УДК 343.9

Аліна Владиславівна КАЛІНІНА,
кандидат юридичних наук,
науковий співробітник відділу кримінологічних досліджень
Науково-дослідного інституту вивчення проблем злочинності ім. акад. В. В. Сташиса
Національної академії правових наук України

«КОРОНАВІРУСНИЙ» НАПРЯМОК У КІБЕРШАХРАЙСТВІ[2]

Збентеження населення новопосталою проблемою – потенційним зараженням вірусом SARS-CoV-2 (коронавірусом) та наслідками хвороби, яку він викликає, – більш, ніж благодатний ґрунт для різного роду маніпуляцій із людською свідомістю. Адже емоція страху – головна зброя в цьому випадку. До неї додаються ще і стресовий стан, в якому опинилася особа через введення карантинних заходів в Україні, острах за життя і здоров'я (як своє, так і близьких і рідних), недовіра до статистичних даних про кількість хворих та померлих саме від коронавірусної хвороби, різні сюжети у ЗМІ з цієї тематики (переважно негативного забарвлення) тощо. Отже, людина готова повірити у будь-що, аби убезпечити себе від загрози, що одразу ж намагаються використати зловмисники, у тому числі й ті, які «працюють» в Інтернет-просторі. Адже злочинність завжди чутлива до змін у суспільстві. Особливо, коли ці зміни – потенційне середовище для її продукування.

Життя сучасної людини важко уявити без Інтернету. Наразі для багатьох саме цей ресурс є першочерговим в отриманні інформації. Тому із появою нового фактора (загроза захворювання на коронавірус), який значно вплинув на життєдіяльність людини (у виді масштабних карантинних заходів, запроваджених у державі), Інтернет-простір став активно використовуватися і злочинцями. Значного поширення набуло вчинення діянь, які можна охарактеризувати терміном «кібершахрайство» – тобто, шахрайство, що вчиняється шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ч. 3 статті 190 КК України). Зокрема, за даними Національної поліції на тлі

2 Тези підготовлено на виконання теми фундаментального наукового дослідження НДІ ВПЗ «Стратегія зменшення можливостей вчинення злочинів: теорія та практика».

загального зниження рівня злочинності в державі рівень шахрайств з використанням мережі Інтернет протягом карантину збільшився на 15 % [1]. Тенденція до зростання кількості «кібершахрайств» прогнозована. Використання паніки серед громадян, пов'язаної із епідемічною ситуацією в Україні та світі, зміни в організації виробничих процесів, а також перехід на «дистанційний режим праці» деяких злочинців – головні умови для збільшення кількості таких злочинів. Необхідно підкреслити, що кібершахрайства, пов'язані із COVID-19, мають «інтернаціональний характер»: результат аналізу повідомлень у пресі та на інформаційних інтернет-ресурсах (у тому числі й державних і правоохоронних органів) підтверджує цю тезу [див., напр. 2; 3 та ін.].

За висновками зарубіжних дослідників 71 % з більше, ніж 400 опитаних експертів (спеціалістів у сфері IT та інформаційної безпеки) вказують на активне використання злочинцями змін в роботі багатьох організацій [3]. Як головну загрозу більшість респондентів називають спроби фішингу (55 %), на другому місці – існування шкідливих вебсайтів, що нібито містять інформацію про коронавірус (32 %); далі – збільшення кількості шкідливих програм (28 %) та вимагателів (19 %) [3]. Коронавірус став головною темою в злочинних схемах із використанням соціальної інженерії (знань про людську поведінку та фактори, які на неї впливають, для злочинного вивідування даних) [4].

«Кібершахрайства», що активізувалися під час пандемії COVID-19, можна умовно розподілити на:

1. *Фішинг* – діяльність злочинців, що заснована на «гачках» для користувачів Інтернету: даних про COVID-19, інформації про методи, засоби та способи лікування коронавірусної хвороби і її профілактику, різних видах компенсацій грошових коштів у зв'язку із карантинними заходами (як то: державна допомога, благодійна допомога, відтермінування виплат за кредитами; компенсація за білети на різного виду транспорт, рейси якого відмінилися тощо), участь в інтернет-опитуваннях тощо. Основна «зброя» фішингу – листи на електронну пошту, вебсайти та додатки для смартфонів. Мета фішингу – отримання персональних банківських даних особи задля доступу до коштів жертви [4]. У технології фішингу можуть використовуватися назви міжнародних організацій, державних органів та установ (наприклад, Всесвітньої організації охорони здоров'я, Міністерства охорони здоров'я тощо).

