вщині, починаючи з 1995 року. За 4,5 місяця, які в Харкові тестували систему, вона допомогла розкрити близько 300 злочинів.

Для опрацювання зазначених пропозицій доцільним вбачається створення рішенням обласної ради спільної робочої групи, до якої увійшли б представники ГУНП в Харківській області, зокрема Управління інформаційного забезпечення, а також представники зацікавлених департаментів і служб Харківської обласної державної адміністрації та Харківської обласної ради.

Одержано 11.04.2016

*

УДК 004.056:55(043.2)

Алла Петрівна Синиця,
курсант 3 курсу факультету № 4 ХНУВС
Науковий керівник: канд. техн. наук Світличний В. А.

ВИЯВЛЕННЯ ПРИСТРОЇВ ДЛЯ НЕЗАКОННОГО ВТРУЧАННЯ В РОБОТУ БАНКОМАТІВ

За даними експертів та американської компанії Visa Inc., надає послуги проведення платіжних операцій, лідерами серед незаконних операцій з банківськими картами являються скіммінг і online-шахрайство. Скіммінг (від англ. skim – знімати вершки) – створення копії магнітної смуги для виготовлення клону карти користувача за допомогою спеціалізованих пристроїв, які називаються «скімери» і «шиммери» і найчастіше встановлюються на банкомати. За принципом дії ці пристрої не відрізняються один від одного і потребують використання прихованих відеокамер або накладок на клавіатуру банкомату для отримання PIN-коду.

Однак в шиммінгу замість традиційних громіздких скіммерів на щілину приймача пластикових карт банкоматів використовується дуже тонка, гнучка плата, впроваджується через цю щілину в середину банкомата. «Шим» підсаджується за допомогою спеціальної карти – носія: її просовують у щілину банкомату, де тонкий «шим» приєднується до контактів, що прочитує дані з карт, після чого картка-носій видаляється. Далі все працює, як і при традиційному скіммінгу – тобто вставляються в банкомат пластикових карт, де зчитуються всі важливі дані, які потім використовуються зловмисниками для виробництва карток – дублікатів та зняття з їх допомогою грошей. Єдине, але дуже важливе на відміну від скіммінгу полягає у відсутності будь-яких зовнішніх ознак шиммінгу того, що в банкоматі сидить «жучок». Виходячи зі специфікацій, що регулюють розміри щілини кард-рідера, товщина «шима» не повинна перевищувати 0,1 мм, інакше він буде заважати пластиковим картам. Це приблизно вдвічі тонше людської волосини.

Для власників банківських платіжних карток розроблено величезну кількість різноманітних інструкцій і правил безпеки. Основні з них наступні:

1. При проведенні операцій з карткою користуйтеся тільки тими банкоматами, які розташовані в безпечних місцях і обладнані системою відеоспостереження і охороною: у державних установах, банках, великих торгівельних центрах і т. д.

2. Звертайте увагу на картоприймач і клавіатуру банкомату. Якщо вони обладнані якими-небудь додатковими пристроями, то від використання даного банкомата краще утриматися і повідомити про свої підозри за вказаним на моніторі банкомату телефону.

3. У випадку некоректної роботи банкомату – якщо він довгий час перебуває в режимі очікування або мимоволі перезавантажується – відмовтеся від його використання. Велика ймовірність того, що він перепрограмований зловмисниками.

4. Ніколи не піддавайтесь допомозі порадам сторонніх осіб при проведенні операцій з банківської картки в банкоматах. Зв'яжіться з Вашим банком – він зобов'язаний надати консультаційні послуги по роботі з картою.

5. У торгових точках, ресторанах і кафе всі дії з Вашою картою повинні відбуватися у Вашій присутності. В іншому випадку шахраї можуть отримати реквізити Вашої картки за допомогою спеціальних пристроїв і використовувати їх в подальшому для виготовлення підробки.

Одержано 18.04.2016

НАУКОВИЙ ГУРТОК КАФЕДРИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАХИСТУ ІНФОРМАЦІЇ ФАКУЛЬТЕТУ № 6

УДК 343.98

Тетяна Сергіївна Передерій,
студент 3 курсу факультету № 6 *ХНУВС*
Науковий керівник: канд. техн. наук, доц. Тулупов В В.

ПРОБЛЕМНІ ПИТАННЯ ТРАНСНАЦІОНАЛЬНОЇ КІБЕРЗЛОЧИННОСТІ

Сьогодні не існує загальноприйнятого визначення терміну «кіберзлочин», що характеризується експертами як злочин, здійснений із застосуванням високих інформаційних технологій. Злочин може бути здійснений засобами телекомунікаційних систем і мереж, в телекомунікаційній системі або мережі.

З врахуванням усіх міжнародних телекомунікаційних мереж, що існують сьогодні в світі менш вірогідним стає те, що всі елементи кіберзлочинності будуть обмежені територією однієї держави. Залежно від стосунків між зацікавленими державами, характеру відповідної інформації та інших чинників може виникнути потреба в розробці повноважень і процедур в міжнародних угодах та стандартах.

Здійснення відповідно до статей Європейської Конвенції про взаємодопомогу з кримінальних справ між державами-учасниками Європейського Союзу загальні дії при розслідуванні транснаціональних злочинів ускладнюються з таких причинах:

– традиційні форми співпраці передбачають письмові клопотання про надання правової допомоги, а це пов'язано з втратою часу в разі розслідування кіберзлочинів, та втрату доказів унаслідок знищення;

– виявлення, закріплення, вилучення «історичних даних» (слідів) є можливим відносно двох держав (держави – місця знаходження потерпілого і держави, в якій знаходиться злочинець);

– законами однієї держави проводяться розмежування між пошуком і перехопленням даних в процесі їх передачі або пошуку, які зберігаються, тоді як в правових системах інших держав чітке розмежування відсутнє.

Аналіз основних міжнародних документів правового регулювання інформаційних технологій дозволяє зробити висновок, що для ефективної діяльності по розслідуванню транснаціональних кіберзлочинів необхідно:

– уніфікувати кримінальне і кримінальне процесуальне законодавство кожної держави щодо протидії кіберзлочинам;

– усунути норми подвійного права;