УДК 343.537:343.346.8:343.974

Стосовно деяких аспектів запобігання шахрайству, що вчиняється організованими злочинними групами з використанням комп'ютерних мереж

Шапочка Сергій Володимирович –
науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, магістр права

Статтю присвячено аналізу проблеми боротьби з шахрайством, що вчиняється з використанням мережі Інтернет, а також запропоновано заходи протидії такій діяльності.

Ключові слова: шахрайство, Інтернет-шахрайство, кіберзлочинність, попередження кіберзлочинності.

Постановка проблеми. Колишній оглядач газети "Бостон Глоуб" Джон Елліс (John Ellis) слушно зауважив: "Мережа Інтернет змінює все, чого б не торкнулася, а торкається вона практично всього".

Нині життя людини суттєво змінюється під впливом науково-технічного прогресу та процесів глобалізації. Сучасні комп'ютерні технології відіграють усе більшу роль у політичних й економічних процесах України і світу.

Завдяки їм еволюціонує і злочинність. Як наслідок, відбувається розвиток міжнародних кримінальних зв'язків, укладення та реалізація міжнародних злочинних угод, встановлення і підтримання комунікацій між злочинними групами та співтовариствами не лише у межах однієї країни, але й на транснаціональному рівні.

Можливості мережі Інтернет дедалі частіше використовуються для вчинення шахрайств, убивств і тероризму, вчинення атак на інформаційно-телекомунікаційні системи і мережі важливих політичних та адміністративних структур держави. Вони допомагають легалізації (відмиванню) доходів, одержаних злочинним шляхом, і нелегальному обігу наркотичних засобів. Мережеві технології також тісно пов'язані з виготовленням, збутом і розповсюдженням порнографії, в тому числі й дитячої, незаконним обігом зброї, нелегальною міграцією, службовими злочинами, порушенням авторських прав, злочинами у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку тощо.

Серйозну загрозу для людства несе розробка і поширення в інформаційному просторі програм, які становлять пряму загрозу життю людей (атака на імплантати). На окрему увагу заслуговують злочини, пов'язані з виникненням криптовалют (Bitcoin, Litecoin, Namecoin, Zerocoin, Quark), якими розраховуються сотні організацій по всьому світу, в тому числі й організовані злочинні угруповання, та використання альтернативного Інтернету – DarkNet, що функціонує на основі системи TOR (The Onion Router) [1].

Аналіз останніх публікацій за темою дослідження. Проведенням наукових досліджень окремих аспектів щодо боротьби зі злочинами, що вчиняються з використанням мережі Інтернет взагалі та шахрайства зокрема, займаються такі вчені, як І. Г. Богатирьов, В. М. Бутузов, В. Д. Гавловський, Д. О. Зиков, А. А. Комаров, В. Д. Ларичев, А. К. Лебедєв, О. В. Лисодєд, А. В. Микитчик, О. В. Смаглюк, К. В. Тітуніна, С. С. Чернявський, В. І. Шакун, В. П. Шеломенцев, О. М. Юрченко та інші, а також автор представленої статті.

Позаяк комп'ютерно-телекомунікаційні системи набули статусу невід'ємного інструменту ведення бізнесу, забезпечення реалізації комунікативно-інформаційної складової політичної, адміністративно-управлінської, правоохоронної та інших форм діяльності як державних установ, так і приватного сектору, їх можливості достатньо активно й ефективно використовуються організованими злочинними групами під час вчинення злочинів, у тому числі пов'язаних із обманом і зловживанням довірою – шахрайством, що спонукає нас до подальших наукових досліджень.

Мета статті. В попередніх наукових публікаціях нами вивчалися різні аспекти шахрайства, що вчиняється з використанням можливостей мережі Інтернет. Ця стаття є логічним продовженням здійснюваного нами дослідження і містить спробу висвітлити особливості вчи-

нення кібершахрайства організованими злочинними групами.

Виклад основного матеріалу. Одне з найбільших досягнень європейського способу життя – вільне пересування людей, товарів, коштів, надання широкого спектру послуг, розвиток електронної комерції одночасно є каталізатором швидкої динамічної еволюції та сприяє прогресії злочинності, в тому числі й організованої.

Дані закордонної правоохоронної практики свідчать про те, що зростання рівня злочинності з використанням комп'ютерних мереж відбувається з величезною швидкістю. Це підтверджують і дослідження у сфері кіберзлочинності Центру стратегічних міжнародних досліджень США (Center for Strategic and International Studies, CSIS), за якими найбільші економіки світу втрачають від 375 до 575 млрд дол. щорічно через кібератаки, що становить 0,5 % від усієї світової економіки (ВВП), який майже наздогнав частку від незаконної торгівлі наркотиками (0,9 %) [2].

