовно окремого сегменту сучасної електронної торгівлі відносять також купівлю-продаж іншого майна із застосуванням Інтернет через так звані електронні крамниці (е-крамниці), електронні магазини (е-магазини). Розквіт електронної торгівлі речами пов’язується переважно із розвитком веб-технологій, а доставка речових товарів здійснюється споживачу безпосередньо у призначене ним місце, або споживач послуг завершує товарообмін (отримання товару і оплату за нього) безпосередньо у місці знаходження товару.

Переваги електронної торгівлі у порівнянні з традиційною оптовою і роздрібною торгівлею полягають у тому, що для її організації потрібно менше фінансових ресурсів. Економія здійснюється переважно на зменшенні затрат, пов’язаних із орендою чи будівництвом офісних приміщень, складських приміщень для зберігання товарів, а також на зменшені затрат, пов’язаних із обслуговуючим персоналом, затратами на комунальні послуги і т.д. [1].

За своєю природою суспільні відносини, пов’язані із електронною торгівлею, довгий час здійснювалися у приватноправовому полі із застосуванням аналогії права та аналогії закону без участі держави як регулятора, виходячи із технічних і технологічних можливостей Інтернет. У основі вказаного були принципи довіри, консенсусу, добрих звичаїв, традицій, дотримання норм суспільної моралі щодо виконання взятих сторонами зобов’язань. Публічно-правовий аспект електронної торгівлі здійснювався у межах цивільного права, цивільно-правових відносин.

Проте, як і будь-яке соціальне явище, що набуває масового суспільного прояву, і що пов’язане із науково-технічним прогресом, рано чи пізно стає об’єктом антисоціальних проявів, зловживань, діянь, що мають ознаки правопорушень, у тому числі злочинів. У зв’язку з цим виникає питання безпеки суспільних відносин. Це у повній мірі відноситься і до електронної торгівлі як соціально-технологічного явища, що набуло масового поширення і пов’язаного із здобутками науково-технічного прогресу у галузі інформатики та телематики.

У зв’язку з цим, щоб електронна торгівля як бізнес давала переважно позитивний суспільний ефект, потенційним учасникам її потрібно гарантувати відповідну безпеку, у тому числі від держави.

Аналіз досліджень, де започатковано розв’язання проблем безпеки електронної торгівлі, свідчить, що їх розв’язанню присвячено досить багато публікацій у різних організаційних аспектах: технічних, технологічних, соціально-етичних, адміністративних, правових, кримінологічних тощо. Серед них пропонується відзначити праці, пов’язані з електронною торгівлею, таких дослідників як: Л. Бабенко, В. Быков, О. Макаревич, О. Спиридонов [2]; Ф. Баско [3]; С. Бєлов, С. Мартиненко [4]; В. Брижко [5, 6], А. Новицький [7], О. Золотар [8] та інші.

У своїх дослідженнях автори звертають увагу переважно на опис різних потенційних та реальних ризиків загроз безпеки, що можна розглядати у аспекті і електронного бізнесу, зокрема: порушення права інтелектуальної власності, у тому числі порушення авторського права, комп’ютерне піратство; недобросовісна конкуренція; порушення прав споживачів, шахрайства; спам (нав’язлива реклама) тощо. Також дослідниками аналізуються і такі аспекти загроз безпеці електронної торгівлі як: політичні, соціально-психологічні (ментальні), правові, адміністративні та інші реальні і потенційні загрози безпеки у контексті реалізації електронної торгівлі.

Метою статті є забезпечення безпеки електронної торгівлі на приватноправовому та публічно-правовому рівнях.

Об’єктом дослідження визначено суспільні відносини, пов’язані з організацією безпеки електронної торгівлі. Предмет дослідження – окремі організаційно-правові аспекти безпеки електронної торгівлі.

Виклад основних положень. Як свідчать дослідження, за експертними оцінками, ризики безпеки електронної торгівлі переважно пов’язані із відкритістю природи Інтернет. При цьому швидкість їх змін досить стрімка. Кількість протиправних дій в Інтернеті (наприклад, віддалені інформаційно-програмні атаки, шахрайство, перехоплення конфіденційної інформації тощо) щороку стрімко зростає. У зв’язку з цим виникає питання теоретико-практичного змісту: що захищати? Відповідь – перш за все інформаційну систему. Для, прикладу, пропонується звернути увагу, що електронна платіжна система PayPal, що належить www.ebay.com, обслуговує 85 % укладання угод на аукціонах. Багато продавців підкреслюють, що віддають перевагу платежу саме через PayPal при покупці їх товарів [9].

