УДК 346.544.4:004.738.5

В. БРИЖКО, *кандидат юридичних наук (Ph. D),*
старший науковий співробітник

ЕЛЕКТРОННА КОМЕРЦІЯ: ГОЛОВНІ АСПЕКТИ НОРМАТИВНО-ПРАВОВОГО УПОРЯДКУВАННЯ СУСПІЛЬНИХ ВІДНОСИН

Анотація. *Про стан та перспективи спеціального нормативно-правового упорядкування суспільних відносин у сфері електронної комерції.*

1. Щодо закону України про електронну комерцію

В сучасних умовах широке застосування інформаційно-комп’ютерних технологій та телекомунікаційних мереж у комерційній діяльності завдяки, зокрема, електронному обміну даними та укладенням за допомогою електронних засобів договорів у підприємництві стає реальністю.

В Україні є відповідна нормативно-правова база щодо підприємницької діяльності, до якої належать, зокрема, такі законодавчі акти: Цивільний кодекс України від 16 січня 2003 р. № 435-IV, Господарський кодекс України від 16 січня 2003 р. № 436-IV, Закон України “Про підприємства в Україні” від 27 березня 1991 р. № 887-XII, Закон України “Про захист від недобросовісної конкуренції” від 7 червня 1996 р. № 236/96-ВР, Закон України “Про оподаткування прибутку підприємств” від 28 грудня 1994 р. № 334/94-ВР та багато ін.

Проте, в електронно-інформаційній сфері, публічно-правове регулювання підприємницької діяльності має свої особливості, що потребує узагальнення та створення спеціальних юридичних норм і правил, адресованих безпосередньо електронній комерції.

У зв'язку з цим у законодавстві й торгових звичаях розвинених країн, а також у міжнародному праві порівняно швидко з найшли закріплення і були введені в юридичну практику такі базові поняття, як: “електронна комерція” (або “електронна торгівля”), “електронний обмін даними”, “електронний (зокрема цифровий) підпис” і значне число інших пов'язаних з ними правових конструкцій: “електронна операція”, “електронні документи”, “електронні платежі і розрахунки” тощо.

Юридична сфера електронної комерції дуже широка. За визначенням Типового закону ООН “Про електронну торгівлю” 1997 р. (ЮНСІТРАЛ) [1] вона охоплює питання, що виникають у зв'язку з всіма відносинами комерційного змісту, які включають, але не обмежуються такими операціями: покупка/продаж, поставка, угода про розподіл продукції, торгове представництво (агентство), факторинг, лізинг, проектування, консалтинг, інжиніринг, інвестиційні контракти, страхування, угоди про експлуатацію і концесію, банківські послуги, спільну діяльність та інші форми промислової і ділової співпраці.

Також за кордоном розроблені та застосовуються нормативні положення, що відносяться до електронних комерційних операцій нового покоління, так званих “послуг інформаційного суспільства”. Вони визначають правовий статус постачальників послуг інформаційного суспільства; регламентують обов'язки постачальників надавати клієнтам відомості про порядок дій, необхідних для укладання договору, або відміну помилкових замовлень, забезпечення клієнтам можливості заздалегідь ознайомитися з умовами договору, зокрема, за допомогою технологічного відсилання до іншого документа.

У державах-членах Європейського Союзу та Ради Європи існує значна кількість нормативних документів (стандартів), які прямо або опосередковано визначають підходи до правового регулювання відносин у сфері електронної комерції [2].

Головним стандартом (рамковим актом) щодо сфери електронної комерції є **Директива 2000/31/ЄС Європейського Парламенту і Ради “Про правові аспекти інформаційних послуг щодо електронної комерції на внутрішньому ринку” (“Про електронну комерцію”)** від 08.06.2000 р. [3].

Директива 2000/31/ЄС “Про правові аспекти інформаційних послуг щодо електронної комерції на внутрішньому ринку” (“Про електронну комерцію”) була розроблена на базі рекомендацій Комісії ЄС 1998 р., які визначили основні проблеми правового регулювання у сфері електронної комерції (див. Таблицю) [4].

