УДК 342:339.1

М. ГУЦАЛЮК, *кандидат юридичних наук, доцент*

БЕЗПЕКА ІНТЕРНЕТ-ТОРГІВЛІ

Анотація. *Щодо необхідності комплексного вирішення проблеми безпеки в Інтернет.*

У жовтні 2006 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 Інтернет.

В Україні, незважаючи на те, що Інтернет-технології вже мають високий рівень поширення, номенклатура товарів досить обмежена.

Однією з причин, які зупиняють Інтернет-торгівлю, є сумніви щодо безпеки Інтернет-переказів. Тому найбільшою популярністю користуються Інтернет-магазини, які пропонують придбати книги, CD, продукти харчування тощо. Адже, як свідчить приказка, у кожної медалі є два боки, тому і переваги Інтернет-технологій (розташування по всьому світу без кордонів, миттєва передача даних тощо) є водночас і їх вразливими місцями.

Відповідно до поширення використання Інтернет-технологій та зростання обсягів коштів, які переказуються через глобальну мережу, злочинці також починають використовувати новітні технології. Ось типовий приклад [1].

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 з-закордону, 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.

У зв’язку з тим, що бази даних Інтернет-магазинів містять досить значні обсяги приватної інформації, вони є постійною мішенню хакерів.

Влітку поточного року в Інтернет-розсилках з’явилося повідомлення про можливість отримання за відносно невисоку ціну бази даних електронних адрес 2 мільйонів користувачів платіжної системи WebMoney Transfer. Наприклад, для розсилки повідомлень типу “спам”. Цікаво, що продавець, який зумів написати відповідну програму доступу до бази, відзначив, що він не порушував закон, адже він отримав те, що відкрито для користувачів системи...

Кількість протиправних схем, які існують у глобальній мережі, обмежується лише уявою зловмисників. Серед найпоширеніших з них – це віртуальний шантаж, шахрайства, пов’язані з електронними переказами, викрадення комп’ютерних даних, фішинг тощо.

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

Відповідно до Європейської Конвенції про кіберзлочинність необхідно вирішити питання щодо створення Міжвідомчого центру з проблем боротьби з комп’ютерною злочинністю, на базі якого організувати цілодобовий контактний пункт, який би підтримував зв’язок як з провайдерами, так і з правоохоронними органами.

Такі центри (контактні пункти) створені в багатьох країнах. У нас ідея створення Міжвідомчого центру з проблем боротьби з комп’ютерною злочинністю опрацьовувалась ще з 2001 року [2] (це передбачено у відповідному указі Президента України). Проте центр і по-сьогодні не існує.

У Російській Федерації у зв’язку з поширенням злочинів, пов’язаних з використанням високих технологій Бюро спеціальних технічних заходів МВС розробило низку пропозицій. При цьому заступник начальника БСТЗ генерал-майор міліції К.Мачабелі зазначив, що серед кіберзлочинів найбільш поширеними є шахрайства, зокрема – *помилкові пропозиції товарів і послуг через Інтернет, послуги по організації атак хакерів, афери з електронними платіжними картами і рахунками клієнтів електронних платіжних систем*. У 2005 році було розкрито або попереджено понад 450 таких злочинів. Статистика вказує, що майже в 43% випадків жертвами комп'ютерних шахраїв стають учасники он-лайнових аукціонів – коли покупець відповідає на несумлінну пропозицію придбати будь-який товар за дуже низькою ціною, але з передоплатою.

Центр по реагуванню на скарги на протизаконні дії в Інтернет (ЦРСПДІ) є системою обліку скарг від громадян Сполучених Штатів й інших країн на протизаконні дії в Інтернеті. За допомогою заяв, поданих у режимі он-лайн, а також завдяки роботі цілої команди фахівців і аналітиків ЦРСПДІ здійснює свою діяльність в інтересах громадян, а також американських і міжнародних правоохоронних органів, що розслідують злочини в Інтернет.

Концепція створення Центру виникла в 1998 році після визнання того факту, що злочинність проникає в Інтернет слідом за бізнесом, тож ФБР вирішило мати можливість здійснювати контроль за цією діяльністю і розвивати відповідні методи для боротьби зі злочинністю в Інтернеті.

Реальність сьогодення така, що більшість правоохоронних органів не можуть розслідувати справи з відносно невеликим збитком, наприклад в 100 доларів. Більшість правопорушників діють у режимі он-лайн для того, щоб розширити коло своїх жертв і збільшити можливості наживи. Кіберзлочинці майже ніколи не обмежується однією жертвою. Таким чином, якщо фахівцям ЦРСПДІ вдається зв'язати кілька аналогічних скарг і сформувати з них справу про збиток у розмірі 10 тис. або 100 тис. доларів з кількістю потерпілих від 100 до 1000, злочин має більшу соціальну небезпеку і правоохоронні органи отримують можливість розслідувати його [3].

В Україні зазначений центр намагаються створити, наприклад, у Запоріжжі, з лютого 2006 року. У Запорізькому юридичному університеті для надання консультаційної допомоги жертвам шахрайства в Інтернет створено юридичну клініку “Stop Internet Scam”. Для досягнення поставлених цілей юридична клініка вирішує, зокрема, наступні задачі [4]:

- безоплатний захист законних інтересів громадян і організацій шляхом надання професійної юридичної допомоги;
- навчання юристів та інших категорій громадян у формі разових лекцій, консультацій і семінарів, що не супроводжуються підсумковою атестацією або видачею документів про освіту і (або) кваліфікації;
- розробка і тестування учбово-методичних матеріалів, застосовуваних при навчанні студентів, юристів і громадян;
- проведення наукових досліджень в області протидії комп'ютерній злочинності.

Проте, на нашу думку, проблему безпеки в Інтернет потрібно вирішувати більш комплексно. Мається на увазі підготовка фахівців спеціалізованих навчальних закладів, а також опанування випускниками середніх шкіл основ інформаційної культури та захисту інформації. В Україні вже склалася відповідна наукова школа з такими провідними вченими, як М.Я.Швець, Р.А.Калюжний, В.С.Цимбалюк, В.Д.Гавловський, В.М.Бутузов та ін. Видано низку посібників з даної проблематики. Тому безпека Інтернет-торгівлі певною мірою залежить і від вирішення зазначених вище питань.

Використана література

1. //www.ukranews.com

2. М. Гуцалюк. Міжвідомчий центр боротьби з комп'ютерною злочинністю // Тези доповідей на п'ятій Міжнародній науково-практичній конференції “Безпека інформації в інформаційно-телекомунікаційних системах”. – К.: НТУУ “КПІ”, 2002. – С. 23-24.

3. //www.usinfo.state.gov.

4. //www.crime-research.ru.

5. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: Наук.-практ. посіб. / Б.В. Романюк, В.Д. Гавловський, М.В. Гуцалюк, В.М. Бутузов. – К.: вид. Паливода А.В., 2004. – 144 с.; Гуцалюк М.В., Гайсенюк Н.А. Організація захисту інформації: Навчальний посібник. – К.: Альтерпрес, 2005. – 244 с.

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