УДК 342.6; 342.7
DOI https://doi.org/10.32782/2524-0374/2021-11/44

СУЧАСНИЙ СТАН ПРОТИДІЇ РОЗПОВСЮДЖЕННЮ ПІДРОБЛЕНИХ ПРОДУКТІВ, ПОВ'ЯЗАНИХ ІЗ ПАНДЕМІЄЮ COVID-19

CURRENT STATE OF COMBATING COUNTERFEITS RELATED TO THE COVID-19

Коваль О.М., к.ю.н., доцент,
доцент кафедри приватного та публічного права,
Київський національний університет технологій та дизайну

Стецюра І.Р., студент IV курсу
Науковий інститут права та сучасних технологій навчання
Київського національного університету технологій та дизайну

У статті автори здійснили дослідження сучасного стану протидії розповсюдженню підробок, пов'язаних із пандемією COVID-19, у її теоретичному та практичному сенсі. Актуальність дослідження зумовлена значним збільшенням таких діянь у сучасному вимірі. Проаналізовані способи розповсюдження підроблених продуктів і протидія правопорушникам, котрі прагнуть використати ситуацію з пандемією для отримання фінансової вигоди.

Зроблений висновок, що потрібно продовжувати розробляти нові моделі співробітництва та партнерства, щоб прискорити глобальні заходи з побудови цифрового світу, призначеного для захисту від небезпечного втручання правопорушників, яке становить серйозну небезпеку для здоров'я населення.

Наголошується на тому, що між правоохоронними органами й органами, котрі регулюють охорону здоров'я, необхідно налагодити координацію, яка може відігравати життєво важливу роль у забезпеченні безпеки людей і благополуччя спільнот. Зазначені вище органи повинні мати необхідні навички для боротьби із цифровою злочинністю на національному, регіональному та міжнародному рівнях. Чим суворіші правила для нещеплених, тим вищий стимул отримати підробку. В Україні було зламано базу даних Національної служби охорони здоров'я, що дозволило злочинцям запровадити неправдиву інформацію про вакцинацію у додатку Дія. Більш того, шахраї стверджують, що мають доступ до європейської бази даних вакцинованих людей European Center for Disease Prevention and Controls, а це у теорії дає їм змогу зареєструвати людину як по-справжньому вакциновану, адже не усі достатньо обізнані, щоб перевірити вебсайт, який надсилають їм правопорушники. Очевидно, що потрібно розслідувати та домагатися судового переслідування злочинців, котрі користуються громадським прагненням до вакцинації від COVID-19, і тих, хто наражає на небезпеку життя людей, яких покликані захищати вакцини.

Ключові слова: ендемічна корупція, шахрайство, підроблення сертифікатів, підроблення ПЛР тестів, кіберзлочини, кібербезпека, інновації.

In the article, the authors conducted a study of the current state of combating counterfeits related to the COVID-19 in its theoretical and practical sense. The relevance of the study is due to a significant increase in these actions in cyberspace. Methods of distribution of counterfeit products and counteraction to scammers seeking to exploit the pandemic situation for financial benefit are analyzed.

It is concluded that it is necessary to continue to develop new models of cooperation and partnership to accelerate global efforts to build a digital world designed to protect against dangerous interference by scammers posing a serious threat to public health.

It emphasizes the need for coordination between law enforcement and health regulators, which can play a vital role in ensuring the safety of people and the well-being of communities. The above authorities must have the necessary skills to combat digital crime at the national, regional, and international levels.

The stricter the rules for the unvaccinated, the higher the incentive to get a fake. Thus, in Ukraine, the database of the National Health Service was hacked, which allowed criminals to enter false information about vaccination in the Appendix Action. Moreover, fraudsters claim to have access to the European Vaccination Database, the European Center for Disease Prevention and Control, which, in theory, allows them to register people as genuinely vaccinated, but not all are necessary for verification to verify a website that is to him offenders. Clearly, there is a need to investigate and prosecute criminals who use the public's desire to be vaccinated against COVID-19 and those who endanger the lives of those who are called to protect vaccines.

Key words: endemic corruption, scam, certificate fraud, cybercrime, cybersecurity, innovation.

Актуальність обраної теми зумовлена тим, що із початком пандемії COVID-19 глобальний ландшафт шахрайства істотно погіршився. Оскільки доказ вакцинації стає дедалі важливішим у повсякденному житті людини, зростає попит на підробку продуктів, пов'язаних із пандемією. Цей злочин продовжує розвиватися разом із технологічним прогресом.

