УДК 346.544:681.3

В.В. КАРАСЮК, *кандидат технічних наук, доцент,*
Національна юридична академія України ім. Я.Мудрого
М.А. СУДЕЙКО, студентка 3 курсу факультету № 3
Національної юридичної академії України ім. Я.Мудрого

ЕЛЕКТРОННА КОМЕРЦІЯ: ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТРАНЗАКЦІЙ

Анотація. *Про вразливість електронної комерції з боку комп’ютерних злочинців та напрями вдосконалення законодавства з метою запобігання цим злочинам.*

Використання Інтернету для розширення доступу до інформаційно-комунікаційних послуг розглядається як умова інтеграції України у світовий інформаційний простір і розбудови сучасного суспільства [1]. Електронна комерція (далі – ЕК) впевнено займає своє місце серед традиційних засобів бізнесу.

Поняття “електронна комерція”. Концепції “електронного бізнесу” та “електронної комерції” виникли в США у 1980-х роках і стали результатом розвитку більш ранніх ідей глобальної інформаційної економіки, що були теоретичною основою створення внутрішньофірмових і корпоративних інформаційних мереж для використання інформаційних технологій у процесі функціонування організацій [2, с. 47]. Одне з перших визначень “електронної торгівлі” було запропоновано в 1996 році професором В. Звасом [3]. Він терміни “електронний бізнес”, “електронна комерція” та “електронна торгівля” використовував як синоніми. У проаналізованих інформаційних джерелах термін “електронна торгівля” розглядається як складова частина таких більш широких понять, як “електронна комерція” і “електронний бізнес” [4-14].

Вивченням питань електронної торгівлі займалися науковці різних країн. Серед них англійці П. Доулінг, Б. Тейлор, Дж. Тестерман, А. Козьэ, Ф. Трилівен, К. Пейтел, М.І. Мак-Картні; росіяни Л.А. Брагіна, І.Т. Балабанов, А.В. Волокітін, М.В. Макарова, А.П. Маношкін, А.В. Солдатенков, С.А. Савченко, Ю.А. Петров, С.В. Лопаткін. Також питання становлення, формування, розвитку та правового забезпечення електронної торгівлі в Україні розроблюють вітчизняні науковці: В. Брижко, А. Береза, А. Білоусов, І. Голодовський, І. Козак, А. Новицький, Н. Меджибовська, І. Успенський, А. Ходжаев, В. Цимбалюк, А. Чучковська, М. Швець, Ф. Шевченко та інші. Ці дослідження сприяють розвитку електронної комерції як каталізатора поширення сучасних бізнесових технологій у суспільстві.

В цілому електронна торгівля являє собою складну систему інформаційних, економічних і бізнес-процесів, спрямованих на віртуальну реалізацію торгівлі. Поширеним є розуміння електронної комерції як укладення шляхом обміну електронними документами наступних угод: купівля-продаж, поставка, угода про розподіл продукції, агентські відносини, факторинг, лізинг, проектування, консалтинг, інженерія, інвестиційні контракти, страхування, угоди про експлуатацію та концесії, банківські послуги, спільна діяльність та інші форми ділового співробітництва, транспортні послуги тощо [15-17].

В українському законодавстві формальне визначення поняття “електронна комерція” відсутнє. Але це поняття фактично вже визначено практикою його використання і розвитку в суспільстві. Повний аналіз електронної комерції як суспільного явища, його

сутності і змісту наведений у [18], де запропоновано сучасне визначення: *електронна торгівля є формою ділової активності (бізнесу, підприємницької діяльності) за сферами економічної діяльності, змістом якої є будь-які операції, що здійснюються за цивільно-правовими договорами, що передбачають передачу прав власності на товари, надання послуг та проведення робіт шляхом комп’ютерної обробки інформації та передачі повідомлень через комп’ютерну мережу із використанням можливостей інформаційно-телекомунікаційних технологій.*

З іншого боку, необхідно зазначити, що технології електронної комерції є досить привабливими для комп’ютерних злочинців. Цьому є цілий ряд пояснень, що базуються на існуючих принципах обміну інформацією у глобальній комп’ютерній мережі і недосконалостях поширених технологій захисту інформації. В Україні ще не існує чіткої системи протидії комп’ютерним злочинам і захисту сучасних технологій, що базуються на обміні інформацією через мережу Інтернет.

Метою статті є аналіз технологічної та правової вразливості електронної комерції і визначення напрямів подальшого розвитку вітчизняного законодавства з огляду на попередження технологічних правопорушень у цій сфері.

Технологічна основа електронної комерції. Електронна комерція є комплексним поняттям, яке у технологічному плані спирається на обмін комерційною інформацією через мережу Інтернет, а у правовому плані має своєю основою такі категорії, як електронний документ, електронний підпис, електронний обмін документами, електронний договір, електронні розрахунки та деякі інші. Ці категорії мають свій зв’язок і визначають ефективність електронної комерції в цілому.

