**В.П. Сабадаш***

# ФІШИНГ ЯК НАЙБІЛЬШ РОЗВИНЕНИЙ ВИД ШАХРАЙСТВА В ІНТЕРНЕТІ

В умовах науково-технічного прогресу інформація стає об'єктом специфічних суспільних відносин, що виникають з моменту її створення, в процесі накопичення, зберігання, обробки та використання, набуття товарного вигляду. Формування, обробка та використання інформаційних ресурсів здійснюється в процесі інформатизації різних галузей людської діяльності, шляхом застосування сучасних інформаційних технологій. Однак застосування сучасних інформаційних технологій, крім всього позитивного в рамках розвитку суспільства, має потенційну можливість використання сучасних комп'ютерних технологій із корисливою метою. Інтенсивне впровадження автоматизованих систем в економіці, управлінні та особливо в кредитно-банківській діяльності обумовило виникнення нового класу злочинів — злочинів у галузі комп'ютерної інформації або комп'ютерних злочинів.

За даними експертів, світова кіберзлочинність вже дає більше прибутків, ніж торгівля наркотичними засобами. Так, тільки за 2004 рік кіберзлочинність дала понад $ 105 млрд. прибутку[1]. В той же час за даними британської дослідницької компанії Mi2g, у 2004 році в світі збиток від комп'ютерних злочинів сягнув $ 411 млрд., що майже у два рази перевищує показники 2003 року. У світі збиток від одних тільки шкідливих програм у 2004 році досяг $ 165 млрд. Рік у рік він подвоюється — в 2003 році збитки від вірусів становили $ 83 млрд.[2] Жодна країна світу не має імунітету до комп'ютерної злочинності. Найбільш поширеними на сучасному етапі інформатизації суспільства є шахрайські дії.

Актуальність теми статті зумовлена тим, що поряд із очевидними успіхами світового співтовариства в галузі інформатизації й високих технологій чітко спостерігається ріст кількості злочинних дій, що здійснюються за допомогою високих технологій, вдосконалюються традиційних видів злочинів, зокрема шахрайство, у зв'язку із чим необхідні дослідження в даній сфері з метою вдосконалення політики протидії шахрайству в Інтернеті.

Термін "шахрайство в Інтернеті" можна застосовувати в цілому до шахрайських махінацій будь-якого виду, де використовуються один або кілька елементів Інтернету (кімнати в чатах, електронна пошта, дошки оголошень або Web-сайти) для залучення потенційних жертв, проведення шахрайських угод або для передачі повідомлень від шахраїв до фінансових установ або іншим особам, які беруть участь у таких махінаціях.

Проблема шахрайства в Інтернеті дуже актуальна, оскільки ситуація розвивається. Дані, накопичені Інтерполом, підтверджують той факт, що за останні роки WorldWideWeb став сферою дуже активного росту злочинності порівняно з всіма існуючими галузями людської діяльності.

Вивчення стану наукових розробок проблем протидії шахрайству в Інтернеті показало, що на сучасному етапі спеціального дослідження з цих проблем не проводилось. Проте необхідно відмітити, що окремі аспекти шахрайства в рамках методики розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж



* *доцент кафедри кримінального права та правосуддя Запорізького національного університету, кандидат юридичних наук*

[1] "Киберпреступность" принесла 105 млрд. долларов прибыли в 2004 году // www.uabanker.net/news/1231.html.

[2] В 2004 г. мировой ущерб от компьютерных преступлений составил $411 млрд // www. anti-virus.by/press/viruses/1485.html.

www.univer.km.ua Університетські наукові записки, 2006, № 1 (17), с. 228-233.

розглядалися у працях таких вчених, як Ю.М. Батурін, П.Д. Біленчук, М.С. Вертузаєв, В.Б. Вєхов, В.О. Голубєв, М.Д. Діхтяренко, Н.А. Селіванов.

За даними Центру по моніторингу шахрайства в Інтернеті (Internet Fraud Complaint Centre — IFCC), в 2001 році збитки від віртуальних аферистів у всьому світі склали $ 17 млн., в 2002 році — $ 54 млн., в 2003 році сума досягла $ 1,5 млрд.[3] Vnunet.com з посиланням на матеріали аналітичної компанії Gartner повідомила в лютому 2005 року, що 9,5 млн. осіб стали жертвами онлайнових афер у 2004 році. Загальна сума, отримана шахраями, становила приблизно $ 1,2 млрд. Значна частина цих коштів дісталася організованим злочинним угрупованням зі Східної Європи та Африки[4].