Таблиця

Проблеми	Основні питання в рамках проблеми
Регулювання діяльності провайдерів послуг інформаційного суспільства (сервіс-провайдерів)	Порядок визначення місця надання послуги “он-лайну”. Порядок початку діяльності за надання послуг “он-лайну” (дозвільний або повідомний). Рамки застосування принципу “свободи установи” (freedom of establishment), закріпленого ст. 52 Договору про створення ЄС.
Комерційні повідомлення	Визначення поняття “комерційні повідомлення”. Правила надання послуг особами так званих регульованих професій (адвокати та ін.). Забезпечення добросовісної конкуренції. Забезпечення прозорості умов надання послуг. Виключення практики “нав'язування послуг”.
Укладення договорів з використанням електронних засобів	Визнання дійсності договорів, що укладаються в електронний спосіб. Юридична сила дій сторін при укладенні договору.
Відповідальність посередників	Відповідальність посередників за передачу незаконної інформації. Здатність посередників контролювати інформацію, що передається.
Вирішення спорів в області електронної комерції	Засоби механізмів правового захисту, які були б найбільш швидкодійними (з урахуванням географічної віддаленості контрагентів) і ефективними (з урахуванням особливостей електронного бізнесу). Ступінь застосування позасудових механізмів урегулювання спорів. Поліпшення співпраці між регулюючими і судовими органами країн.
Реалізація норм Директиви 2000/31/ЄС в законодавстві держав-членів ЄС	Визначення принципів наглядової юрисдикції тієї або іншої держави при трансграничній електронній комерції. Введення уніфікованих правил надання інформації про провайдерів. Надання одноманітних гарантій діяльності сервіс-провайдерів.

Порівняно з Типовим законом ООН “Про електронну торгівлю” 1997 р. Директива 2000/31/ЄС є достатньо обширним документом, що регулює значне коло суспільних відносин у сфері електронної комерції. Так зокрема, врегульована діяльність провайдерів та інших постачальників інформаційних послуг; встановлюється принцип, що виключає необхідність отримання попередніх санкцій або дозволів для здійснення діяльності подібних організацій; встановлені правила відповідальності провайдерів та інших інформаційних посередників; визначені умови, при настанні яких, на вимогу національних органів судової влади на ці організації може бути покладено обов'язок по контролю і пошуку фактів або обставин, що вказують на незаконний зміст діяльності. Достатньо

детально врегульовано механізм укладення електронних договорів, визначені вимоги яким вони повинні відповідати, встановлені правила визначення моменту укладення договору.

Метою застосування згаданих спеціальних норм в окремому нормативно-правовому акті є створення відповідного правового поля щодо гармонізації національних законодавчих актів за умов вільного надання інформаційних послуг та забезпечення підвищених юридичних гарантій всім учасникам підприємницької діяльності, у першу чергу малим та середнім підприємствам, які здійснюють ділові операції за допомогою Інтернету.

Важливо підкреслити, що в Директиві 2000/31/ЄС окремо визначається, що захист осіб у зв’язку з обробкою персональних даних регулюється виключно Директивою 95/46/ЄС від 24.10.1995 р. “Про захист осіб у зв’язку з обробкою персональних даних та вільним обігом цих даних” та Директивою 97/66/ЄС від 15.12.1997 р. “Про обробку персональних даних та захист прав у телекомунікаційному секторі”, які повною мірою можуть бути застосовані до інформаційних послуг. Ці директиви вже визначають правову структуру в сфері обробки персональних даних. Таким чином, немає потреби роз'яснювати цю проблему в Директиві 2000/31/ЄС з тим, щоб забезпечити ефективне функціонування внутрішнього ринку, зокрема, вільне переміщення персональних даних між державами-членами. Запровадження та застосування цієї Директиви 2000/31/ЄС має бути здійснене у повній відповідності з принципами, що стосуються захисту персональних даних, зокрема, стосовно надсилання комерційного повідомлення без згоди одержувача та відповідальності посередників. Конфіденційність повідомлень гарантується статтею 5 Директиви 97/66/ЄС, згідно з якою держави-члени повинні заборонити будь-який вид перехоплень чи контроль повідомлень іншими суб'єктами, окрім випадків дозволу на таку діяльність згідно із законом.

Щодо реалій застосування у практиці електронної комерції, то у 1998 р. організація “Азіатсько-Тихоокеанське економічне співробітництво” (Asia Pacific Economic Cooperation), до якої входять Австралія, Бруней, В'єтнам, Гонконг, Індонезія, Канада, Китай, Малайзія, Мексика, Нова Зеландія, Папуа Нова Гвінея, Перу, Росія, Сінгапур, США, Таїланд, Тайвань, Філіппіни, Чилі, Південна Корея, Японія) [5], доручила компанії Price Waterhouse Coopers (PWC) провести дослідження на тему: як розповсюджується, розвивається і використовується електронна комерція в малому і середньому бізнесі країнчленів цієї організації. Компанії цієї категорії чисельно становлять найбільшу частину гравців на полі електронної комерції типу B2B. І ті з них, хто активно використовує технології електронної комерції, мають значні конкурентні переваги. Великі і транснаціональні компанії, що реалізовують B2B-стратегію, дуже часто залучають малий і середній бізнес до своїх ланцюжків поставок.

