***Горелік Д.С.**, здобувач вищої освіти факультету підготовки фахівців для підрозділів кримінальної поліції Дніпропетровського державного університету внутрішніх справ*

Науковий керівник:
***Телійчук В. Г.**, доцент кафедри оперативно-розшукової діяльності факультету підготовки фахівців для підрозділів кримінальної поліції Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, старший науковий співробітник, доцент*

ЩОДО ВИЗНАЧЕННЯ СПОСОБУ ВЧИНЕННЯ ШАХРАЙСТВА В МЕРЕЖІ ІНТЕРНЕТ ЯК ЕЛЕМЕНТУ ОПЕРАТИВНО-РОЗШУКОВОЇ ХАРАКТЕРИСТИКИ

Використання елементів оперативно-розшукової характеристики сприяє здійсненню оперативно-розшукових заходів у межах загальних форм оперативно-розшукової діяльності Національної поліції України, а саме: оперативної розробки за оперативно-розшуковими справами; організації негласної роботи; ведення профілактичних, криміналістичних та оперативних обліків; оперативної профілактики тощо. Серед основних елементів оперативно-розшукової характеристики злочину домінуючу позицію займає *спосіб* його вчинення. Він охоплює систему взаємопов'язаних дій суб'єкта, що вчиняються з певною послідовністю, із застосуванням різних знарядь і засобів та спрямовані на досягнення мети злочину [1].

З початку XXI століття Інтернет остаточно закріпив за собою статус невід'ємної частини життєдіяльності людства. Приблизно у цей час починає з'являтися велика кількість соціальних мереж, торгових майданчиків та інших «організацій», що надають послуги в різних сферах життєдіяльності. Окреслені нововведення швидко набирають популярність і в першу чергу це пов'язано з тим, що Інтернет пропонує значно нижчу ціну, аніж в звичного роду торгових місцях, більшу кількість послуг та асортимент, в тому числі рідкісні та заборонені для вільного продажу товари, і все це для зручності здебільшого сконцентровано на одному Інтернет ресурсі. В той же час, Інтернет надає можливість розрахунків за отримані послуги та товари електронними платіжками. На жаль, не завжди ці технології використовуються на благо. У наші дні існує величезна кількість прийомів і хитрощів, вигаданих для того, щоб шляхом обману, тобто шахрайства, заволодіти майном інших осіб. Зокрема, враховуючи, що Інтернет є практично непідконтрольною правоохоронним органам сферою життєдіяльності людства, він притягує до себе увагу злочинного середовища, який маніпулюючи людськими почуттями (починаючи від допомоги,

благодійності ближньому, армії, державі, до банального почуття – жадібності, бажання максимально заощадити, отримати безкоштовні подарунки тощо) намагається заволодіти чужою власністю, коштами та іншими матеріальними та нематеріальними об'єктами спираючись на можливості Інтернету, при цьому уникнути відповідальності, оскільки спілкування та домовленості відбуваються у віртуальному просторі. Принагідно зазначимо, що результати аналізу емпіричного матеріалу свідчать про те, що сьогодні навіть приблизну кількість способів підготовки та вчинення шахрайств за допомогою Інтернету не можливо чітко визначити, оскільки кожного дня злочинці вигадують нові. З цього приводу слід навести думку американського Девіда Пога, який виділив найбільш розповсюджені види шахрайства в Інтернеті. Зокрема, вказаний дослідник зазначає, що більшість користувачів знають способи «порівняно чесного відбирання грошей», й тим не менше мільйони людей щорічно страждає від вказаного виду злочинності, зокрема щорічно інтернетшахраї отримують прибуток в розмірі 13 млрд. доларів. Разом з цим, складаючи свій рейтинг найпопулярніших видів мережевого шахрайства, Д. Пог дійшов простого висновку про те, що найдієвіші види шахрайства будуються по одному і тому ж принципу – починаються з дуже цікавої пропозиції придбавання чогось або надання послуг (найчастіше – отримати безкоштовно те, що стоїть значних грошей), отримання на перед за це грошових коштів та зникання з поля зору потерпілої особи. Отже, до популярних видів шахрайства Д. Пог відніс такі:

1) нігерійські листи щастя (так звані повідомлення про те, що десь далеко помер родич, та залишив спадок потерпілому, та необхідно переказати кошти для вирішення всіх формальних питань);