Як наслідок, поширення підроблених сертифікатів на вакцини ускладнює лікування потоку нових хворих. Дедалі більше і більше пацієнтів, які здаються вакцинованими та мають помірні чи тяжкі форми вірусу, визнають, що вони не вакциновані. Такі підробки легко отримати та важко відстежити, вони є симптомом ендемічної корупції та свідчать про поширену недовіру до вакцин від коронавірусу.

Ще у грудні 2020 р. інтернет-користувачам стало відомо, що у мережі Darknet з'явилися сотні рекламних оголошень, які пропонують для продажу підроблені сертифікати, свідоцтва про одужання та негативні результати тестів COVID-19. Згодом шахраї почали використовувати скептицизм людей щодо вакцинації та поширювати фейки сертифікатів у соціальних мережах, спонукаючи купувати їх, що призвело до продажу підробки у популярному додатку для обміну повідомленнями Telegram.

Чим більше зростає потреба і попит, тим більше злочинці розширюють свою діяльність. Сьогодні вже виявлено, що продавці пропонують підроблені сертифікати із більшості європейських країн, таких як: Італія, Франція, Іспанія, Португалія, Німеччина, Бельгія, Нідерланди, Греція, Фінляндія, Румунія, Росія, Болгарія, Швейцарія, Австрія, Польща, Чехія, Латвія, Ірландія, Мальта, Велика Британія, Україна; Азіатсько-Тихоокеанський регіон: Австралія, Індонезія, Індія, Сінгапур, Таїланд.

Дослідники з Check Point [1] виявили нові методи, які використовують злочинці, щоб продавати більше підроблених COVID-документів. Наприклад, в Австрії вони знайшли Telegram-бота, котрий безкоштовно створює підроблені сертифікати. Все, що потрібно зробити – це заповнити відповідні поля, після чого буде надано доступ до pdf-файлу, який буде містити заповнені дані, наприклад, негативний результат ПЛР.

Згідно з іншими висновками зазначених вище дослідників додаток Telegram було визнано винним у сприянні поширенню підроблених цифрових сертифікатів COVID Європейського Союзу, а також карт вакцинації від COVID Національної служби охорони здоров'я Великої Британії (NHS) і Центру США з контролю та профілактики захворювань (CDC). Сертифікати на вакцини COVID, поширювані через додаток Telegram, виявилися більш доступними, ніж у мережі Darknet, внаслідок чого кількість продавців збільшилася із 1 000 у серпні 2021 р. до приблизно 10 000 у вересні.

Згідно з даними Irish Times [2] в Ірландії також зафіксовані факти підроблення документів COVID-19. Особи, які не завершили процес вакцинації, хочуть подорожувати без обмежень, пов'язаних із коронавірусом.

Так само, як і офіційна форма карти вакцинації, сертифікат, куплений у правопорушника, містить унікальний QR-код, що показує ім'я власника під час його сканування. Крім цифрової версії, видається також ірландський паспорт HSE у друкованому вигляді, який не можна відрізнити від оригінальної форми документа.

Більш того, шахраї стверджують, що мають доступ до європейської бази даних вакцинованих людей European Center for Disease Prevention and Controls, а це у теорії дає їм змогу зареєструвати людину як по-справжньому вакциновану, адже не усі достатньо обізнані, щоб перевірити веб-сайт, який надсилають їм правопорушники. Справа у тому, що URL-адреса була вбудована в QR-код, отриманий від продавця. Отже, QR-код покаже посилання на підроблену європейську базу даних.

Як з'ясувалося на початку листопада, у Європейському Союзі стався витік цифрового ключа, який використовується для підпису та перевірки сертифікату COVID-19. Це призвело до поширення в Інтернеті декількох кодів підроблених сертифікатів COVID-19. Кожен, хто отримав код або бачив його на різних інтернет-майданчиках, міг відсканувати його та побачити [3].

Вважається, що ті, хто незаконно використовував систему, видавали підроблені сертифікати на імена вигаданих персонажів – Міккі Мауса, Губки Боба – та на засновника нацистської партії Адольфа Гітлера. Всі ці документи були визнані офіційними урядовими додатками, а це означає, що вони були повністю дійсними у разі, якщо вони мали бути використані для в'їзду в будь-яку із країн-членів Європейського Союзу.

