УДК 343.9+343.53:354.42/44

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

ДО ПИТАННЯ БОРОТЬБИ З ШАХРАЙСТВОМ, ЯКЕ ВЧИНЯЄТЬСЯ З ВИКОРИСТАННЯМ МОЖЛИВОСТЕЙ МЕРЕЖІ ІНТЕРНЕТ

Анотація. *У статті проаналізовано окремі аспекти шахрайства, що вчиняється з використанням можливостей мережі Інтернет у контексті інформаційної безпеки, а також запропоновано заходи протидії такій діяльності.*

Ключові слова: *інформаційна безпека, шахрайство, Інтернет-шахрайство.*

Аннотация. *В статье проанализированы отдельные аспекты мошенничества, совершаемого с использованием сети Интернет в контексте информационной безопасности, а также предложены меры противодействия такой деятельности.*

Ключевые слова: *информационная безопасность, мошенничество, Интернет-мошенничество.*

Summary. *The paper analyzes some aspects of fraud committed using the Internet in the context of information security, as well as proposes countermeasures for such activities.*

Keywords: *information security, fraud, Internet fraud.*

Постановка проблеми. З огляду на реалії сьогодення, очевидно, що виклики та загрози національній безпеці України, які, наразі, не лише набули масштабних проявів, а й реалізовані у втратах, яких вона зазнала, продовжують чинити деструктивний вплив на всі сфери життєдіяльності країни. Як наслідок, наша держава стоїть на порозі системних перетворень у сфері забезпечення національної безпеки, в тому числі й інформаційної.

Інформаційний простір України в цілому досі залишається позбавленим цілісної системи регулювання. Якщо в питанні розвитку інформаційного суспільства є певна системність, то питання забезпечення інформаційної безпеки як у частині державного управління, законодавчого регулювання, так і бюджетного фінансування, врегульоване меншою мірою [1]. Внаслідок чого спостерігається низка негативних явищ, які стоять на заваді як розвитку суб’єктів ринку, так і забезпеченню інформаційних прав та свобод громадян, а подекуди й створюють загрози національній безпеці України.

На фоні зазначених проблем на другий план відходить системний наступальний підхід до питань боротьби зі злочинністю взагалі та злочинами, що вчиняються з використанням мережі Інтернет, шахрайством зокрема. Але, останні події, пов’язані з виявленням і ліквідацією СБ України шкідливого програмного забезпечення, яке мало знищити на сервері ЦВК результати президентських виборів 25 травня поточного року, наочно доводять, що ІТ-злочинність чинить дієвий вплив на інформаційну безпеку України.

Ще одним аргументом на користь нагальності вирішення проблеми боротьби зі злочинністю в мережі Інтернет є звіт-прогноз Європейського центру по боротьбі з кіберзлочинністю при Європолі (Project 2020) [2], зроблений 25 вересня 2013 року з описом можливих сценаріїв розвитку кіберзлочинності в Європі до 2020 року. На думку фахівців, злочинці зможуть зламувати величезну кількість пристроїв, зокрема: електронне

обладнання автомобілів, медичні прилади, імплантати, безпілотні літальні апарати тощо. Також, експерти прогнозують виникнення принципово нових видів загроз: межа між комп’ютерною та фізичною атакою на людину в багатьох випадках зникне, відбудеться конвергенція біотехнологій, комп’ютерних технологій і віртуальної реальності, як наслідок, – можуть виникнути такі атаки.

Окрім цього існують наступні можливі сценарії розвитку нових типів комп’ютерних атак та інших проявів кіберзлочинності в Європі до 2020 року :

– ринок скремблерів для розпізнавання настроїв користувачів, симуляції дистанційної присутності, технології Near Field Communication;

– дуже розподілені DoS-атаки через хмарні сервіси;.

– перехід від ботнетів на пристроях до хмарних ботнетів, використання чужих обчислювальних ресурсів;

– розвиток підпільного ринку віртуальних товарів – як викрадених, так і контрафактних;

– електронні атаки на критичну інфраструктуру, включаючи джерела енергії, транспорт і інформаційні служби з використанням потенційних можливостей соціальних мереж;

– мікро-злочинність, у тому числі крадіжка і генерація фальшивих мікро-платежів;

– біозлами елементів багатофакторної ідентифікації;

– війни кіберугруповань;

– таргетовані крадіжки особистості та злом аватарів;

– складні маніпуляції з репутацією;

– підробка додаткової реальності для шахрайства, що вчиняється з використанням соціальної інженерії.

