Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Легалізація доходів, одержаних у сфері кіберзлочинності

Коломієць Ю.М.
майор поліції
старший викладач кафедри
спеціальної фізичної підготовки
Симонова Г.М.
рядовий поліції
курсант 4 курсу факультету № 3

Сьогодні відбувається впровадження новітніх технологічних досягнень майже в усі сфери людського життя. Науково-технологічний процес не оминув і Україну. Так, стрімко розвиваються телекомунікації, інформаційні технології, зокрема, мережа Інтернет. Із року в рік новітні технології все активніше проникають у життя громадян, що з одного боку надає безмежні можливості у пошуку інформації, а з другого боку – можливості інформаційної сфери за сучасних умов одразу ж взяли на озброєння представники криміналітету, утворивши найприбутковіший на сьогоднішній день вид протиправної діяльності.

Сучасне суспільство – це суспільство інформаційних технологій, що базується на повсякденному використанні комп'ютерної техніки, мереж зв'язку, мобільних засобів комунікації та інших технічних засобів. Щоденна робота урядових структур, банківської, енергетичної, транспортної та інших систем неможлива без надійної роботи комп'ютерної техніки та засобів комунікацій. Інформаційні технології стали постійним супутником сучасної людини не лише на робочому місці, вони увійшли майже в усі сфери людського життя [1].

У сучасному світі економічна злочинність, вийшовши за рамки національних кордонів, перетворилися на транснаціональне явище та глобальну загрозу людству. А стрімкість фінансової глобалізації, формування глобальної фінансової системи та ускладнення світової фінансової архітектури поруч із розвитком інформаційно-комунікаційних технологій зумовили виведення на провідні позиції у міжнародному вимірі економічної злочинності таку її форму, як легалізація кримінальних доходів [2].

На відміну від «традиційного» відмивання доходів, для здійснення якого використовується банківська система, кібервідмивання засновано на використанні різних видів операцій та постачальників фінансових послуг, починаючи від банківських переказів, внесення чи зняття готівки, використання електронних грошей та закінчуючи «грошовими мулами» та послугами по переказу грошей.

Основні механізми легалізації злочинних доходів здобуті злочинним шляхом доходи вимагають від злочинців швидкого та ефективного проведення їх легалізації. При чому, з огляду на специфіку кіберзлочинності – організатори та виконавці схем переважно є освіченими та технічно грамотними, відповідно і методи, які ними використовуються при легалізації отриманих коштів, можуть також бути досить складними та нестандартними.

Інформація чи гроші викрадаються через мережу Інтернет, що надає додаткові можливості для переказу коштів із рахунків фізичних або юридичних осіб на рахунки зловмисників, насамперед за допомогою вірусних програм для зчитування паролів і конфіденційної інформації. Віруси, вражаючи комп'ютерні системи, копіюють паролі, ключі, зберігають скриншоти, пов'язані з фінансовою чи іншою важливою інформацією, та передають дані кіберзлочинцям. Небезпечним винаходом є програми, здатні впливати на роботу та спричиняти збій у функціонуванні стратегічних об'єктів, телекомунікаційних мереж чи банківської інфраструктури. Збитків завдають так звані DDoS-атаки, що здійснюються за допомогою ботнетів та блокують сервіси дистанційного банківського обслуговування [3].

Кіберзлочини здійснюються за рахунок інноваційних підходів та проведення високоінтелектуальних операцій, застосування нестандартних рішень і урізноманітнення методів. Організація злочинних груп є високоструктурованою та вирізняється вузькою спеціалізацією ролей і обов'язків. Водночас складнішим та витонченішим стає доступ до інформації, що реалізується на підпільних ринках.

Отже, причиною популярністю та стрімкого росту кіберзлочинності як бізнесу є його значна прибутковість, а також те, що успіх справи не пов'язан із великим ризиком. Доходи, які отримують кіберзлочинці за декілька секунд чи хвилин, можуть перевищувати мільйони доларів. Тому на сьогодні кіберзлочинність – проблема номер один у світі. Її вирішенню приділяється дуже багато уваги, використовуються програми співробітництва між спеціальними органами багатьох країн. У зв'язку з

цим хотілось би, щоб Україна, як одна із країн, в якій активно використовуються інтернет-технології та кількість користувачів постійно зростає, мала активні засоби захисту та протидії кіберзлочинності та активно готувала кваліфікованих спеціалістів, які б завжди були готові захистити інтереси держави.