Особи, котрі сканували код за допомогою італійської Verifica C19, могли побачити назву сертифікату, на якому було написано «Гітлер Адольф», а також дату народження, однак незабаром після того, як кілька людей повідомили про QR-код, закритий ключ, що використовувався для перевірки так званої перепустки Гітлера та двох інших перепусток, був визнаний недійсним.

Слід відзначити, що підроблені сертифікати можуть заподіяти незручності у поїздках власникам цифрового сертифікату COVID-19 ЄС, оскільки дійсність сертифікатів нині ставиться під сумнів.

За даними Федеральної торгової комісії США (FTC), у 2020 р. було подано близько 205 000 повідомлень про шахрайство, пов'язаних із COVID-19, що склало збитки на суму 145 млн доларів [4]. Зловмисники створюють додатки з такими назвами, як «вакцина», «COVID», «сертифікат», «паспорти вакцини», «карти вакцини» тощо і публікують оголошення про продаж сертифікатів COVID-19. Така статистика обурює та спонукає до рішучих дій проти поширення підроблених тестів на коронавірус і свідоцтв про вакцинацію.

Наприклад, в Україні Уряд погодив ініційований МОЗ законопроєкт про кримінальну відповідальність за продаж і користування підробленими COVID-сертифікатами. За використання підроблених COVID-сертифікатів українцям загрожує штраф до 34 тис. гривень або до двух років обмеження волі; медпрацівникам, що вносять неправдиві відомості у бази даних, – штраф до 68 тис. гривень або до двух років обмеження волі та позбавлення права обіймати посаду; за виготовлення та продаж підроблених COVID-сертифікатів – штраф до 170 тис. гривень або позбавлення волі до трьох років [5].

У Сполучених Штатах Америки деякі закони, такі як шахрайство з використанням телеграфних і поштових повідомлень, передбачають покарання у розмірі до 250 000 доларів США і тюремне ув'язнення терміном на 20 років за кожен електронний лист, відвідування веб-сайту, дзвінок або посилку, відправлену в рамках схеми [6]. Подеколи ці збори можуть складатися так, що людині, котра відправила електронного листа, буде загрожувати 60 років тюремного ув'язнення і штраф у розмірі 750 000 доларів, але на практиці закон дає прокурорам і суддям величезну свободу дій щодо того, як звинувачувати і засуджувати подібних правопорушників. Зазвичай судді враховують ступінь заподіяної шкоди або вартість речі, яка була придбана помилково. У разі підроблених COVID-сертифікатів вони шукають схожий прецедент у вітчизняній практиці, після чого вирішують ступінь покарання до певної особи.

Чим суворіші правила для нещеплених, тим вищий стимул отримати підробку.

В Україні було зламано базу даних Національної служби охорони здоров'я, що дозволило злочинцям запровадити неправдиву інформацію про вакцинацію у додатку Дія.

Згідно з висновками СБУ [7] шахрайство організували сімейні лікарі місцевого медичного закладу. Їхній спільник, місцевий житель шукав клієнтів через мобільний додаток. Отримавши передоплату, фізична особа передала дані лікарям для надання фальшивих довідок. Медичний персонал вніс неправдиві дані про вакцинацію до національної бази даних охорони здоров'я.

Розслідування встановило, що люди насправді не були вакциновані, проте лікарі втручалися у сервісний додаток e-gov, щоб ввести у них хибні дані.

Нині у слідчих органах багатьох країн ведеться безліч справ за фактом виготовлення фальшивих довідок про вакцинацію. Проблема ускладнюється тим, що деякі медичні працівники виступають проти вакцини від коронавірусу та свідомо стають співучасниками протизаконних схем. Їхня роль полягає у підробленні аналізів. Так, у Латвії прокуратура зупинила протиправні дії медсестри. Вона брала мазок із носа та горла і відправляла ім'я іншої людини до лабораторії, щоб клієнт міг отримати негативний результат і виїхати за кордон.

Нам вдалося виділити такі процедури придбання фальшивих сертифікатів: клієнтів направляють до конкретного співробітника медичного пункту, який просто імітує вакцинацію. Вакцина вводиться у ватному тампоні або зовсім не вводиться, така практика має неофіційну назву «вакцина у раковину». Також є окремі випадки, коли у плече вводять фізіологічний розчин, після чого людина отримує довідку про вакцинацію.