Згідно зі статистикою, у вказаному регіоні налічується понад 40 млн. малих і середніх бізнесових організацій, які становлять понад 95 % усіх підприємств. Вони забезпечують зайнятість близько 84 % всієї наявної робочої сили регіону і виробляють від 30 до 60 % ВНП, а їх продукція становить понад 35 % всього експорту.

До таких, що перешкоджають ширшому розповсюдженню електронної комерції серед малих і середніх підприємств, відносяться наступні проблеми [6]:

- низький рівень використання електронної комерції споживачами і постачальниками послуг;
- проблеми захисту даних;
- наявність правових проблем і проблем відповідальності;
- висока вартість комп'ютерних і мережних технологій;

- обмежені знання в області моделей і технологій електронної комерції;
- невпевненість компаній у можливості виграшу від електронної комерції;
- неадекватність якості телекомунікаційного сервісу для електронної комерції.

Учасниками дослідження була запропонована низка заходів, спрямованих на подолання існуючих бар'єрів і таким чином сприяючих ширшому запровадженню та використанню електронної комерції. Найважливішими заходами, що підлягають ухваленню на рівні урядів, були наступні:

- розробка національної стратеги електронної комерції;
- захист даних;
- навчання електронної комерції;
- зрозуміла податкова політика;
- зменшення правових бар'єрів;
- поліпшення сервісу веб-сайтів уряду в Інтернеті.

Результати досліджень також показали, що малий і середній бізнес значною мірою переконаний у важливості урядової підтримки та дій щодо розвитку електронної комерції. Уряд повинен виконувати очолюючу роль у багатьох напрямах, зокрема у поліпшенні телекомунікаційної інфраструктури, підвищенні безпеки транзакцій, у розширенні доступу малих підприємств до Інтернету та у вирішенні правових і регулюючих проблем, що виникають при використанні електронної комерції.

У зазначеному контексті голова комітету торговельно-промислової палати РФ по інформаційному забезпеченню підприємництва О. Іоффе зазначає: *“Світова практика показує, що електронна торгівля є одним з основних видів підтримки і розвитку малого і середнього бізнесу: використання механізмів електронної торгівлі при мінімальних витратах відкриває малому і середньому бізнесу доступ до всього ринку потенційних покупців. За даними НАУЕТ (м. Москва), в 2007 році більше 60 % операцій припало на частку малого і середнього бізнесу, в першому півріччі їх обсяг становив 2,543 млрд. доларів, тобто менше ніж за рік обсяг електронних контрактів, одержаних малим бізнесом, виріс на 117 %. У 2008 році малий і середній бізнес одержать контрактів на 7 млрд. доларів, припускають експерти”* [7].

Виходячи з європейських поглядів на електронну комерцію можна говорити про необхідність розробки окремого нормативно-правового акту – закону України, що регулює питання зазначеної діяльності, включаючи положення про укладення договорів за допомогою електронних засобів і юридичного їх визнання, про правовий статус, обов'язки і відповідальність інформаційних посередників в електронній комерції.

Структура закону про електронну комерцію може передбачати наступні складові частини:

Преамбула (сфера застосування).

Розділ 1. Загальні положення:

- мета;
- визначення (електронна комерція, постачальник інформаційних послуг (інформаційні посередники), одержувач послуг, споживач, комерційне повідомлення щодо електронної комерції);
- законодавство про електронну комерцію;
- основні принципи;
- суб’єкти електронної комерції.

Розділ 2. Постачальники послуг:

- інформація стосовно постачальника (провайдера) інформаційних послуг щодо електронної комерції;

• умови відповідальності постачальника (провайдера) інформаційних послуг за збереження, конвертацію та передачу комерційної інформації;

• захист даних, зокрема, персональних даних.

Розділ 3. Комерційні повідомлення:

• інформація щодо комерційних повідомлень;

• комерційні повідомлення, що надсилаються без згоди одержувача.