Аналіз діючих систем дозволив сформувати загальну схему інтегрованого середовища електронної комерції [19]. Послідовність основних дій при використанні засобів електронної комерції наведена на Рис.1.

На рисунку стрілочками показані інформаційні потоки між основними суб’єктами комерційної діяльності через електронну мережу. Підписи стрілок (номери) вказують на послідовність операцій у технологічному процесі ЕК. Поза увагою залишимо провайдерів покупця, магазину, банку, клірингові центри, сервери магазину, службу маркетингу продавця, сервери банків та деяких інших проміжних суб’єктів цього процесу як таких, що забезпечують виключно технічні допоміжні процедури.

Процес взаємодії починається з того, що зацікавлений покупець заходить на сайт електронного магазину і обирає на ньому потрібний йому товар (1). При першій спробі оформити покупку у магазині необхідно зареєструватися і вказати основні дані про себе – включаючи поштову адресу (для доставки товарів) і пароль. У подальшому, при наступних покупках, потрібно буде вказувати тільки пароль. Покупець формує “корзину товарів” і обирає спосіб оплати через Інтернет кредитною карткою.

Параметри кредитної картки (номер, ім’я володаря, строк дії) передаються платіжній системі Інтернет для подальшої авторизації. При чому це найчастіше виконують (2) через сайт магазину, але покупець також сам може передати дані про кредитну картку на сервер платіжній системі (3).

Платіжна система Інтернет передає запит на авторизацію до традиційної платіжної системи (4).

Банк-емітент платіжної картки покупця отримує запит від процесінгового центру платіжної системи (5), перевіряє параметри картки покупця по своїй базі даних рахунків і повертає відповідь (6) процесінговому центру платіжної системи.

Результат процедури авторизації і платоспроможності передається платіжній системі Інтернет (7).

Продавець (Інтернет-магазин) отримує результат авторизації кредитної карти (8).

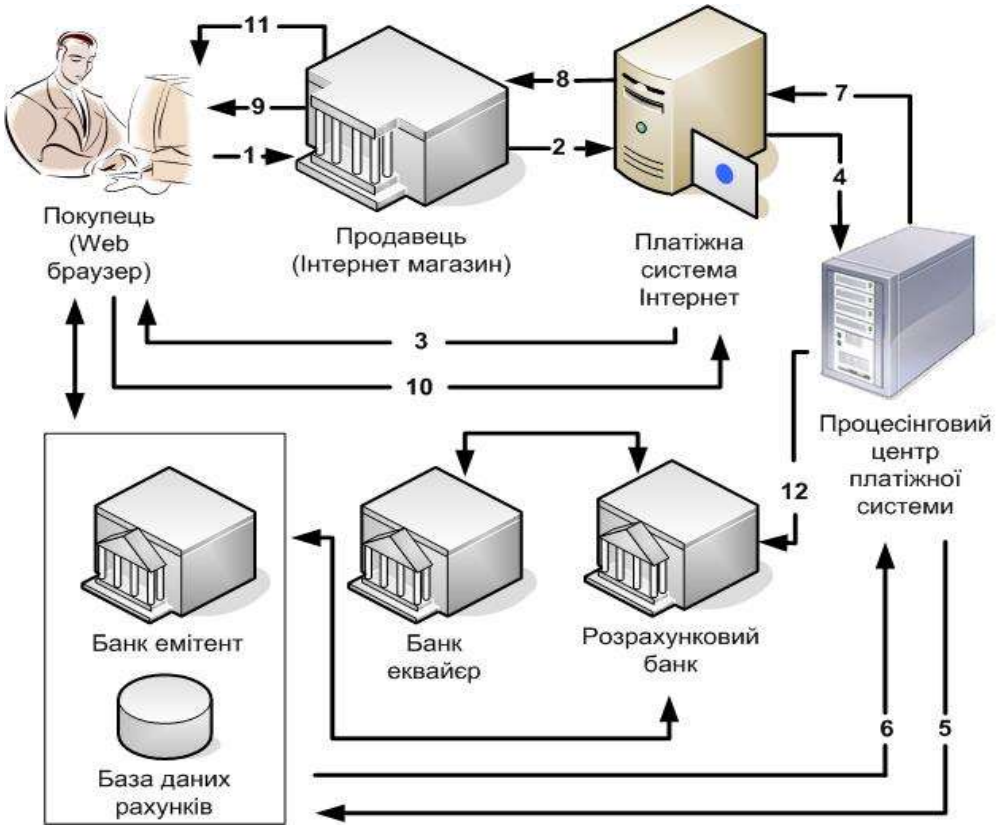

Рис.1. Схема інтегрованого середовища електронної комерції та основних дій при використанні засобів ЕК.

Покупець отримує результат авторизації через сайт магазину (9) або безпосередньо від платіжної системи Інтернет (10).