Люди з підробленими свідченнями про вакцинацію вже зареєстровані у системі як повністю вакциновані. Щоб отримати вакцинацію «офіційно», їм доведеться почекати, доки вони не отримають право на третю ревакцинацію, хоча насправді це буде їхня перша вакцинація.

Як наслідок, у лікарнях аналізуються випадки тяжкого захворювання пацієнтів, котрі були вакциновані. Під час тестування на антитіла у вакцинованих пацієнтів стає відомо, що вони відсутні. Якщо антитіл немає, цей випадок додають у підозрілі.

Таким чином, Уряд Латвії виявив 17 підозрілих випадків у вересні 2021 р. Дані за жовтень зі значним збільшенням кількості госпіталізованих пацієнтів із COVID-19 ще не зібрані, але LTV зазначає, що кількість підозрілих випадків буде щонайменше вдвічі вищою.

У таких випадках, перш ніж ухвалити рішення про відміну довідки, лікарі повинні спочатку з'ясувати, чому немає антитіл. Для анулювання сертифіката необхідно зібрати докази його хибності. Нині поліції Латвії вдалося домогтися анулювання приблизно 30 довідок.

У сучасному вимірі цієї проблематики зазначимо таке. Кіберзлочинці створюють незаконні веб-сайти, видаючи себе за законні національні або світові організації, які

пропонують попередні замовлення на вакцини проти вірусу COVID-19. Загалом такі веб-сайти пропонують платежі у біткойнах та інші способи обробки платежів.

Мережі, що стоять за цими злочинами, мають глобальні амбіції. Жодна країна чи регіон не можуть боротися із цим видом злочинів самотужки.

Підроблені веб-сайти, які використовують логотипи товарних знаків великих фармацевтичних компаній, котрі виробляють схвалені вакцини проти COVID-19, підозрюються у тому, що вони використовують атаки фішингу й обманюють жертв, прикриваючись фондом благодійних пожертвувань.

Люди не лише відкривають свої комп'ютери для кібератак у разі спроби придбати передбачувані вакцини проти COVID-19 в Інтернеті, а й ризикують отримати крадіжку їхніх особистих даних.

Наголошуємо на тому, що схвалені вакцини зараз недоступні для продажу через Інтернет. Будь-яка вакцина, що рекламується на веб-сайтах або у Darknet, не є законною, вона не протестована і може бути небезпечною.

Будь-яка людина, котра купує таку вакцину, наражає себе на ризик і, швидше за все, віддає свої гроші організованій злочинності.

У грудні 2020 р. HIS [8] захопило три веб-сайти, які нібито належать біотехнологічним компаніям, що розробляють ліки від вірусу COVID-19. Натомість вони використовувалися для збирання особистої інформації осіб, які відвідують сайти, з метою використання інформації у злочинних цілях, включаючи шахрайство, фішингові атаки та розгортання шкідливих програм.

Атаки шкідливих програм також проводилися проти лікарень, лабораторій, органів місцевого самоврядування та інших цілей, віддалено блокуючи комп'ютерні системи та вимагаючи оплати за їхнє звільнення.

Враховуючи необхідність глобального реагування на ці види шахрайства з використанням кіберзлочинів і фінансових злочинів, Інтерпол створив у 2020 р. Глобальну цільову групу з фінансових злочинів (IGFCTF) [9] із країнами-членами з метою розширення міжнародного співробітництва й інновацій із партнерами з державного та приватного секторів.

Із приводу цього 11 листопада 2021 р. була проведена спільна 9-та конференція Європолу й Інтерполу, на якій обговорювалися інновації для прискорення боротьби проти кіберзлочинності.

Конференція щодо кіберзлочинності завершилася закликом розробити інноваційні рішення для правоохоронних органів, щоб активізувати розслідування кіберзлочинів і допомогти країнам використовувати цифрові докази.

Зі звіту конференції нам вдалося дізнатися, що правоохоронні органи повинні мати необхідні навички для боротьби із цифровою злочинністю на національному, регіональному та міжнародному рівнях, а також цілеспрямоване і спеціалізоване нарощування потенціалу, орієнтованого на інновації у роботі поліції.

Обговорення показали, як соціальні та технологічні досягнення можуть дозволити поліції боротися з кіберзлочинністю за допомогою новаторських рішень, таких як розшифрування доказів, законно одержаних внаслідок кримінальних розслідувань, і роль лабораторій в інноваціях правоохоронних органів.