Спільні риси з електронною комерцією має й Інтернет-банкінг. Подібність їх – здійснення фінансових операцій через публічні канали Інтернет із застосуванням веб-технологій, а фінансові транзакції здійснюються через банківські рахунки у електронній формі. Проте вони мають і відмінності. Інтернет-банкінг більшою мірою технологічно є закритою мережевою системою, тобто надає послуги тільки своїм клієнтам, пов’язаним угодами за термінами членства, й тому ґрунтується на договірних засадах і може не підтримувати низку необхідних технічних стандартів та міжнародних правових норм. Електронна комерція є відкритою системою. У технологічному змісті електронна комерція не має жорстких вимог щодо членства, послуги надаються клієнтам будь-якого банку, в будь-якій країні, а отже, електронна комерція може функціонувати виключно на уніфікованих технічних стандартах і уніфікованій правовій базі: норми правил поведінки повинні бути зрозумілими суб’єктам правовідносин незалежно від того, під юрисдикцією якої країни вони знаходяться. В іншому випадку угоди не будуть реалізовуватися.

На думку експертів, більшість електронних технологій в українській банківській системі розвивалися так, що вимоги до стандартизації Інтернет-банкінгу “послаблювалися”. Як наслідок – на практиці впроваджуються “нові” автоматизовані системи, що почасти не мають належних сучасним вимогам технологій захисту, як вирішального чинника безпеки. Швидше за все, керівництво підприємств і менеджери інформаційних технологій, які планують та вибирають системи для впровадження, просто не мають чіткої уяви про ризики, а отже, і про відповідні технології безпеки та їх технічні стандарти. Водночас міжнародна практика свідчить, що основа успіху електронного бізнесу – створення надійного, захищеного і стандартизованого середовища [4].

Загалом, як свідчить практика, із дотримання технічних стандартів (насамперед – міжнародних), як техніко-юридичних (чи технолого-юридичних) норм поведінки людини з технічним електронним середовищем, а також взаємних відносин між їх суб’єктами із застосуванням електронних засобів комунікації і починається універсалізація інструментів електронного бізнесу на транскордонному рівні. З цього також визначаються уніфіковані засоби та заходи захисту фінансово-інформаційних систем для вирішення різних завдань безпеки: авторизація на будь-яких рівнях комп’ютерної мережі – операційних систем, систем управління базами даних в комп’ютерній системі (далі – СУБД) та окремих комп’ютерних програм; захищений внутрішній документообіг у корпоративній мережі (Інтранет), зокрема із застосуванням електронної пошти інтернет, інтранет та Інтернет, організація в них захищених з’єднань абонентів; надійний захист авторизованого доступу до мережевих пристроїв телекомунікації та веб-вузлів). При цьому пропонується звернути увагу, що застосовуються дві категорії, що мають однакову сутність, але різний семантичний організаційно-технічний, організаційно-технологічний та організаційно-правовий зміст у просторовому прояві залежно від написання першої літери слова: інтернет (написання з малої літери) – це телекомунікаційна електронна система, що функціонує у реальному масштабі часу за колом осіб у просторі юрисдикції певної країни; а Інтернет (написання з великої літери) – це глобальна, транскордонна, інтернаціональна електронна мережа телекомунікації. Під інтранет пропонується розуміти локальну електронну систему телекомунікації, що функціонує в межах окремої установи, організації, підприємства, корпорації та інших підприємницьких структур. Як правило, технологічно (на основі IP-протоколу) ці системи функціонують інтегровано, але усвідомлення їх просторових і суб’єктних меж визначає технічні, технологічні, адміністративні, правові рівні режимів

організації безпеки у контексті визначення відносин політики охорони, оборони, захисту від небажаних проявів, що можуть становити загрозу нормальному (бажаному) функціонуванню конкретного рівня інформаційної системи.