Окрім цього у матеріалах CSIS за 2013 рік зазначено, що близько 3 тис. компаній зазнали хакерських атак, а кількість постраждалих склала 40 млн осіб, при цьому, кожен сьомий з них зазнав збитків від шахрайства, що вчиняється з використанням мережі Інтернет (розкрадання з кредитних карт і злам мобільного банкінгу), що в сумі становило 160 млрд дол. збитків.

Шахрайство з використанням можливостей мережі Інтернет зберігає сталу тенденцію до еволюціонування, з'являються нові його види чи удосконалюються вже відомі, такі як: у сфері дистанційного банківського обслуговування, з електронними платіжними системами і системами експрес-оплати товарів і послуг (жебрацтво, фейкові банки, біржі праці, електронні віртуальні гаманці, фейкові листи від чужого імені, Інтернет-аукціони, Інтернет-лотереї, віртуальні казино й тоталізатори), кредитне шахрайство, кіберсквоттинг, рерайтинг, серфінг, креммінг, банкоматне шахрайство (фішинг, скіммінг, використання "білого пластику"), використання шпигунських програм (spyware, keyloggers), використання ноах-програмного забезпечення, SMS-шахрайство тощо [3, с. 330].

Більшість із перелічених шахрайств із використанням можливостей мережі Інтернет вчиняються організованими групами та мають окрім необхідних ознак, таких як: систематичність або постійне, здебільшого у вигляді промислу (злочинного підприємства), вчинення умисних злочинів, спрямованих на отримання сталих високих прибутків та їх легалізацію на основі утворення злочинного об'єднання і спеціально організованої системи забезпечення його підтримки органами влади чи її представниками з метою прикриття від соціального контролю та відповідальності [4, с. 312–313], і специфічні характеристики, такі як вихід у своїй злочинній діяльності за межі кордону однієї держави – транснаціональний чи транскордонний характер. Адже, шахраї, використовуючи статус анонімності, несучи за свої дії мінімальну відповідальність, мають можливість, використовуючи комп'ютерно-телекомунікаційні пристрої, вчиняти злочини у будь-якій країні, без обмеження в часі й просторі, а також мають змогу обрати об'єкт посягання у країні, де відсутня відповідальність за таку діяльність, чи покарання є достатньо м'яким, у порівнянні з іншими державами.

Думається, що, насамперед, потрібно виходити з того, що організована злочинність – це багатозначний різнорівневий та складно структурований феномен суспільного життя, який виник і розвивається в результаті прагнення (активності) частини членів суспільства змінити у кримінальний спосіб його цивілізовану, перш за все, правову упорядкованість, в інтересах власного збагачення та отримання на цій основі фактичної влади. Наведена характеристика належить загальносуспільному рівню сприйняття організованої злочинності, де проявляється її суспільно деструктивний вплив, у тому числі, передусім, соціально-економічний, соціально-психологічний, криміногенний [4, с. 305].

При цьому вершиною організації убезпечення діяльності злочинних об'єднань є їх "хождение во власть" та захоплення фактичної влади. Кінцевою метою організованої злочинності стає руйнація економічної безпеки держави та фактичне підкорення економіки своїм інтересам, за чим іде й підкорення влади [4, с. 294]. Слушною є думка А. Макієнко про те, що на підставі глибокого політико-кримінологічного аналізу стану і найбільш загального розуміння організованої злочинності, низки її внутрішніх характеристик і залежностей від неї вона перетворилася на "чинник соціально-політичного й економічного загальнодержавного впливу і, звичайно, випрацювала відповідні механізми впливу, спрямування або примусу стосовно ключових механізмів, інституцій і структур, включаючи засоби масової інформації і комунікації" та пов'язаних з нею суспільних відносин [5, с. 83].

Тобто, організована злочинність, її категоріальне поняття, характеризується не лише кількістю учасників злочинних груп, їх стійкістю, зорганізованістю, ієрархією тощо, а й реальним змістом, небезпекою для держави.

З погляду американського кримінолога Д. Албанезе (Albanese, Jay S.), організована злочинність є постійно діючим кримінальним підприємством, яке працює раціонально для одержання прибутку від незаконної діяльності, що користується суспільним попитом [6, с. 3].

Особливістю вчинення шахрайства з використанням мережі Інтернет організованою групою є створення у потерпілих відчуття відкритості, офіційності, легальності, легітимності своєї діяльності шляхом проведення широкої рекламної компанії, використання маркетингових шаблонів, витрати на іміджеві інституції, показовий зв'язок і партнерські стосунки із відомими компаніями. А тому зазначений вид злочинів характеризується високою латентністю, вели-

кою кількістю способів учинення, необмеженими часом і простором, можливостями щодо вчинення.

