

для запобігання кібершахрайству на загальнодержавному рівні [3].

Досягнення позитивних результатів у сфері протидії кіберзлочинності є абсолютно неможливим без відповідної профілактичної роботи серед населення та інформування суспільства про нові види кіберзагроз. При цьому вказані функції повинні реалізовуватися не тільки правоохоронними органами, а й громадськими організаціями масштабу Transparency International, Greenpeace, Amnesty International тощо.

Наостанок відмітимо, що кіберзлочинність – проблема ХХІ століття, яка невпинно зростає та поглинає все більше фінансових ресурсів. Незважаючи на заходи, що вживаються окремими особами, як фізичними, так і юридичними, державою, це явище продовжує існувати та розширює масштаби своєї діяльності, збільшуючи прибутки правопорушників. Тому на сьогодні особливо важливим питанням є усвідомлення глибини даної проблеми, прогнозування подальших напрямів її розвитку та дія на випередження.

Список використаних джерел:

1. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і безпека*. 2015. № 2. С. 107-113.
2. До питання протидії кіберзлочинності в Україні. URL: http://www.akademia.gp.gov.ua/userfiles/file/Academia2016/Akt_schema/123441234524.pdf. (дата звернення: 28.10.2017).
3. Протидія кіберзлочинності. URL: <https://nabu.ua/ua/protidiya-kiberzlochinnosti.html> (дата звернення: 28.10.2017).

Одержано 30.10.2017

УДК 342.98

Віктор Миколайович ПЛЕТЕНЕЦЬ,

кандидат юридичних наук, доцент кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ

Катерина Вікторівна КАРАБУТА,

курсант КМ-443 факультету підготовки фахівців для підрозділів кримінальної поліції Дніпропетровського державного університету внутрішніх справ

**ШАХРАЙСТВО У КІБЕРПРОСТОРІ:
ОКРЕМІ АСПЕКТИ ПРОТИДІЇ**

На сучасному етапі розвитку інформаційних технологій шахрайство посідає особливе місце. Це пов'язано з тим, що з

кожним роком інформаційні технології все більше проникають в наше повсякденне життя. Останнім кроком буде перехід на електронні гроші. Це ми можемо побачити, з сучасної політики передових країн світу.

Однак дане положення провокує появу інтелектуальних правопорушників «хакерів». Дана ситуація виходить з того, що вислідити правопорушників дуже складно, бо вони працюють дистанційно.

Згідно тлумачення видатного криміналіста Р. С. Белкіна комп'ютерна інформація – інформація на машинному носії, в ЕОМ, системі або мережі ЕОМ – також може бути криміналістично значимою, при розслідуванні і комп'ютерних злочинів, і посягань, де ЕОМ виступає як об'єкт (крадіжка комп'ютера, незаконне використання машинного часу) або засіб скоєння злочину (використання ЕОМ для накопичення інформації, підробки документів і ін.). Програмні продукти теж можуть використовуватися і в якості об'єкту злочину (незаконне копіювання, спричинення збитку застосуванням руйнівних програм - вірусів), і в якості інструменту скоєння злочину (несанкціоноване проникнення в комп'ютерну систему, спотворення і підробки інформації) [1, с. 945].

Необхідно відзначити, що підвищення ефективності попереднього розслідування у кримінальних справах про кіберзлочинність неможливе без визначення чинників, які здатні робити помітний негативний вплив на якість процедури розслідування кримінального провадження. По-перше, це стосується недосконалості норм вітчизняного кримінального права, що передбачають відповідальність за кіберзлочинності. Ця проблема зумовлює неминуче виникнення труднощів в правильній кваліфікації даного різновиду шахрайства. По-друге, відсутнє повною мірою адекватне криміногенній ситуації, що склалася, криміналістичне забезпечення процедури розслідування цієї категорії кримінальних справ (як на рівні криміналістичної методики, так і на рівнях криміналістичної тактики і техніки). По-третє, міра професійної кваліфікації суб'єктів розслідування не завжди повною мірою відповідає сучасним вимогам, що, безумовно, не може не позначитися на якості. По-четверте, негативне дію чинить недостатня координація спільних зусиль правоохоронних органів з державними і недержавними структурами, що спеціалізуються на забезпеченні безпеки у сфері телекомунікації і комп'ютерній інформації [2, с. 213].

