[Текст] : монографія / Джужа А. О. ; Нац. акад. внутр. справ. - К. : [б. в.], 2013. - 193 с.
2. Сахарук Т.В. Проблеми призначення покарання неповнолітнім// Питання боротьби зі злочинністю: Зб. наук. праць. Вип.8. – Х., 2004. – С.53-59.
3. Судова практика у справах про злочини неповнолітніх і втягнення їх у злочинну діяльність// Вісник Верховного суду України. – 2003. - № 4(38). – С.25.
4. Флямер Р., Карнозова Л. «Детская юстиция». Обзор экспериментальных проектов в России// Движение за ювенальную юстицию в современной России. – М.: МОО Центр «Судебно-правовая реформа», 2003. – 172 с.
5. Надання допомоги дітям-жертвам злочинів, пов'язаних із торгівлею дітьми, дитячою проституцією, дитячою порнографією, проти статевої свободи та статевої недоторканості дитини, з урахуванням національної та міжнародної практик / Авт.: Волинець Л. С., Гурковська Л. П., Савчук І. В. — К.: ТОВ "К.І.С.", 2011 — 132 с.
14. Конвенція про права дитини //Бюлетень законодавства і юридичної практики України. – 1997. – № 5. – К.: Юрінком, 1997. – С. 35-54.

Шапочка С. В.,
науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, магістр права

СТОСОВНО НОВИХ ВИДІВ ШАХРАЙСТВА, ЩО ВЧИНЯЄТЬСЯ З ВИКОРИСТАННЯМ МОЖЛИВОСТЕЙ МЕРЕЖІ ІНТЕРНЕТ

Проблема кіберзлочинності набула міжнародних масштабів та демонструє сталу тенденцію до зростання [1, с. 58]. Результати аналізу її характеристик дозволяють прогнозувати ускладнення боротьби з нею з огляду на те, що способи вчинення комп'ютерних злочинів з кожним роком

набувають усе досконаліших форм. До вирішення цієї проблеми необхідно підходити комплексно, вивчаючи динаміку розвитку кіберзлочинності і виникнення нових її видів.

Відповідно до Закону України "Про основи національної безпеки України" від 19 червня 2003 року № 964-IV система забезпечення інформаційної безпеки є складовою частиною національної безпеки держави й однією з найважливіших її функцій, що полягає в захищеності людини, суспільства і держави, забезпеченні охорони та захисту інформаційних ресурсів, мінімізації шкоди від негативних інформаційних впливів, небажаних наслідків використання інформаційних продуктів і інформаційних технологій [2].

Однією з потенційних загроз національній безпеці вже давно стали високотехнологічні злочини, що вчиняються з використанням мережі Інтернет організованими злочинними угрупованнями.

Нові інформаційні технології дали поштовх розвитку міжнародних зв'язків організованої злочинності, укладенню та реалізації міжнародних злочинних угод, надали нові інструменти для вчинення злочинів. Власне, глобальна мережа Інтернет, і, вже існуюча міжнародна злочинність, стали основними джерелами для виникнення нового типу організованої злочинності – кіберзлочинності, з характерними їй "традиційними" ознаками: стійкість, попередня зорганізованість членів або структурних частин для спільної злочинної діяльності, ієрархія, з чітким розподілом ролей і обов'язків, сувора дисципліна, транснаціональний характер тощо, а також новими ознаками: відсутність чітко визначених географічних меж, складність у визначенні часу, місця вчинення злочину, наявність у злочинців спеціальних знань у галузі інформаційно-телекомунікаційних систем тощо.

Необхідно зазначити, що поява нових засобів зв'язку й комп'ютерних технологій полегшили встановлення і підтримання комунікації між злочинними групами та співтовариствами не лише у рамках однієї країни, але і на міжнародному рівні, дозволяючи вчиняти злочини з використанням можливостей мережі Інтернет, а саме: шахрайство, вбивство, тероризм, легалізація (відмивання) доходів, одержаних злочинним шляхом, злочини у сфері обігу наркотичних засобів, пов'язані з виготовленням, збутом і розповсюдженням порнографії, в тому

числі і дитячої, незаконний обіг зброї, незаконна міграція, службові злочини, порушення авторських прав, злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку тощо).

Варто зазначити, що шахрайство, з використанням комп'ютерної мережі Інтернет становить понад 60 % кіберзлочинів, тобто, більш ніж половину злочинних посягань на право власності від загальної кількості "білокомірцевих" злочинів.

Даному виду злочинів притаманні такі характеристики як велика суспільна небезпека, слабкий контроль з боку суспільства й правоохоронних органів, інтелектуальність, висока латентність, низький ступінь ризику для злочинця і, при цьому, порівняно легкий успіх, конфіденційність дій, анонімність будь-якого користувача-злочинця, відсутність кордонів, вчинення в будь-який час, з будь-якого місця планети, транснаціональний організований характер.