Розділ 4. Договори та інші правочини в електронній комерції:

• електронний договір;

• умови договору;

• укладення договору (оферта та акцепт);

• юридична сила електронного документу;

Розділ 5. Вирішення спорів:

• поза межами суду;

• судові позови;

• електронний документ в якості доказу у суді.

Розділ 6. Відповідальність.

Розділ 7. Прикінцеві положення.

Правове регулювання електронної комерції має ґрунтуватися на принципах рівності усіх учасників, свободи договору, безперешкодного здійснення підприємницької діяльності, вільного переміщення товарів, послуг і коштів на всій території України, а також гарантіях судового захисту даних і прав споживачів.

Фізичні і юридичні особи вільні у встановленні своїх прав і обов'язків на підставі договору та у визначенні умов договору, що не суперечать чинному законодавству.

Проектом закону України необхідно передбачити, що договір в електронній комерції може бути укладений шляхом обміну електронними документами, який дозволяє чітко встановити, що документ виходить від сторони за договором. Якщо при укладанні договору використовуються електронні документи, то умови договору та зобов'язання сторін, що випливають з них, не можуть бути оскаржені сторонами тільки з тих підстав, що він укладений шляхом обміну електронними документами.

Також необхідно передбачити можливість подання електронних документів, підписаних за допомогою електронного підпису, як письмових доказів. Ці докази не можуть заперечуватися тільки з тих підстав, що вони надані у формі електронних документів.

У проекті закону необхідно зазначити, що в разі, якщо законом передбачається вимога нотаріального посвідчення цивільно-правової угоди, така угода, оформлена шляхом створення електронного документа, повинна бути скріплена електронним підписом нотаріуса у порядку, встановленому Законом “Про нотаріат”.

При укладанні договору в електронній комерції пропозиція укласти договір однієї з сторін, тобто оферта, прийняття пропозиції іншою стороною, іншими словами – її акцепт, можуть бути відправлені й отримані у вигляді електронних документів.

Пропозицію укласти договір може бути спрямовано самим оферентом чи інформаційною системою, запрограмованою оферентом або від його імені і діючою автоматично. Договір визнається укладеним з моменту одержання акцепту особою, що направила оферту.

При цьому є потреба у вирішенні питань щодо:

• надання широкого визначення терміну “електронна комерція” виходячи з того, що вона може бути обмеженою (стосується лише торгівлі – Інтернет-торгівля), частково обмеженою (стосується підприємницької діяльності – Інтернет-комерція) або спрямова-

на на поступове впровадження електронних технологій в усі процеси бізнес-діяльності (Інтернет-бізнес);

• внесення змін до Цивільного кодексу України та Господарського кодексу України в частині, що стосується предмета закону;

• внесення змін до положень податкового законодавства, які повинні враховувати особливості електронно-комерційної діяльності.

2. Особливості захисту даних

Захист даних у більшості випадків становить предмет комерційної таємниці.

Згідно зі статтею 30 Закону України “Про підприємства в Україні” від 27.03.1991 р. № 887-XII: *“Під комерційною таємницею підприємства маються на увазі відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, що не є державною таємницею, розголошення (передача, витік) яких може завдати шкоди його інтересам... Склад і обсяг відомостей, що становлять комерційну таємницю, порядок їх захисту визначаються керівником підприємства”.* Порушення комерційної таємниці розглядається з точки зору недобросовісної конкуренції, яка може зашкодити діловій репутації або майну іншого підприємця, що передбачає накладення штрафу відповідно до Кодексу України про адміністративні правопорушення.

Постановою Кабінету Міністрів України від 03.08.1993 р. № 611 був встановлений перелік відомостей, що не становлять комерційної таємниці, до яких віднесені:

• установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами;

• інформація за всіма встановленими формами державної звітності;

• дані, необхідні для перевірки обчислення і сплати податків та інших обов’язкових платежів;

• відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць;

• документи про сплату податків і обов’язкових платежів;

• інформація про забруднення навколишнього середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров’ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;

• документи про платоспроможність;

• відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об’єднаннях та інших організаціях, які займаються підприємницькою діяльністю;

• відомості, що відповідно до законодавства підлягають оголошенню.

Слід звернути увагу на те, що державна таємниця не може бути комерційною таємницею, оскільки в іншому разі мала б місце торгівля державними інтересами. З іншого боку, комерційна таємниця може бути державною таємницею, і тоді вона підлягає захисту не тільки з боку підприємства, а й держави.

