УДК 343.721+343.98
DOI: 10.31733/17-03-2023-542-545

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

Катерина ГУНЬКО
здобувач вищої освіти
Дніпропетровського державного університету
внутрішніх справ

ЩОДО ПРОБЛЕМ ПРОТИДІЇ ШАХРАЙСТВУ В МЕРЕЖІ ІНТЕРНЕТ ЯК СКЛАДОВОГО ЕЛЕМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

Комп'ютер став одним із найпоширеніших засобів спілкування людей у сучасному світі, зберігання, створення, збору, обробки та використання інформації в будь-якій галузі діяльності людини. Бурхливий розвиток використання мережі «Інтернет» як постачальник товару та різних послуг, а відповідно і сфери грошового обігу призвів до того, що все більша кількість населення України стає жертвами шахрайств, скоєних з використанням мережі Інтернет. Враховуючи вимоги законодавства України, зокрема Конституції України, Кримінального, Кримінального процесуального кодексів та Законів України «Про Національну поліцію», «Про оперативно-розшукову діяльність» актуальним є завдання суттєвого покращення діяльності правоохоронних органів щодо запобігання, виявлення зазначеної категорії злочинів та їх ефективного досудового розслідування в умовах воєнного стану [1].

Шахрайство є однією з найбільш поширених злочинних дій не тільки в Україні, а й у світі. Це явище відбувається в різних формах, таких як кібершахрайство, фінансове шахрайство, шахрайство з нерухомістю та багато інших. 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.

За останні кілька років в Україні спостерігається значне збільшення кількості випадків шахрайства. Наприклад, за даними МВС України, у 2020 році було зареєстровано майже 30 тисяч випадків шахрайства, що на 14 % більше, ніж у 2019 році. Однією з найпоширеніших форм шахрайства є кібершахрайство. Згідно з дослідженнями, проведеними компанією Kaspersky, Україна є лідером серед країн Східної Європи за кількістю кібератак. Більшість кібератак спрямовані на злам корпоративних мереж та крадіжку конфіденційної інформації [2]. Іншою формою шахрайства є фінансове шахрайство. Наприклад, банківські картки часто стають об'єктом атак шахраїв, які намагаються отримати доступ до банківських рахунків та викрадають гроші з рахунку.

Коли більшість українців і представників бізнесу намагаються вижити в умовах воєнного стану в країні та допомогти по можливості Захисникам, шахраї вже підлаштувалися під реалії війни та вигадують все нові шляхи для обману громадян. В умовах воєнного стану онлайн-шахрайства нікуди не зникли, а набули інших форм та масштабів [3]. Сучасний стан свідчить, що, якщо до повномасштабного вторгнення кіберполіція фіксувала 15-20 тис. звернень громадян щодо фінансового шахрайства, то 2022 року ця статистика значно зросла. За 2022 рік Національний банк України виявив та заблокував 4,5 тис. шахрайських сайтів, які дублюють державні для заволодіння даними українців. Зі слів заступника голови НБУ Олексія Шабана, основними авторами таких фішингових сайтів в Україні є спецслужби РФ [4]. Найбільш поширеними видами шахрайства в Україні є такі:

1) організація добровільних, благодійних внесків, зокрема для хворих дітей та

бійців АТО;

2) використання електронних торгових майданчиків, зокрема HIFI FORUM, OLX та ін;

3) розповсюдження за акцією або за заниженою ціною будь-яких товарів чи речей;

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

5) поширення фішингових програм та вірусного програмного забезпечення;

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

7) соціальний інжиніринг (метод проникнення в захищені системи, заснований на використанні соціальної психології) використовується із застосуванням комп'ютера або телефону для доступу до рахунку або полегшення такого доступу або отримання цінної інформації (адреса електронної пошти особи) для цілеспрямованого крадіжки в персональних дачах;

8) пропозиція явно неіснуючої послуги чи методики (генератора електронних засобів, поповнення про гаманців з електронними грошима, ставки спорт);