Як зазначає більшість фахівців, на практиці для запобігання реалізації загроз безпеці електронного бізнесу корпоративна політика організації безпеки у технічному її аспекті має підтримуватися рядом адміністративних (організаційно-управлінських) заходів. Ці заходи класифікуються наступним чином. Визначення і узгодження ряду правил-принципів у рамкових нормах (технічних, технологічних, юридичних, техніко-юридичних, юридико-технічних): аутентифікації, конфіденційності, цілісності, невідмовності (non-repudiation) при інформаційному обміні між сторонами відносин. Якість реалізація адміністративних заходів у значній мірі визначається правовим статусом їх формалізації, як прояву легалізованої стандартизації: технічні стандарти, регламенти, інструкції, положення, настанови, накази, розпорядження, вказівки тощо, що визначається правовим статусом суб’єкта, уповноваженого приймати відповідні форми управлінських рішень.

Для прикладу, в електронній банківській справі критичним чинником вважається наявність і можливість підтвердження, що кожна окрема комунікація/з’єднання, транзакція чи запит на доступ цільової взаємодії є узгодженими (легітимними, правомірними), що знайшло відповідне легалізоване відображення, у формі відповідного нормативно-правового акту уповноваженого суб’єкта з владними правами. На цьому базуються і відносини між банком і його клієнтом. У разі непрямого (віртуального) контакту між банком і клієнтом відповідно для цього потрібно застосовувати надійні методи перевірки ідентичності між ними, авторизації один одного, для подальшого ініціювання електронних транзакцій. У практиці подібних правовідносин зазначене знаходить вираз у такому слові як *аутентифікація*. Технологічних методів аутентифікації існує кілька, проте переважно застосовуються такі вже традиційні як: PIN (персональний ідентифікаційний номер), паролі. Поряд з цим поступово знаходять розповсюдження – інтелектуальні картки, біометричні чи цифрові сертифікати інфраструктури відкритих ключів електронної ідентифікації (PKI) тощо.

Наступним організаційно-правовим заходом безпеки електронного бізнесу вважається *конфіденційність*. Під цим терміном серед фахівців з інформаційної безпеки розуміють правовий режим доступу до інформації, що поширюється електронною мережею. З таким правовим режимом інформація має бути доступна лише уповноваженим особам (сторонам конкретних правочинів) і не може бути доступна чи повідомлена іншим, без згоди споживача послуг за винятком випадків визначених законодавством у кримінально-правових справах (при реалізації окремих кримінально-процесуальних дій у конкретних справах).

Класифікаційним критерієм інформаційної безпеки вважається також *цілісність інформації у електронних транзакціях*. Під цілісністю розуміють – правовий режим інформації стосовно того, що вона не може бути без узгодження між сторонами (несанкціоновано) піддаватися змінам, а будь-яка зміна однією із сторін чи сторонніми особами може легко визначатися іншою стороною, або обома сторонами угоди.

Невідмова – розглядається в організації інформаційної безпеки як безперечна відповідальність за зобов’язання у транзакції (у правовому аспекті – оферти і акцепти), що включає створення доказу походження та доставки адресатам (сторонам угоди) електронної інформації про зміст правовідносин. Це, як правовий доказ застосовується для можливого захисту відправника (інформанта) з метою спростування обманної заяви

адресата (інформованого) про те, що дані (повідомлення) не було отримано, і навпаки – для захисту одержувача (інформованого) з метою спростування обманної заяви відправника (інформанта), що дані не відправлялися безпосередньо ним.

Ризик такої відмови від трансакції – це проблема не тільки “чисто” електронної торгівлі, але і таких, що вже стали звичайними, розрахункових операцій, як, наприклад, транзакцій із застосуванням кредитних чи дебіторських карток у електронних грошових операціях. При здійсненні електронного банкінгу та електронної торгівлі цей ризик підвищується, оскільки неможливо однозначно, в умовах реального часу, підтвердити (аутентифікувати) ідентичність та повноваження учасників транзакції як правочину в угоді. Ризик підвищується також через можливі підроблення чи перекручення електронних транзакцій і потенційну можливість з боку користувачів стверджувати, що транзакції було змінено начебто сторонньою (третьою) особою – зловмисником, який не санкціоновано сторонами угоди отримав доступ до інформації.