У СРСР відомості щодо економічного, технічного або виробничого змісту в результаті оперативної діяльності організацій та підприємств (за виключенням відомостей, які становили державну таємницю) мали узагальнююче поняття “комерційної інформації” (наприклад, Наказ Державного комітету СРСР по винаходах і відкриттях від 27.11.1990 р. № 146, який вводив у дію Положення про комерційну таємницю у системі Держкомвинаходів СРСР).

За кордоном встановлення режиму застосування інформації щодо комерції розглядається в межах поняття “діловий секрет” (trade secret).

Діловий секрет – це цінна інформація, яка:

• є власністю фізичної або юридичної особи;

* має самостійну економічну цінність (фактичну або потенційну) в результаті того, що вона не є загальновідомою, легко встановлюваною належними засобами іншими особами, що можуть одержати економічне збагачення від її розкриття або використання;

* є об'єктом зусиль, розумно необхідних за відповідних обставин для підтримки її секретності.

Поняття “діловий секрет” включає відомості про техніку, технологію, спосіб, формулу, модель, програму, пристрій, метод та ін., а також особливості їх створення.

В основі поняття ділового секрету лежить конфіденційність, що поширюється не тільки на виробництво й торгівлю, а й на дослідження. Тому діловий секрет – узагальнююче поняття для усіх секретів.

Для ділового секрету характерним є статичний стан, який відбиває власність юридичної або фізичної особи.

Коли діловий секрет стає об’єктом передачі права власності, він характеризується станом динамічності та набуває статусу “ноу-хау”.

Зазначимо, що нині законодавства країн світу щодо “ділового секрету” продовжують мати розбіжності.

У **США,** наприклад, у ще у 1979 р. питання ділових секретів виділили із законодавства щодо інтелектуальної власності та прийняли єдиний, окремий закон.

У **Великобританії** шляхом виділення ділових секретів в окремий закон не пішли, проте їх захист не підпадає під регулювання захисту інтелектуальної власності.

У **Канаді** в 1990 р. здійснили фундаментальну реформу законодавства щодо ділових секретів у напрямі деталізації відносин в окремому законі, де значна увага приділена процесуальнім діям судів та їх рішень. Зокрема, у § 4(1) закону про ділові секрети встановлено, що суд повинен виходити з того, що діловий секрет охороняється законом, а також враховувати зміни по відношенню до права на діловий секрет. Суд має можливість врегулювати будь-які взаємовідносини сторін виходячи з того, що перевагу має та сторона, яка спочатку володіла правом власності на секрет. З іншого боку, суд може встановити строк дії права на діловий секрет, який визнає розумним для усунення тих комерційних переваг, які інакше одержить відповідач.

У **СРСР** термін “діловий секрет” перекладався та трактувався по-різному: промисловий секрет, виробничий секрет, торговельна таємниця, фірмова таємниця, комерційна таємниця або комерційний секрет тощо.

Співвідношення понять “комерційна таємниця” і “комерційний секрет” різне. Найчастіше таємниця передбачає привнесення будь-чого нового в будь-який предмет (об’єкт), процес, а під секретом розуміється не тільки сам предмет (об’єкт), а й особливість його створення, наприклад:

* промисловий секрет – це предмет новації (патенту) і будь-які особливості його створення, патентування та виробництва;

* виробничий секрет – привнесення будь-чого нового в процес виробництва;

* торговельна таємниця – отримання знань із закупівлі товарів, списків покупців та інше;

* фірмова таємниця – таємниця індивідуальних особливостей виробництва і підприємництва.

У реальному житті комерційна таємниця завжди виступає у формі комерційного секрету. Тому будь-яка таємниця є секретом, але не всякий секрет є таємницею (помилкове віднесення відомостей до комерційної таємниці).

Виходячи з цього можна сформулювати робочі визначення комерційної таємниці і комерційного секрету.

Комерційна таємниця – навмисно приховувані з комерційних міркувань економічні інтереси й відомості про різні сторони і сфери виробничо-господарської, управлінської, науково-технічної, фінансової діяльності підприємства, захист яких обумовлений загрозами недобросовісної конкуренції. Ця таємниця виникає тоді, коли вона представляє інтерес для комерції.

Комерційна таємниця може виступати в наступних основних формах:

- конфіденційність (з англ. confidence – довіра);
- договірні умови;
- контрактні відносини;
- зобов'язання (підписка про зобов'язання зберігати комерційні секрети).

Комерційні секрети – форма прояву комерційної таємниці, матеріалізовані певним чином (у вигляді документів, схем, виробів та ін.) відомості, що відносяться до комерційної таємниці та підлягають захисту від можливих посягань шляхом заволодіння, вивідування, витоку та ін.