За оцінками Business Week, які були зроблені на основі даних правоохоронних органів й аналітиків, фінансові афери в Мережі обходяться фірмам і споживачам у $ 22 млрд. у рік[5].

Найбільш поширеним видом шахрайства в Інтернеті на сьогоднішній день вважається фішинг.

*Метою* цієї статті є виділення основних елементів такого виду шахрайства в Інтернеті, як фішинг, дослідження статистичних даних за структурою й динамікою розвитку даного виду злочинного посягання й формулювання основних напрямків політики протидії шахрайству в Інтернеті.

Фішинг (*phishing* — похідне від англійського слова fishing (риболовля)) — це відносно новий вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів Мережі персональних даних клієнтів онлайнових аукціонів, сервісів із переведення або обміну валюти, інтернет-магазинів. Шахраї використовують усілякі прийоми, які найчастіше змушують користувачів особисто повідомити конфіденційні дані (наприклад, шляхом надсилання електронних листів із пропозиціями підтвердити реєстрацію аккаунта, що містять посилання на сайт, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів).

Вперше phishing з'явився у 1996 р., коли передплатники служби America Online почали одержувати підроблені повідомлення, в яких просили повідомити їхній пароль для входу в систему нібито "для модифікації інформації". Тоді мета полягала в тому, щоб уникнути плати за підписку, використовуючи чужі рахунки. Шахраї просто користувалися Інтернетом, оплачуючи його за допомогою чужих рахунків. Однак розвиток мережі банкінгу й залучення злочинних елементів у шахрайство, пов'язане з ненадійною електронною поштою й Інтернетом, перетворило phishing у найбільш розвинений вид шахрайства в Інтернеті.

На сьогоднішній день ми можемо виділити три види фішингу — поштовий, онлайновий та комбінований.

Перший із них — найстаріший. Він полягає у надсиланні жертві спеціального листа електронною поштою з вимогою надіслати у відповідь будь-які відомості. А як наочний приклад можна навести найпримітивніший спосіб одержання даних для виходу в Інтернет. Зловмисник просто представляється співробітником провайдера користувача Інтернету й, розповідаючи історію про "базу даних, яка вийшла з ладу", просить останнього вислати його логін та пароль. Причому для більшої переконливості шахрай може використати поштову скриньку з назвою сервера, що схожий на назву сервера провайдера.

В рамках дослідження проблеми поширення шахрайства в Інтернеті, Ponemon Institute, що займається питаннями privacy і цивільних свобод, опитав 1335 американських інтернет-користувачів. У результаті опитування виявилося, що 76 % респондентів знайомі з електронними листами — "обманками". 70 % із цього числа заходили на "сайт-обманку", посилання на який

[3] Факты. – 2004. – 18 июня. — С. 27.
[4] Жертвы онлайновых афер в 2004 году потеряли 1,2 миллиарда долларов // www.anti-virus.by/press/viruses/1202.html.
[5] www.crime-research.ru.

Університетські наукові записки, 2006, № 1 (17), с. 228-233. www.univer.km.ua

були в підробленому листі, 15 % залишали на цьому сайті свої персональні дані, а 2 % зізналися в тому, що зазнали фінансових втрати в результаті фішингу. Крім того, Ponemon Institute у своєму звіті називає суму в $ 500 млн. збитків, яких можуть зазнати користувачі Інтернету від такого виду шахрайства[6].

Дослідження компанії Javelin Strategy & Research, у ході якого було опитано 4000 чоловік, показало, що шахраї все частіше користуються Інтернетом для крадіжки персональних даних. У середньому збиток від одного випадку крадіжки особистих даних становить 15607 доларів США, у той час як жертви фішингу зазнають збитків у розмірі 2320 доларів США. В 2004 році загальний збиток від крадіжки персональних даних жителів США становив $ 52,6 млрд. Від дій злочинців постраждали 509 чоловік із числа опитаних[7].