Серед сучасних методів захисту електронного бізнесу найкращим (найуніверсальнішим) із поширених у складі його інформаційної безпеки, зокрема її інфраструктурної складової телекомунікації, вважається електронно-цифровий підпис (чи електронний підпис, чи цифровий сертифікат). Це стосується більшою мірою електронного документообігу у відкритій (загально доступній) інфраструктурі телекомунікації з, так званими, відкритими ключами (PKI, Public Key Infrastructure). Нині інфраструктура PKI визначається низкою технічних стандартів, що склалися переважно об’єктивно з урахуванням масштабів поширення певної техніки та технологій: глобальних міжнародних (ISO – International Organization for Standardization; RFC – Request for Comments), регіонально-міжнародних, зокрема – європейських (ETSI – European Telecommunications Standards Institute) та ін.

У міжнародній практиці електронної комерції, в її основі, покладено єдині відкриті технічні стандарти. Подібно до телефонної системи, глобальна система електронної комерції через Інтернет вважається настільки ефективною, наскільки збільшується кількість клієнтів, включених до системи, що можливо лише за уніфікації технічних стандартів між країнами. Як приклад із масового впровадження науково-технічного прогресу у суспільні відносини щодо конвергенції засобів телекомунікації можна привести приклад із розвитку мобільної радіотелефонії – на початку впровадження вона була коштовною розкішшю для багатіїв, а тепер – вже масове явище, доступне великій кількості населення із середнім та нижче середнього достатку.

Нині найпоширеніщими реалізаціями технічних стандартів PKI вважаються комп’ютерні програми Identrus, SWIFT (на базі PKI Identrus), VISA. Так, IdentrusTM LLC (Identrus) – заснована у квітні 1999 році – дає можливість керувати бізнес-ризиками Інтернет-комерції через довірчі відносини клієнтів з їхніми фінансовими установами в межах систем електронного банкінгу, електронної торгівлі. Юридико-технічна інфраструктура Identrus ґрунтується на міжнародних технічних стандартах PKI, типових однорідних системних правочинах, нормах, правилах, контрактах. Система є відкритою для фінансових установ та їхніх клієнтів у всьому світі. У грудні 1999 року Identrus здобув вищу нагороду “CIB/BT Financial Technology Awards” у номінації моделі захисту B2B (Business-to-Business, бізнес для бізнесу). У серпні 2001 року Європейська комісія сертифікувала Identrus як провідний стандарт захисту в електронній комерції в межах Євросоюзу. Нині в Identrus входить більш 60 глобальних фінансових установ. Хоча ця інформаційна система призначена для цивільних фінансових потреб, вона також застосовується низкою урядових агенцій США, включаючи Міністерство оборони. Система Identrus PKI побудована так, що кожна установа (наприклад, банк) в системі та

кожен споживач послуг (клієнт) мають унікальний ідентифікатор, зазначений у персональних електронно-цифрових сертифікатах. Таким чином, клієнти різних установ можуть встановлювати між собою комерційні правовідносини у електронній формі.

Розвитку електронної комерції особливо сприяло створення системи TrustAct SWIFT та інтеграція можливостей SWIFT та Identrus для спільного вирішення завдань B2B: фінансові установи та їхні клієнти змогли об’єднати можливості захисту Identrus з можливостями передачі повідомлень SWIFT через Інтернет. Крім того, TrustAct зберігає реєстрацію повідомлень, а отже, забезпечує функції для можливого арбітражу та цілковиту “невідмову” від трансакцій у разі забезпечення доказів у спорі.

Для трансакцій з платіжними картками міжнародних платіжних систем розроблено технологічний стандарт 3-D Secure VISA. На сьогодні всі установи, які здійснюють трансакції через Інтернет із застосуванням транскордонних платіжних карток VISA та Europay, повинні обов’язково підтримувати цей технологічний стандарт, що також базується на PKI-стандартах. В Україні також вважається перспективним напрямом електронної комерції із застосуванням PKI-стандартів. При цьому обов’язковим для успішного розвитку інтернет-банкінгу є побудова системи PKI з урахуванням вимог IdentrusTM LLC та стандарту 3-D Secure VISA.

На зазначеному прикладі технологічної конвергенції електронного бізнесу можна спостерігати як приватноправова його природа набуває публічно-правових ознак. При цьому виникає питання: наскільки можливе застосування таких міжнародних технічних стандартів у межах чинного законодавства України?