Шахрайство в мережі Інтернет зберігає сталу тенденцію до еволюціонування, з'являються нові його види чи удосконалюються вже відомі, такі як: фішинг, скіммінг, використання шпигунських програм (spyware, keyloggers), обман під час купівлі-продажу товарів в Інтернет-магазинах, шахрайство в Інтернет-аукціонах, SMS- шахрайство, рерайтинг, серфінг, креммінг, шахрайство з криптовалютами тощо [3, с. 330].

Завдячуючи стрімкому розвитку електроніки та інформаційних технологій виникають нові види злочинів, що вчиняються з використанням мережі Інтернет.

З'явилося і нове явище, що виникло в мережі Інтернет менше п'яти років тому. Йдеться про широке розповсюдження і популяризацію використання децентралізованих віртуальних криптовалют (Bitcoin, Litecoin, Namecoin, Zerocoin, Quark, Megacoin, Namecoin, Peercoin, Worldcoin, тощо), темпи приросту капіталу їх власників склали 100 %, 200 % і навіть 1000 % на день. Криптовалюта стала одним із видів електронних платіжних засобів для оплати товарів і послуг в мережі Інтернет, яку також можна обміняти на реальні гроші.

По суті, кожна з цих платіжних систем стала новим валютним ринком, що нестримно набирає популярність, а

валютна торгівля перетворилася на глобальну азартну гру. Включитися в цю гру легко може будь-хто. Для цього навіть не потрібно нічого знати про криптовалютах – досить купити віртуальні монети на біржі, як фішки в казино. Тобто криптовалюти – це величезні світові шахрайські піраміди [4].

Нерегульована сфера віртуальних валют користується великою популярністю серед організованих злочинних угруповань, що вже приймають оплату за свої послуги в віртуальній валюті, використовуючи альтернативний Інтернет – DarkNet, що функціонує на основі системи TOR (The Onion Router).

Окрім того, в Канаді та США вже з'явилися Bitcoin-банкомати, Bitcoin-біржі, що дають можливість створити відчуття попиту і ліквідності криптовалюти, а як наслідок – призвести до стрімкого росту її курсу, зробити віртуальні гроші платіжним засобом організованих злочинних угруповань та предметом вчинення злочинів у мережі Інтернет.

Різке зростання популярності криптовалют змусило багатьох українців також замислитися про те, щоб здійснювати такі розрахунки, а також заробляти на майнінгу – видобутку Bitcoin. Загальний порядок проведення переказу коштів у межах України, відповідальність суб'єктів переказу коштів, а також правові вимоги до здійснення випуску і використання електронних грошей в Україні встановлені Законом України "Про платіжні системи і переказ коштів в Україні" [5]. А відповідно до статті 9 цього Закону платіжні організації платіжних систем, учасники платіжних систем і оператори послуг платіжної інфраструктури мають право здійснювати діяльність в Україні виключно після їх реєстрації Національним банком України. Відповідно до вимог статті 15 Закону право випуску електронних грошей надане виключно банку. На сьогодні в Національний банк України не зверталися банки або інші юридичні особи з приводу реєстрації платіжної системи Bitcoin або з приводу узгодження правив використання електронних грошей Bitcoin. НБУ застерігає українців від використання такої системи [5].

В той же час, в деяких країнах, зокрема – в Китаї, Росії Bitcoin вже фактично поза законом.

З огляду на світові тенденції формування глобального інформаційного простору при високій динаміці розвитку інформаційних технологій, очевидно, що проблема забезпечення

інформаційної безпеки є однією з найбільш актуальних, а небезпека потенційних загроз у вигляді ІТ-злочинності, шахрайства з криптовалютами – реальною, що потребує системної, наступальної реакції держави. українського законодавства.

Разом з цим, далеко не всі проблеми, пов'язані з питанням протидії використанню мережі Інтернет організованими злочинними угрупованнями досліджені, піддані необхідному аналізу, узагальненню і відповідному відображенню.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Протидія кіберзлочинності в Україні : правові та організаційні засади : навч. посіб. / [О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.]. – К. : Видавничий дім "Скіф", 2012. – 728 с.
2. Про основи національної безпеки України: Закон України від 19 червня 2003 р. № 964-IV [Електронний ресурс]. – Режим доступу :
   http://zakon4.rada.gov.ua/laws/show/964-15.
3. Шапочка С. В. Кримінологічна характеристика шахрайства, що вчиняється з використанням комп'ютерних мереж / С. В. Шапочка // Боротьба з організованою злочинністю і корупцією (теорія і практика) : наук. - практ. журнал ; МНДЦ при РНБО України. — К., 2011. — № 2-3.— С. 329 — 336.
4. В мире бум криптовалютных пирамид / [Электронный ресурс]. – Режим доступа :
   http://finance.eizvestia.com/full/244-cryptocurrency-pyramid.
5. Про платіжні системи і переказ коштів в Україні: Закон України від 5 rdsnня 2001 р. № 2346-III [Електронний ресурс]. – Режим доступу :
   http://zakon4.rada.gov.ua/laws/show/2346-14/page.
6. НБУ не рекомендует украинцам пользоваться Bitcoin: официальный комментарий / [Электронный ресурс]. – Режим доступа :
   http://ain.ua/2014/02/14/513124.