Summary

The article describes external economic structure of enterprise. It tells us about the necessary of adaptation on the macroeconomic level. The author concludes that Ukrainian enterprises shouldn't use only one external economic organization form. They should take into account the conjuncture of a market using different external economic forms.

УДК 336.717.1:681.3

***Савченко А.С.**, Національний банк України*

ЕЛЕКТРОННА КОМЕРЦІЯ З ВИКОРИСТАННЯМ ЗАСОБІВ INTERNET

В статті розглянуто застосування і можливості сучасних електронних платіжних систем в процесі купівлі товарів та надання послуг. Вказано на проблеми, пов'язані із впровадженням електронної комерції, та шляхи їх вирішення.

Ключові слова: Internet, системи організації платежів, захист платежів.

Існування загальносвітових комп'ютерних мереж викликає невпізнанні зміни у людському суспільстві. Зменшується залежність від таких факторів як відстань та місцезнаходження, зникають кордони та обмеження для переміщення інформації. Завдяки Internet виникає єдина телекомунікаційна інфраструктура, і більшість споживачів у всьому світі незабаром матимуть можливість користуватися рядом послуг та здійснювати купівлю товарів, залишаючись вдома. Це означає, що велика частка комерційних операцій перейде з традиційної сфери до нового комунікаційного середовища, у зв'язку з чим виникнуть нові типи комерційних установ, діяльність яких стане реальною лише завдяки необмеженим можливостям, які створює це середовище.

Традиційні засоби платежів, наприклад, готівка і навіть більш сучасні досягнення у сфері платіжних систем – кредитні картки чи перерахування коштів за допомогою торговельних платіжних терміналів – виявляються або зовсім непридатними для використання як платіжні механізми у цьому новому середовищі, або недостатньо надійними через проблеми безпеки чи неефективності. До того ж, оскільки технології, що базуються на використанні інтелектуальних карток, не відрізняються принципово від тих, які застосовуються в глобальних мережах, такі системи заміни готівки в "реальному" світі можуть бути інтегровані з мережними платіжними механізмами так само, як телебачення може бути інтегроване з іншими формами передачі інформації та телекомунікації.

Завдяки комерційному використанню нової інфраструктури компанії розгортають діяльність, спрямовану на максимальне застосування режиму on-line і можливостей глобальної мережі в процесі купівлі товарів та надання послуг. Компанії, які працюють у галузі інформаційних та телекомунікаційних технологій, отримують нові широкі можливості для свого розвитку і новий перспективний ринок. Провідну роль у всіх цих змінах відіграють електронні платіжні системи.

Організація платежів у мережі Internet

Розрахунки з використанням телекомунікаційної інфраструктури здебільшого здійснюються у режимі on-line. При цьому перевіряється можливість здійснення платежу – достатність коштів у платника.

Більшість систем, що використовуються для електронної комерції в Internet, виконують кліринг усіх платежів у єдиному розрахунковому банку. Однак існує можливість позбавитися цього обмеження.

Найбільш поширена в Internet електронна комерція з використанням номерів кредитних карток. Існують також самостійні платіжні системи, хоча вони менш поширені.

Завдяки незначній спеціалізації, відкритості практично для будь-якого продавця та малим затратам на телекомунікації платіжні системи з використанням "електронних грошей" та відкритих мереж Internet характеризуються дуже невисокою вартістю трансакцій. Точна статистика щодо цих систем відсутня, але за деякими оцінками вартість однієї трансакції в ній становить 1-5 цента, а можливо, навіть і менше.

В Internet нині запроваджуються платіжні системи, які забезпечують обмежену анонімність платежів. Неанонімні системи дозволяють ідентифікувати кожну конкретну покупку. Перевагою таких систем вважається можливість створювати високоефективні бази даних для маркетингу, а також розробляти стратегію змішнення стосунків з клієнтами. Вважається також, що анонімність сприяє кримінальній діяльності та ухиленню від сплати податків. З іншого боку, часто висуваються аргументи, що відсутність анонімності є втручанням у приватне життя споживачів. Тому поєднання позитивних властивостей обох підходів паралельно з обмеженням притаманних їм недоліків є дуже перспективним.