Якщо результат авторизації позитивний і покупець є платоспроможний, то продавець надсилає замовлений товар покупцю або надає замовлену послугу (11). Тут можуть використовуватись кур’єрська доставка або послуги звичайної пошти. Одночасно процесінговий центр передає у розрахунковий банк відомості про виконану транзакцію (12). Гроші з рахунка покупця у банку-емітенті перераховуються через розрахунковий банк на рахунок магазину у банку-еквайрі.

Схема купівлі товару за допомогою комп’ютера, яка була розглянута, є принциповою. На основі цієї схеми процес купівлі-продажу може ускладнюватися відповідно до умов реалізації. Розглянемо, наприклад, схему купівлі-продажу за допомогою мобільного телефону. *Мобільна комерція (м-комерція) – це використання мініатюрних (кишенькових) переносних пристроїв для комунікаційного мобільного зв'язку з приватними і державними мережами*. Або формальніше – *використання персоніфікованих пристроїв бездротової стільникової комунікації й одержання послуг за допомогою високошвидкісного доступу до Інтернету* [8]. На Рис. 2 схематично показана взаємодія суб’єктів ЕК при використанні мобільних пристроїв.

Мобільний покупець при виконанні кожної транзакції з метою купівлі товару звертається до оператора мобільного зв’язку, який, в свою чергу, звертається до провайдера послуг Інтернету, а той вже звертається до продавця (в Інтернет-магазин), до платіжної системи Інтернет та інших суб’єктів цієї технології. Мобільний покупець ознайомлюється з асортиментом товарів і вибирає товар для купівлі. Магазин через

провайдера в Інтернеті, через оператора мобільного зв’язку пропонує мобільному покупцеві оплатити. Мобільний покупець через оператора мобільного зв’язку, провайдера в Інтернеті звертається до платіжної системи з інформацією про свою кредитну картку і розпорядженням на оплату товару. Далі відбувається “оплата” банком товару, який вибрав у магазині мобільний покупець. І на останньому етапі магазин доставляє мобільному покупцеві товар.

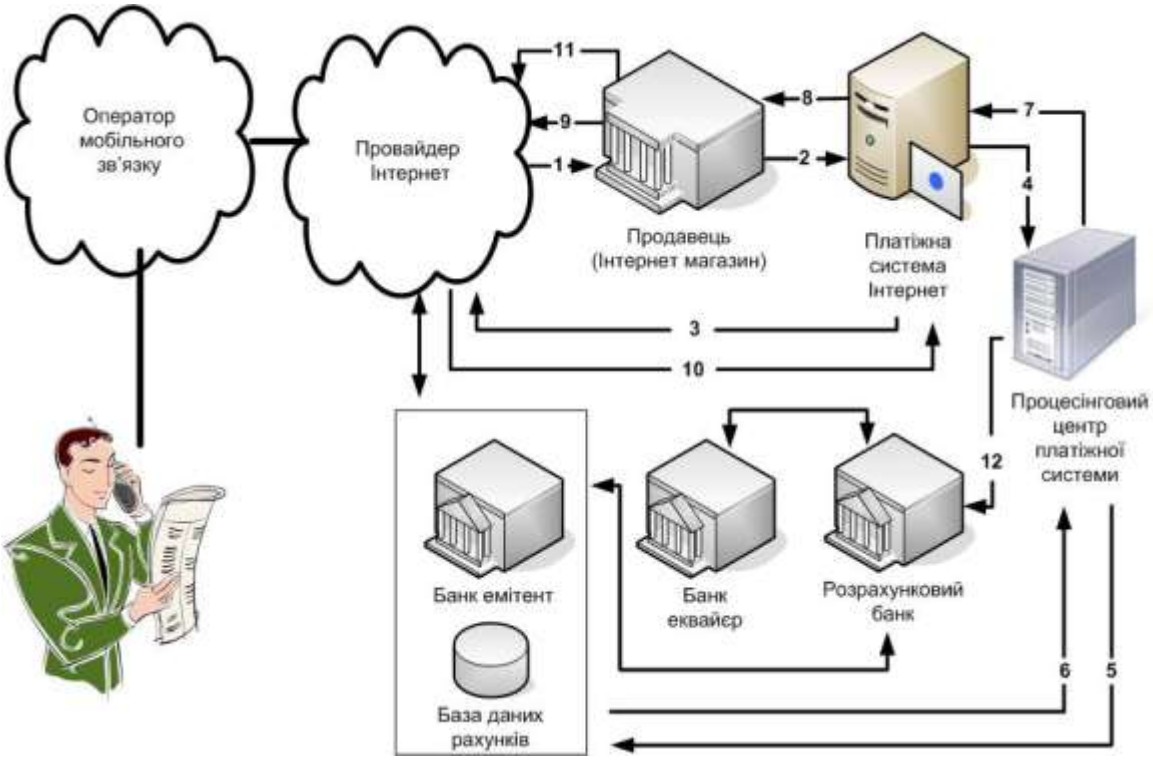

Рис. 2. Схема середовища ЕК та основних інформаційних потоків при використанні мобільних пристроїв.