Проведенням наукових досліджень окремих аспектів щодо інформаційної безпеки, боротьби зі злочинами, що вчиняються з використанням мережі Інтернет взагалі та шахрайства зокрема, займаються такі вчені, як І.Г. Богатирьов, В.Д. Гавловський, О.М. Голембіовська, Д.О. Зиков, А.А. Комаров, В.Д. Ларичев, А.К. Лебедєв, О.В. Лисодєд, А.В. Микитчик, О.В. Смаглюк, С.С. Чернявський, В.І. Шакун, О.М. Юрченко та ін.

Не викликає жодних сумнівів актуальність дослідження питань інформаційної безпеки та різних аспектів Інтернет-шахрайства, адже більше половини злочинів, що вчиняються за допомогою комп’ютерних мереж, здійснюється, з використанням обману чи зловживанням довірою [3, с. 226]. Інтернет-шахрайство зберігає сталу тенденцію до еволюціонування, що спонукає до подальших наукових досліджень.

Метою статті є дослідження окремих аспектів шахрайства, що вчиняється з використанням можливостей Інтернет.

Виклад основних положень. Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [4, с. 58]. Законодавець саме так у статті 17 Основного закону визначив інформаційну безпеку як одну з найважливіших функцій держави.

Відповідно до Закону України “Про основи національної безпеки України” [5] система забезпечення інформаційної безпеки є складовою частиною національної безпеки держави й однією з найважливіших її функцій. В тому числі й забезпечення інформаційного суверенітету України.

Сьогодні законодавчого визначення поняття інформаційної безпеки в нашій державі немає*, але законодавець зробив спробу врегулювати відносини у цій сфері внесенням проекту Закону України “Про засади інформаційної безпеки України” [6, ст. 328]. Проектом Закону України передбачається визначити основні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства і держави в інформаційній сфері, та організації забезпечення інформаційної безпеки в умовах формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору.

Відповідно до цього проекту інформаційна безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому здійснюється завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій.

Захищати інформацію повинна кожна держава у такий спосіб, який вважає за доцільне та який має технологічні й правові можливості це зробити. Але, не потрібно забувати про те, що тотальний захист інформації може призвести до інформаційної цифрової резервації.

Разом із цим, однією з основних реальних і потенційних загроз інформаційній безпеці України є поширення кіберзлочинності в інформаційній сфері, невідповідність законодавства України сучасним викликам і загрозам інформаційній безпеці. А своєчасне виявлення, запобігання і припинення злочинів у інформаційній сфері є одним із основних напрямів діяльності держави у сфері забезпечення інформаційної безпеки.

Зазначений стан захищеності знаходиться у прямій залежності від обізнаності, підготовленості, ресурсної та технічної забезпеченості, нормативно-правової урегульованості діяльності правоохоронних, контролюючих та інших органів державної влади й управління, які діють у взаємодії з юридичними та фізичними особами у питаннях забезпечення інформаційної безпеки і боротьби зі злочинністю з використанням мережі Інтернет.

Глобальність сучасних можливостей і досягнень прямо пропорційні глобальності загроз і злочинних проявів. У той же час, розвиток Інтернет-технологій, глобальної і локальних мереж дозволили підняти на новий інтернаціонально-континентальний рівень торговельно-економічні відносини та електронну комерцію. Еволюціонували, зміцнившись, і позиції транснаціональної злочинності, набули нових рис, необмежених можливостей [7, с. 63].

Сформувались злочинні посягання “нового покоління”, це злочини, які вчиняються з використанням досягнень науково-технічного прогресу, але при цьому за своєю

---

* ***Від редакції.*** Відповідно до п. 13 Закону України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки” від 09.01.07 р. № 537-V : Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через:

неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив;

негативні наслідки застосування інформаційних технологій;

несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

сутністю і кваліфікуючими ознаками вони залишаються, так би мовити, традиційними видами злочинів, такими як шахрайство, крадіжка, вимагання, вбивство, тероризм тощо.

Оскільки процеси інформатизації в країнах ЄС розпочалися раніше ніж у державах пострадянського простору, то і надбання у сферах інформаційної безпеки, боротьби з кіберзлочинністю є більш вагомими.