2. *Організація фальшивого продажу засобів індивідуального захисту та антисептиків, тестів на зараження COVID-19, медичних препаратів від коронавірусу та засобів його профілактики, інших продовольчих товарів та товарів особистого вжитку*, що полягає у створенні фейкових сайтів, сторінок у соціальних мережах, телеграм-каналів тощо із пропозицією продажу такої продукції [4; 5; 6 та ін.]. Наприклад, кіберполіція України за місяць карантину виявила та заблокувала діяльність 179 Інтернет-посилань, за якими шахраї ошукували громадян, продаючи неіснуючий товар, під час пандемії та встановила 236 осіб, що займалися вказаною вище діяльністю. Головна умова придбання таких товарів – стовідсоткова передплата їх вартості [6].

3. *Розповсюдження шкідливого програмного забезпечення під виглядом інформації про COVID-19*. Із цією метою використовуються доменні ім'я, пов'язані зі словами Coronavirus, COVID-19 тощо. Кінцева мета – завантаження користувачем шкідливого програмного забезпечення на його пристрій (наприклад, «троянів») під виглядом карти розповсюдження коронавірусу чи місць перебування хворих на нього, додатку чи спеціальної програми про COVID-19 тощо, метою якого є отримання доступу до фінансової (платіжної) інформації користувача [7].

Окрім зазначеного, можна ще додати про надшвидке поширення фейкової інформації про коронавірус та його лікування, у тому числі, й від імені офіційних установ.

Таким чином, в умовах світової пандемії COVID-19 активізувалися «дистанційні» форми злочинної активності, а саме вчинення шахрайств у мережі Інтернет. Головною рисою таких шахрайств є маніпуляція інформацією, що пов'язана із захворюванням на коронавірус. Це потребує підвищеної уваги з боку правоохоронних органів та посилення заходів боротьби зі злочинністю.

Список бібліографічних посилань

1. Продовження та пом'якшення карантину обговорили на нараді в Офісі Президента // Президент України : офіц. інтернет-представництво. 21.04.2020. URL: https://www.president.gov.ua/news/prodovzhennya-ta-pomyakshennya-karantinu-obgovorili-na-narad-60757 (дата звернення: 29.04.2020).
2. Coronavirus (COVID-19): advice on how to protect yourself and your business from fraud and cyber crime // United Kingdom public sector information website. 27.04.2020. URL: https://www.gov.uk/government/publications/

coronavirus-covid-19-fraud-and-cyber-crime/coronavirus-covid-19-advice-on-how-to-protect-yourself-and-your-business-from-fraud-and-cyber-crime (дата звернення: 30.04.2020).
3. Мельникова Ю. Коронавирус – друг кибермошенников // Comnews : сайт. 09.04.2020. URL: https://www.comnews.ru/content/205491/2020-04-09/2020-w15/koronavirus-drug-kibermoshennikov (дата звернення: 30.04.2020).
4. Маніпуляції та шахраї під час епідемії коронавірусу: хто і як виграє, коли інші страждають // Рубрика : сайт. 19.03.2020. URL: https://rubryka.com/article/koronovirus-manipulation-crooks/ (дата звернення: 30.04.2020).
5. COVID-19: Increasing Risk of Cyber Fraud // McCann FitzGerald. 21.04.2020. URL: https://www.mccannfitzgerald.com/knowledge/disputes/covid-19-increasing-risk-of-cyber-fraud (дата звернення: 30.04.2020).
6. З початку карантину кіберполіцейські перевірили 576 інформацій щодо можливих протиправних дій, пов'язаних з коронавірусом // Кіберполіція України : офіц. сайт. 17.04.2020. URL: https://cyberpolice.gov.ua/news/z-pochatku-karantynu-kiberpoliczejski-pereviryly--informaczij-shhodo-mozhlyvyx-protypravnyx-dij-povyazanyx-z-koronovirusom-6129/ (дата звернення: 30.04.2020).
7. Комаровская В. Коронабизнес: как на пандемии коронавируса зарабатывают мошенники // COMMENTS.UA : сайт. 01.04.2020. URL: https://comments.ua/news/it/Internet/649763-koronabiznes-kak-na-pandemii-koronavirusa-zarabatyvayut-kibermoshenniki.html (дата звернення: 30.04.2020).

Одержано 01.05.2020