9) розсилання різного роду електронних листів на електронні поштові скриньки, текст яких вводить в оману одержувача, акцентує увагу останнього на необхідності певного роду платежем [1];

10) збір коштів для військових. Протягом останнього року українці з усього світу намагаються допомогти нашим Захисникам хто чим може: купують спорядження, продукти та інші речі. Однак добрі справи для звичайних людей для шахраїв стали можливістю нагріти руки й тут. Збір коштів для військових одна з найпопулярніших схем серед шахраї, де вони під виглядом волонтерів збирають гроші на амуніцію, лікування чи інші необхідні для військових речі. Проте, такі всевдоволонтери привласнюють усі донати собі. Або ніби то пропонують товар для військових і просять скинути передоплату, але після переказу коштів продавці замовлення не виконують і разом з так званим товаром хутко зникають з радарів. Також, популярний трюк шахраїв – продаж цигарок, які вони пропонують купити за вигідною ціною блоку тютюнових виробів, проте після передоплати покупець втрачає і гроші, і такий собі примарний товар. Ще одна зі схем, коли аферисти збирають кошти певній людині, яка нібито потім їх передасть захисникам, але як і в попередніх ситуаціях, кошти також залишаються у шахраїв. Для того, щоб уникнути участі у зборі коштів для військових шахраями слід довіряти лише перевіреним благодійним організаціям або державним спеціальним рахункам, перевіряти правильність назв сайтів, на які переходять громадяни та де потрібно внести свої персональні дані. Не слід довіряти неперевіреним та незнайомим людям;

11) ваші рідні безвісти зникли або потрапили у полон. Розміщуючи інформацію про пошук рідних слід обачно вказувати інформацію, адже цими даними можуть скористатися шахраї. Також зловмисники можуть телефонувати батькам або іншим родичам зниклих та називаючи ім'я та прізвище зниклого родича та повідомляють, що нібито він перебуває у полоні, але для того, щоб його визволити потрібно сплатити гроші. У таких випадках слід не панікувати, не піддаватися емоціям та самостійно зв'язатися з родичем, або ж зателефонувати до Об'єднаного центру з пошуку та звільнення полонених або зверніться до найближчої військової адміністрації чи правоохоронців;

12) повідомлення про евакуаційний рейс за умови передплати. Дбаючи про безпеку своїх рідних і близьких, люди готові віддати останнє, щоб уберегти їх і саме на цьому почутті грають шахраї, розміщуючи такі оголошення. Шахраї розміщують оголошення в Інтернеті про перевезення громадян із зони бойових дій до більш безпечного місця. Проте, за свої послуги вони вимагають оплату наперед. Треба пам'ятати, що евакуаційні рейси з небезпечних районів організовує держава і вони безкоштовні;

13) фейкова фінансова допомога. У перші дні повномасштабного вторгнення російської армії в Україну президент Володимир Зеленський оголосив про старт програми фінансової підтримки. В її межах громадяни із зони бойових дій могли подати заявку на отримання 6500 грн. І хоча заявки приймалися до 31 березня через застосунок «Дія», а гроші виплачувалися на спеціальні картки «є Підтримка», однак це не завадило шахраям створити безліч фішингових сайтів, які виманюють карткові дані. Аферисти створили на сайті, замаскованому під Урядовий портал, сторінку «Державні послуги онлайн» та підрубрику з виплати українцям грошей від ООН. Для підтвердження такого нібито «переказу» необхідно сплатити державне мито у визначеному розмірі. Інформацію про програми підтримки від держави завжди публікують офіційні джерела (домен gov.ua).

Також відповідні сповіщення з'являються в «Дії». Тож необхідно ретельно перевіряти онлайн-ресурси, які мають виплачувати допомогу [3].