Як повідомляє Anti-Phishing Working Group, ефективність надсилань фішерів може сягати 5 %. Це значить, що кожен 20-й одержувач підробленого листа втратить гроші. Наприклад, активність організаторів фішинг-атак у липні 2005 року, за даними експертів дослідницької компанії Postini, побила всі попередні рекорди. Так, у липні 2005 року користувачам було надіслано 19,2 мільйони фішинг-листів, що на 16 відсотків перевищило показник попереднього місяця. У червні 2005 року фахівці Postini зафіксували 16,6 мільйона фішинг-листів, що теж виявилося рекордним показником[8].

Онлайновий фішинг — афери, коли зловмисники копіюють які-небудь сайти, найчастіше інтернет-магазини. При цьому вони використовують схожі доменні імена й ідентичний дизайн. Число жертв від таких злочинних дій постійно зростає, адже зловмисники найчастіше пропонують різні речі буквально за демпінговими цінами (вони ж їх насправді не продають). А підозри, які могли б виникнути у потенційних жертв, розсіюються завдяки популярності сайту, що копіюється. Таким чином, користувачі Інтернету вважають, що вони перебувають на веб-сервері реально діючого магазина, який має гарну репутацію. Вирішивши придбати товар, користувач Інтернету реєструється в системі. При цьому є досить велика ймовірність того, що для цього він буде використовувати той самий пароль, як і в інших сервісах (багато користувачів Інтернету завжди використовують одне ключове слово, незважаючи на всі попередження з боку фахівців інформаційної безпеки). Крім того, для покупки товару користувач введе номер та інші дані своєї пластикової карти. Саме це й потрібно зловмисникові, що може відразу скористатися кредитною карткою жертви.

За 2004 рік 57 млн. осіб зазнали фішингових атак, у яких використовувались торговельні марки 122 відомих компаній і біля половини атак проводилося з використанням шпигунських програм або іншого шкідливого коду. Так, наприклад, одна з подібних атак, зафіксована датською консалтинговою фірмою Secunia, вводила користувачів в оману шляхом модифікації файлів операційної системи Windows, після чого під час набору користувачем адреси Web-сайта браузер жертви перенаправлявся на підставний сервер. Подібним способом були проведені кілька атак, результатом чого стала підміна адрес деяких південно-американських банків[9].

Обидва описаних види фішингу існують вже давно. Вони досить примітивні, так що уважна і скептично настроєна людина зможе уникнути настільки простої пастки, тим більше, що останнім часом загальний рівень освіченості користувачів Інтернету в галузі інформаційної безпеки став трохи вищим. Тому поштовий та онлайновий фішинги перетворилися в неефективні види онлайнового шахрайства. Однак їм на зміну прийшов третій тип фішингу (комбінований), і він майже відразу ж набув поширення. Суть цього способу обману полягає в наступному. Зловмисник

[6] www.ponemon.org.
[7] Отчет компании Javelin Strategy & Research за 2004 год // www.novikov.com.ua/ru/news/5175.
[8] В июле наблюдался пик активности фишеров // www.bezpeka.com.
[9] Фишинг: мошенники всё больше изощряются // www.anti-virus.by/press/viruses/ 1165.html.

www.univer.km.ua Університетські наукові записки, 2006, № 1 (17), с. 228-233.

створює підроблений сайт якої-небудь організації, а потім заманює на нього користувачів за допомогою листів-принад. Головна небезпека комбінованого фішингу полягає в його високій правдоподібності. І дійсно, ніхто не жадає від людини надсилання пароля електронною поштою. Їй лише пропонують зайти на корпоративний сайт за наведеним посиланням (насправді це всього лише підробка) і самому зробити необхідні операції.

Антіфішингова робоча група (APWG) називає такий вид шахрайства фармінгом і попереджає користувачів Інтернету про розкрадання ідентифікаційних даних за допомогою шпигунського програмного обладнання — spyware. Так, за даними APWG, у червні 2005 року число випадків звичайного фішингу становило 15050 випадків, у той же час фармінг-атаки (атаки з перенаправленням користувачів на фальшиві сайти) виросли на 6 %, а число розкрадань ідентифікаційних даних за допомогою шпигунських програм зросло на 95 %[10].

