УДК 343.72:004.773+578.834.1

Сергій Миколайович ГУСАРОВ,
доктор юридичних наук, професор,
член-кореспондент Національної академії правових наук України,
заслужений юрист України, професор кафедри адміністративного права та процесу факультету № 1 Харківського національного університету внутрішніх справ

В'ячеслав Валерійович МАРКОВ,
кандидат юридичних наук, старший науковий співробітник,
декан факультету № 4 Харківського національного університету внутрішніх справ

НОВІ СХЕМИ КІБЕРШАХРАЇВ, ПОВ'ЯЗАНІ З ПОШИРЕННЯМ ГОСТРОЇ РЕСПІРАТОРНОЇ ХВОРОБИ COVID-19, СПРИЧИНЕНОЇ КОРОНАВІРУСОМ SARS-COV-2

У грудні 2019 року Муніципальна комісія охорони здоров'я м. Ухань, Китай, повідомила про виявлення групи випадків захворювання пневмонією у м. Ухань провінції Хубей. Згодом було встановлено, що збудником захворювання був новий коронавірус, який в подальшому отримав назву SARS-CoV-2.

11 березня 2020 року Всесвітня організація охорони здоров'я дійшла висновку, що спалах нового захворювання під назвою COVID-19 можна охарактеризувати як пандемію [1].

В Україні першу інфіковану особу було виявлено 03 березня 2020 року [2].

11 березня Кабінет Міністрів оголосив на всій території України карантин [3].

Майже з самого початку виявлення у Китаї нової короновірусної хвороби це широко висвітлювалося як закордонними, так і вітчизняними ЗМІ та медіа.

Мешканці багатьох країн світу, у тому числі українці, читаючи друковані видання та електронні джерела інформації, дивлячись новини по

телевізору чи в інтернет, та слухаючи їх по радіо, майже щодня чули про небезпеку поширення світом гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2.

У певної частини населення виникли побоювання, що вони або вже захворіли COVID-19, або можуть захворіти у будь-який момент.

Серед населення, через комп'ютерні соціальні мережі та інтернет-месенджери, почала поширюватися неправдива інформація про короновірус та протидію йому. Так на початку березня 2020 року в України швидко поширились неправдиві чутки про обробку в нічний час за допомогою вертольотів хімікатами вулиць населених пунктів для дезінфекції від короновірусу [4].

Серед певної частини українців виникла паніка, пов'язана з Covid-19, через що вони втратили пильність та стали більш вразливими та довірливими. Цим вирішили скористуватися аферисти, які для незаконного заволодіння коштами громадян почали використовувати сучасні цифрові комунікації та мережу інтернет для вчинення протиправних дій.

Так станом на 04 травня 2020 року працівниками підрозділів Департаменту кіберполіції Національної поліції України було перевірено 642 інформації щодо вчинення можливих протиправних дій, у тому числі онлайн-шахрайств, пов'язаних з коронавірусом. За результатами перевірок розпочато 58 кримінальних проваджень. Було ідентифіковано 166 осіб, які причетні до організації чи участі в шахрайських схемах, де використовувалась ситуація з COVID-19. Крім цього, за матеріалами українських кіберполіцейских складено 40 адміністративних протоколів за фактами порушення карантинних заходів та реалізації виробів медичного призначення та дезінфікуючих засобів.

Українська кіберполіція відзвітувала, що із початку запровадження в Україні карантинних заходів вони заблокували 9954 інтернет-посилання, що використовувалися шахраями в злочинних цілях, і 1945 шахрайських фінансових операцій за банківськими рахунками [5].

За даними Служби безпеки України станом на 04 травня 2020 року, за період дії карантинних заходів кіберфахівці СБУ заблокували понад 2,1 тисячі інтернет-спільнот із загальною аудиторією понад 900 тис. користувачів, викрили 301 інтернет-агітатора, які поширювали різноманітні фейки про епідемію COVID-19.