Урядом України вжито ряд заходів для боротьби з шахрайством. Зокрема, було створено спеціальну службу (3 жовтня 2015 року була створена нова Кіберполіція, як структурний підрозділ Національної поліції), метою якої було реформування та розвиток підрозділів МВС України, що забезпечило підготовку та функціонування висококваліфікованих фахівців в експертних, оперативних та слідчих підрозділах поліції, залучених у протидії кіберзлочинності, та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності. Також, було прийнято законодавчі зміни, які передбачають суворіше покарання для шахраїв: в п. 11 ч. 1 ст. 67 КК України закріплено, що вчинення кримінального правопорушення в умовах воєнного стану як обставина, яка обтяжує покарання. Наприклад, частиною першою статтею 190 Кримінального кодексу України передбачено, що заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою (шахрайство) карається штрафом від двох тисяч до трьох тисяч неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк від двохсот до двохсот сорока годин, або виправними роботами на строк до двох років, або обмеженням волі на строк до трьох років [5].

У випадку використання умов воєнного стану для вчинення шахрайства, буде братись до уваги найтяжче покарання, а саме обмеження волі на строк до 3 років. Таким чином, відповідальність за вчинення цього кримінального правопорушення за умов воєнного стану не є визначеною, але береться до уваги найтяжча міра покарання, яка закріплена в Кримінальному кодексу України. Проте, для ефективної боротьби з цим явищем, необхідно здійснити ряд заходів за наступними напрямами діяльності. Зокрема, для цього необхідна тісна взаємодія всіх зацікавлених сторін, таких як правоохоронні органи, банки, провайдери інтернет-послуг та інші компанії. Однак, діяльність оперативних підрозділів не є повністю ефективною, а тому потребує удосконалення. Шахраї та кіберзлочинці постійно вдосконалюють свої методи та технології, що ускладнює роботу правоохоронних органів. Крім того, існує ризик порушення прав людини та неправильного застосування силових методів у боротьбі зі злочинністю. Діяльність оперативних підрозділів також потребує підвищення рівня відповідних фінансових та технічних ресурсів для ефективного виконання своїх завдань. Необхідно вдосконалювати технічне обладнання та програмне забезпечення для забезпечення операційної діяльності та розвідки. Крім того, слід забезпечити належну підготовку та кваліфікацію оперативників з метою підвищення ефективності їх роботи.

Окрім того, важливо проводити інформаційну роботу серед громадян про те, як уникнути стати жертвою шахраїв. Зокрема, потрібно регулярно здійснювати консультації про необхідність не ділитися конфіденційною інформацією з незнайомими людьми, не відкривати підозрілі посилання та використовувати надійні паролі для доступу до важливої інформації. У цьому процесі не менш важливою є співпраця з міжнародними партнерами, оскільки шахраїв та кіберзлочинців можна відстежити та покарати тільки за допомогою міжнародної співпраці. Одним з перспективних напрямків розвитку боротьби з шахрайством є використання новітніх технологій, таких як штучний інтелект та блокчейн. Наприклад, за допомогою штучного інтелекту можна виявляти та блокувати підозрілі транзакції, а блокчейн дозволяє зберігати інформацію про транзакції без можливості її зміни та підробки.

Щоб убезпечити себе від аферистів в онлайн просторі необхідно дотримуватися наступних порад:

– не відкривайте жодні посилання в месенджерах, соціальних мережах, SMS. Особливо це стосується скорочених посилань, наприклад, «bit.ly», адже ви не можете знати, що за ними приховано та куди вони ведуть. Завжди перевіряйте інформацію з SMS.;

– не вводьте на сторонніх сайтах дані своєї картки. Слід пам'ятати, що шахраї розраховують на неуважних і технічно неосвічених людей, як правило старшого покоління. Тому попередьте своїх рідних похилого віку, щоб вони не переходили на жодні посилання [4].

