УДК 343.9

Липкан І.І.
здобувач Науково-дослідного інституту публічного права,
https://orcid.org/0009-0000-6685-2650

СУЧАСНІ ВИДИ ШАХРАЙСТВ, ВЧИНЕНИХ З ВИКОРИСТАННЯМ ЦИФРОВИХ ТЕХНОЛОГІЙ

У статті проаналізовано сучасні види шахрайств, вчинених з використанням цифрових технологій. Зазначено, що швидкий розвиток технологій, особливо в області інформаційних технологій, значно розширює як можливості для правопорушників, так і для органів правопорядку, які намагаються адаптуватися до нових умов. З одного боку, технології дають переваги для розвитку економіки та суспільства, зокрема через покращення комунікацій і процесів обміну інформацією. З іншого боку, ці ж технології використовуються для вчинення кримінальних правопорушень, зокрема тих, що стосуються власності, наприклад, через комп'ютерні кримінальні правопорушення, кібершахрайство та інші форми інтернет-злочинів. Встановлено, що судова практика в цій галузі є незамінним джерелом для розуміння того, як застосовуються норми кримінального права до новітніх форм кримінальних правопорушень, що вчиняються за допомогою цифрових технологій. Завдяки використанню автоматизованих систем пошуку в Єдиному державному реєстрі судових рішень, виокремлено судові рішення стають репрезентативними для загальної картини правозастосування в Україні.

Ключові слова: *кібершахрайство, кримінальні правопорушення у сфері цифрових технологій, фішинг, скам, інтернет-торгівля, шахрайські дії.*

Постановка проблеми. Швидкий розвиток технологій, особливо в області інформаційних технологій, значно розширює як можливості для правопорушників, так і для органів правопорядку, які намагаються адаптуватися до нових умов. З одного боку, технології дають переваги для розвитку економіки та суспільства, зокрема через покращення комунікацій і процесів обміну інформацією. З іншого боку, ці ж технології використовуються для вчинення злочинів, зокрема тих, що стосуються власності, наприклад, через комп'ютерні кримінальні правопорушення, кібершахрайство та інші форми інтернет-злочинів.

У науці кримінального права виникає необхідність уточнення понять «комп'ютерне кримінальне правопорушення» та «кіберзлочин». Ці терміни не завжди однозначно визначаються, що призводить до різних підходів у практиці застосування кримінальних норм, а також до необхідності оновлення законодавства для чіткої кримінально-правової оцінки таких кримінальних правопорушень.

Погоджуємося з науковцями у тому, що розвиток інформаційних технологій вимагає перегляду існуючих підходів до правової оцінки комп'ютерних та кіберзлочинів. У зв'язку з цим, важливо визначити нові правові норми та удосконалити існуючі для забезпечення ефективного протидії кримінально протиправним посяганням, що здійснюються з використанням інформаційних технологій [1; 2; 3].

Стан опрацювання цієї проблематики. Вагомий внесок у дослідження теоретичних та практичних питань, пов'язаних з методикою розслідування шахрайств, здійснили такі відомі вчені: Л.І. Аркуша, В.П. Бахін, В.Д. Берназ, О.О. Вакулик, А.Ф. Волобуєв, В.Г. Дрозд, В.А. Журавель, А.В. Іщенко, Н.І. Клименко, О.Н. Колесніченко, В.О. Коновалова, В.С. Кузьмічов, В.К. Лисиченко, В.Г. Лукашевич, Є.Д. Лук'янчиков, Г.А. Матусовський, О.В. Одерій, І.В. Пиріг, О.В. Пчеліна, М.В. Салтевський, Р.Л. Степанюк, В.В. Тіщенко, Л.Д. Удалова, К.О. Чаплинський, Ю.М. Чорноус, В.Ю. Шепітько та ін.

Метою наукової статті є вивчення сучасних видів шахрайств, які вчиняються з використанням цифрових технологій, а також проведення зіставного аналізу із найбільш розповсюдженими видами у практиці правоохоронних органів.

Виклад основного матеріалу. Кібершахрайство охоплює широкий спектр шахрайських дій, що здійснюються за допомогою інформаційних та комунікаційних технологій. Воно може проявлятися в різних формах, від крадіжки персональних даних до маніпуляцій із фінансовими ресурсами в Інтернеті.

Кібершахрайство має різноманітні форми та методи здійснення, включаючи:

1. Фішинг – шахрайська практика, коли зловмисники маскуються під надійні установи (банки, інтернет-магазини, платіжні системи тощо) для того, щоб отримати конфіденційну інформацію (паролі, логіни, номери карток) через фальшиві електронні листи, вебсайти або SMS-повідомлення.

2. Вишинг (Voice phishing) – це вид фішингу, де шахраї використовують телефонні дзвінки для того, щоб під виглядом банківського працівника або іншої установи отримати від жертви важливу інформацію, наприклад, паролі або номери карток.

3. Смішинг (SMS phishing) – шахрайство через текстові повідомлення, де злочинці надсилають посилання або просять повідомити персональні дані.