Таким чином, необхідно констатувати зміну характеру злочинів, пов'язаних із використанням фішинга. Шахраї вигадують нові, все більше витончені, способи обману й підвищують рівень підготовки атак із метою крадіжки паролів, номерів кредитних карток і банківських рахунків й іншої конфіденційної інформації. Якщо раніше шахраї діяли від імені відомих банків і компаній, посилаючи мільйони листів, наприклад, із темою "необхідне відновлення облікового запису", які заманювали наївних користувачів на підставні Web-сайти, то тепер посилання на фальшиві сервери ховають усередину коду листа, показуючи користувачеві посилання у вигляді дійсної адреси, тобто збільшується кількість випадків використання вірусів-хробаків і шпигунських програм для непомітного перенаправлення користувачів на фальшиві сайти. Крім того, самі фішингові атаки стали більш ефективними. Відбулося це завдяки персоніфікації: тепер для того, щоб виманити у жертви секретні дані про кредитну карту, шахраї використовують реальну інформацію про власника рахунку. За повідомленнями експертів, від нової технології фішинга вже постраждали клієнти багатьох великих фінансових структур. Раніше листи шахраїв в основному містили інформацію про банк, його співробітників і посилання на спеціальний сайт, що був повністю ідентичний порталу фінансової організації й контролювався зловмисниками. Зараз же на зміну такому грубому способу з'являються більше ефективні персоніфіковані атаки. Тобто нібито банківські листи містять тепер не тільки інформацію про банк, але й особисті дані клієнта. Серед цих даних звичайно трапляються номер рахунку, ім'я клієнта й адреса його електронної пошти. Повідомлення розсилаються від імені банків нібито для підтвердження інформації про рахунок: особистого ідентифікаційного номера або коду кредитної карти (ряд цифр, надрукованих зі зворотної сторони). Для більшої переконливості в електронному повідомленні використовуються логотипи банку, імена й прізвища реальних керівників організації. Потім усе відбувається за давно налагодженою схемою: жертві пропонується зайти на ідентичний банківському сайт і "підтвердити" інформацію про рахунок. Необхідність таких дій шахраї пояснюють виходом із ладу ПО банку або атакою хакерів[11].

Фахівці у сфері Інтернет-безпеки виявили також нову троянську програму, що сканує банківську активність користувача в Інтернеті, а також особливості його Web-серфінга. Троян Banker-AJ націлений на Windows-компьютери клієнтів таких британських банків, як Abbey, Barclays, Egg, HSBC, Lloyds TSB, Nationwide й NatWest. Встановлений на машині троян нічим не проявляє себе доти, поки користувач не відвідає Web-сайт одного із зазначених банків. Тоді Banker-AJ активізується, сканує пароль входу в систему, зберігає скрін-шоти проведених сесій і

[10] Антифишинговая группа APWG заинтересовалась шпионскими программами // www.bezpeka.com/ru/news/2005/08/05/4902.html.
[11] Клиенты банков пострадали от новой фишинговой схемы // www.bezpeka.com/ru/news/2005/05/17/3864.html.

Університетські наукові записки, 2006, № 1 (17), с. 228-233. www.univer.km.ua

відсилає їх зловмисникові. Тобто дана програма є представником нового покоління засобів для фішингу. Вона використовується для крадіжки інформації при заході на зовсім легальні сайти[12].

У 2005 році на Україні також зафіксовані масові фішинг-атаки. Так, у квітні 2005 року в українському сегменті Інтернету з'явилися масові розсилки, підписані службою безпеки "Приват 24" (торговельна марка послуги електронного банкінгу Дніпропетровського Приватбанку). Про це повідомила українська корпорація UNA, розроблювач комплексних систем антивірусного захисту.