Якщо порівняти обидві схеми, то можна побачити, що принцип купівлі-продажу фактично один і той же. Єдина різниця в тому, що в схемі на рис. 2 “шлях” інформаційних потоків покупця до магазину ускладнився появою в цьому ланцюгу оператора мобільного зв’язку та провайдера в Інтернеті. До речі, з 6,5 млрд. людей на Землі менше 1 млрд. мають банківські рахунки, але користувачів мобільних телефонів маємо понад 2,5 млрд. Тому слід передбачати випереджаючий ріст кількості клієнтів мобільної комерції.

Практична реалізація ідей електронного бізнесу пов’язана з вирішенням низки технологічних питань. Серед них найбільш складною є проблема безпечного об’єднання різнорідних інформаційних ресурсів, що використовуються на різних етапах ЕК, і створення надійного механізму обміну даними між різними додатками як всередині корпоративних систем, що забезпечують ЕК, так і між ними. Також необхідно зазначити, що апаратно-програмні ресурси системи електронної комерції є розподіленими і розміщуються як на апаратно-програмній платформі власника системи ЕК (Інтернет-магазину); на апаратно-програмних платформах організацій, що надають послуги у супроводженні систем ЕК; так і на апаратно-програмній платформі компанії – оператора зв’язку (Інтернет-провайдера). А це збільшує ризик несанкціонованого зовнішнього втручання у технологічну послідовність операцій ЕК.

Правова основа електронної комерції. Сьогодні спеціальне законодавство України стосовно електронної комерції відсутнє. Є його окремі складові, зокрема звернемо увагу на нормативні акти щодо запровадження електронного цифрового підпису (ЕЦП) і електронного документообігу [20]. Електронний документ являє собою правову основу електронної комерції як явища, пов’язаного з обміном документами у відкритій комп’ютерній мережі. Так, в юридичній літературі поняття електронного документа визначається як інформація, представлена у формі набору станів елементів електронної обчислювальної техніки, інших засобів оброблення, зберігання та передачі інформації, яка може бути перетворена у форму, придатну для однозначного сприйняття людиною, та яка має атрибути ідентифікації документа. У статті 5 Закону України “Про електронні документи та електронний документообіг” від 22.05.2003 р. № 851-4 наведено формальне визначення, а саме: електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа.

Електронний документ має місце тоді, коли відбулося встановлення контакту між потенційним замовником (покупцем) і постачальником (магазином), здійснився обмін інформацією, покупець через мережу Інтернет в онлайновому магазині вибрав товар, заповнив у формі необхідні дані, автоматично поставив електронний підпис у цьому документі. Тепер цей документ являє сукупність даних, отриману за допомогою криптографічного перетворення вмісту електронного документа, яка дає змогу підтвердити його цілісність та ідентифікувати особу, яка його підписала [21]. Після цього виконується процес формування наступних документів, їх оброблення, зберігання, відправлення, одержання, перевірка та використання, що становить собою електронний документообіг. А вже після цієї перевірки (авторизації) відбуваються електронні розрахунки з використанням електронного переказу грошей, кредитних карток, електронних чеків, електронних грошей за укладеним електронним договором, в результаті яких банк перераховує з персонального рахунку покупця гроші на рахунок магазину.

Щодо практичної реалізації технології ЕЦП, то сьогодні в Україні створений і функціонує центральний засвідчувальний орган, декілька центрів сертифікації ключів успішно пройшли процедуру акредитації у відповідності із законодавством, розроблено ряд нормативних документів для забезпечення процедур ЕЦП [22]. Але цього ще явно недостатньо для повноцінної підтримки технології ЕК.

Для зацікавленого дослідника наведемо перелік нормативних документів, що є правовою основою використання електронної комерції в Україні:

Закони України “Про Національну програму інформатизації” № 74/98-ВР, “Про Концепцію Національної програми інформатизації” № 75/98-ВР, “Про затвердження загальної Національної програми інформатизації на 1998-2000 роки” № 76/98-ВР, “Про платіжні системи та переказ грошей в Україні” № 2346-3, “Про електронні документи та електронний документообіг” № 851-4, “Про електронний цифровий підпис” № 852-4, “Про внесення змін до Закону України “Про платіжні системи та переказ грошей в Україні” № 2056-4;

Постанова ВР України “Про затвердження завдань Національної програми інформатизації на 2006 – 2008 роки” № 3075-4, Розпорядження ВР України № 552-р “Про затвердження переліку завдань Національної програми інформатизації на 2006 рік, їх державних замовників та обсягів фінансування”;

Постанова Національного банку України від 10.06.1999 р. № 280, якою затверджено Правила організації захисту електронних банківських документів;

Постанова КМ України “Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу” від 26.05.2004 р.