Розуміючи серйозність реальних і потенційних загроз злочинності в мережі Інтернет національній, в тому числі інформаційній та кібернетичній безпеці зокрема, Європейський парламент, після заслуховування доповіді Європолу про стан злочинності в ЄС і нових явищах та тенденціях у кримінальній сфері, схвалив план дій на 2014 – 2019 рр. щодо боротьби з новими видами злочинності, відмиванням грошей та корупцією [8].

Згідно з даними Європолу кіберзлочинність стосується всіх країн-членів ЄС і пов’язана, передусім, із фінансовим шахрайством. Відповідно до досліджень Єврокомісії 8 % користувачів мережі Інтернет у ЄС були потерпілими від крадіжки особистості і 12 % постраждали від Інтернет-шахрайства. Крім того, шкідливе програмне забезпечення нанесло шкоду мільйонам сімей, а загальна кількість банківських шахрайств, учинених з використанням мережі Інтернет, зростає з кожним роком. Відповідно до звіту країн-членів ЄС щодо кіберзлочинності лише про понад 30 % від загальної кількості кіберзлочинів, таких як шахрайство, крадіжка особистості (як готування до вчинення шахрайства) потерпілі повідомляють правоохоронні органи.

Кіберзлочинність має потенціал, щоб зменшити довіру громадян до роздрібної он-лайн-торгівлі і банківського сектору. Втрата довіри у безпеку електронної комерції має прямий вплив на функціонування комерційних об’єктів, дистанційне банківське обслуговування, а, як наслідок, – фінансову безпеку держави.

Процес інфікування комп’ютерно-телекомунікаційних пристроїв потенційних жертв шкідливим програмним забезпеченням – ключовий компонент цифрової підпільної економіки. Європейська дослідна компанія з безпеки вважає, що близько 38 % комп’ютерних систем і пристроїв у будь-якій країні ЄС інфіковані.

Кіберзлочинці більше не концентрують увагу виключно на хакерських атаках проти користувачів, з метою отримання доступу до особистої інформації, а більше уваги приділяють постачальникам послуг. Здійснюючи відповідну атаку і злам комп’ютерних систем провайдерів, злочинці отримують доступ до великих обсягів даних, котрі вони можуть потім підпільно продати, використати для вчинення Інтернет-шахрайства.

За прогнозами Європолу, кількість кіберзлочинів у майбутньому буде зростати, оскільки Інтернет набуває все більшого значення для людини в її повсякденному житті, а комп’ютерно-телекомунікаційні пристрої стали невід’ємною частиною життєдіяльності будь-якого активного члена суспільства. При цьому зростання кількості мобільних пристроїв, як первинного засобу для доступу до ресурсів мережі Інтернет, призводитиме до збільшення кількості атак на ці пристрої злочинцями.

Ймовірно, набуде подальшого розвитку використання можливостей віртуальних серверів – хмарного сховища даних “cloud storage” та злочинних посягань у цій сфері.

Останнім часом широкого поширення і популяризації набуло використання децентралізованих віртуальних криптовалют : Bitcoin (BTC), Litecoin (LTC), Namecoin, Zerocoin, Quark, Megacoin, Namecoin, Peercoin, Worldcoin тощо [9]. Нерегульована сфера обігу віртуальних валют стала користуватися великою популярністю також серед організованих злочинних угруповань, що приймають оплату за свої послуги у віртуальній валюті, використовуючи альтернативний “темний” Інтернет – DarkNet, що функціонує на основі системи The Onion Router. Досліджені особливості криптовалют

свідчать про великі потенційні можливості їх використання під час вчинення шахрайства. Це створює реальні та потенційні загрози національній безпеці України в частині використання віртуальних грошей.

Окрім зазначених проявів Інтернет-шахрайства набули поширення такі його види: 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 hoax-програмного забезпечення, SMS-шахрайство.

Основні тенденції щодо розвитку кіберзлочинності та злочинної діяльності Інтернет-шахраїв продовжують зберігатися. Відбувається консолідація ІТ-злочинців у групи, з подальшим їх укрупненням до злочинних угруповань, злочинних організацій, що діють на постійній основі – “професійна кіберзлочинність”. Також, має місце швидке налагодження та зміцнення зв’язків між злочинними угрупованнями, що дає змогу забезпечити оперативний обмін інформацією щодо об’єктів шахрайського посягання шляхом надання у користування бот-мереж, здійснення обміну прийомами та способами вчинення злочинів, способами переведення електронних коштів у готівку тощо.

