2. Предборський В. А. Теорія тіньової економіки в умовах трансформаційних процесів : монографія / В. А. Предборський. – Київ : Задруга, 2014. – 400 с.
3. Рівень тіньової економіки знизився до 35 % від ВВП [Електронний ресурс] : матеріали прес-служби Міністерства економічного розвитку і торгівлі України, 2017. – Режим доступу: http://www.me.gov.ua/News/Detail?lang=uk-UA&id=dc0d7cd5-ad6a-42ff-963a-e0d45ee23888&title=RivenTinovoiEkonomikiZnizivsia Do35-VidVvp. – Назва з екрана.

Криволапов В. М. – ад'юнкт наукової лабораторії з проблем досудового розслідування Національної академії внутрішніх справ

КІБЕРЗЛОЧИННІСТЬ ЯК НЕГАТИВНИЙ ЧИННИК ЗРОСТАННЯ ТІНЬОВОЇ ЕКОНОМІКИ

Поширення нових інформаційних технологій, підґрунтям чого є активне використання комп'ютерної техніки та засобів комунікацій, оптимізації та автоматизації процесів в усіх без виключення сферах життєдіяльності, спричинило нівелювання кордонів та переплетення національних економік та національних інфраструктур країн світу. Вказані тенденції сприяли формуванню єдиного світового інформаційного простору, де кожен може отримати доступ до будь-якої інформації в будь-якій точці планети, дистанційно управляти власними активами та активами компанії, укладати господарські угоди з іноземними суб'єктами господарювання без необхідності особистого контакту тощо. Так, інформаційний простір став водночас місцем і безпосередньо інструментом вчинення злочинів. Відтепер злочин не потребує попередньої «обробки клієнта» та особистого контакту з потенційною жертвою. Головним інструментом правопорушника стає лише комп'ютер та доступ до інформаційно-комунікаційних систем, де він за допомогою комп'ютерних вірусів та інших заборонених технічних засобів може отримати доступ до баз даних, банківських рахунків, автоматизованих систем управління тощо.

Популярність Інтернету цілком закономірна, оскільки користувач має: цілодобовий доступ до значних обсягів інформації; можливість швидко здійснювати обмін інформацією з іншими користувачами; змогу проводити банківські, торгові, біржові операції з будь-якого місця у зручний час тощо. Банківська система України є однією зі сфер, де найбільш широко та активно використовують сучасні можливості інформаційних технологій та Інтернет-мережі. Таким чином, ця сфера привертає все більшу увагу злочинців. Несанкціоноване списання коштів з банківських рахунків, шахрайство з платіжними картками, втручання в роботу Інтернет-банкінгу, розповсюдження комп'ютерних вірусів, DDoS атаки на Інтернет-ресурси, шахрайство в інформаційних мережах – це не повний перелік кіберзлочинів, тобто злочинів у сфері інформаційних та комп'ютерних технологій. За оцінками експертів щорічні збитки від діяльності кіберзлочинців перевищують 100 млрд доларів США [1].

Нові технології обману стали доступні передусім завдяки широкому поширенню банківських карт і онлайн-банкінгу. За інформацією Національного банку України, в банківській системі України найчастіше вчиняють такі види кіберзлочинів у сфері карткового бізнесу.

1. Банкоматне шахрайство:

– скімінг – виготовлення, збут і встановлення на банкомати пристроїв зчитування/копіювання інформації з магнітної смуги платіжної картки та отримання ПІН-коду до неї;

– використання «білого пластику» для підроблення (клонування) платіжної картки та зняття готівки в банкоматах;

– Transaction Reversal Fraud – втручання в роботу банкомату під час проведення операцій з видачі готівки, яке залишає незмінним баланс карткового рахунку після фактичному отриманні готівки зловмисником;

– Cash Trapping – заклеювання диспансеру банкомата для присвоєння зловмисником готівки, яка була списана з карткового рахунку законного утримувача картки.

2. Шахрайські операції в торговельно-сервісних мережах:

– укладання фіктивних угод торговельного еквайрингу для обслуговування підроблених платіжних карток;

– викрадення реквізитів платіжних карток, зокрема із застосуванням технічних засобів їх «клонування»;

– операції на суму нижче встановленого ліміту без проведення авторизації;

– використання в платіжних системах втрачених (викрадених, підроблених) платіжних карт.

3. Шахрайство в Інтернет-мережі:

– викрадення реквізитів платіжних карток;

– проведення операцій із використанням викрадених реквізитів платіжних карток;

– діяльність щодо створення програмних засобів для викрадення реквізитів платіжних карток (фітинг – створення фіктивних web-сайтів і здійснення фальсифікованої інформаційної розсилки повідомлень, поширення комп'ютерних вірусів та троянських програм, перехоплення трафіку тощо).

4. Шахрайські схеми в системах дистанційного банківського обслуговування (ДБО):

– впровадження комп'ютерних вірусів і троянських програм для прихованого перехоплення управління ПК клієнта з установленим програмним забезпеченням ДБО (віруси типу Gamker і Carberp, банківські трояни для крадіжки інформації (Neverquest));

– відкриття рахунків, проведення несанкціонованих операцій та отримання готівки в результаті неправомірних операцій у системах ДБО;

– незаконне отримання платежів від закордонних відправників через міжнародну систему SWIFT унаслідок втручання в роботу комп'ютерів і клієнтських систем ДБО закордонних банків. Розглянемо більш детально один із виділених нами типів кіберзлочинів у сфері карткового бізнесу. Скімінг (від англ. *skim* – знімати вершки) – це різновид шахрайства з платіжними картками, за якого на банкомат встановлюють спеціальний пристрій (скімер). Скімінговий пристрій – це електронний пристрій, який прикріплюють до отвору для введення картки в банкомат для зчитування персональної інформації з магнітної стрічки банківської картки

клієнта. Щоб дізнатися PIN-код, шахраї встановлюють на банкомати міні-камери і накладки на клавіатуру. Після цього злочинці мають доступ до карткових рахунків громадян [2].

За інформацією прес-служби Міністерства внутрішніх справ України, очевидною є тенденція щодо зростання використання шахрайських пристроїв. Так, у 2013 р. було виявлено близько 160 скімінгових пристроїв на банкоматах, в 2012 р. – 73, у 2011 р. – 45.

Проблема пошуку ефективних способів протидії злочинам із застосуванням інформаційно-комунікаційних систем уже доволі тривалий час перебуває в центрі уваги як міжнародної спільноти, так і державних органів України. Зважаючи, що піднесення технологій проходить швидше ніж приймаються нормативно-правові акти, які їх регулюють, а об'єми незаконно отриманих коштів кіберзлочинцями зростають, потрібно на сталій основі віднаходити шляхи розв'язання нових проблем, пов'язаних з такими галузями, як транскордонний доступ правоохоронних служб до даних, захист даних та обмін інформацією між приватними і державними структурами. З огляду на імовірні негативні наслідки даного явища, міжнародна спільнота постійно працює над пошуком заходів, які дозволяють зменшити загрози впливу кіберзлочинності на суспільство.

Список використаних джерел

1. В Україні зростає фінансова кіберзлочинність [Електронний ресурс]. – Режим доступу: http://news.finance.ua/ua/~/2/0/all/2013/12/15/314801. – Назва з екрана.

2. Киберпреступность: украинские банки на линии удара (информационно-аналитические материалы) : круглый стол [Електронний ресурс]. – Режим доступу: http://lfr.org.ua/ru/analytics/822-2013-26-11-analytics.html. – Назва з екрана.