**Список бібліографічних посилань**

1. Бельський Ю. Щодо визначення поняття кіберзлочину. *Юридичний вісник*. 2014. № 6. С. 414-418.

2. Аль-мзіраві Н. А., Мисливий В. А. Поняття та сутність кібернетичної злочинності // Науково-практична інтернет-конференція. 08.12.2016. URL: http://legalactivity.com.ua/index.php?option=com_content&view=article&id=1425%3A091216-07&catid=170%3A5-1216&Itemid=211&lang=en (дата звернення: 31.10.2018).

3. Тихомиров О. О. Кіберзлочин: теоретико-правові проблеми // Зб. матеріалів наук.-практ. конф. «Інформаційна безпека: виклики і загрози сучасності»; 5 квітня 2013 р. К. : Наук.-вид. центр НА СБ України. 2013. С. 179-182

4. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія. К. : КИТ, 2010. 148 с.

*Одержано 01.11.2018*

УДК 004.056.53

**Микола Олександрович УДЯНСЬКИЙ,**
*магістр факультету № 6*
*Харківського національного університету внутрішніх справ*

# ДЕЯКІ ТЕНДЕНЦІЇ ПОШИРЕННЯ ЗЛОЧИНІВ З ВИКОРИСТАННЯМ КРИПТОВАЛЮТ

Інформаційні технології стали постійним супутником сучасної людини не тільки на робочому місці, вони увійшли майже в усі сфери людського життя. Поширення нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки і засобів комунікацій, оптимізації та автоматизації процесів у всіх без винятку сферах життєдіяльності, призвело разом з цим до нівелювання меж і переплетення національних економік і національних інфраструктур країн світу.

Більш того, зазначені тенденції привели до формування єдиного світового інформаційного простору, де кожен може отримати доступ до будь-якої інформації в будь-якій точці планети, здійснювати дистанційно управління власними активами і активами компанії, укладати господарські договори з іноземними суб'єктами господарювання без необхідності особистого контакту і т.д.

Все це призводить до зростання такого явища як кіберзлочинність, а поява такого інструменту для анонімних розрахунків як криптовалюта ще більш загострило і так не просту ситуацію в боротьбі з цим видом злочинів.

Упродовж останнього року, велика кількість інтернет-видань стала отримувати скарги від користувачів, що їх сторінки стали дуже повільними. З'ясувалося, що винен у цьому скрипт-майнер, який було вбудовано в сайти цих відань для видобутку криптовалюти

невідомими особами. Проблеми з незаконним майнінгом виникали і раніше – різні програмні продукти з вбудованими майнерами успішно розповсюджуваються через торренти не перший рік, але вперше від шахраїв постраждали відомі видання з надійною, як вважалося системою безпеки.

У серпні 2018 року експерти з кібербезпеки поширили інформацію, що набирає популярність підступний спосіб вимагання грошей через Інтернет. Кіберзлочинці шантажують користувачів тим, що розкажуть їх друзям і близьким про перегляд порно. Хакери відправляють електронного листа, в якому приводять використовувані жертвою логіни і паролі, витік яких, швидше за все, стався раніше. Автори повідомлення стверджують, що зламали веб-камеру і зняли, як людина дивиться порнографічні ролики і що робить в цей час. Потім шахраї вимагають викуп у біткоінах за те, щоб вони не розсилали відео, яке нібито є у них.

В одному з таких листів було написано наступне: «Я знаю, що це ваш пароль. Спочатку ми записали відео, яке ви дивилися (у вас хороший смак, ха-ха), а потім зробили запис з вашої веб-камери (так, саме те місце, де ви займаєтеся брудними справами).»

У цьому повідомленні хакери вимагають перерахувати $ 1400. на біткоін-гаманець протягом 24 годин. Як доказ вони виявляють готовність розіслати інтимне відео кільком друзям. Користувачі, які бояться заплямованою репутації, погоджуються на вимоги шахраїв. На такій схемі, як розповів виданню Motherboard генеральний директор компанії Banbreach Суман Кар (Suman Kar), шахраї з мінімальними зусиллями змогли заробити $ 500 тис., використовуючи старі бази паролів.

У Banbreach вивчили близько 770 електронних гаманців, які вказували шахраї в повідомленнях про порно-шантаж. Більшість (540) гаманців були порожніми, але в 230 помічені більше 1 тис. транзакцій на загальну суму в 71 біткоін. Деякі зловмисники знаходять жертв в соціальних мережах і вебкам-чатах, знайомляться з ними від імені привабливої жінки або чоловіка і втягують користувача в відверту розмову, метою якої є віртуальний статевий акт. Як тільки злочинцям вдається зафіксувати жертву на камеру або отримати скріншот інтимного листування, вони починають шантажувати її, погрожуючи опублікувати відео- і фотоматеріали у відкритому доступі.

З початку 2017 року кіберзлочинці викрали близько $ 1,2 млрд в різних криптовалютах. Такі дані містяться в звіті міжнародної некомерційної організації Anti-Phishing Working Group (APWG). Витяги з дослідження 24 травня 2018 року опублікувало агентство Reuters.

В інтерв'ю агентству голова APWG Дейв Джеванс (Dave Jevans), який також очолює компанію CipherTrace, що спеціалізується на питаннях безпеки в сфері криптовалют, заявив, що крадіжка токенів

зловмисниками – поширена проблема, на додаток до контрабанди наркотиків і відмивання грошей з використанням криптовалют.