Література:

1. Кіберзлочинність та відмивання коштів // Департамент фінансових розслідувань Державна служба фінансового моніторингу України // [Електронний ресурс]. - Режим доступу: http://www.sdfm.gov.ua/content/file/site_docs/2013/20131230/tipolog2013.pdf
2. Markets for Cybercrime Tools and Stolen Data [Електронний ресурс]. – Режим доступу: http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/ RAND_RR610.pdf
3. Киберпреступность [Електронний ресурс]. – Режим доступу: http://n-auditor.com.ua/ru/component/na_archive/773?view=material

Кіберзлочини у фінансово-банквський сфері: скімінг та способи його викорінення

Дарвін О.В.
Студент 3 курсу факультету №4 ОДУВС
Олексієнко Д.
Слухач магістратури 2 курсу ПОД
Науковий керівник: О.В. Косаревська
кандидат педагогічних наук, доцент
доцент кафедри кібербезпеки та
інформаційного забезпечення ОДУВС

На сьогоднішній день кіберзлочинність поширена скрізь, одним із чимало важливих видів кіберзлочинності є скімінг. Актуальність платіжних карток на часі важко переоцінити. Українці все частіше розраховуються ними за покупки на лише в інтернет-магазинах, але й у звичайних торгових мережах.

Карткою дійсно легше розраховуватися у супермаркеті,не треба кожного дня думати, скільки брати з собою грошей та перейматися, щоб у вас часом не витягали гаманець у метро чи іншому людному місці. Проте й у цієї медалі є і інший бік – шахраї вже доволі давно досягли того рівня, коли з легкістю можуть спустошити ваш банківський рахунок. Для цього вам лише треба «засвітити» картку у будь-якому банкоматі, магазині або навіть кафе. Це один з самих привабливих способів шахрайства з банківськими картами існує вже досить-таки давно і є реальною небезпекою для всіх власників пластикових карток. Метою скімінга є виготовлення дубліката платіжної картки та зняття з неї всієї готівки в банкоматі, але при цьому справжня картка знаходиться у нас. Ми навіть можемо і не підозрювати, що нас обкрадають. Це дійсно дуже погана погана і неприємна ситуація, з якою може зіткнутися кожен з нас. Ми навіть можемо і не підозрювати, що нас обкрадають. Це дійсно дуже погана і неприємна ситуація, з якою може зіткнутися кожен з нас.

Саме слово «скімінг» з'явилося на початку 90-х років минулого сторіччя, від аналогічної назви спеціального електронного пристрою, який злодії прикріплюють до картоприймача в банкоматі, і з того часу розпочав набирати обертів, як з кількості вчинених злочинів, так і в плані удосконалення прийомів та технічних засобів, що використовуються злочинцями [2].

На актуальність боротьби з даним видом злочинів в Україні вказує створення Управління боротьби з кіберзлочинністю МВС України та Департаменту кіберполіції Національної поліції України, функцією яких є розкриття злочинів пов'язаних з банківською сферою та платіжними системами.

Огляд сучасної наукової думки стосовно протидії скімінгу, а саме робіт Кійкова В.М. та Онищенко Ю.М. доводить, що найбільш ефективними технологіями банківської боротьби за скімінгом є : фізичний моніторинг, пасивний анти-скімінг і активний санти-скімінг [1].

Фізичний моніторинг банкоматів включає в себе періодичний огляд банкомату співробітниками банку, інкасаторами, або фахівцями сервісної служби на аутсорсингу. В ході перевірки за графіком заповнюється спеціальний журнал перевірок, щоб в разі знаходження чужорідного пристрою виявити проміжок часу, протягом якого був ризик компрометації карт. На практиці це ненадійний і дорогий спосіб боротьби зі скімінгом.

Пасивний анти-скімінг проявляється в тому, що банк встановлює на щілину карто приймача спеціальні анти-скімінгові накладки, що підключені до спеціального датчика, який спрацьовує в разі