

УДК 343.7

Олексій Георгійович БАРБАШОВ,

курсант 3 курсу групи Ф4-301 факультету № 4 (кіберполіції)

Харківського національного університету внутрішніх справ;

ORCID: <https://orcid.org/0000-0002-8790-0997>;

Денис Олександрович ГРИЩЕНКО,

старший викладач кафедри кібербезпеки факультету № 4 (кіберполіції)

Харківського національного університету внутрішніх справ

ЩОДО ПИТАНЬ НЕДОСКОНАЛОСТІ ЗАКОНОДАВСТВА У ЗЛОЧИНАХ ВЧИНЕНИХ ШЛЯХОМ НЕЗАКОННИХ ОПЕРАЦІЙ З ВИКОРИСТАННЯМ ЕЛЕКТРОННО- ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

Однією з основ розвитку та існування правової, демократичної держави, безумовно, є вдосконалення чинного законодавства, запровадження нових ідеологій та стратегій розвитку сучасної країни. Застосовуючи норми права на практиці, ми часто відчуваємо наявність певних недоліків. Хоча не лише наявність зазначених недоліків створює передумови для удосконалення законодавства, а й сам розвиток суспільних відносин в цілому. Інакше кажучи, на певному етапі становлення та розвитку нашого суспільства, усяка норма права може виявитися не здатною для врегулювання сучасних суспільних відносин. Що стосується практичної складової засудження винних до кримінальної відповідальності за ознаками складу злочину передбаченого ч. 3 ст. 190 Кримінального Кодексу (далі – КК) України, а саме за шахрайство вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки, то дана нормативно-правова норма показала ряд суттєвих прогалин. Виходячи з вищевказаного, обумовлюється актуальність даної тематики.

Аналіз кримінального законодавства та практики його застосування свідчить, що для забезпечення ефективної боротьби з шахрайством, учиненим із використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК України), та подібними діями необхідне подальше вдосконалення норм КК України, які мають відображати особливості комп'ютерних шахрайств сучасного періоду, закріплювати визнану у світі термінологію та детальніше визначати суспільну небезпеку таких злочинів.

Оскільки у практичній діяльності виникають деякі розбіжності при кваліфікації скоєного діяння особою за ч. 3 ст. 190 КК України. Так, вироком Залізничного районного суду м. Львова від 17.10.2017 ОСОБА_1, діючи за попередньою змовою з невстановленою досудовим розслідуванням особою на ім'я ОСОБА_4, матеріали щодо якого виділене в окреме провадження, умисно з корисливих мотивів для власного збагачення, шляхом обману, для вчинення шахрайських

дій, взяли в оренду приміщення офісу, що за адресою: АДРЕСА_2, де в подальшому у 2017 році точної дати в ході проведення досудового розслідування не встановлено, перебуваючи за адресою: АДРЕСА_2 створили сайт під назвою ІНФОРМАЦІЯ_2, на якому спеціально розмістили оголошення про продаж техніки марки «Apple», якої в наявності не мали. В подальшому ОСОБА_1, з невстановленою досудовим розслідування особою на ім'я ОСОБА_4, перебуваючи за вище вказаною адресою, в ході переписки через форму зворотнього зв'язку сайту ІНФОРМАЦІЯ_2, з потерпілим ОСОБА_5, запевнили останнього в правдивості оголошення, та попередньо домовившись про купівлю мобільного телефону марки «Apple Iphone 7 plus 256 Gb», 18.05.2017 ОСОБА_5, в якості передоплати переказав грошові кошти в сумі 18150 гривень на наданий попередньо ОСОБА_1, банківський рахунок НОМЕР_1 ПАТ КБ «Приватбанк», який належить ОСОБА_4, які в подальшому 18.05.2017 ОСОБА_1, зняв з банкомату ПАТ КБ «Приватбанк», що за адресою: м. Львів вул. Виговського, 29. Після цього ОСОБА_1, з невстановленою досудовим розслідуванням особою на ім'я ОСОБА_4, на контакт із ОСОБА_5, не виходили, а гроші витратили на власні потреби [1].

Часом суди не вбачають в даних діяннях складу злочину передбаченого ч. 3 ст. 190 та перекваліфікують діяння на ч. 1, ч. 2 ст. 190 КК України, аргументуючи це тим, що електронно - обчислювальна техніка – це комплекс технічних засобів, призначених для автоматичної обробки інформації в процесі вирішення обчислювальних та інформаційних завдань. Операція з використанням електронно-обчислювальної техніки має бути незаконною, тобто такою, що не відповідає вимогам законодавства. Зважаючи, що підсудним таких дій учинено не було, оскільки перерахування коштів на рахунок через банківську установу або банківським переказом не є незаконною операцією. Так, вироком Нікопольського міськрайонного суду Дніпропетровської області від 24.03.2016 р. ОСОБА_1 в лютому 2015 року знаходилась за адресою свого місця проживання АДРЕСА_1, де з використанням електронно-обчислювальної техніки, а саме стаціонарного комп'ютера підключеного до глобальної мережі Інтернет, в неї виник умисел на заволодіння чужим майном шляхом обману, а саме зареєструватися на Інтернет – сайті під приводом продажу одягу та взуття, вказувати вигадані дані щодо товару, а також додавати до оголошень фотознімки товарів, яких не мала насправді в наявності, з метою надання ознак правдивості своїм злочинним намірам, шляхом внесення завідомо неправдивої інформації за допомогою електронно-обчислювальної техніки, направленої на досягнення своєї злочинної мети [1]. Звернемо увагу, що у цих випадках суди не враховують самого механізму вчинення злочинних дій, тобто мова йде саме про реєстрацію на сайті, виставлення оголошень, які є вигаданими, а далі вже отримання передоплати. Дані операції ми не можемо вважати незаконними операціями з

використанням електронно-обчислювальної техніки. Особа правомірно використовує терени глобальної мережі Інтернет. А для кваліфікації діяння за ч. 3 ст. 190 КК України, має бути саме «незаконні» дії, тобто такі, які не відповідають чинному законодавству. Таким чином, можемо сказати, що дана ситуація свідчить про необхідність виключення з ч. 3 ст. 190 КК України вказівки на «незаконні операції», щоб ч. 3 ст. 190 КК України мала таку конструкцію: «Шахрайство, учинене з використанням електронно-обчислювальної техніки».