Фахівці Служби безпеки України нейтралізували 103 кібератаки на інформаційні ресурси державних органів влади протягом першого

кварталу 2020 року. Починаючи з березня, значна кількість атак відбувається проти відомств, що забезпечують боротьбу з COVID-19 – протидії таким атакам приділяється особлива увага.

Також СБУ зазначає, що з початку карантину хакерські угруповання, зокрема, масово направляють на поштові скриньки державних установ електронні листи на тематику коронавірусу. Насправді до цих листів прикріплені файли зі шкідливим програмним кодом, який активізується при відкриванні листа.

За оприлюдненою інформацією більшість хакерських атак скеровані російськими спецслужбами, що намагаються отримати віддалений доступ до комп'ютерів українських держорганів. Потім вони планують спотворювати чи знищувати дані, поширювати фейки нібито від імені держструктур, а також дискредитувати дії української влади. Загалом у січні-березні СБУ припинила роботу майже 2 тисяч вебресурсів, які хакери використовували для здійснення кібератак [6].

До речі, через зазначений вище спосіб поширення шкідливого програмного забезпечення, кібертерористи також можуть розповсюджувати віруси-шифрувальники, які знищують інформацію на зараженому пристрої [7].

Шахрайства пов'язані із поширенням COVID-19 скоюють не тільки в Україні. Так кіберспеціалісти поліції та спецслужб Федеративної республіки Німеччини виявили близько 90 шахрайських сайтів німецькою мовою, метою яких було привласнення державної фінансової допомоги для постраждалих підприємств від наслідків обмежувальних заходів щодо протидії епідемії COVID-19.

Так на початку квітня 2020 року було виявлено фішинговий вебсайт Міністерства економіки федеральної землі Північний Рейн-Вестфалія, який містив усі розділи і вбудовані елементи справжнього сайту Міністерства. Підробка мала один додатковий розділ – а саме онлайн-заявку на отримання субсидії для індивідуальних підприємців, які зазнають збитків через епідемію COVID-19 у Німеччині і заходи для боротьби з нею. Як вважають фахівці, від 3500 до 4000 осіб могли заповнити фейкову заявку, надавши шахраям усі конфіденційні дані, які ті, своєю чергою, використовують уже під час подавання справжніх заявок. Тільки банківські реквізити у цьому випадку будуть фейковими. Замість них будуть використовуватися так звані bankdrops – банківські рахунки, доступ до яких раніше отримали шахраї

Тільки з початку березня у світі зареєстровано близько 80 тисяч доменних імен зі словами Corona і COVID-19. Скільки з них призначені для добрих, а скільки – для злочинних цілей, ніхто навіть не береться оцінювати [8].

Для скоєння протиправних дій кібершахраї також надсилають фішингові електронні листи чи повідомлення у месенджерах та соціальних комп'ютерних мережах від імені, наприклад, Всесвітньої організації охорони здоров'я, Міністерства охорони здоров'я України, Центру громадського здоров'я МОЗ України, відомих лікарів тощо.

Зазвичай такі фейкові повідомлення та електронні листі містять або посилання на фішингові вебсайти, або вкладення із файлами, які шляхом застосування шахраями методів соціального інжинірингу, користувачі відкривають щоб ознайомитися із їх вмістом.

На сьогодні можна виділити за змістом наступні типи електронних шахрайських повідомлень та оголошень, пов'язані із поширенням гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2 [9, 10]:

1) від банківських установ про уточнення чи перевірку даних клієнта для:

— отримання ним соціальних виплат (по безробіттю, пенсіонерам та іншим категоріям громадян);

— уникнення ним штрафів за несвоєчасні платежі за кредитом;

2) від міжнародних організацій та благодійних організацій з проханням перевести кошти на боротьбу з вірусом;

3) від закордонних (наприклад, з азіатських країн) медичних організації чи дослідницьких центрів, які пропонують отримати чималі кошти за участь у анкетуванні щодо вивчення стану поширення короновірусу у певному регіоні;

4) від продавців товарів для боротьби із короновірусом:

— засобів індивідуального захисту (медичних та захисних масок, респіраторів, халатів тощо);

— медичних виробів (термометрів тощо);

— дезінфекторів;

— тестів на короновірус;

— неіснуючих ліків від короновірусу;

5) про начебто приховування органами державної влади:

– реальної кількість захворілих;
– способи поширення вірусу;
– ефективних способів лікування.