Інтернет шахраї є вигадливими не тільки у способах вчинення, й маскування свої дій. Так, 30 вересня 2017 року працівниками кіберполіції було затримано інтернет-шахрая, який ретельно конспірував свою злочинну діяльність: розміщував оголошення на сайті, знаходячись у громадських місцях, де є вільний доступ до мережі Інтернет, аби ускладнити пошук його місцезнаходження. У знайомого він придбав банківські картки, на які отримував гроші від потерпілих. А знімав гроші з банкоматів у медичній масці, аби камери терміналів не зафіксували його обличчя [3]. І подібні випадки є непоодинокими.

Однак, як відзначає Шاپочка С. В. [4, с. 227] з'явилася 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, 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. На даний час, 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) [4, с. 227]. В таких країнах, як Росія, Тайланд та Китай Bitcoin фактично поза законом. Взяти наприклад Національний банк Китайської Народної Республіки, який наклав заборону на кредитно-фінансові установи проводити будь-які операції із використанням крипто валюти Bitcoin.

В Україні, жорстка реакція з боку влади, щодо здійснення банківських операцій з використанням криптовалюти відсутня. Ми можемо погодитися з думкою Шاپочки С. В., що це пов'язано з недооцінкою рівня можливого негативного впливу криптовалюти на економіку, стан злочинності та функціонування кредитно-банківської системи держави.

З огляду на вище викладене, ми можемо дійти висновку, що даний напрям наукового дослідження дуже актуальний в наш час, і відкритий для подальшого вивчення та вдосконалення.

Список використаних джерел:

1. Криминалистика: учебник для вузов / под ред. Р. С. Белкина. – М. : НОРМА, 2001. – С. 990.
2. Антонов И. О., Шилимов А. Н. Актуальные проблемы расследования мошенничества с использованием компьютерной информации. *Ученые записки Казанского университета*. 2015. Том 157, Кн. 6. С. 212–220.
3. Працівники кіберполіції затримали інтернет-шахрая, який переховувався від органів слідства. URL: <https://cyberpolice.gov.ua/news/praczivnyky-kiberpolicziyi-zatymaly-internet-shahraya-yakuj-perexovuvavsya-vid-organiv-slidstva-637/> (дата звернення: 25.10.2017).
4. Шапочка С. В. Щодо шахрайства, що вчиняється з використанням можливостей мережі інтернет // Збірник науково-практичної конференції «Актуальні проблеми управління інформаційною безпекою держави» (20.03.2014 р., м. Київ,) у 2-х частинах. Ч. 1. С. 226-230.

Одержано 25.10.2017

УДК 343.9 : [343.431 : 061.2] (477)

Максим Юрійович ПОГУЦА,

курсант факультету № 2 Харківського національного університету внутрішніх справ

ЩОДО СУБ'ЄКТІВ ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ В УКРАЇНІ

Свобода людини є однією з головних цінностей сучасного цивілізованого суспільства, а забезпечення недоторканності свободи особи – одна з головних функцій держави. Відповідно до норм міжнародного законодавства, кожна країна, що поважає права людини, повинна гарантувати їх виконання, зокрема запобігання насильству, покарання злочинців, забезпечення компетентного розслідування актів насильства і надання компенсації людині, що постраждала. Однак, за останні роки в умовах глобалізації суспільства набула особливої актуальності проблема торгівлі людьми. Вона охопила всі регіони та країни і стала глобальною.

На сьогоднішній день протидію торгівлі людьми простежуємо на всіх рівнях: глобальному (ООН, Інтерпол), регіональному (ОБСЄ, Рада Європи, ЄС) та державному (державні механізми протидії) [1, с.83].

Протидія торгівлі людьми є одним із пріоритетних напрямів діяльності у сфері захисту прав людини органів законодавчої і виконавчої влади нашої країни. Адже Україна в міжнародній системі ідентифікована як країна – постачальниця