У країнах ЄС, США, Канаді та інших електронно-цифрові підписи, їх сертифікати затверджено на рівні законодавства, як еквівалент власноручного підпису; законодавчо визначено зміст термінів “електронний підпис”, “електронні документи” та пов’язані з ними інші поняття, терміни, категорії. Країни ЄС ухвалили національні законодавчі акти, що цілком відповідають Директиві Європарламенту та Ради Міністрів ЄС 1999/93/ЄС про систему електронних підписів, що застосовується в межах Співтовариства, та рішенню Комісії 2000/709/ЄС Європарламенту і Ради, а також узгоджено з положеннями Директиви 2000/31 Європейського парламенту та Ради “Про деякі правові аспекти інформаційних послуг, зокрема електронної комерції, на внутрішньому ринку (Директива про електронну комерцію)”, від 08.06.2000 року [10]. Нині усі положення Директиви 1999/93/ЕС реалізовано у формі таких міжнародних юридико-технічних актів як міжнародні та європейські технічні стандарти (ETSI та RFC), що є обов’язковою нормативно-правовою базою для країн, де розвивається міжнародна електронна комерція із застосуванням Інтернет.

Свого часу в Україні, калькуючи практику фрагментарного законотворення в європейських країнах, Верховною Радою були прийняті ряд Законів: “Про електронний цифровий підпис” [13], “Про електронні документи та електронний документообіг” [14], “Про платіжні системи та переказ грошей в Україні” [15].

Проведений правовий аналіз дозволяє констатувати, що у єдності ці закони не відповідають ні європейському праву в цілому, ні техніко-технічній складовій сутності електронного підпису та принципам його застосування (в термінах міжнародних і європейських технічних стандартів). Наприклад, електронний підпис у термінах ЄС повинен забезпечувати *аутентифікацію та цілісність*. В термінах Закону України “Про електронний цифровий підпис” електронний підпис – це дані в електронній формі, що додаються до інших електронних даних або логічно з ними пов’язані та призначені *лише для ідентифікації* підписувача цих даних. При цьому також у зазначеному Законі подається визначення і електронного цифрового підпису у змісті електронного підпису

у розумінні терміну ЄС: електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, що додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його *цілісність та ідентифікувати* підписувача. У визначенні ЄС існує така категорія як “посилений електронний підпис” – це електронний підпис ЄС та додаткові вимоги стосовно надійності, що технічно означають, що засіб створення підпису має задовольняти вимоги стандартів FIPS 140-1, 140-2 level 2, 3 (Federal Information Processing Standards, U. S.). Такого терміна в Законі України немає, натомість є термін “електронний цифровий підпис”, що за змістом відповідає електронному підпису ЄС у межах криптографії з відкритими ключами. В терміни ЄС і відповідні європейські та міжнародні стандарти введено термін “кваліфікований електронний підпис”, чого у зазначених законах немає.

До речі, система PKI Identrus передбачає посилений чи кваліфікований електронний підпис, що у законодавстві України не визначено взагалі. Відтак на практиці українське законодавство не може бути застосованим до відкритих мереж міжнародного електронного бізнесу (наприклад, у електронній торгівлі). Це створює, у свою чергу, загрози інформаційній безпеці у електронній комерції із застосуванням Інтернет у міжнародних торгівельних відносинах, що є, відповідно, і правовим ризиком для безпеки бізнесу закордонних інвесторів на території України. Все це можна розглядати і як причини, умови, що сприяють зниженню рівня економічної безпеки України, оскільки українські підприємці, які займаються міжнародною торгівлею, надають перевагу укладанню угод з іноземними контрагентами через офшорні зони на території різних країн, що зменшує надходження фінансових ресурсів через податкову систему до державного бюджету в Україні.

Висновки.

1. У організаційно-правовому аспекті на державному рівні пропонується для прискореного розвитку українського сегменту міжнародного електронного бізнесу поглибити співпрацю держави з Міжнародній організацією зі стандартизації ISO і прискорити впровадження необхідних технічних та інших правових стандартів, що вже чинні у Європі.

2. Для законодавчого врегулювання прискорити ухвалення Закону України “Про електронну торгівлю” (проект від 17.02.03 р. № 3114), що, за визначенням більшості фахівців, відповідає вимогам ЄС і узгоджується з міжнародними та європейськими стандартами.

3. Адаптувати вже ухвалені закони, що мають відношення до електронної торгівлі, до вимог європейського законодавства на понятійному рівні.