За оцінкою Дейва Джеванс, із зазначеної суми в $ 1,2 млрд лише близько 20% вдалося повернути силами правоохоронців. За його словами, органи правопорядку по всьому світові зайняті відстеженням зловмисників, причетних до крадіжки цифрових грошей. Про черговий гучний інцидент, пов'язаний з кріптовалютним шахрайством, стало відомо в травні 2018 року. Агентство Bloomberg повідомило про розпочате в США розслідування з приводу передбачуваних маніпуляцій з курсом біткоіну та інших криптовалют.

Міністерство юстиції США з'ясовує, чи не вдавалися трейдери до незаконних практик, що впливають на котирування, таким як спуфінг. Під даним терміном розуміється наповнення ринку фейковими заявками з метою підштовхнути інших трейдерів до купівлі або продажу криптовалюти.

Мін'юст співпрацює в розслідуванні з Комісією з ф'ючерсної торгівлі сировинними товарами (CFTC), яка є фінансовим регулятором ринку деривативів на біткоінів.

22 травня 2017 року українського хакера Вадима Ермоловича засудила до 2,5 років тюремного ув'язнення за участь у злочинній схемі, яка дозволила зловмисникам заробити більше $ 100 млн. Про це йдеться в повідомленні міністерства юстиції США.

Вирок 29-річному українцю, затриманому в 2014 році, винесла окружний суддя Ньюарка (Нью-Джерсі, США) Мадлен Кокс Арлі (Madeline Cox Arleo). Про судовий вердикт публічно розповів виконуючий обов'язки федерального прокурора Вільям Фітцпатрік (William Fitzpatrick).

Вадим Єрмолович визнав себе винним в участі в злочинній змові з метою злому комп'ютерів і розкрадання персональних даних. Шахраї крали у компаній прес-релізи до їх офіційної публікації і продавали інсайдерську інформацію трейдерам, які потім використовували ці дані для заробітку на акціях. У махінаціях брали участь і російські трейдери. Вони становили для хакерів списки прес-релізів і імена кращих компаній. Серед них - Caterpillar, Home Depot і Panera Bread.

За даними американської влади, хакери викрали більше 150 тис. призначених для ЗМІ корпоративних повідомлень з порталів Business Wire, Marketwired і PR Newswire в період з лютого 2010 року по серпень 2015 р. Кіберзлочинці заробили на цьому близько $ 100 млн.

Reuters зазначає, що мова йде про найбільшу відому хакерську схему, яка застосовується для гри на фінансових ринках, а 29-річний Вадим Єрмолович з Києва став першим учасником цього угруповання, що зізнався у скоєнні злочину. З огляду на цю пом'якшувальну обставину, суддя засудила його лише до 30 місяців в'язниці.

Комісія з цінних паперів і бірж США висунула звинувачення понад 40 людям. Десять обвинувачених – троє хакерів і сім трейдерів –

притягнуті до кримінальної відповідальності в Нью-Джерсі і Нью-Йорку. П'ятеро із них зізналися в злочинах.

Також жертвами криптовалютних аферистів стають досить відомі в світі бізнесу люди. За інформацією BBC у жовтні 2018 р. хакери зламали кілька верифікованих облікових записів в Twitter і виманили у користувачів під виглядом глави SpaceX Ілона Маска криптовалюти на суму понад $ 150 тис. Відзначається, що після того, як зловмисники зламували перевірені акаунти, вони змінювали імена та фотографії так, щоб вони були схожі на сторінку Маска. Після цього хакери розміщували оголошення про роздачу криптовалюти, для участі користувачам треба було перевести невелику суму у біткоінах.

В Україні також поширюється хвиля шахрайств, пов'язаних з криптовалютами. Так за інформацією Кіберполіції України у 2017 році шахраї викрали у власників bitcoin- гаманців на blockchain.info близько 700 BTC.

Користувачі сервісу стали жертвами фішингу: замість сайту blockchain.info вони прямували на підробні сайти зі схожими назвами. В результаті шахраї отримували дані для доступу до справжніх гаманців. Уперше про проблему повідомили представники Cisco, які виявили фішингову мережу у кінці 2017 року. Імовірно, більшість користувачів переходили на заражені сайти через Google Adwords – рекламну мережу Google, яка дозволяє показувати рекламу вище за результати пошуку. У 2018 році корпорація прийняла нові правила перевірки оголошень, після чого масштаб атак помітно знизився.

Криптовалюта, як анонімний платіжний засіб, буде завжди привабливим інструментом для самих різних злочинних схем, як то відмивання брудних коштів від наркоторгівлі, шантажу, торгівлі зброєю, дитячою порнографією тощо. Тому ефективна протидія відмиванню злочинних доходів і зниження рівня злочинності в цій сфері можливі завдяки своєчасному виявленню фінансових операцій, які можуть бути пов'язані з відмиванням доходів, отриманих в сфері кіберзлочинності, та ефективному міжнародному співробітництву, а також співпраці між державним і приватним сектором.

*Одержано 06.11.2018*

УДК 004.056.53

**Гліб Вікторович УШАКОВ,**
*магістр факультету № 6*
*Харківського національного університету внутрішніх справ*

## ГЛОБАЛЬНІ РИЗИКИ КІБЕРПРОСТОРУ

Інформаційний простір став місцем і, в той же час, безпосередньо інструментом злочину, відтепер злочин не вимагає попередньої «обробки клієнта» і особистого контакту з потенційною жертвою. Головним інструментом злочинця стає лише комп'ютер і доступ до