Методи захисту платежів у мережі Internet

Слабким місцем мережної інфраструктури є незахищені канали зв'язку, де існує можливість появи неіснуючих платежів, перехоплення та несанкціонованого використання платіжних даних, інших проявів шахрайства та зловживань. Такі випадки траплялися в

Internet. Існують два шляхи захисту передачі інформації: ізолювання мережі, яка використовується для обробки платежів, тобто використання приватних мереж, і шифрування даних.

Загальновизнано, що асиметричні алгоритми шифрування забезпечують вищий рівень надійності та безпеки. Найбільш поширене шифрування за допомогою відкритих ключів. Для розшифрування використовуються таємні ключі. Кількість можливих комбінацій, придатних для розшифрування зашифрованої за допомогою відкритих ключів інформації, залежить від довжини ключа в бітах. Вживання довших послідовностей у ролі ключів дозволяє випереджати можливості сучасних комп'ютерів, забезпечуючи надійний захист найважливішої інформації. Донедавна в Internet для захисту інформації найчастіше застосовувалися ключі довжиною 40 біт. Але ці ключі були легко розкриті (слід зазначити, що використання такого ненадійного засобу було наслідком дуже жорстких обмежень на експорт із США потужних шифрувальних засобів). Нині в Internet розповсюджені ключі довжиною 1024 біт або навіть довші, що робить практично неможливим їх розкриття.

У платіжних системах важливим завданням є ідентифікація учасників платежу (автентифікація). Це робиться для обмеження доступу до платіжних засобів, надаючи право на такий доступ лише їх власникам, та для забезпечення можливості одержувати повідомлення про платіжні операції лише тим, кому вони адресовані. Надійна автентифікація сприяє також підвищенню рівня взаємної довіри між учасниками електронної комерції. На поточний момент в Internet застосовуються різноманітні засоби автентифікації. До них належить персональний ідентифікаційний код (PIN-код), який потрібно ввести перед виконанням фінансової операції. Але незначна довжина таких кодів дозволяє шахраям досить легко долати такі методи захисту.

Для захисту більш вдалим виявилося використання комп'ютерних паролів, які мають більшу довжину і складнішу структуру, що робить важчим їх розгадування. Цей метод досить широко застосовується в Internet, оскільки в ньому доступ до локальних систем контролюється шляхом використання паролів, але надійний результат можна мати лише за умови правильного використання.

Дуже ефективним засобом захисту є електронний підпис. Його застосування передбачає наявність у того, хто цей підпис перевіряє, відкритого ключа, що відповідає застосованому особистому ключу (підпису) відправника електронного документа. Однак, при отриманні такого відкритого ключа не виключено шахрайство, внаслідок якого буде передано підроблений відкритий ключ, який автентифікуватиме підроблені повідомлення. Щоб запобігти цьому, застосовується практика сертифікування (підтвердження) відкритих ключів з боку уповноваженої на це установи або організації, яка заслуговує на довіру. Таку установу чи організацію називають сертифікуючою, і вона ставить свій електронний підпис на відкритих ключах, які надаються користувачам платіжної системи. Відкритий ключ сертифікуючої установи повинен надаватися з використанням надійно захищених каналів. Ця установа сертифікує відкриті ключі учасників системи лише після перевірки їх тотожності з використанням захищених каналів або інших методів, що забезпечують достатній рівень безпеки, і лише підтверджені нею відкриті ключі вважаються чинними. Жодна з платіжних систем, які на поточний момент використовуються або випробовуються для електронної комерції через Internet, не є монопольною і не займає виключних позицій. Порівняно із загальною кількістю користувачів Internet кожна з них задовольняє потреби незначної групи. Далі розглядаються деякі з них.

Для виконання платежів через Internet широко використовується система з трьох протоколів ІКР (i = 1, 2, 3). Відмінність між протоколами пов'язана з рівнем безпеки і полягає у різній кількості сторін (покупець, продавець та еквайр), що користуються парами відкритих ключів для розшифрування надісланої до них інформації. На першому рівні таку пару ключів використовує лише еквайр, на другому – також і продавець, а на третьому – всі учасники торговельної операції. При цьому застосовуються лише загальновідомі методи криптографії з використанням відкритих ключів. Результат – надійно захищений протокол доступу в Internet, який практично виключає можливість зловживання з боку будь-якого учасника комерційної операції. Мережею передається лише авторизація покупця, тобто дозвіл перерахувати гроші з його рахунка. Для перерахування коштів використовуються існуючі механізми платежів.