4. У перспективі, при розробці проекту Кодексу України про інформацію, як основ законодавства щодо інформації, у спеціальній його частині слід визначити рамкові норми, де буде визначений правовий гіперзв’язок із спеціальним законодавством, що регламентує правовідносини до електронної торгівлі у комплексі державними технічними стандартами України на основі міжнародних технічних стандартів (ISO, ETSI та RFC).

Використана література

1. UNCTAD. E-commerce and Development Report 2004. United Nations. N.Y. and Geneva, 2004. – 244 p. Eastern Europe E-Commerce Report 2009 // yStats.com GmbH & Co. KG, 2010. – 110 p. Global Internet and E-Commerce Trends 2010 // yStats.com GmbH & Co. KG, 2010. – 251 p.

2. Бабенко Л.К. Новое в технологии электронного бизнеса и безопасности / [Л.К. Бабенко, В.А. Быков, О.Б. Макаревич, О.Б. Спиридонов]. – М. : Радио и связь, 2001. – 376 с.

3. Баско Ф. B2B в России : проблемы и перспективы. – eCommerce World. – 2005. – № 3. – С. 22 – 24;

4. Бєлов С. Ризикована привабливість / С. Бєлов, С. Мартиненко. – Режим доступу : //www.business.if.ua/themes/business

5. Брижко В. е-майбутнє та інформаційне право / [В. Брижко, В. Цимбалюк, М. Коваль, Ю. Базанов та ін.]. – К. : НДЦПІ АПрН України. 2006. – 234 с.

6. Брижко В. Інформаційне право та правова інформатика у сфері захисту персональних даних : монографія / [В. Брижко, М. Гуцалюк та ін.]. – К. : НДЦПІ АПрН України, 2005. – 334 с.

7. Новицький А.М. Електронна торгівля (правовий аспект регулювання) : монографія / [А.М. Новицький, В.С. Гаркуша, Н.Б. Новицька, В.С. Цимбалюк та ін.] ; за заг. ред. д.ю.н., професора Костицького В. В. – К.: МП “Леся”. 2007. – 212 с.

8. Золотар О. О. Перспективи розвитку законодавства у сфері захисту інформаційної безпеки / О.О. Золотар ; матеріали VI міжнародної наукової конференції студентів та молодих учених. – К. : НАУ, 2006. – С. 533.

9. – Режим доступу : //www.group4.com.ua/zagalni-ponyattya/paypal-elektronna-platizhna-systema

10. Директива Європарламенту та Ради Міністрів ЄС 1999/93/ЄС про систему електронних підписів, що застосовується в межах Співтовариства ; рішення Комісії 2000/709/ЄС Європарламенту і Ради ; Директива 2000/31 Європейського парламенту та Ради “Про деякі правові аспекти інформаційних послуг, зокрема електронної комерції, на внутрішньому ринку (Директива про електронну комерцію)” від 08.06.00 р. // Інформаційне законодавство : зб. законодавчих актів : У 6 т. ; за заг. ред. Ю.С. Шемшученка, І.С. Чижа. – Т.5. Міжнародно-правові акти в інформаційній сфері. – К. : ТОВ “Видавництво “Юридична думка”, 2005. – С. 255 – 270.

11. Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки: Закон України від 9.01.07 р. № 537-V // Бібліотека баз даних і знань в галузі держави і права. – К. : НДЦПІ. 2011, липень. – (Електронний ресурс на DVD).

12. Про затвердження Концепції легалізації програмного забезпечення та боротьби з нелегальним його використанням : Розпорядження Кабінету Міністрів України від 15.05.02 р. № 247-р.

13. Про електронний цифровий підпис : Закон України від 22.05.03 р. №852-IV із змінами, внесеними згідно із Законом України від 15.01.09 р. № 879-VI // Відомості Верховної Ради України (ВВР). – 2003. – № 36. – Ст. 276.

14. Про електронні документи та електронний документообіг : Закон України від 22.05.03 р. № 851-IV із змінами, внесеними згідно із Законом України від 31.05.05 р. № 2599-IV // Відомості Верховної Ради України (ВВР). – 2003. – № 36. – Ст. 275).

15. Про платіжні системи та переказ грошей в Україні : Закон України від 5.04.01 р. № 2346-III // Відомості Верховної Ради України (ВВР). – 2001. – № 29. – Ст. 137.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~