Нерідко зарубіжні фахівці в області планування і управління виробництвом відносять збір інформації про конкуруючі фірми і компанії до звичного маркетингу разом з такими підсистемами інформації, як інформація про потенційних споживачів, репутацію фірми, державне регулювання на ринку і т. п. При цьому, електронно-інформаційне середовище надає значно більше можливостей для збору будь-якої інформації.

Свого часу французький дослідник Ж. Бержьє склав *“список засобів отримання інформації про конкурентів, який застосовують американські промисловці”* [8], до якого віднесено:

1. Публікації конкурентів і звіти про процеси та результати, що одержані.
2. Відомості, які публічно надані колишніми працівниками конкурента.
3. Огляди ринків.
4. Фінансові звіти.
5. Влаштовувані конкурентами ярмарки і виставки та брошури, які надаються.
6. Аналіз виробів (продукті) конкурентів.
7. Звіти комівояжерів і закупівельних відділів.
8. Питання, що ставляться фахівцям конкурента на спеціальних конгресах.
9. Безпосереднє таємне спостереження.
10. Переговори з конкурентом нібито для придбання ліцензії на один з патентів.
11. Використання професійних шпигунів для отримання інформації.
12. Зманювання з роботи працівників конкурента для отримання інформації.
13. Посягання на власність конкурента.
14. Підкуп співробітників закупівельного відділу конкурента або його працівників.
15. Засилання агентів до працівників або фахівців конкурента.
16. Викрадання креслень, зразків, документів тощо.
17. Підслуховування розмов у конкурента.
18. Шантаж і різні способи тиску; зрозуміло, конкурент вдається до тих же засобів.

Існують три основних види інформації про конкурентів, до яких відносяться:

1. Інформація про ринок:

- ціни, знижки, умови договорів, специфікація продукту;

- обсяг, історія, тенденція і прогноз для конкретного продукту;
- частка на ринку і тенденції її зміни;
- канали, методи збуту і плани;
- чисельність і розміщення торгових агентів;
- контингент споживачів (зокрема, дисконтні картки) і відносини з ними;
- репутація;
- програма реклами.

2. Інформація про виробництво і продукцію:

- оцінка якості й ефективності;
- номенклатура виробів;
- технологія і устаткування;
- рівень витрат;
- виробничі потужності;
- розміщення і розмір виробничих підрозділів і складів;
- доставка;
- результати проведення науково-дослідної роботи.

3. Інформація про організаційні особливості і фінанси:

- персональні дані і філософія осіб фірми, які ухвалюють ключові рішення;
- фінансові умови і перспективи;
- програми розширення і придбань;
- головні проблеми і можливості;
- програма науково-дослідної роботи.

У наш час завдяки застосуванню техніко-технологічних засобів можливості отримання комерційної інформації значно поширились, а отже, потребують більшого її захисту. Сучасні технології та мережі надають відповідні переваги в комерційній діяльності, з одного боку, а з іншого – створюють більше умов для несанкціонованого отримання будь-яких відомостей.

Так, збирання комерційної інформації може відбуватися за допомогою звичайних каналів зв'язку. Виключити ведення ділових переговорів з використанням телефону або електронної пошти, звичайно, не можна. Тому фахівцям рекомендують в процесі спілкування виявляти обережність і надійно ідентифікувати свого співбесідника. Зрозуміло, повинна використовуватися тільки інформація, що відноситься до співбесідника.

Для отримання комерційної інформації конкурента можуть використовувати різного роду мікрофони, мініатюрні передавачі та ін. У зв'язку з цим, перед початком наради, переговорів ретельно перевіряють приміщення, в якому вони вестимуться. У західних країнах діє розгалужена мережа фірм, що виконують цю роботу за замовленням. Створені спеціальні прилади, які дозволяють встановити захисний екран, що виключає будь-яке прослуховування в таких приміщеннях.

Вважається, що значне просочування комерційної інформації відбувається в ході ведення переговорів і ділового листування. Трапляється це з різних причин: невміння правильно рекламувати свою продукцію, престиж, що невірно розуміється, і т. д. Тут велику роль мають вже згадувані виховання і навчання співробітників. Ще до початку переговорів співробітник повинен чітко представляти, яку інформацію він має право передати партнеру по переговорах, що повинен залишити “за кадром”; необхідно вчити фахівців проводити рекламу за методом “чорного ящика” – вхідні параметри виробу, одержаний результат, а як результат – одержаний секрет фірми. Врешті-решт, працівник, якій веде переговори, повинен усвідомлювати, що від успішно проведених переговорів залежить як процвітання підприємства, так і його особисте благополуччя.