№ 680 (зі змінами), Постанова КМ України “Про деякі питання здійснення розрахунків за продані товари (надані послуги) з використанням спеціальних платіжних засобів” від 29.03.2006 р. № 377, Тимчасове положення “Про застосування мобільного платіжного інструмента в Національній системі масових електронних платежів” від 31.08.2006 р. № 71, Розпорядження Кабінету Міністрів України від 26.04.2007 р. № 238 “Про затвердження заходів щодо виконання в 2007 році Плану дій Україна-ЄС”, Угода між Кабінетом Міністрів України та Урядом Республіки Польща про співробітництво у сфері інформатизації від 11.04.2005 року, затверджено Постановою Кабінету Міністрів України № 992;

Указ Президента України “Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні” від 31.07.2000 р. № 928;

Наказ “Про затвердження Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації” від 12.06.2007 р. № 144, Наказ “Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної та відкритої інформації з використання цифрового підпису” від 20.07.2007 р. №141.

Безпека здійснення електронної комерції. Основним гальмом на шляху широкого розповсюдження електронної комерції є недостатня її безпека.

Безпека електронної комерції являє собою стан захищеності інтересів суб’єктів відносин, які здійснюють комерційні операції за допомогою технологій ЕК від загроз матеріальних та інших втрат. Загроз дуже багато. Кількість протиправних схем, які існують у глобальній мережі, обмежується лише уявою зловмисників. Серед найпоширеніших з них – фітинг, шахрайства, пов’язані з електронними переказами, викрадення комп’ютерних даних, віртуальний шантаж тощо.

На початок 2007 року кількість веб-сайтів у світі перевищила 100 млн. Значна частина з них присвячена Інтернет-торгівлі, яка є зручним механізмом для прискорення бізнесу. Можливість не виходячи з дому чи офісу замовляти собі будь-які товари, починаючи від піцци і закінчуючи дорогими автомобілями, оцінили мільйони користувачів Інтернету. У своєму виступі наприкінці 2007 року голова виконавчої влади ЄС Жозе Мануель Баррозу заявив “…ми чекаємо, що у найближчі п’ять років обсяги Інтернет-торгівлі подвояться і досягнуть 263 мільярдів євро на рік…”. При цьому найходовішим товаром є книжки (купують 212 мільйонів людей), далі ідуть DVD і відеоігри (135 мільйонів покупців). Приблизно стільки ж оплачують через Інтернет авіаквитки, а 128 мільйонів людей користується он-лайн-сервісами для купівлі одягу і взуття. За даними соціологічних опитувань, чверть жителів великих міст України купляли товари через Інтернет. Майже половина громадян у віці до 30-ти років робили покупки за допомогою Інтернету. Серед респондентів у віці 30-40 років таких уже третина. Серед людей похилого віку Інтернет-покупців виявилося тільки 6 % [23]. До відома, кількість користувачів мережі Інтернет в Україні на 2008 рік становить 21 % загальної кількості жителів. До кінця 2010 року кількість передбачуваних Інтернет-користувачів в Україні підвищиться до 27 %. За даними Асоціації учасників електронного бізнесу України ринок Інтернет-торгівлі України росте на 100 % на рік. Найбільш прибутковою виявилася торгівля одягом. Серед вдалих проектів Інтернет-торгівлі можна згадати магазин Azbooka (//www.azbooka. com), електронний магазин фірми “КАПРО” (//www.kapro.com.ua), сайт видавницької фірми “Мак Сим” (//www.knig.net) та інші.

Відповідно до поширення використання Інтернет-технологій та зростання обсягів коштів, які переказуються через глобальну мережу, злочинці також починають використовувати новітні технології.

Як стверджує статистика злочинів МВС, у сфері високих інформаційних технологій за 2005 рік було скоєно 615 злочинів, за 2006 рік – 583, за 2007 рік – 656, а за 2008 – 691 [24]. І тільки в лютому 2005 р. експерти спеціально створеної робочої групи по протидії фішингу виявили 2625 шахрайських сайтів і більше 13000 електронних листів. Тобто злочинність на цьому напрямку зростає.

Повернемося до схеми на рис. 1 і проаналізуємо можливі фактори спричинення шкоди. Основними вразливими місцями у даній схемі є: процесінговий центр платіжної системи, бази даних рахунків і процес передачі параметрів кредитної картки по мережі. Особливо небезпечною є операція передачі параметрів кредитної картки, яка виконується або безпосередньо через заповнення форми на сайті магазину (2), після чого дані передаються платіжній системі Інтернет, або заповнення форми на сервері платіжної системи (3).

На етапі вибору товару (1) покупець може звернутися до неіснуючого магазину, прийнявши його за справжній. Покупець вибере товар, оформить покупку, тобто заповнить необхідні параметри своєї картки на запропонованій формі веб-сторінки неіснуючого магазину, банк переведе гроші з рахунка покупця на рахунок шахрайського магазину, і в результаті покупець витратить гроші і не отримає товар.