2) онлайн-продаж (шахрай, прикидаючись покупцем, пише продавцеві, що готовий надіслати поштою чек, який покриває і вартість покупки і суму, яка необхідна для пересилки; продавець і справді отримує чек, оплачує відправку товару, а потім з'ясовується, що чек був фальшивий, продавець позбавляється як товару, так і грошей);

3) ідеальна дівчина (розповсюджений вид шахрайства на сайтах знайомств – «ідеальний» партнер бажає приїхати в гості до майбутньої потерпілої особи, однак не має коштів та позичає їх в нього, після чого пропадає зі зв'язку);

4) фішинг (шахраї присилають потенційній жертві лист з банку або платіжної системи, наприклад, PayPal, у листі написано, що з рахунком жертви є проблеми для вирішення яких необхідно перейти за посиланням з листа; найчастіше ця вимога супроводжується загрозою блокування банківського рахунку, після чого отримуючи персональні дані, всі кошти з банківських сайтів зникають) [2];

5) підроблена банківська карта (популярний в США і Канаді вид мережевого шахрайства: жертва отримує повідомлення з електронної пошти щодо пропозиції отримати кредитну карту з великим лімітом і надзвичайно

низькою процентною ставкою; все, що потрібно від жертви, – це внести невелику абонплату);

6) допомога друзям, знайомим чи іншим особам (найпопулярніша схема; може застосовуватися з використанням самих різних методів комунікації – електронної пошти, соцмереж, месенджерів; потерпіла особа отримує повідомлення від одного або навіть родича, в якому міститься опис якоїсь неприємності, яка трапилася з ним / нею; у будь-якому випадку терміново потрібні гроші, які необхідно вислати на певний рахунок);

7) робота на дому (шахраї пропонують жертвам високооплачувану роботу на дому. Однак, «здобувачу» потрібно спочатку щось купити – клей для марок, якесь обладнання, або ж сплатити хостинг для веб-сайту);

8) підроблений вірус (потерпіла особа відвідує якийсь сайт в Інтернеті, раптово вискакує віконце з попередженням «ваш комп'ютер заражений!», далі жертві пропонують пройти за посиланням для «сканування» комп'ютера і очищення від вірусів за сплату певної суми грошей) [3].

Згідно з даними Української міжбанківської асоціації членів платіжних систем ЕМА, у 2016 році кожен сотий власник платіжної картки в Україні став жертвою шахраїв. Внаслідок вішингу (телефонне шахрайство з виманюванням реквізитів банківських карток і переказом коштів на карту злодіїв) з рахунків українців було вкрадено 275,45 млн. грн., а внаслідок фішингу (виманювання конфіденційних даних – паролів, номерів банківських карток, PIN-кодів тощо) – 63,68 млн. грн. Загалом – 339,13 млн. грн. Для порівняння, у 2015 році шахраї викрали з рахунків українців 84,36 млн. грн. Як зазначають аналітики, рекордно зросла кількість фішингових сайтів (в 4,5 рази – з 38 до 174), а, в цілому, від фішингу та інших видів шахрайства в Інтернеті постраждало 0,59% клієнтів-власників банківських карт. Жертвами телефонного шахрайства стали 0,63% власників карт. За даними ЕМА, з 1 серпня по 26 вересня 2017 року кількість шахрайських операцій за картами досягла 1 928. Сума, яку зловмисникам вдалося вкрасти з рахунків менш ніж за два місяці, оцінюється приблизно в 238 млн. грн. І це при тому, що за весь 2016 рік злочинці вкрали з карток українців 340 млн. грн. У зв'язку з цим в системі НПУкраїни створено спеціальні підрозділи щодо протидії кіберзлочинам, що напрацьовують практику з цього напряму організаційної, слідчої, оперативно-розшукової та іншої діяльності.

Невипадково такі види злочинів ще у 1992 році були внесені ООН до списку 14 видів транснаціональних організованих злочинів, поставивши їх в один ряд із «незаконним відмиванням» грошей, терористичною діяльністю, організованим наркобізнесом, крадіжками витворів мистецтв, інтелектуальної власності, незаконною торгівлею зброєю, захопленням повітряних суден, морським піратством, заволодінням наземного транспорту, шахрайством, екологічними злочинами, торгівлею людьми і людськими органами.