Разом із цим, оскільки вартість комп’ютерної техніки постійно зменшується, умови користування нею не вимагають спеціальних освіти чи навичок, зберігається тенденція до вчинення шахрайства злочинцями з низьким рівнем чи за відсутності технічної освіти. Це означає, що будь-хто, за наявності злого умислу, має можливість вчинити шахрайство з використанням комп’ютерно-телекомунікаційних пристроїв і комп’ютерних мереж та мереж електрозв’язку.

У зв’язку з цим, коло можливих фігурантів для діяльності правоохоронних органів є досить широким. А, з огляду на анонімність, можливість використання шахраями систем зв’язку з вільним доступом, придбання необмеженої кількості “sim-card”, створення акаунтів на різних ресурсах, сервери яких розташовані і належать різним країнам, суттєво ускладнюють практичний бік боротьби із зазначеним видом злочинів.

Крім того, наявність низки бюрократичних складових під час виконання запитів щодо розслідування фактів Інтернет-шахрайства зводить нанівець роботу правоохоронців через великі терміни проходження документів. Компанії-власники серверів Інтернет-ресурсів не забезпечують зберігання всього обсягу даних, що проходить через їх устаткування довгий період часу. А тому від швидкості, своєчасності і сумлінності виконання запиту щодо злочину повною мірою залежить рівень ефективності розслідування.

Наприклад, США надають інформацію щодо вчинення злочинів, пов’язаних з міжнародним тероризмом, вбивствами, дитячою порнографією, торгівлею людьми, маючи змогу відмовити у задоволенні запиту в разі, якщо вважатимуть, що зазначені відомості пов’язані з політикою. В усіх інших випадках – отримання даних за запитом є складним процедурним процесом і закінчується відмовою, ненаданням відповіді взагалі чи наданням вже непотрібної через великий проміжок часу застарілої інформації або відповіді про те, що інформація вже відсутня на сервері ІТ-компанії. Однією з підстав для відмови у наданні відповіді, що зустрічається найбільш часто, є суттєві відмінності між законодавством різних країн, у той час як стосовно тероризму, вбивств, дитячої порнографії, торгівлі людьми система правових норм є схожою.

У зв’язку з цим, правоохоронці можуть результативно діяти лише використовуючи власні контакти у структурах, що зобов’язані виконувати зазначені запити, повідомляючи заздалегідь про вчинений злочин, а також запит, який надійде згодом, та отримують загальну інформацію щодо існування необхідних даних, місця знаходження злочинців, самого факту злочину. Іноземні правоохоронці роблять запит у ІТ-компанію, чим унеможливлюють втрату речових доказів через часовий проміжок між надсиланням-надходженням-виконанням-наданням відповіді.

На підставі викладеного вище вважаємо, що необхідним є поглиблення практичної складової міжнародного співробітництва з питань боротьби з кіберзлочинністю взагалі та кібершахрайством зокрема в частині оперативного обміну інформацією. Разом з тим, міжнародна співпраця повинна містити угоди про видачу кібершахраїв, надання взаємної правової допомоги та консультацій із роз’ясненнями змісту норм та кваліфікуючих ознак злочинів за національним законодавством. Необхідно активізувати процеси імплементації та гармонізації міжнародного законодавства та законодавчої бази України в інформаційній сфері.

Важливим, на нашу думку, є обмін інформацією між оперативними підрозділами різних країн про багатоепізодні кібершахрайства, що вже вчинені чи готуються. Найкращим способом боротьби, найефективнішим для будь-яких видів злочинів є його недопущення, попередження, виявлення при цьому причин і умов, які сприяють його вчиненню, їх обмеження, нейтралізація, усунення, а вже потім – розкриття [10, с. 189].

Оскільки, міжнародна комп’ютерна мережа Інтернет є відкритим середовищем, що надає можливість користувачам вчиняти дії різного характеру, в тому числі й злочини, перебуваючи за межами держави, в якій знаходяться об’єкти посягання, злочинці можуть вибирати держави з правовим середовищем, у якому їх дії не підлягають кримінальній відповідальності, або санкції статей, за якими передбачено відповідальність, є м’якшими. В той час, як правоохоронні органи, здебільшого, повинні обмежуватись у діях на територією власної держави.