Для ілюстрації такої схеми розглянемо один приклад. У березні 2006 р. співробітники підрозділу контррозвідувального захисту економіки Управління Служби безпеки України в Луганській області та Національного бюро Інтерполу США викрили і припинили масштабне транснаціональне шахрайство, пов’язане з торгівлею через Інтернет. Мешкаючи на території України, підозрювані обманювали клієнтів із-за кордону, пропонуючи через Інтернет-аукціон “e-Bay” різні товари, однак після того, як отримували гроші, не надавали їх. Організаторами шахрайства, за даними СБУ, виявилися 23 і 28-літній українці, яким сприяли співробітники Луганської філії одного з вітчизняних комерційних банків. Вони відкрили на підставних осіб кілька поточних рахунків у доларах США, на які протягом останніх двох років перераховували кошти, отримані від фіктивного продажу товарів через Інтернет-аукціон. Зацікавлені товарами клієнти перераховували кошти нібито на рахунки закордонних компаній, які насправді відкрили українці, котрі постійно мешкають у США і котрі допомагали організаторам. Готівку знімали підставні особи або самі організатори за підробленими документами. Таким чином, їм вдалося отримати понад 150 тис. доларів [25].

У зв’язку з тим, що бази даних Інтернет-магазинів містять значні обсяги приватної інформації, вони є постійною мішенню хакерів. Для запобігання виникнення наведених ситуацій, покупець при кожній купівлі товару в магазині повинен оцінювати надійність продавця. А саме, можна передбачити, що операція з компанією, що має крім електронного магазину ще і реальний бізнес, менш ризикована. Кількість найменувань товарів у каталозі дозволяє судити про розмір компанії (чим вона більша, тим менший ризик).

На веб-сайті повинна бути наведена не тільки адреса електронної пошти, а й фізична (юридична) адреса, телефон фірми, за яким покупці могли б звернутися у випадку виникнення певних проблем. Має значення і популярність торгової марки, а також організаційна форма підприємства, що стоїть за Інтернет-магазином (із загальних міркувань, ЗАТ або ТОВ надійніше, ніж ПП). Якщо серед партнерів електронного магазину є відомі компанії, це також може вплинути на рівень довіри до нього, оскільки

більшість великих фірм, особливо західних, пильнують власну репутацію, працюють тільки з перевіреними організаціями.

Про серйозність магазину можна судити (хоч і вельми умовно) навіть за адресою в мережі (URL). Якщо магазин розташований за звичайною адресою чи за IP-адресою (наприклад, 190.127.64.135) або на безкоштовному сервері, то це повинно викликати певну підозру. Або адресу ще просто не встигли зареєструвати, або на це немає грошей (хоч сума дуже невелика). Можна враховувати різні непрямі дані. Наприклад, якість виготовлення веб-сайта (електронної вітрини), електронного магазину, набір додаткових послуг (гарантійне зобов’язання, повернення грошей при незадовільному обслуговуванні), пророблена система он-лайн-допомоги покупцеві, виразне пояснення способів усунення можливих недоліків. Комплексний розгляд всіх перелічених вище чинників повинен допомогти покупцеві здійснити раціональний вибір.

На етапі авторизації платника покупець підтверджує намір купівлі, заповнює електронні документи і ставить електронний підпис. На цьому етапі злочинець може запропонувати заповнити фальшиву форму, яка повністю збігається з формою реального магазину, вписати в неї номер банківського рахунку. Цей “трюк” називається фішингом, що являє собою вид Інтернет-шахрайства, мета якого – отримати персональні дані користувачів. Якщо покупець по необачності впише в запропоновану форму свої дані, то злочинець, скориставшись номером рахунку, зніме всі кошти, які на ньому містяться.

В описану вище “пастку” може потрапити покупець-початківець, а вже досвідчений клієнт може бути введений в оману іншим способом. Після того як він заповнить документи і відправить їх, злочинець надішле покупцю прохання повторити заповнення, пояснивши це технічним збоєм. Заволодіє відомостями і, начебто від імені покупця, здійснить покупку: дасть банку команду “оплатити”, банк переведе суму на рахунок магазину, а той відправить товар на адресу злочинця, а не покупця.

Щоб цього не сталося, банк при команді покупця “оплатити” повинен перевірити істинність покупця. Це здійснюється за допомогою таких методів захисту, таких як:

- аутентифікація;
- шифрування;
- авторизація;
- використання брандмауерів.

Аутентифікація попереджує неавторизований доступ до інформації обмеженого поширення і звичайно здійснюється за допомогою паролів.

Шифрування забезпечує те, що інформація, яка передається по мережі, може бути прочитана і модифікована тільки авторизованими користувачами.

Системи авторизації гарантують, що неавторизовані користувачі не зможуть отримати доступ до файлів і даних, призначених для обмеженого поширення.

Як стверджує статистика, використання брандмауера може зупинити до 90 % спроб неавторизованого доступу.

