ПРОБЛЕМИ БЕЗПЕКИ ЕЛЕКТРОННОЇ КОМЕРЦІЇ В МЕРЕЖІ ІНТЕРНЕТ

Ю.А. Балагур
Науковий керівник: О.Б. Раца, к.е.н., асистент
Чернівецький національний університетім. Ю. Федьковича

Всесвітня мережа Інтернет охопила всі галузі діяльності людини. Величезними темпами розвивається сектор бізнес-послуг, що надаються за допомогою Інтернету. Серед прогресуючих напрямків, важливу роль відіграють системи Інтернет-торгівлі – електронна комерція. Цей сектор бізнесу пов'язаний з наданням послуг або продукції кінцевому споживачеві. Основний тип даних систем – електронний магазин – автоматизована система електронної торгівлі в мережі Інтернет.

Безпека є ключовим питанням для впровадження електронної комерції. Основною перешкодою, що виникає на шляху розвитку ринку Інтернет-платежів, є психологічний фактор, пов'язаний з усвідомленням загрози потенційного шахрайства. Люди досі не розглядають Інтернет як безпечне середовище, чому сприяє об'єктивна інформація про ступінь безпеки роботи в Інтернеті. Опитування показують, що найбільше люди бояться потенційної загрози отримання будь-ким їх персональних даних при роботі через Інтернет. За даними платіжної системи VISA близько 23 % транзакцій з банківськими картами так і не виробляються через острах клієнта ввести запитувану електронним магазином персональну інформацію про клієнта. В результаті, люди головним чином використовують Інтернет в якості інформаційного каналу для отримання цікавої для них інформації [1].

Прийнято виділяти такі види ризиків шахрайства з електронними грошима в мережі Інтернет:

– ризик дублювання технічного пристрою (електронного гаманця або жорсткого диска комп’ютера);

– ризик зміни або дублювання відомостей або програм;

– ризик зміни повідомлень;

– ризик крадіжки;

– ризик відмови операцій [2].

Заходи, що вживаються учасниками електронної комерції для забезпечення безпечних розрахунків в мережі Інтернет досить різноманітні.

Перш за все, це навчання власників банківських карт мінімальним навичкам для забезпечення власної безпеки: користування тільки знайомими Інтернет-ресурсами, вивчення порядку доставки товарів і надання послуг, перевірка використання інтернет-комерсантом сертифікованих протоколів, які гарантують безпеку переданої інформації [3].

Одним з ефективних напрямків захисту інформації є криптографія або криптографічна інформація, широко застосовувана в різних сферах діяльності в державних і комерційних структурах [4].

На відміну від традиційних систем шифрування, в яких один і той же ключ використовується і для шифрування, в методах несиметричного шифрування – системах з відкритим ключем, передбачені два ключа, кожен з яких неможливо обчислити з іншого. Один ключ – відкритий, використовується відправником для шифрування інформації, інший – закритий, одержувач розшифровує отриманий зашифрований текст. Електронний цифровий підпис – механізм частіше використовується при обслуговуванні банками компаній, але іноді його пропонують і індивідуальним клієнтам. Перевага електронного цифрового підпису в тому, що вона дозволяє однозначно ідентифікувати користувача. Недолік же полягає в тому, що електронний цифровий підпис також може бути вразливий для шахраїв. Зловмисники можуть дістатися до ключа від цифрового підпису, заразивши комп’ютер шкідливим програмним забезпеченням.

Але все ж вирішити проблему забезпечення надійності інформаційної безпеки виключно за допомогою технічних засобів і програмного забезпечення неможливо. На думку фахівців, захист корпоративних інформаційних систем залежить від ряду факторів: на 30% – від застосовуваних технічних рішень; на 40% – від проведених в установі організаційних заходів і на 30% – від морально-етичного стану суспільства і загальнокультурного рівня користувача [5].

Необхідно пам’ятати, що проблеми безпеки онлайнових послуг пов'язані також і з відсутністю нормативно-правової бази: закону про електронно-цифрового підпису, комплекту нормативних актів, які прямо регулюють права і обов’язки учасників обороту онлайнових фінансових послуг, гарантій щодо виконання розпоряджень, відданих в електронній формі, тлумачення подібних операцій відповідними контролюючими та наглядовими відомствами, всі ці обставини гальмують розвиток електронних банківських послуг.

Список використаних джерел

1. Голдовський І.П. Безпека платежів в Інтернеті. / І.П. Годовський. – Харків: Інтер, 2001. – 240 с.

2. Горюк Є.В. Електронні гроші: розвиток, напрямки використання в сучасній банківській практиці / Є.В. Горюк, О.В. Котина. [Електронний ресурс] – Режим доступу: http://bankir.ru/tehnologii/s/elektronnie-dengi-razvitie-napravleniya-ispolzovaniya-v-sovremennoi-bankovskoi-praktikeokonchanie-1373402/.

3. Гончаров В.В. Безпека і захист інтернет-платежів / В.В. Гончарова // Розрахунки і операційна робота в комерційному банку. – 2010.

4. Мухачев В.А. Інформаційна технологія. Криптографічний захист інформації. Процедури вироблення і перевірки: навч. посіб. / В.А. Мухачев, В.А. Хорошко. – Київ : Знання, 2007.

5. Тимошкин А.В. Еволюція фінансового контролю тіньової економіки. Захист інформації та технологій – умова стабільності банківської системи / А.В. Тимошкин // Банківська справа. – 2009.