Наявність “країн-інформаційних сховищ”, у яких не є пріоритетним скорочення чи запобігання неправомірному використанню комп’ютерних мереж, боротьба з кіберзлочинністю не є пріоритетом або відсутні ефективні процесуальні норми, що виступає вагомим чинником, який нівелює зусилля інших держав, спрямовані на боротьбу зі злочинністю з використанням комп’ютерних мереж. Це означає, що для боротьби зі злочинами у відкритих комп’ютерних мережах, у тому числі й для протидії шахрайствам, що вчиняються з використанням комп’ютерних мереж, необхідною є активізація міжнародного співробітництва на всіх рівнях, з метою забезпечення відповідної взаємодії та координації узгоджених заходів боротьби з кіберзлочинністю у світі.

Висновки.

Проблема забезпечення інформаційної безпеки є однією з найбільш актуальних, а небезпека потенційних загроз у вигляді ІТ-злочинності, шахрайства з використанням можливостей мережі Інтернет – реальною, що вимагає системної, наступальної реакції держави, українського законодавства.

Потребує подальшого розвитку і міжнародна співпраця у питаннях забезпечення інформаційної безпеки, боротьби зі злочинами, що вчиняються з використанням можливостей мережі Інтернет взагалі та Інтернет-шахрайством зокрема. Особливо необхідним є удосконалення практичної складової цієї діяльності на функціональному рівні структурних підрозділів правоохоронних органів та інших державних і міжнародних організацій.

Перспективи подальших досліджень. На переконання автора, використання у ході правотворчої та правозастосовної практики вказаних вище висновків має сприяти не лише підвищенню ефективності правової охорони конституційних прав громадян України, а й захисту життєво важливих інтересів нашої держави шляхом запобігання та нейтралізації реальних і потенційних загроз національній, в тому числі інформаційній безпеці України, протидії шахрайству, що вчиняється з використанням можливостей мережі Інтернет. Дослідження зазначеної проблематики є актуальним і доречним у реаліях сьогодення та має перспективи на майбутнє.

Використана література

1. Про затвердження Стратегії розвитку інформаційного простору України : пояснювальна записка до проекту Указу Президента України. – Режим доступу : //www.comin.kmu.gov.ua/control /uk/publish/article?art_id=112649&cat_id=61025

2. Project 2020 Scenarios for the Future of Cybercrime. – Режим доступа : //www.europol.europa.eu/content/project-2020-scenarios-future-cybercrime

3. Шапочка С.В. Щодо шахрайства, що вчиняється з використанням можливостей мережі Інтернет : матеріали V наук.-практ. конф. [“Актуальні проблеми управління інформаційною безпекою держави”], (Київ, 20 березня 2014 р.). – К. : НАСБУ, 2014. – С. 226-230.

4. Коментар до Конституції України. – К. : Ін-т законодавства Верховної Ради України, 1996. – 376 с.

5. Про основи національної безпеки України : Закон України від 19.06.03 р. № 964-IV. – Режим доступу : //www.zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=964-15

6. Про засади інформаційної безпеки України : проект Закону України від 28.05.14 р. № 4949. – Режим доступу : //www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51123

7. Шапочка С. В. До питання запобігання окремим видам шахрайства, яке вчиняється з використанням можливостей мережі інтернет // Боротьба з організованою злочинністю і корупцією (теорія і практика) : наук.-практ. журнал. – К. : МНДЦ при РНБО України. – 2014. – № 1 (32). – С. 213-225.

8. EU Serious and Organised Crime Threat Assessment (SOCTA 2013). – Режим доступу : //www.europol.europa.eu/content/eu-serious-and-organised-crime-threat-assessment-socta

9. Shapochka S. Preventing Fraud Using Computer Networks / Serhiy Vladimirovich Shapochka // Internal Security. – 2013. – № 2. – P. 63-75.

10. Шапочка С.В. Інформаційна безпека та кібершахрайство : матеріали міжнар. наук.-практ. конф. [“Внутрішні та зовнішні загрози національній безпеці держави”], (Київ, 2 квітня 2013 р.); НАВС. – К. : ТОВ “Три К”, 2013. – С. 188-191.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~