Для захисту інформації про покупця, що передається по мережі, від перехоплення використовуються протоколи шифрування SSL (Secure Sockets Layer) і SET (Secure Electronic Transaction). В основі SSL лежить принцип асиметричного шифрування з відкритим ключем, а у якості шифрувальної схеми використовується алгоритм RSA, хоча з огляду на технічні особливості цей алгоритм вважається менш надійним. SET є більш захищеним протоколом, але технологічно він складніший і дорожчий у застосуванні. Тому його широке впровадження не відбувається і питання безпеки є відкритим.

Наведемо приклади злочинів, побудованих за такою схемою. Відомим став скандал з “Politshop”. Шахраї створили простий магазин, оформили неяскраву вітрину, підключилися до платіжної системи Cyberplat і стали активно знімати гроші з кредитних карток, за допомогою їх номерів. При реєстрації на сайтах система просила ввести номер кредитної картки, а після цього пропонувала здійснити “безкоштовний” ознайомчий тур. Користувач підписувався на послуги, позбавлені цін. За це з картки знімалися гроші (від $ 20 до $ 90). У такий спосіб “Crescent Publishing Group, Inc” заробила 188 мільйонів доларів. А за вироком суду компанія сплатила клієнтам всього 30 мільйонів [26].

Інший приклад. “Хакери зламали сайт МВС Великої Британії і використали його для здійснення Інтернет-шахрайств” – пише “Газета. Зламщики створили на сайті підробну сторінку, потім розіслали мільйонам користувачів Інтернет-мережі так звані фішинг-листи від імені італійського банку, запрошуючи користувачів відвідати сторінку і підтвердити свої банківські паролі. Будь-який користувач, який залишив тут свій пароль, відкривав шахраям доступ до свого банківського рахунку [27]. Таких випадків досить багато.

Що ж стосується останніх етапів схеми розрахунків у електронному магазині, то злочини, скоєні на них, найчастіше є продовженням злочинів, скоєних на попередніх етапах.

Щодо порад користувачам Інтернет-магазинів, то серед традиційних, таких як: не замовляти занадто дешеві товари, що в звичайному магазині коштують набагато дорожче, переконатися по телефону про наявність служби підтримки, не висилати свої паролі, не копіювати безкоштовного програмного забезпечення тощо, слід підкреслити наступне: користувачі Інтернету разі втрати електронних коштів повинні також мати змогу швидко звернутися до певної організаційної структури, адже докази щодо викрадення комп’ютерної інформації, щодо шахрайства в мережі довго не існують.

Недоліки правової підтримки безпеки електронної комерції в Україні. Серед положень багатьох правових актів, що опосередковано висвітлюють поняття “електронна комерція” є чимало прогалин у регулюванні цієї сучасної технології.

Щоб визначитися з недоліками, які впливають на безпеку ЕК, згадаємо вразливості основних операцій технологічної послідовності ЕК.

При виборі товару на сайті електронного магазину покупець наражається на небезпеку спілкування з шахрайською веб-сторінкою. Відповідальність за створення копії (за підробку) у Інтернет-просторі справжнього магазину не встановлено, за винятком порушення при певних умовах норм авторського права. Чинний Кримінальний кодекс у розділі 16 “Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку” не містить статей, які встановлювали б покарання за такий злочин. Тому пропонуємо доопрацювати розділ XVI КК і прийняти статтю 361^3, наприклад у такій редакції:

“Стаття 361^3. Несанкціоноване втручання у процес здійснення електронної комерції

Підміна даних, незаконне отримання паролів, ідентифікаційних даних за допомогою шкідливих програм, підробних веб-сторінок, втручання в роботу мобільних мереж з метою отримання паролів та ідентифікаційних даних, їх несанкціоноване використання в електронній комерції, караються... ”

Наступна важлива операція, пов’язана з авторизацією покупця (платника) не є повністю захищеною. Вона регулюється законами України “Про електронні документи

та електронний документообіг” та “Про електронний цифровий підпис”. Неврегульованою залишається ситуація, пов’язана з тим, що злочинець, ввівши в оману покупця за допомогою неіснуючого магазину, намагається злочинним шляхом отримати конфіденційну інформацію, щоб у подальшому отримати гроші або товар. Тож можемо зробити висновок, що Кримінальний кодекс не містить норм, які б встановлювали відповідальність за фішинг у електронній комерції. Тому знову звертаємо увагу на доцільність наведеного формулювання статті 361^3.

Інші дії технологічної послідовності ЕК можуть бути розглянуті як такі, що до їх порушень можуть бути застосованими норми чинного Кримінального кодексу.

Підкреслимо, що в даному дослідженні не торкаємося проблем, підпорядкованих нормам цивільного права, проблем інтелектуальної власності тощо.

Висновки.

У результаті проведеного дослідження технологічних основ електронної комерції і їх правового забезпечення робимо висновок, що дані дії не мають у повній мірі правового захисту. Але вони є суттєвими і впливають на безпеку проведення операцій електронної комерції.

Тому для забезпечення ефективності і надійності технології електронної комерції необхідно внести доповнення до Кримінального кодексу України (ст. 361^3, розділ 16) та прийняти низку інших нормативних документів для вдосконалення механізмів функціонування електронного бізнесу в Україні, системи державного контролю та правоохоронної діяльності з урахуванням світового досвіду в цій сфері.