Зазвичай всі вищезначені шахрайські схеми направлені на незаконне отримання інформації про номер банківської картки, термін її дії та коду безпеки, для подальшого несанкціонованого списання коштів з банківського рахунку потерпілого, або на незаконне заволодіння коштами потерпілої особи під час продажу несправжніх або неіснуючих товарів та послуг.

Список бібліографічних посилань

1. COVID-19 – хронология действий ВОЗ // Всемирная организация здравоохранения : офиц. сайт. 27.04.2020. URL: https://www.who.int/ru/news-room/detail/27-04-2020-who-timeline---covid-19 (дата звернення: 10.05.2020).
2. В Україні підтвердили перший випадок зараження коронавірусом // РБК-Україна : сайт. 03.03.2020. URL: https://www.rbc.ua/ukr/news/ukraine-podtverdili-pervyy-sluchay-zarazheniya-1583227440.html (дата звернення: 10.05.2020).
3. Про запобігання поширенню на території України коронавірусу COVID-19 : Постанова Кабінету Міністрів України від 11.03.2020 № 211 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/211-2020-п (дата звернення: 10.05.2020).
4. СБУ спростувала фейк про нічне розпилення «хімікатів від коронавірусу» над Києвом // 5 канал : сайт. 17.03.2020. URL: https://www.5.ua/kyiv/sbu-sprostuvala-feik-pro-nichne-rozpylennia-khimikativ-vid-koronavirusu-nad-kyievom-210548.html (дата звернення: 10.05.2020).
5. Кіберполіція заблокувала майже 10 000 Інтернет-посилань, які шахраї використовували під час пандемії // Кіберполіція України : офіц. сайт. 04.05.2020. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-zablokuvala-internet-posylan-yaki-shaxrayi-vykorystovuvaly-pid-chas-pandemiyi-6499/ (дата звернення: 10.05.2020).
6. СБУ нейтралізувала 103 кібератаки і завадила російським хакерам отримати дані держустанов // Служба безпеки України : офіц. сайт. 06.05.2020. URL: https://ssu.gov.ua/ua/news/3/category/21/view/7559 (дата звернення: 10.05.2020).
7. Бєляєва Є. Г., Рвачов О. М. Віруси-шифрувальники як головна зброя кібертерористів // Актуальні питання протидії кіберзлочинності та торгівлі

людьми : зб. матеріалів Всеукр. наук.-практ. конф. (м. Харків, 15 листоп. 2017 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2017. С. 121–124.

8. Як шахраї в Німеччині використовують коронавірус у своїх цілях // Deutsche Welle : сайт. 20.04.2020. URL: https://www.dw.com/uk/a-53147244 (дата звернення: 10.05.2020).
9. Увага, шахраї! Коронавірус допомагає аферистам створювати нові шахрайські схеми // Незалежна асоціація банків України : сайт. 27.03.2020. URL: https://nabu.ua/ua/uvaga-shahrayi-koronavirus-dopomagaye-aferistam.html (дата звернення: 10.05.2020).
10. Засаднюк А. Ліки «від коронавірусу» та інші шахрайства. Як легко померти через власну довірливість // УНІАН : сайт. 27.04.2020. URL: https://www.unian.ua/society/liki-vid-koronavirusu-ta-inshi-shahraystva-yak-legko-pomerti-cherez-vlasnu-dovirlivist-novini-ukrajini-10975121.html (дата звернення: 10.05.2020).

Одержано 11.05.2020