Ще один цікавий аспект, який стосується удосконалення законодавства стосовно ч. 3 ст. 190 КК України висловлено в думці Ю. Шуляка. Він зазначає, що злочинці для шахрайських намірів здебільшого застосовують спеціальні шкідливі програми чи різного роду технічні засоби, про що також може свідчити досвід Зведення законів США, КК Голландії, КК Данії або КК ФРН. Автор пропонує, запровадити до ч. 3 ст. 190 КК України вказівки на конструкцію « шляхом використання шкідливих програмних чи технічних засобів». Це на його думку слугуватиме додатковим засобом боротьби з «кіберзлочинами» [2, с. 15].

Продовжуючи розвивати дану думку, слід зазначити, що зараз шахрайство вчиняється за допомогою різного роду пристроїв, форм і способів. Ми говоримо саме про мобільну телефонію та згадану вище мережу Інтернет. На сучасному етапі не криміналізоване телефонне шахрайство, яке на зараз дуже часто проявляється у повсякденному житті. Так наприклад, несанкціоноване списання коштів із рахунку чужого абонента; незаконне прохання подзвонити за певним номером телефону без попередження про зняття коштів під час такого телефонування; незаконні махінації із засобами поповнення рахунків абонентів мобільної телефонії тощо. Отже, наведені вище твердження, дають підставу стверджувати, що термін «електронно-обчислювальна техніка» є застарілим. Необхідно даний вираз замінити більш модерним, наприклад, Д. Азаров запропонував вживати – «комп'ютерна система» і «телекомунікаційна мережа» [3, с. 172].

Отже, розглянувши та проаналізувавши національні законодавчі положення та суддівську практику, зазначене дозволяє зробити висновок, що до проблем за напрямом кібербезпеки в Україні правоохоронні органи ставляться зухвало. Потрібно значно удосконалювати наше законодавство у сфері інформаційних технологій, бо дані суспільні відносини все частіше стають предметом злочинних діянь. Задля того, щоб удосконалити законодавство відносно шахрайства, вчиненого шляхом незаконних операцій із використанням електронно-обчислювальної техніки, замість цих трьох слів «електронно-обчислювальна техніка» варто впроваджувати такі терміни, як «комп'ютерна система» й «телекомунікаційна мережа». Також доцільно буде доповнити КК України новими складами злочинів: комп'ютерне та телекомунікаційне шахрайство, а також

крадіжка, учинена шляхом незаконних операцій із використанням комп'ютерних систем та телекомунікаційних мереж.

Список бібліографічних посилань

1. Єдиний державний реєстр судових рішень України URL: <http://www.reyestr.court.gov.ua> (дата звернення: 29.10.2018)

2. Шуляк Ю. Л. Кримінальна відповідальність за шахрайство : порівняльно-правове дослідження : автореф. дис. ... канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право»; Нац. академія внутр. справ. К., 2011. 20 с.

3. Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) : монографія. К. : Атіка, 2007. 304 с.

Одержано 29.10.2018

УДК 65.012.8+004

Єлизавета Георгіївна БЄЛЯЄВА,

*курсант 3 курсу групи Ф4-302 факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;*

Олексій Михайлович РВАЧОВ,

*старший викладач кафедри кібербезпеки факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: <https://orcid.org/0000-0002-3500-9393>*

МЕРЕЖА ІНТЕРНЕТ ЯК ДЖЕРЕЛО ПІДВИЩЕНОЇ НЕБЕЗПЕКИ ДЛЯ ДІТЕЙ

З моменту своєї появи мережа Інтернет стала глобальною – досягла неймовірних масштабів.

Інтернет використовується як для поширення знання по всьому світу, так і надає нескінченні можливості для марної трати часу і розвитку нездорових звичок, наприклад, таких як одержимість соціальними мережами.

За даними проведеного дослідження в II кварталі 2018 року компанією Factum Group Ukraine – 65% громадян України є регулярними користувачами мережі Інтернет.

Зараз Інтернет є найбільш популярним серед дітей, підлітків, молоді, і попри корисність використання цього ресурсу також існує велика кількість загроз для його користувачів.

Взагалі це доволі актуальна проблема, вивченням якої займались такі вчені як В. Плешаков (вивчав небезпеку для дітей та підлітків в Інтернеті та негативні наслідки кіберсоціалізації), С. Лівінгстон, Л. Хеддон (вивчали можливості та ризики в Інтернеті), Є. Золотова, Т. Нестік, Є. Розсказова, Г. Солдатов (вивчали ризики, пов'язані з небезпечним медіазмістом) та багато інших науковців, що в котрий раз підкреслює особливу важливість вирішення цього питання.

Метою даного дослідження було проаналізувати існуючі загрози та небезпеки в мережі Інтернет, особливо ті, з якими може зіткнутися