Збирання даних за допомогою Інтернету та інших мереж телекомунікацій сьогодні взагалі звичайне явище. Проте ця надзвичайно приваблива можливість може привести до пошкодження даних, що обробляються на комп’ютері, а саме: ураження комп’ютера різноманітними вірусними програмами, несанкціонованого доступу до даних у локальній мережі та при роботі в Інтернеті, за допомогою так званих програм-шпигунів тощо [9, с. 93-117].

Значне зростання кількості користувачів цієї мережі призвело водночас до поширення кіберзлочинності, в тому числі щодо використання та поширення персональних даних. Комп’ютерні технології та міжнародні комп’ютерні мережі, які є необхідними складовими міжнародної фінансової та банківської діяльності, надали можливість вчинення злочинів економічної спрямованості на національному та міжнародному рівнях. Організовані злочинні угруповання та кримінальні елементи використовують новітні технології для відмивання “брудних” коштів, фінансових махінацій, несанкціонованого доступу до інформаційних систем, поширення неправдивої інформації та інших правопорушень.

На окрему увагу заслуговують файли “cookie”. Ці файли створюються веб-серверами для запису інформації про переглянуті сторінки: дату й час, паролі користувача тощо. Ця інформація використовується для аналізу статистичних даних та створення так званих профілів користувачів (які сторінки переважно переглядає користувач, які товари замовляв тощо). Тому для припинення такої діяльності використовують або знищення файлів “cookie” на вінчестері, або блокування цих файлів завдяки опціям браузерів.

Сьогодні збитки від кіберзлочинності перевищують 100 млрд дол. США [9, с. 113]. За даними американського Інституту комп’ютерної безпеки (Computer Security Institute), хакери використовують такі найпоширеніші методи: підбір ключів, паролів – у 13,9 % злочинів; заміна IP-адрес – у 12,4 % (цей метод атаки передбачає заміну IP-адрес пакетів, що передаються в Інтернеті, так, що вони мають вигляд переданих внутрішніх повідомлень, де кожний вузол довіряє адресній інформації іншого); ініціювання відмови в обслуговуванні (denial of service) – у 16,3 % (вплив на мережу або її окремі частини з метою порушення порядку її штатного функціонування); аналіз трафіка – 11,2 % (прослуховування та дешифрування з метою збирання інформації щодо ключів, паролів тощо); сканування – у 15,9 % (передбачає використання програми, яка перебирає можливі точки входження до системи); підміна, нав’язування, переупорядкування або заміна даних, що передаються мережею, – у 15,6 %; інші методи – 14,7 %. Таким чином, платою за користування Інтернетом є загальне зниження інформаційної безпеки.

Важливим засобом захисту комерційної інформації є встановлення порядку поводження з її носіями, такими як різні документи, креслення, магнітні носії, використовувані в роботі з ПК. Набутий в цій сфері досвід може бути прийнятий як рекомендації при захисті комерційних секретів і передбачає необхідність наявності на носіях комерційної інформації відмітних позначок, що розрізняються залежно від рівня секретності інформації, яка міститься в документі.

Намагатися повністю захистити комерційні відомості, накладаючи обмеження на доступ до них, навряд чи можливо. Сучасне підприємство не може дозволити собі засекречувати всю циркулюючу в ньому комерційну інформацію, тим більше в умовах функціонування глобальної мережі Інтернет, електронної пошти тощо. Це дуже дорого і невигідно, певна частина відомостей повинна використовуватися в рекламі, велика кількість засекречених матеріалів створює непотрібні перешкоди в роботі. Крім того, неможливо підібрати такі штати співробітників, які до всієї інформації ставитимуться як до інформації з обмеженим доступом.

Але здійснювати протидію суперникам по конкурентній боротьбі на ринку теж необхідно. Тут і має відіграти свою роль діяльність щодо визначення ключової інформації, що дійсно є комерційною таємницею підприємства, виявлення імовірних каналів витоку і пошуку можливих шляхів її захисту. Головне – при цьому слід розуміти, що технікотехнологічні засоби, якими б досконалими вони не були, не здатні забезпечити належний захист даних без чітких нормативно-правових та організаційних заходів і суворого нагляду за ними.

Деякі висновки.