Використана література

1. Концепція розвитку телекомунікацій в Україні до 2010 року : Розпорядження Кабінету Міністрів України від 7 червня 2006 р. № 316-р. – Режим доступу: //www.zakon1.rada.gov.ua/ cgi-bin/laws/main.cgi?page=1&nreg=316-2006-%F0

2. Міщенко В.І. Електронний бізнес на ринку фінансових послуг : практич. посіб. / В.І. Міщенко, А.В. Шаповалов, Г.В. Юрчук. – К. : “Знання”, КОО, 2003. – 278 с.

3. Zwass V. Electronic Commerce: Structures and Issues / International Journal of Electronic Commerce. – 1996. – Vol. 1. – № 1. – P. 3-23. – Режим доступу: //www.gvsu.edu/ssd/ijec/v1n1/p003 full.html

4. Волокитин А.В. Электронная коммерция : учеб. пособ. / А.В. Волокитин, А.П. Маношкин, А.В. Солдатенков и др. ; под общ. ред. Л.Д. Реймана – М. : НТЦ “ФИОРД-ИНФО”, 2002. – 272 с.

5. Филин С.А., Никольская Н.В. Электронный бизнес экономики информационного общества // Финансы и кредит. – 2006. – № 16. – С. 60-71.

6. Електронна комерція : навч. посібник / [А.М. Береза, І.А. Козак, Ф.А. Шевченко та ін.]. – К.: КНЕУ, 2002. – 326 с.

7. Макарова М.В. Електронна комерція : посібник для студ. вищ. навч. закл. / М.В. Макарова. – К.: Видавничий центр “Академія”, 2002. – 272 с.

8. Брижко В., Швець М. До питання е-торгівлі та захисту персональних даних // Правова інформатика. – 2007 – № 1(13). – С. 14-27.

9. Балабанов И.Т. Интерактивный бизнес / И.Т. Балабанов. – СПб, 2001. – 73 с.

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

11. Симонович С.В. Інформатика для юристів та економістів / С.В. Симонович. – СПб, 2001. – 345 с.

12. Танасюк П. Роздрібна Internet-торгівля в Україні: стан та перспективи розвитку. – Режим доступу: //www.ise.kiev.ua.pubn.tanasuk_ec.htm

13. Электронная коммерция : учеб. пособие ; под общ. ред. Л.А. Брагина. – М. : Экономистъ, 2005. – 14, (1) с.

14. Ильичев С.К. Особенности налогообложения в сфере электронной коммерции / С.К. Ильичев. – М. : Маркет ДС, 2004. – 12, [1] с.

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

16. Соловяненко Н.И. Правовые проблемы электронной коммерции в РФ. – Режим доступу: //www.fe.msk.ru/otstavnov/compunomika/v0.n05a03.htm

17. Наумов В. Ключевые вопросы государственного регулирования Интернет-коммерции в РФ. – Режим доступу: //www.russianlaw.net

18. Новицький А., Позняков С. Сутність та зміст поняття “електронна торгівля” // Правова інформатика. – 2007. – № 1(13). – С. 7-13.

19. Тищенко Е.Н., Строкачева О.А. Проблематика оценки защищенности информационных ресурсов на примере систем электронной коммерции // Информационное противодействие угрозам терроризма. – 2008. – № 11. – С. 32-40. – (Науч.-практический журнал).

20. В. Брижко. Електронна комерція: правові засади та заходи удосконалення : монографія / В. Брижко, А. Новицький, М. Швець ; за ред. А. Москаленка, к. ф.-м. наук О. Гладківської. – К. : НДЦПІ АПрН України, 2008. – 149 с.

21. Дутов М. Правовое обеспечение развития электронной коммерции // Підприємництво, господарство та право. – 2001. – № 4. – С. 33.

22. В Украине уже можно использовать электронную подпись. – (По материалам УНИАН. – 2006). – Режим доступу: //www.podrobnosti.ua/ptheme/internet/2006/09 /26/351767.html

23. Четверть украинцев покупают товары в Интернете (соцопрос) // Информационное агентство “Экономические новости”. – 2008. – Режим доступу: //www.economic-ua.com/articles /45422

24. Статистика МВС. – (Офіційний веб-сайт Міністерства внутрішніх справ). – Режим доступу: //www.mvs.gov.ua/mvs/control

25. Новости агентства / Українські новини, від 11.09.2007 р. – Режим доступу: //www.ukra news.com

26. Интернет-надувательство / Интернет-реклама. Реклама и бизнес в Интернете. – (Статьи о интернет-рекламе и электронной коммерции). – Режим доступу: //www.reklamirui.com/article. php?articleid=105

27. Хакеры взломали сайт МВД Британии. – Режим доступу: //www.ua.glavred.info/arc hive/2008/06/08/115940-14.html

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