Традиційні для кримінології загально соціальний, спеціально-кримінологічний та індивідуальний рівні попередження злочинності можна розглядати з урахуванням специфіки шахрайства, що вчиняється з використанням комп'ютерних мереж, виділяючи при цьому основні форми впливу: віктимологічну профілактику і заходи забезпечення інформаційної безпеки.

На загальному рівні необхідно сформувати правильну і стабільну кримінальну політику, яка б забезпечила ефективну реалізацію обов'язку держави у сфері діяльності із захисту громадян і суспільства від злочинних посягань шляхом розробки цілей і завдань, принципів, стратегії і тактики, напрацювання засобів і методів боротьби зі злочинністю. Кримінальна політика являє собою складний інструмент регулювання суспільних відносин, оскільки містить довгострокові плани з питань реформування і вдосконалення кримінального законодавства.

Окрім цього, необхідно організувати і забезпечити реалізацію соціально-правового контролю, правове регулювання кримінологічної експертизи, правове регулювання мережі Інтернет. Облік злочинів, що вчиняються, має за мету здійснити оцінку ефективності діяльності правоохоронних органів і зберегти соціальний спокій суспільства, демонструючи відносно помірні картини стану злочинності. Але існуюча система кримінальної статистики уже не справляється зі своїми обов'язками. У статистичній звітності МВС України, Генеральної прокуратури України, Судової адміністрації України відсутні виокремлені дані щодо кількісно-якісних показників учинення шахрайства з використанням комп'ютерних мереж.

Згідно зі статистичними даними МВС України [7], за 9 місяців 2014 року зареєстровано кримінальних правопорушень, вчинених з ознаками ст. 190 КК України (Шахрайство), – 4926, з них 544 особам повідомлено про підозру в учиненні кримінального правопорушення. При цьому за 6 місяців поточного року зареєстровано кримінальних правопорушень, вчинених з ознаками ст. 190 КК України (Шахрайство), – 5491, з них 715 особам повідомлено про підозру в учиненні кримінального правопорушення. Тобто, за 9 місяців кількісні показники є меншими, аніж за 6 місяців.

При цьому, згідно зі статистичними даними Генеральної прокуратури України, за аналогічний період часу (за 9 міс. і за 6 міс.) обліковано кримінальних правопорушень 33 872 (за ч. 3 ст. 190 – 2040) і 25 542 (за ч. 3 ст. 190 – 1538) відповідно, а повідомлення про підозру вручено 8355 (за ч. 3 ст. 190 – 988) і 5719 (за ч. 3 ст. 190 – 723) особам відповідно [8].

Зазначені розбіжності у статистичних даних ілюструють різні системи обліку кримінальних правопорушень в МВС України та в ГП України.

При цьому вказану різницю статистичних даних між звітними періодами за 6 і 9 місяців у даних МВС можна пояснити тим, що по частині кримінальних правопорушень провадження було закрито, по частині проваджень досудове розслідування було зупинене відповідно до ст. 280 КПК України через: захворювання підозрюваного; невідоме місцезнаходження підозрюваного; виконання процесуальних дій у межах міжнародного співробітництва. Також, частина проваджень про кримінальні правопорушення направлена до суду з клопотанням про звільнення від кримінальної відповідальності.

Разом з цим, статистичні дані в кращому випадку показують кількісні значення вчинення шахрайства відповідно до частини третьої ст. 190 КК України, тобто шахрайство, вчинене у великих розмірах або шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ЕОТ), не виокремлюючи останню складову – з використанням ЕОТ.

Зазначений стан речей ускладнює або й унеможливлює здійснення належного ефективного кримінологічного прогнозування, як процесу встановлення всіх параметрів злочинності в перспективі, виявлення на цій основі небажаних тенденцій та пошуку засобів їх зміни у позитивному напрямі [9, с. 161]. З огляду на те, що обгрунтованість та ефективність планування багато в чому залежить від точності прогнозу тенденцій у динаміці й структурі злочинності та можливостей ефективності заходів боротьби з нею, кримінологічний прогноз є необхідною інформацією для прийняття рішень і планування боротьби зі злочинністю на майбутнє [10, с. 189–199]. Що дасть можливість передбачення майбутніх змін у динаміці, рівні, структурі й географії злочинності; можливих наслідків реалізації заходів боротьби зі злочинністю; можливої майбутньої поведінки осіб, засуджених за вчинення злочинів.