Загалом, протидія шахрайству є складним та довготривалим процесом, який потребує постійного удосконалення та адаптації до нових викликів. Однак, за наявності ефективної системи протидії шахрайству та кіберзлочинності, можна забезпечити безпеку для громадян та бізнесу в Україні, що сприятиме розвитку економіки та підвищенню довіри до державних інституцій [6]. Отже шахрайство є серйозною проблемою в Україні, яка стає все більш актуальною в контексті розвитку кібертехнологій. Для ефективної боротьби з цим явищем

необхідно залучати всіх зацікавлених сторін та проводити інформаційну роботу серед громадян. Тільки так можна досягти значних результатів у боротьбі з шахрайством та забезпечити безпеку для громадян та бізнесу в Україні. Використання сил та засобів оперативних підрозділів є ефективним способом протидії цим явищам. Проте, необхідно вдосконалювати їх діяльність та забезпечувати належні ресурси для їх ефективної роботи. 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 визнані стримувати особу від наміру вчинити злочин чи довести злочинний намір до кінця. Протидія шахрайству в мережі Інтернет оперативно-розшуковими заходами включає систему оперативно-розшукових та інших заходів і реалізується в окремих організаційно-тактичних формах. Попередження злочинів є комплексною діяльністю. Запобігання злочинам – складний процес, яке зміст відрізняється від інших видів діяльності. При цьому виділяють низку складових, а саме: профілактика, запобігання та припинення злочинів. Кожен із цих елементів у порівнянні самостійний, але вони взаємопов'язані, мають одну й ту саму мету – не допустити скоєння злочину.

1. Телійчук В., Горілик Д. Оперативно-розшукова протидя шахрайству, що здійснюється через мережу Інтернет. Міжнародний науково-практичний правовий журнал «Legea si Viata». 2019. № 12 (336). С. 105-110. URL: https://ibn.idsi.md/sites/default/files/ imag_file/105-111_1.pdf.

2. Протидія шахрайству. URL: https://bit.ly/3JK2pMg.

3. Інтернет-шахрайства в умовах воєнного стану: як не потрапити на гачок до аферистів. URL: https://legalaid.gov.ua/publikatsiyi/internet-shahrajstva-v-umovah-voyennogo-stanu-yak-ne-potrapyty-na-gachok-do-aferystiv.

4. Нацбанк за 2022 рік заблокував 4,5 тис. шахрайських сайтів. URL: https://lb.ua/economics/2023/02/15/545966_natsbank_2022_rik_zablokuvav_45.html.

5. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

6. Капустник І. Проблемні аспекти правового регулювання оперативно-розшукової протидії шахрайствам, що вчиняються організованими групами. URL: https://bit.ly/3n1v5Yb.

УДК 343.721+343.98
DOI: 10.31733/17-03-2023-545-546

Денис БРАЖНИК
аспірант кафедри криміналістики
та домедичної підготовки
Дніпропетровського державного
університету внутрішніх справ

ПОНЯТТЯ ТА ВИДИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ, ЩО ВИКОРИСТОВУЮТЬСЯ ПІД ЧАС ВЧИНЕННЯ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ, ПОВ'ЯЗАНОГО ІЗ ЛЕГАЛІЗАЦІЄЮ (ВІДМИВАННЯМ) МАЙНА, ОДЕРЖАНОГО ЗЛОЧИННИМ ШЛЯХОМ

Мережа Інтернет, як глобальний інструмент обміну даними між користувачами, мобільні пристрої, різноманітні додатки, месенджери, соціальні мережі, активно інтегруються у всі сфери нашого життя. Окрім того, останнім часом спостерігається стрімкий розвиток інтернет-банкінгу (системи клієнт-банку), купівля товарів та послуг на онлайн біржах та аукціонах, що в свою чергу, призводить до «цифровізації» валютних цінностей, тобто фактично перехід від готівкових коштів або цінностей до електронних. При цьому, і надалі у світі залишається досить актуальною проблемою вчинення злочинів в економічній або суміжних з нею сферах, результатом якої є заволодіння майном фізичних або юридичних осіб.

У зв'язку із такою фактично «фінансовою революцією» у світі стали поширюватися випадки легалізації (відмивання) майна, одержаного злочинним шляхом із використанням інформаційно-телекомунікаційних систем та технологій. Натомість, у практиці розслідування таких кримінальних правопорушень виникають питання, пов'язані із необхідністю виокремлення основних видів інформаційно-телекомунікаційних систем та технологій, які найчастіше використовуються під час вчинення злочинів пов'язаних із