На відміну від вищезазначеного підходу, система STT (Secure Transaction Technology), що була розроблена VISA International разом із Microsoft в 1995 році, передбачає певний платіжний механізм. Це – віртуальна система платежів за допомогою кредитних карток, яка забезпечує захист платіжних операцій у загальнодоступній мережі, якою і є Internet. Кожний учасник системи має дві пари ключів. В одній парі ключ для шифрування є відкритим, а для розшифрування використовується таємний ключ. В іншій парі відкритим є ключ розшифрування, а відповідний шифрувальний ключ відіграє роль електронного підпису. Усі відкриті ключі сертифікує Асоціація кредитних карток, яка засвідчує своїм електронним підписом, що ключ належить певному користувачеві.

Майже одночасно з розробкою STT MasterCard у співпраці з IBM та з іншими компаніями розробили систему SEPP (Secure Electronic Payment Protocol), що також відображає в Internet існуючу систему платежів за допомогою кредитних карток і використовує відкриті ключі та практику електронної сертифікації. Ця технологія передбачає більш ширше використання приватних банківських мереж для здійснення платежів. Банки-учасники платіжної операції можуть навіть не надавати послуги через Internet, де мусить діяти лише центральна сертифікуюча установа.

В 1996 році на базі STT і SEPP обидві конкуруючі асоціації створили єдиний стандарт – SET. Перш за

все, його варто розглядати як комунікаційний стандарт, а не як платіжний механізм.

Дослідна експлуатація системи DigiCash в Internet розпочалася ще в 1994 році, а з 1995-го вона функціонує на комерційній основі. Користувачі цієї системи (як клієнти, так і продавці) повинні мати рахунки у банку-емітенті відповідних електронних грошей. Зараз такі банки є в чотирьох країнах: США, Фінляндії, Швеції та Німеччині. DigiCash надає можливість відстежувати платежі лише тому користувачеві, який здійснює відповідний платіж. Дані про трансакцію зберігаються у зашифрованому вигляді й ключ для розшифрування має лише платник.

Система First Virtual діє в Internet як механізм виставлення рахунків за платежі з використанням кредитних карток. Її можна уявити як щось на зразок електронного торговельного центру, що складається з великої кількості маленьких крамниць, де замовлення товарів та отримання грошей здійснюється за допомогою електронної пошти через мережу Internet. Кожний користувач відкриває у системі "рахунок", який містить ім'я, адресу електронної пошти та дані кредитної картки, що надаються за телефоном. Здійснюючи покупку, користувач повідомляє електронній крамниці своє ім'я та адресу електронної пошти, вона видає товар і передає рахунок для обробки у систему, яка дебетує кредитну картку покупця, отримавши його згоду електронною поштою. Ця процедура проста і дешева, але досить повільна (термін виконання платежу інколи перевищує 3 місяці) і недостатньо захищена. Щоправда, вона не створює умов для значного шахрайства, адже шахрайським шляхом можна отримати лише послуги, а не гроші.

CyberCash – найпоширеніша система надання в Internet надійно захищених послуг щодо платежів з використанням карток. У ній використовується програмний захист платіжної інформації на основі шифрування. Система характеризується досить високим рівнем контролю трансакцій та відносно високою вартістю. Тому вона більш придатна для платежів великими сумами.

Дуже простою і зручною системою платежів із використанням "електронних грошей" є NetCash. Користувач надсилає до банку гроші в якійсь формі, наприклад, у вигляді звичайного чека. Банк електронною поштою повідомляє систему про отриману суму із урахуванням його комісійних та "номер електронної банкноти". Користувач витрачає ці гроші, передаючи "банкноту" продавцю електронною поштою. Продавець перевіряє справжність "електронної банкноти" у банку і, в разі підтвердження, може отримати від банку аналогічну "електронну банкноту" або внести ці гроші на свій рахунок. Система NetCash – дешева і не потребує додаткового програмного забезпечення, але в ній відсутні будь-яке шифрування чи анонімність. Для дрібних платежів ризик може бути обмежений завдяки використанню "електронних банкнот" малої номінальної вартості.

