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

легалізацією (відмиванням) майна, одержаного злочинним шляхом.

Відповідно до ст. 1 Закону України «Про захист інформації в інформаційно-комунікаційних системах» (в редакції від 04.07.2020 року), інформаційно-телекомунікаційна система - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле [1]. Водночас, телекомунікаційна система – це сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб [1].

Нами досліджено судову практику в Україні за останні десять років, а також аналітичні звіти деяких правоохоронних органів іноземних країн, які займаються боротьбою зі злочинністю, пов'язаною із легалізацією майна, отриманого злочинним шляхом, та виокремлено основні види інформаційно-телекомунікаційних систем та технологій, які використовуються з метою вчинення даного виду злочину, серед яких інформаційно-телекомунікаційні технології (ІКТ) та інформаційно-телекомунікаційні системи (ІКС).

Для загального розуміння проблематики розслідування кримінальних правопорушень, пов'язаних із легалізацією (відмиванням) майна, одержаного злочинним шляхом, із використанням інформаційно-телекомунікаційних систем та технологій, необхідно зазначити, що злочинці при вчиненні таких протиправних діянь використовують такі інформаційно-телекомунікаційні технології (ІКТ):

- комп'ютерна техніка, мобільні пристрої та встановлене на них програмне забезпечення, що в сукупності становить електронно-обчислювальні машини (ЕОМ) [2];
- телекомунікаційні системи (бездротовий телефонний або інтернет зв'язок, застосування медіа трансляцій, мессенджерів та додатків або програмного забезпечення задля усіх видів обробки відео та аудіо файлів);
- інтернет-банкінг (система дистанційного обслуговування клієнтів банку або інших фінансових інструментів);
- цифрові платіжні системи (наприклад, Google Pay, Pay Pall), онлайн гаманці (наприклад, Epay, WebMoney), електронні-валютні біржі та аукціони (наприклад, Binance);
- інші інструменти ІКТ та ІКС тощо.

Отже, «світова фінансова революція» та розвиток «передових цифрових технологій», проникнення мережі Інтернет на ЕОМ в усі сфери нашого життя, є результатом появи різноманітних способів легалізації (відмивання) майна, одержаного злочинних шляхом за допомогою різних видів інформаційно-телекомунікаційних систем та технологій. У зв'язку із чим постає питання в чіткому законодавчо закріпленому розмежуванні понять, які є суміжними з такою областю знань, як інформаційні технології (ІТ), що, в свою чергу, потребує більш досконалої розробки диспозицій статей особливої частини КК України з метою неможливості уникнення відповідальності за вчинені злочини.

---

1. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР (в редакції від 04.07.2020 року): URL: https://zakon.rada.gov.ua/laws/main/index (дата звернення 12.01.2023 р.).
2. Верховний Суд України – офіційний веб-сайт, URL: https://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7C00499C02 (дата звернення 19.01.2023 р.).

УДК 004.77+355.02
DOI: 10.31733/17-03-2023-546-549

Сергій РОМАШКО
аспірант кафедри
економіки та соціально-трудових відносин
Університету митної справи та фінансів

КОНКУРЕНЦІЯ НА РИНКУ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ ЯК ФАКТОР ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ВІЙСЬКОВИЙ ЧАС

Під час надзвичайних ситуацій та воєнного часу інформаційна безпека стає ще більш важливою, ніж у мирний час, адже це може бути питанням життя чи смерті. Своєчасне та точне поширення інформації може допомогти запобігти та пом'якшити наслідки катастроф,