ЛЕВКІВСЬКА ЯРОСЛАВА ВІКТОРІВНА

Національний університет «Одеська юридична академія», аспірантка кафедри кримінального процесу, детективної та оперативно-розшукової діяльності

ВПЛИВ ВОЄННОГО СТАНУ НА ТРАНСФОРМУВАННЯ ТА РОЗВИТОК ІНТЕРНЕТ-ШАХРАЙСТВА В УКРАЇНІ

24 лютого 2022 року у зв'язку з нападом Російської Федерації на суверенну територію України було введено воєнний стан, що глобальним чином вплинув на життя кожного. Зараз одними із найголовніших пріоритетів для кожного громадянина стали власне життя та безпека своїх близьких. Це стало одним із факторів активізації інтернет-шахраїв, які використовуючи вразливий стан населення України та ажіотаж навколо військового протистояння, маніпулюючи вкрай болючими темами, віднайшли в цьому додаткові умови для здійснення шахрайства в мережі Інтернет.

Досліджуючи особливості інтернет-шахрайства як різновиду шахрайства взагалі, необхідно встановити дефініцію останнього. Так, згідно КК України шахрайство – це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою (ст. 190 КК України). У науковій літературі інколи як синоніми інтернет-шахрайства використовуються інші назви, наприклад, «комп'ютерне шахрайство», «кібершахрайство», «мережеве шахрайство», «hi-tech шахрайство» тощо [1]. Варто погодитися із думкою науковців, які вказують, що цей вид шахрайства «є результатом еволюції традиційного шахрайства, оскільки деякі його види зустрічаються в Інтернеті без будь-яких серйозних змін в методиці реалізації злочинного замислу; з іншого боку – це якісно нова група кримінальних правопорушень, оскільки при схожості методів реалізації, конкретні способи мають істотні відмінності» [2, с. 41].

У воєнний час активно розвиваються такі схеми шахрайства як пропозиції з оренди неіснуючого чи вже зайнятого житла для вимушених переселенців; фейкові пасажирські перевезення; недійсні талони на паливо; продаж неіснуючих товарів (тих, що є найбільш затребуваними у цей час – військова амуніція, технічні пристрої, рідкісні ліки тощо); надання недостовірної інформації про зниклих громадян чи визволення останніх з полону.

Основою більшості таких схем є фейкова або ж неправдива інформація, за допомогою якої здійснюється маніпуляція свідомістю громадян, формування у них панічних настроїв, агресії, гніву, розпачу, а відтак різких необдуманих вчинків, у тому числі й щодо розпорядження своїми персональними даними, конфіденційною інформацією тощо.

Так, інтернет-шахраї використовують сотні фейкових благодійних сайтів, щоб обдурити людей, які хочуть пожертвувати гроші на допомогу Україні. Потерпілий потрапляє на фейковий сайт, що майже не відрізняється від сайту справжньої благодійної організації, де нібито можна допомогти ЗСУ фінансово. Шахрайство здійснювалося або ж заволодінням коштів, що не йшли за цільовим призначенням вказаним на сайті або ж заволодінням персональних даних та даних платіжних карток. Також злочинці вдаються до фішингу, що є найбільш поширений методом крадіжки реквізитів платіжних карт, що полягає у створенні шахраями сайту, який буде користуватися довірою у користувача, наприклад – сайт, схожий на сайт банку, через який і крадуться реквізити платіжних карт. Фішинг як різновид шахрайства може бути реалізований за допомогою сервісів обміну повідомленнями, сайтів, засобів стільникового або телефонного зв'язку, причому як окремо, так і в комбінації [3].

Однією із найпоширеніших схем фішингу під час воєнного стану є пропозиція отримання грошової допомоги, замаскована під грошову допомогу від держави Україна, Організації Об'єднаних Націй, благодійних фондів тощо для окремих категорій осіб. Головною відмінністю таких фішингових атак є вимога авторизації за схемою, яка передбачає певний реєстраційний механізм з введенням своїх особистих даних, номеру телефону, інформації про банківські рахунки, де завершення процедури підтверджується прийняттям дзвінка або текстового повідомлення, після чого з картки отримувача списуються кошти.

Варто зазначити, що фахівці Національного Банку України вказують [4] на поширеність наразі схем інтернет-шахрайства у вигляді пропозиції оренди неіснуючого житла переселенцям. Так, шахраї публікують фейкові оголошення про готовність здати в оренду житло у безпечних регіонах. Особливістю таких пропозицій є обов'язкова передплата. Звісно, після отримання коштів шахрай зникає, вийти з ним на зв'язок не вдається, а житла такого переважно не існує, або воно належить особі, яка не мала наміру його здавати в оренду. Підкреслимо, що така схема шахрайства існувала і в умовах довоєнного стану, але, враховуючи зростання попиту на оренду житла в умовах збільшення кількості вимушених переселенців, вона набула гострого значення.

Отже, Інтернет-шахрайство, як спосіб незаконного заволодіння майном іншої особи, існувало як тільки почали розвиватися різні інтернет-ресурси, особливо інформаційні. В умовах неможливості перевірити інформацію та вразливості емоційного стану, злочинці реагують на ці зміни, адаптуються до умов суспільного життя, використовуючи у своїх схемах актуальні питання та обставини. Тож за досить короткий час виникла ціла низка нових шахрайських схем, побудованих на маніпуляції із найболючішими питаннями, пов'язаними з військовим протистоянням.

Список використаних джерел:

1. Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження. Г. М. Чернишов URL : http://www.pjv.nuoua.od.ua/v3_2018/2018_3
2. Криміналістична профілактика економічних злочинів: Науково-практичний посібник / Кол. авт.: С. В. Веліканов, А. Ф. Волобуєв, В. А. Журавель та ін. Х. : «Харків юридичний», 2006. 236 с.
3. Секреты хакеров. Безопасность сетей – готовые решения, 3-е издание. : Пер. с англ. – М. : Издательский дом «Вильяме», 2002. – 736 с.
4. Шахрайство під час війни: топ-4 схеми і нові тенденції URL : https://minfin.com.ua/ua/2022/03/15/82162508/

Ключові слова: шахрайство під час воєнного стану, шахрайство в мережі Інтернет, фішинг, фейк, персональні дані, схема вчинення інтернет-шахрайства.

Key words: martial law fraud, Internet fraud, phishing, fake, personal data, scheme of Internet fraud.

ФЛЮНТ МАР'ЯНА ОРЕСТІВНА

Національний університет «Одеська юридична академія», аспірантка кафедри кримінального процесу, детективної та оперативно-розшукової діяльності

КІБЕРБЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ПРАВОВІ ВИМОГИ ДО ОРГАНІЗАЦІЇ ТА РЕАЛІЗАЦІЇ

Забезпечення національної безпеки завжди було та залишається однією з основних функцій будь-якої держави та ключовим напрямом її політики.

Так, Закон України «Про національну безпеку України» [1] декларує: «державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо». Водночас, у Стратегії кібербезпеки України 2021 р. [2] зазначено, що кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій.

В сучасних умовах глобальної діджиталізації, збільшення випадків кібератак на державний та приватний сектор, існування та появи нових кіберризиків і кіберзагроз, росту рівня кіберзлочинності та «удосконалення» способів вчинення кіберзлочинів, а також в контексті ведення повномасштабної війни, кібербезпекова політика є не просто складовою національної безпеки України, а й одним з найактуальніших напрямів її реалізації.

Так, у 2016 році було вперше прийнято Стратегію кібербезпеки України [3], метою якої було створення умов для безпечного функціонування