4. Малваре (Malware) – програмне забезпечення, яке встановлюється на комп'ютер або мобільний пристрій жертви без її відома. Це можуть бути віруси, трояни, шпигунські програми, які призначені для крадіжки даних, контролю над пристроєм або його пошкодження.

5. Скам (Scam) – загальний термін для шахрайських схем, таких як «Нагорода за виграш» чи «Чудова інвестиційна можливість», коли жертву обманюють для того, щоб вона передала гроші або інші активи шахраям.

6. Інтернет-торгівля фальшивими товарами – шахрайство через інтернет-магазини, де продаються неіснуючі або підроблені товари. Після отримання передоплати покупець не отримує товар.

7. Крадіжка особистих даних (Identity theft) – отримання зловмисниками особистої інформації (ім'я, адреса, номер паспорта, номер картки) з метою здійснення фінансових операцій або для інших незаконних цілей.

8. Фальшиві онлайн-оголошення та афери з орендою – шахраї пропонують оренду житла або автомобіля за зниженими цінами, вимагаючи передплату, але не надаючи товар або послугу.

9. Шахрайство з криптовалютами – афери, пов'язані з інвестиціями в криптовалюти, коли шахраї обіцяють великий прибуток від інвестицій в невідомі або фальшиві криптовалютні платформи.

10. Аферисти з фальшивими онлайн-платежами – використання підроблених вебсайтів для здійснення платежів, де шахраї отримують гроші за товар або послугу, яку насправді не існує.

11. Шахрайство з кредитними картками – незаконне використання чужих кредитних карток для здійснення покупок або переведення грошей.

12. Маніпуляції в соціальних мережах – використання платформ соціальних медіа для здійснення шахрайства, включаючи створення фальшивих профілів для введення в оману інших користувачів.

13. Платіжні шахрайства через мобільні додатки – зловмисники створюють фальшиві додатки для мобільних пристроїв, що крадуть інформацію про банківські рахунки або платіжні дані.

Ці форми кібершахрайства постійно змінюються та вдосконалюються, оскільки злочинці шукають нові методи обману у відповідь на зміни в технологіях і методах безпеки.

Варто зазначити, що судова практика в цій галузі є незамінним джерелом для розуміння того, як застосовуються норми кримінального права до новітніх форм кримінальних правопорушень, що вчиняються за допомогою інформаційних технологій.

Враховуючи специфіку таких кримінальних правопорушень, як шахрайство в інтернет-просторі чи кібератаки, аналіз судових рішень дозволяє: виявити практичні аспекти застосування законодавства: Як на практиці кваліфікуються різні види злочинів, що здійснюються за допомогою технологій, і які принципи використовуються суддями під час розгляду таких справ; аналізувати правові прогалини та колізії: за результатами судової практики можна виявити недоліки в законодавстві, що потребують уточнення або удосконалення для забезпечення більш ефективної боротьби з кіберзлочинністю; визначити тенденції у покараннях: судові рішення допомагають виявити, які види покарань застосовуються в цих справах і як вони відповідають тяжкості злочинів, а також чи є система покарань достатньо стримуючою для нових форм кримінально протиправної діяльності; формувати правозастосовчу практику: аналізуючи сукупність судових рішень, можна виділити найбільш типові та важливі прецеденти, що можуть стати основою для подальшого розвитку правозастосування у галузі кіберзлочинності.

Аналіз судових рішень, проведений на основі даних із Єдиного державного реєстру судових рішень, підтверджує актуальність і репрезентативність вибраної сукупності. Відзначена тенденція зменшення кількості вироків упродовж останніхроків та подальше скорочення цього

показника в наступні роки вказує на декілька можливих причин, зокрема зміни в ефективності розслідувань, вдосконалення правоохоронної діяльності або трансформацію кримінально протиправних схем.

Завдяки використанню автоматизованих систем пошуку в Єдиному державному реєстрі судових рішень, виокремлено судові рішення стають репрезентативними для загальної картини правозастосування в Україні.

Згідно з отриманими даними, найбільш поширеними серед судових рішень є категорії «продаж товарів або надання послуг» (66 % від загальної кількості вироків) та «несанкціоновані транзакції» (35%). Це свідчить про значне поширення шахрайства через інтернет, де злочинці використовують сучасні технології для обману споживачів.

У категорії «продаж товарів або надання послуг» найбільш поширені випадки обману, пов'язані з продажем товарів або послуг, які фактично не існують. Як правило, такі шахрайства мають такі основні характеристики:

1. Фальшиві пропозиції товарів та послуг: наприклад, злочинці пропонують через інтернет «продаж» одягу, електроніки, меблів, туристичних путівок або навіть «оренду» квартир. Придбання товару або послуги зазвичай передбачає часткову або повну передплату, яку потім шахраї привласнюють.

2. Шахрайські пропозиції послуг: це можуть бути послуги з працевлаштування за кордоном, виготовлення меблів, допомога в отриманні кредитів або інші послуги, які ніколи не надаються після отримання коштів від споживачів.