Система CheckFree використовується для полегшення проведення платежів із використанням чеків. Клієнт передає до системи інформацію про платіж і рахунок, який він отримав певним чином, наприклад, електронною поштою, а система виконує цей платіж за нього в довільно обраній формі. Очевидно, система повинна мати доступ до чекового рахунка користувача. Такий метод оплати є простішим і дешевшим від традиційного пересилання чеків поштою, але не повністю використовує можливості Internet, до того ж користується таким застарілим платіжним інструментом як чеки. Тому останнім часом була розроблена вдосконалена версія під назвою CheckFree Wallet, яка забезпечує автоматичну авторизацію і високий рівень захисту на основі шифрування, але не є анонімною.

Проблеми, пов'язані із впровадженням електронної комерції, та шляхи їх вирішення

Ті, хто надає інформаційні послуги, захоплюються перспективою інформаційного спілкування з аудиторією в будь-якому куточку світу. У той же час уряди, інші органи контролю та влади не схвалюють таку можливість, оскільки в цьому випадку зменшується їх вплив на суспільство та ускладнюється нормативно-регулятивна діяльність. Так, надавачі послуг з-за меж країни не підлягають ні місцевому оподаткуванню, ні місцевим нормативно-законодавчим вимогам.

Запровадження новітніх методів комерції викликає також певні застереження, що безпосередньо або опосередковано стосуються платіжних систем. Центральні банки в усьому світі стурбовані проблемами, породженими впровадженням нових систем електронних платежів. До цих проблем належить не лише ймовірність втрати прибутків від процентів на залишки коштів на рахунках, які отримують деякі з них на поточний момент, але й можливість порушення монетарної стабільності внаслідок безконтрольного введення в обіг електронних еквівалентів місцевих валют. Збільшення загальної грошової маси в обігу може призвести до інфляції. Витісняючи готівку, новітні системи опановують останній механізм масових платежів, який ще залишається під контролем центральних банків – готівковий ринок. Комерційні банки побоюються ослаблення своєї позиції у сфері надання фінансових послуг, оскільки інші установи зможуть займатися діяльністю, еквівалентною традиційним банківським послугам.

Значні дискусії викликає проблема невтручання у приватне життя. Ця проблема пов'язана з питаннями анонімності та захисту приватної інформації. Багатьох непокоїть можливість порушення прав споживачів внаслідок того, що кожну окрему покупку, включаючи дрібні, які зараз оплачують готівкою, можна буде відстежувати. На думку прибічників такої точки зору, збирання та володіння інформацією про приватне життя є неприпустимим і може стати джерелом зловживань. А податкові та правоохоронні органи занепокоєні протилежною проблемою – електронні платежі можна буде виконувати анонімно на будь-якій відстані, що створюватиме ідеальні умови для уникнення від сплати податків, "відмивання" грошей та іншої злочинної діяльності.

Існують неправильні уявлення щодо електронної комерції, наприклад, думка, що електронні гроші по

суті не відрізняються від готівкових і тому їх можна анонімно переміщувати. Тому часто висловлюються побоювання щодо можливостей використання Internet для "відмивання" грошей, здобутих шляхом кримінальної діяльності, або для ухилення від оподаткування. Але насправді, електронна комерція значно менше підлягає загрозі зловживань, ніж традиційна готівка.

Вищезазначених небезпек можна уникнути, або хоча б значно їх зменшити шляхом створення надійної правової та регулятивної бази, здатної обмежити неправомірне використання нових систем. При цьому зовсім не обов'язково відстежувати кожний окремий платіж споживача.

У деяких випадках бажаним є також вдосконалення систем оподаткування із врахуванням можливостей електронних платежів і розрахунків. Наприклад, щоб компенсувати втрати митних зборів або податків на імпорт, можна ввести податок на електронні платіжні операції, що виконуються за кордоном.

Як зазначалося, великих результатів у цій галузі можна досягти завдяки використанню потужних засобів захисту і посиленню контролю за платежами з боку емітентів електронних платіжних інструментів, розрахункових та сертифікуючих установ.

Необхідно також, щоб комерційні структури й споживачі розібралися в особливостях, функціонуванні та можливостях новітніх платіжних систем і могли користуватися ними у спільних інтересах.

Для задоволення постійно зростаючих потреб, забезпечення високого рівня захисту платежів, а також зниження вартості їх виконання останнім часом створюються дедалі більш досконалі платіжні системи. Як наслідок – виникають нові форми відомих платіжних механізмів і принципово нові рішення.

Summary

In clause the application and opportunities of modern electronic payment systems is considered during purchase of the goods and granting of services. Is specified on problems connected to introduction of electronic commerce, and way of their decision.