А тому виникає необхідність перебудови діяльності правоохоронних органів України в частині обліку і реєстрації злочинів даного виду таким чином, щоб вони не лише відображали реальний стан речей, а й відкривали нові можливості для вивчення мережевих шахрайств. При цьому ефективності правоохоронної діяльності необхідно давати оцінку не спираючись на кількісні показники розкритих злочинів, а на підставі відчуття захищеності прав громадян країни. Для цього потрібно організувати дієву тісну взаємодію правоохоронних органів, служб безпеки фінансово-кредитних установ, суспільних організацій щодо сприяння попередженню злочинності. Однією з найважливіших вимог для ефективної роботи у даному напрямі є повна інформатизація цього процесу, його фіксування на магнітних носіях, створення централізованої автоматизованої системи баз даних.

Необхідно враховувати специфіку шахрайства, що вчиняється з використанням можливостей мережі Інтернет, під час законопроектної діяльності з питань законодавчих змін. Доцільним є проведення кримінологічної експертизи, враховуючи при цьому як конкретні історичні обставини, рівень динамічного науково-техніч-

ного розвитку суспільства, так і негативні правові та соціальні наслідки, з метою здійснення правильного прогнозу реалізації даних норм у майбутніх реаліях життя, а також для нейтралізації впливу криміногенних чинників, таких як: низький рівень правосвідомості, правовий нігілізм, невисока результативність діяльності правоохоронних органів.

Міжнародна комп'ютерна мережа Інтернет є відкритим середовищем, яке надає можливість користувачам вчиняти дії різного характеру, в тому числі й злочини, перебуваючи за межами держави, в якій знаходяться об'єкти посягання. Користувачі можуть вибирати такі країни, таке правове середовище, в якому певні діяння, що вчиняються в електронному середовищі, не тягнуть за собою кримінальної відповідальності. Наявність "держав-інформаційних сховищ" є вагомим чинником, котрий нівелює зусилля інших держав, спрямовані на боротьбу зі злочинністю з використанням комп'ютерних мереж.

Таким чином, для боротьби зі злочинами у відкритих комп'ютерних мережах, у тому числі й для протидії шахрайствам, що вчиняються з використанням комп'ютерних мереж організованими злочинними групами, необхідною є активізація міжнародного співробітництва на всіх рівнях шляхом прийняття і використання узгоджених міжнародних заходів, удосконалення національних систем обліку статистичних даних щодо злочинів, учинених з ознаками ч. 3 ст. 190 КК України.

Усе це сприятиме розширенню та вдосконаленню форм і методів боротьби з кіберзлочинністю.

Список використаних джерел

1. Шапочка С. В. До питання запобігання окремим видам шахрайства, яке вчиняється з використанням можливостей мережі Інтернет / С. В. Шапочка // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2014. – № 1 (32). – С. 145–149.

2. Net Losses: Estimating the Global Cost of CybercrimeEconomic impact of cybercrime II / [Electronic resource]. – Mode of access : http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

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). – 2011. – № 2–3.– С. 329–336.

4. Закалюк А. П. Курс сучасної української кримінології: теорія і практика : [у 3 кн.] / А. П. Закалюк. – К. : Видавничий дім "Ін Юре", 2007. – Т. 2. – 706 с.

5. Макиенко А. В. Криминалитет и власть в стране / А. В. Макиенко // Інформ. бюл. Міжвід. наук.-досл. центру з проблем б-би з орг. злоч. – К., 2002. – № 6. – С. 83–84.

6. Organized Crime In Our Times [Electronic resource] / Jay S. Albanese. – [6-th Edition]. – P. 390. – Mode of access : http://www.organized-crime.de/organizedcrimedefinitions.htm#albanese.

7. Статистика МВС України / [Електронний ресурс]. – Режим доступу : http://mvs.gov.ua/mvs/control/main/uk/index.

8. Статистична інформація ГП України / [Електронний ресурс]. – Режим доступу : http://www.gp.gov.ua/ua/stst2011.html?dir_id=111482&libid=100820&c=edit&_c=fo.

9. Кондратьєв Я. Ю. / Кримінологія : підруч. для студ. вищих навч. закл. // Я. Ю. Кондратьєв, О. М. Джужа. – К. : Юрінком Інтер, 2002. – 416 с.

10. Герцензон А. А. Криминология / А. А. Герцензон, В. Н. Кудрявцев. – [3-е изд., испр. и доп.]. – М. : Юрид. лит., 1976. – 440 с.

Статья посвящена анализу проблемы борьбы с мошенничеством, совершаемым с использованием сети Интернет, а также предложены меры противодействия такой деятельности.

This article is devoted to the anti-fraud problem committed by using the Internet, and the measures of counteraction of such activity are given.

Стаття надійшла до редакції журналу 15 жовтня 2014 року.