3. Використання популярних онлайн-майданчиків: шахраї часто створюють акаунти або публікують пропозиції на популярних інтернет-ресурсах або онлайн-майданчиках, що дозволяє їм досягти ширшої аудиторії і здійснити більшу кількість обманів.

4. Створення фальшивих сайтів: у деяких випадках винні особи самостійно створюють спеціалізовані сайти або кілька сайтів для подальшого обману. Вони можуть використовувати такі ресурси для реклами своїх «товарів» або «послуг» та виглядати більш надійно.

Для здійснення шахрайських операцій з товаром або послугами злочинці використовують наступні методи: 1) фальшиві оголошення, а саме створення рекламних оголошень, які виглядають як реальні пропозиції від справжніх продавців або компаній; 2) пропозиції із завищеними цінами: Іноді шахраї пропонують товари або послуги за дуже низькими цінами, що викликає у потенційних жертв бажання здійснити покупку; 3) маніпуляція з відгуками, оскільки часто використовуються фальшиві позитивні відгуки для підвищення довіри до шахрайських сайтів або акаунтів; 4) невизначені умови угоди: Невідомі або непрозорі умови договору про покупку або надання послуг, що дозволяє зловмисникам маніпулювати покупцями.

Категорія «несанкціоновані транзакції» охоплює випадки, коли особи, які не є власниками карткових рахунків, здійснюють фінансові операції без дозволу власників карток, використовуючи їхні платіжні реквізити або інші шахрайські методи.

Категорія «незаконне отримання кредитів» охоплює кримінальні правопорушення, пов'язані з оформленням кредитів або замовленням матеріальних цінностей від імені потерпілих осіб без їх згоди чи відома.

Висновки. Отже, можемо дійти висновку, що суди іноді вважали, що пропозиція неіснуючих товарів через інтернет-платформи є проявом звичайного шахрайства, якщо техніка слугувала лише засобом комунікації, а не інструментом для реалізації незаконних операцій.

Така позиція судів вказує на відсутність чіткої межі між «звичайним шахрайством» та шахрайством із використанням електронно-обчислювальної техніки. Це може спричиняти нерівність у підходах до кримінальної відповідальності в залежності від судового округу або складу суду. Саме тому, на нашу думку, для уникнення неоднакового тлумачення судами кваліфікуючих ознак, доцільно внести уточнення до статті 190 КК України щодо специфіки використання технічних засобів у шахрайських схемах. Тому нами запропоновано викласти ч. 4 ст. 190 КК України у такій редакції: «4. Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням цифрових технологій, - карається позбавленням волі на строк від трьох до восьми років» А також доцільно додати примітку до статті, вказавши, що ч. 4 цієї статті може застосовуватись лише у разі використання як інструменту для реалізації незаконних операцій.

Список використаної літератури:
1. Азаров Д.С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) : монографія. К.: Атіка, 2007. 304 с.
2. Карчевський М.В. Злочин у сфері використання інформаційних технологій: визначення поняття. *Вісник Луганського державного університету внутрішніх справ ім. Е.О. Дідоренка*. 2013. № 4. С. 77–86.
3. Кравцова М.О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ : автореф. дис. ... канд. юрид. наук : 12.00.08. Харків. нац. ун-т внутр. справ. Харків, 2016. 16 с.

Современные виды мошенничеств, совершенных с использованием цифровых технологий

В статье проанализированы современные виды мошенничеств, совершенных с использованием цифровых технологий. технологии дают преимущества для развития экономики и общества, в частности из-за улучшения коммуникаций и процессов обмена информацией. совершение уголовных правонарушений, в том числе касающихся собственности, например через компьютерные уголовные правонарушения, кибермошенничество и другие формы интернет-преступлений Установлено, что судебная практика в этой области является незаменимым источником для понимания того, как применяются нормы уголовного права к новейшим. форм уголовных правонарушений, совершаемых с помощью цифровых технологий. в Едином государственном реестре судебных решений, выделенные судебные решения становятся репрезентативными для общей картины правоприменения в Украине.

Ключевые слова: *кибермошенничество, уголовные правонарушения в сфере цифровых технологий, фишинг, скам, интернет-торговля, мошеннические действия.*

Modern types of fraud committed with the use of digital technologies

The article analyses modern types of frauds committed with the use of digital technologies. It is noted that the rapid development of technology, especially in the field of information technology, significantly expands both the opportunities for offenders and law enforcement agencies trying to adapt to new conditions. On the one hand, technology provides benefits for the development of the economy and society, in particular through improved communications and information exchange. On the other hand, these same technologies are also used to commit crimes, in particular those related to property, for example through computer-related criminal offences, cyber fraud and other forms of online crime. he author establishes that case law in this area is an indispensable source for understanding how criminal law is applied to the newest forms of criminal offences committed through digital technologies. Thanks to the use of automated search systems in the Unified State Register of Court Decisions, selected court decisions become representative of the overall picture of law enforcement in Ukraine.

Key words: *cyber fraud, criminal offences in the field of digital technologies, phishing, scam, online trading, fraudulent actions.*