Українські користувачі Інтернету протягом декількох днів виявляли у себе в електронній поштовій скриньці лист, підписаний службою безпеки Приватбанку, з наполегливими проханнями терміново зайти на сайт та ввести на сторінці, що вискочила і яка віддалено нагадує систему доступу до особистого рахунку, код активації, а також пройти авторизацію. Невідомі хакери-зловмисники у такий спосіб за допомогою підставного сайту, що нібито належить Приватбанку, витягали з клієнтів номери кредитних карток й іншу конфіденційну інформацію. Така фішинг-атака була зафіксована в Україні вперше. Необхідно відмітити, що Інтернет-банк "Приват 24" призначений для керування реальними банківськими рахунками через мережу Інтернет. Дана система надає своїм користувачам комплекс банківських послуг у режимі реального часу, з будь-якої точки земної кулі, що має вихід в Інтернет. За даними співробітників Приватбанку, кількість активних користувачів "Приват 24" станом на початок квітня 2005 року становила 60 тис. осіб[13].

В Україні зафіксована також нова форма мобільного фішингу: шахраї спонукають абонентів до "добровільного" переказу грошей зі свого рахунку на особовий рахунок іншого абонента-шахрая. Про це повідомив фахівець зі зв'язків із громадськістю компанії "Київстар" Віктор Гоцуленко.

Суть обману полягає в тому, що шахраї здійснюють розсилку електронних повідомлень потенційним жертвам і роблять рекламні постинги в популярних українських інтернет-форумах про "можливе" поповнення рахунку, яке повинно завдати шкоди операторові мобільного зв'язку "Київстар". При цьому пропонується здійснити спеціальний набір USSD команд, що призводить до списання грошей із рахунку довірливого абонента, але при цьому страждають самі абоненти. Шахраї не заподіюють великого збитку абонентам, оскільки намагаються спонукати до переказу невеликих сум грошей (10-20 грн., тобто близько 2-4 долари США), але деякі експерти вважають подібну інтернет-розсилку серйозною українською фішинг-атакою[14].

Проведене дослідження дозволяє сформулювати **висновок** про те, що на сьогоднішній день фішинг є найбільш розвиненим видом шахрайства в Інтернеті. Даному виду шахрайства притаманні такі основні риси:

1) викрадення зловмисниками особистої та конфіденційної інформації користувачів Інтернету;

2) динамічний розвиток, до того ж, спостерігається потенційна тенденція до зростання фішинг-атак у світі;

3) фішинг може виступати у трьох основних видах — поштовий, онлайновий та комбінований;

4) найбільш небезпечним для користувачів є комбінований фішинг — фармінг. Фармінг — це різновид фішингу, який полягає в зміні DNS (Domain Name System) адреси так, щоб веб-сторінки, які відвідує користувач, були не оригінальними, а іншими, спеціально створеними зловмисниками для збирання конфіденційної інформації й особливо тієї, яка належить до онлайнових банків;

[12] Новый троян шпионит за банковскими сайтами // www.anti-virus.by/press/viruses/1072.html.
[13] Клиенты услуги электронного банкинга Приватбанка подверглись фишинг-атаке // www.securitylab.ru.
[14] На Украине зафиксирована новая форма мобильного фишинга // www.forum. yasnet.ru/lofiversion/index.php/1770.html.

www.univer.km.ua Університетські наукові записки, 2006, № 1 (17), с. 228-233.

5) постійна якісну зміна характеру злочинів, пов'язаних із використанням фішингу. На сьогоднішній день надсилання на фальшиві сервери ховають усередину коду листа, показуючи користувачеві посилання у вигляді дійсної адреси, тобто збільшується кількість випадків використання вірусів-хробаків і шпигунських програм для непомітного перенаправлення користувачів на фальшиві сайти.

Основними напрямками протидії фішингу в Інтернеті можуть стати:

— розробка нового програмного обладнання та антивірусних програм. Наприклад, TippingPoint, підрозділ компанії 3Com, анонсувала нову лінійку продуктів для запобігання вторгнень — TippingPoint IPS. Справа в тому, що TippingPoint IPS — комплексне мережне рішення для блокування спроб фішинга й протидії крадіжкам персональних даних. Спроби крадіжки персональних даних відбуваються в кілька етапів, і TippingPoint IPS блокує ці спроби на кожному етапі;

— створення системи аутентифікації інтернет-адресів для перевірки відповідності введеної користувачем адреси дійсному серверу;

— більш широке розповсюдження інформації про відомі види Інтернет-шахрайства користувачам Інтернету.

*Стаття рекомендована до друку кафедрою кримінального права та процесу Хмельницького університету управління та права (протокол № 6 від 16 лютого 2006 року)*