Крім цього, в Європі, ще у 2001 році було підписано Конвенцію Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185, яка в нашій країні більш відома під назвою «Конвенція про кіберзлочинність», що була ратифікована Україною у 2005 році. Якщо в соціальній сфері використання новітніх технологій, особливо мережі Інтернет, невпинно зростає і використовується населенням різного, у т.ч. й дошкільного віку, то в діяльності правоохоронних органів і, зокрема Національної поліції, у зв'язку з обмеженням фінансування, їх застосування та вирішення питань ліцензування, здійснюється досить повільно. В той же час автори методичних рекомендацій, вивчивши наявну систему новітніх інформаційних технологій і, зокрема мережі Інтернет, прийшли до висновку, що в ній є невикористані можливості, у тому числі технічні, які нададуть допомогу працівникам підрозділів кримінальної поліції (карного розшуку) та досудового розслідування НП України, без використання додаткових матеріальних витрат удосконалити діяльність, направлену на запобігання й протидію злочинності у сфері сучасних інформаційних технологій та мережі Інтернет, значно підвищити ефективність такої діяльності у протидії кіберзлочинності. Вказане дозволить продовжити дослідження не тільки з технічних, але й правових питань, по розширенню можливостей, напрацюванню пропозицій та рекомендацій щодо удосконалення кримінального процесуального і кримінального законодавства України. Нагальність вказаних проблем сьогодні досить гостро відчувають як вчені, так і оперативні працівники, слідчі, процесуальні керівники та представники інших правоохоронних органів [4].

Аналіз практичної діяльності дозволяє стверджувати, що всі перелічені види шахрайства через мережу Інтернет, також є доволі розповсюдженими в Україні, окрім шахрайства пов'язаного із наданням грошей для допомоги, які, як правило, вчиняються через телефонну мережу. Виявлення і розслідування більшості видів високотехнологічних шахрайств ускладнено тим, що якісні характеристики мережі Інтернет дають можливість злочинним елементам використовувати сервери, що знаходяться поза юрисдикцією України, для приховування фактів своєї злочинної діяльності. Від способу вчинення конкретного злочину залежать хід розслідування, ступінь організованості взаємодії, алгоритм та черговість проведення слідчих (розшукових) дій, у т.ч. негласних [3, с. 9]. Таким чином, спосіб вчинення шахрайства в мережі Інтернет займає домінуючу позицію серед основних елементів оперативно-розшукової характеристики. Він охоплює систему взаємопов'язаних дій суб'єкта, що вчиняються з певною послідовністю, із застосуванням різних засобів та спрямовані на досягнення мети злочину.

Отже, аналізуючи вітчизняну правоохоронну практику, можна дійти висновку, що до сучасного стану кримінальної обстановки притаманні всі із перелічених видів шахрайства через мережу Інтернет, однак найбільш розповсюдженими в Україні є такі:

1) організація добровольчих, благодійних внесків, зокрема для хворих дітей та бійців АТО;

2) використання торгівельних електронних площадок, зокрема «HIFI FORUM», «OLX» тощо;

3) розповсюдження по акції або за заниженою ціною будь-яких товарів або речей;

4) продаж або пропозиція доставки за низькою ціною автомобілів на іноземній реєстрації, або під заказ у «сірих» автодилерів;

5) розповсюдження фішингових програм та вірусного програмного забезпечення;

6) продаж товарів у групах, які функціонують у соціальних мережах.

_____

1.Федосова О,В. Оперативно-розшукова характеристика корисливо-насильницьких злочинів, що вчиняються неповнолітніми. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/2756/operativno_rozshukova_harakteristika_kor.pdf?sequence=2&isAllowed=y

2. Самойлов С. В. «Фішинг» як спосіб вчинення Інтернет-шахрайств / С. В. Самойлов // Актуальні питання сучасних державотворчих та правотворчих процесів: матеріали міжнар. наук.-практ. конф. (м. Запоріжжя, 24 лютого 2011 р.). Запоріжжя: у 3-х частинах. Запорізька міська громадська організація «Істина», 2011. Ч .3 . С . 102-104.

3.Кидалы-онлайн. Названы самые распространенные способы интернет-мошенничества // Новое время: сайт. URL: http://nv.ua/techno/ gadgets/kidaly-onlajn-nazvany-samye-rasprostranennye-sposoby internet moshennichestva-75741.html (дата звернення: 22.10.2017).

4. Алгоритм дій працівників підрозділів карного розшуку під час розкриття шахрайств, вчинених через мережу Інтернет: методичні рекомендації / В.Г. Телійчук, Д.Б. Санакоєв, Я.М. Ковч, О.В. Козорог. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. 55 с.