1. В електронно-інформаційній сфері підприємницька діяльність має свої особливості щодо публічно-правового регулювання відносин і потребує узагальнення та створення спеціальних юридичних норм і правил, адресованих безпосередньо електронній комерції.

Метою застосування спеціальних норм в окремому нормативно-правовому акті є створення відповідного правового поля щодо гармонізації національних законодавчих актів у аспекті вільного надання інформаційних послуг та забезпечення підвищених юридичних гарантій всім учасникам підприємницької діяльності, у першу чергу малим та середнім підприємствам, які здійснюють ділові операції за допомогою Інтернету.

Враховуючи світовий досвід, вбачається можливим (але не обов’язковим) розробка в Україні окремого нормативно-правового акту – закону, регулюючого питання електронної комерції, включаючи положення про укладення за допомогою електронних засобів договорів і юридичного визнання електронних комерційних операцій, правовому статусі, обов'язках і відповідальності інформаційних посередників.

Проте, сьогодні на вулицях України немає демонстрантів з плакатами “Не можу жити без е-комерції !”.

Якщо розвинені країни вважають за потрібне звертати значну увагу на проблеми е-комерції, то автоматичне перенесення їх нормативно-правових поглядів у законодавство країни з не стабільними політико-адміністративними умовами (як говорять “у нас де три чоловіка там два гетьмана”) та відсутності значного соціального прошарку щодо малого та середнього підприємництва, на якому стоїть стабільність і благополуччя сучасного суспільства та держави, може залишитись лише “на папері”.

2. Практика захисту даних у фірмах і компаніях, що склалася на сьогодні в розвинених країнах, свідчить про те, що чисто адміністративно обмежувальні заходи не завжди спрацьовують. Потрібне серйозне ставлення до навчання персоналу прийомам і методам захисту інформації, а головне – розуміння того, що необхідна сумісність технікотехнологічного захисту даних з нормативно-правовим, системним підходом у регулюванні діяльності щодо використання технологій та мереж.

Досить важливою є підтримка держави в аспекті удосконалення нормативно-правового захисту даних, подальшої деталізації процесуальної діяльності позасудового та судового вирішення спорів, зокрема, щодо надання переваг стороні, яка спочатку володіла правом власності на інформацію та єдиного тлумачення судами конкретних обставин справ щодо електронної комерції.

Використана література

1. Типовой закон ЮНСИТРАЛ об электронной торговле. Принят в г. Нью-Йорке 28.05-14.06.1996 г. на 29-ой сессии ЮНСИТРАЛ // Комиссия ООН по праву международной торговли. Ежегодник. 1996 год. – Том XXVII. – Нью-Йорк: Организация Объединенных Наций, 1998. – С. 319-323 // www.uncitral.org/english/ session/unc.

2. *М. Швець, В. Брижко, Б. Романюк, В. Цимбалюк*. Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти та підходи до упорядкування суспільних інформаційних відносин у зв’язку з автоматизованою обробкою даних у правоохоронній діяльності: Посібник. У 2-х кн. Книга 2. – К.: НДЦПІ АПрН України, 2006 р. – 509 с.

3. Директива 2000/31/ЄС Європейського Парламенту і Ради “Про правові аспекти інформаційних послуг щодо електронної комерції на внутрішньому ринку” від 08.06.2000 р. // Правова інформатика. – № 2(6)/2005. – С. 72-89.

4. *Нельзина О.* Правовой фундамент електронной коммерции в российской и международной практике //www.relga.ru/Environ/WebObjects/tgu-www.woa/wa/Main?textid=1954&level1=main&level2=articles.

5. *В. Дрожжинов, А. Штрик*. Азиатско-Тихоокеанский регион плывёт по волнам э-коммерции //www.pcweek.ru/themes/detail.php?ID=56419.

6. //www.apecsec.org.sg/pubs/freepubs.html#1999.

7. *А. Иоффе*: Законодательство по электронной торговле нужно совершенствовать //www.businesspress.ru/newspaper/article_mId_21961_aId_434369.html.

8. *Бержье Жак*. Промышленный шпионаж. Пер. с фр. – М.: “Международные отношения”, 1972.

9. *В. Брижко, В. Цимбалюк, М. Швець, Ю. Базанов*. е-боротьба в інформаційних війнах та інформаційне право: Монографія; За ред. члена-кореспондента АПрН України, доктора економічних наук, професора М. Швеця. – К.: НДЦПІ АПрН України, 2007 р. – 234 с.

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