УДК 343.98:343.72
DOI: 10.31733/15-03-2024/2/84-85

Аріна КАДІРОВА
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції

Віталій ТЕЛІЙЧУК
професор кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук,
старший науковий співробітник, доцент

ДЕЯКІ ПРОБЛЕМИ ОПЕРАТИВНО-РОЗШУКОВОЇ ПРОТИДІЇ ШАХРАЙСТВУ В МЕРЕЖІ ІНТЕРНЕТ В УМОВАХ ВОЄННОГО СТАНУ

Актуальність даної теми полягає у дедалі більшій розповсюдженості в умовах воєнного стану шахрайства у мережі Інтернет. Зазначений вид кримінальних правопорушень набув поширеності через те, що злочинці користуються скрутним становищем людей, вразливістю громадян та наявністю у них внутрішньої тривоги. Умови воєнного стану впливають на різні аспекти життя українців, включаючи сферу кібербезпеки та боротьбу з шахрайством у мережі Інтернет.

Інтернет є безмежним простором, де користувачі можуть отримати доступ до безлічі різноманітних інформаційних ресурсів та сервісів. Однак зростаюча популярність мережі також призвела до зростання кількості шахраїв та зловмисників, які намагаються використовувати Інтернет для здійснення своїх злочинних дій. Тому спеціалізовані організації, такі як кіберполіція, повинні знати та розуміти способи вчинення шахрайства в мережі і мати на озброєнні відповідну оперативно-розшукову характеристику, щоб бути ефективними в боротьбі з цим видом злочинності [1, с. 159].

Шахрайство є одним із найбільш поширених злочинних діянь не тільки в Україні, а й у всьому світі. Це негативне явище відбувається в різних формах, таких як кібершахрайство, фінансове шахрайство, шахрайство з нерухомістю та ін. Шахраї нерідко вдаються до використання новітніх технологій та соціальних мереж, щоб увести в оману своїх жертв. Одним з ефективних засобів протидії шахрайству є використання можливостей оперативних підрозділів, які спеціалізуються на боротьбі з кримінальними правопорушеннями.

У той час як більшість громадян України намагаються надалі жити та розвивати економіку держави, усіляко намагаючись допомогти захисникам, шахраї підлаштовуються під реалії війни та вигадують нові шляхи для обману громадян. В умовах воєнного стану онлайн-шахрайства нікуди не зникли, а набули інших форм та масштабів [1, с. 542].

Серед проблем оперативно-розшукової протидії шахрайству у мережі Інтернет найпоширенішим вважається недостатність технічного оснащення, про що зазначають у своїх дослідженнях В. Телійчук та Г. Іваненко : «…тенденції розвитку оперативно-розшукової діяльності у сфері використання інформаційних технологій спираються на застосування спеціальних технічних засобів контролю, фіксації та обробки інформації. Треба зазначити, що працівники органів Національної поліції відстають від вимог часу, залишаючись технічно недостатньо озброєними в сучасному стані, а саме від цього і залежить ефективне реагування на факти даних кримінальних правопорушень та спонукання до їх розслідування, але через цей та інші фактори ефективність є значно меншою…» [2, с. 228].

До проблем оперативно-розшукової протидії шахрайству варто віднести, як зазначалось раніше, збільшення шахрайських схем. Злочинці є більш навченими та досвідченими у даній сфері діяльності. Вони набувають нових навичок опанування шахрайських схем щодня та прогресують у цій сфері. У той час як працівники, уповноважені на проведення оперативно-розшукової діяльності, не можуть бути настільки компетентними та прогресуючими, бо не є спеціалістами саме у новітніх технологіях та способах шахрайства, чим і користуються злочинці.

Також до проблем можна віднести складність розслідування шахрайства у мережі Інтернет. Є частим явищем діяльність таких шахраїв з-за кордону або на території України з використанням програм, які змінюють справжнє місцезнаходження. Це ускладнює їх ідентифікацію та притягнення винних до відповідальності.

В умовах воєнного стану, який значно вплинув на життя людей, важливо для громадян бути обізнаними та пильними, з чого і випливає наступна проблема. Більшість людей не знають про поширені шахрайські схеми і тому легко стають жертвами обману.

Отже, враховуючи зазначене, можна зробити висновки про необхідність посилення оперативно-розшукової протидії шахрайству в мережі Інтернет шляхом модеренізаціїї та розвитку даної сфери. Пріоритетним напрямом протидії шахрайству в мережі Інтернет, у тому числі й оперативно-розшукової протидії, є запобігання цим злочинам (профілактика, попередження та припинення), що передбачає такі форми, які призначені стримувати особу від наміру вчинити злочин чи довести злочинний намір до завершення. Протидія шахрайству в мережі Інтернет оперативно-розшуковими заходами включає систему оперативно-розшукових та інших заходів і реалізується в окремих організаційно-тактичних формах [1, с. 545]. Шахрайсво в мережі Інтернет – серйозна проблема, яка потребує комплексного вирішення.

1. Гунько К. О. Щодо визначення способів вчинення шахрайства в мережі Інтернет у період воєнного стану. *Збірник матеріалів міжнародного правничого конкурсу наукових статей серед здобувачів закладів вищої освіти : матеріали Міжнар. правн. конкурсу наук. ст. серед здобувачів вищ. освіти* (м. Кропивницький, 21 квіт. 2023 р.). Кропивницький, 2023. С. 159–166.

2. Телійчук В. Г., Гунько К.О. Проблеми протидії шахрайству в мережі Інтернет як складової інформаційної безпеки в умовах воєнного стану. *Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали VII Міжнар. наук.-практ. конф.* (м. Дніпро, 17 бер. 2023 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2023. С. 542–545.

3. Іваненко Г. Є., Телійчук В. Г. Щодо проблеми протидії незаконному обігу вогнепальної зброї в мережі інтернет. *Modern research in world science : The 8 th International scientific and practical conference* (Lviv, October 29-31, 2022). Lviv, Ukraine, 2022. P. 227–230.

УДК 343.98
DOI: 10.31733/15-03-2024/2/85-87

Родіон КОВАЛЕНКО
курсант факультету підготовки
фахівців для підрозділів
кримінальної поліції

Андрій КИСЕЛЬОВ
доцент кафедри
оперативно-розшукової діяльності
Дніпровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

СУЧАСНІ МОЖЛИВОСТІ ТЕХНОЛОГІЇ «OSINT» У КРИМІНАЛЬНОМУ АНАЛІЗІ В УМОВАХ ВОЄННОГО СТАНУ

Особливості технології відкритих джерел інформації (OSINT) в кримінальному аналізі, особливо в умовах воєнного стану, включають в себе використання різноманітних джерел, таких як соціальні мережі, новинні портали, геопросторові дані, мовний аналіз, відкриті бази даних, відео та зображення. Ці джерела надають важливу інформацію щодо змін в планах, поведінці, зв'язках осіб та груп, а також дають можливість отримати актуальну інформацію про ситуацію в місцях конфлікту, тенденції та реакцію громадськості. Аналіз цих даних може бути здійснений шляхом використання програмних засобів для автоматизації процесу збору, фільтрації та аналізу, а також з використанням технологій розпізнавання облич, об'єктів та подій у відео- та фотозображеннях. Важливо пам'ятати про етичні норми та правові вимоги при зборі та використанні інформації з відкритих джерел, а також про необхідність використання OSINT разом з іншими джерелами та методами аналізу для