Оскільки злочинні угруповання виробляють, розповсюджують і продають підроблені вакцини, ризики для населення очевидні: вони можуть включати купівлю продукту, який не тільки не захищає від COVID-19, але й становить серйозну небезпеку для здоров'я у разі проковтування або ін'єкції. Такі продукти не тестуються, не регулюються та не перевіряються на безпеку.

Виходячи з вищезазначеного, слід зауважити, що для того, щоб запобігти таким незаконним діянням, потрібно розробляти нові глобальні моделі співробітництва та партнерства, оскільки кіберзлочинність – це глобальна загроза, яка потребує глобальної відповіді.

Оскільки деякі вакцини COVID-19 ще не затверджені, забезпечення безпеки ланцюжка постачання та виявлення незаконних веб-сайтів, що продають підроблені продукти, матимуть важливе значення.

Необхідність координації між правоохоронними органами й органами, котрі регулюють охорону здоров'я, також відіграватиме життєво важливу роль у забезпеченні безпеки людей та благополуччя спільнот.

Отже, справжні медичні сертифікати не продаються через Інтернет. Той, хто пропонує продати такий документ через Інтернет, явно робить це незаконно. Уповноважені органи повинні стежити та добросовісно керувати центральним сховищем COVID-сертифікатів і ПЛР-тестів. Зазначені документи повинні оброблятися та зашифровуватися безпечним засобом відповідними офіційними органами у кожній країні, а також повинні бути QR-коди, які можна сканувати для цілей аутентифікації.

Законні вакцини не продаються. Вони суворо контролюються та розподіляються національними регулюючими органами у сфері охорони здоров'я. Підроблені вакцини загрожують здоров'ю споживачів, котрих обманюють правопорушники, на жаль, такі особи прагнуть використати ситуацію з пандемією для отримання фінансової вигоди. Очевидно, що потрібно розслідувати та домагатися судового переслідування злочинців, які користуються громадським прагненням до вакцинації від COVID-19, і тих, хто наражає на небезпеку життя людей, котрих покликані захищати вакцини.

Крім того, було би доречним розширити міжнародне співробітництво у боротьбі з підробленням вакцин, COVID-сертифікатів і тестів ПЛР, адже через мережу Інтернет інформація стає доступною для всіх країн.

ЛІТЕРАТУРА

1. Check Point Blog: Black market for fake vaccine certificates booms. URL: https://blog.checkpoint.com/ (дата звернення 01.10.2021).
2. The Irish Times: Crime & Law: Fake Irish vaccine passports for sale on dark web. URL: https://www.irishtimes.com/news/crime-and-law/fake-irish-vaccine-passports-for-sale-on-dark-web-for-350-1.4722949 (дата звернення: 20.11.2021).
3. Schengenvisainfo News: EU Investigates Hacking of COVID Digital Certificates Gateway, After 'Adolf Hitler Certificate' Was Generated. URL: https://www.schengenvisainfo.com/news/eu-investigates-hacking-of-covid-digital-certificates-gateway-after-adolf-hitler-certificate-was-generated/ (дата звернення: 17.11.2021).
4. Federal Trade Commission: Coronavirus (COVID-19) Pandemic: The FTC in Action. URL: https://www.ftc.gov/coronavirus (дата звернення 10.10.2021).
5. Міністерство Охорони Здоров'я України: МОЗ, Мінцифра та Кіберполпротидіють поширенню підроблених COVID-сертифікатів. URL: https://moz.gov.ua/ (дата звернення 12.10.2021).
6. Department of Justice: Criminal: Mail fraud and wire fraud. URL: https://www.justice.gov/jm/jm-9-43000-mail-fraud-and-wire-fraud (дата звернення 11.10.2021).
7. Security Service of Ukraine: SSU dismantles a scheme to fake COVID certificates. URL: https://ssu.gov.ua/en/novyny/ (дата звернення: 19.11.2021).
8. U.S. Immigration and Customs Enforcement: HSI investigation results in seizure of 3 domain names purporting to be biotechnology company websites with COVID-19 treatments. URL: https://www.ice.gov/news/releases/hsi-investigation-results-seizure-3-domain-names-purporting-be-biotechnology-company (Дата звернення: 25.11.2021).
9. Interpol: Online vaccine scams: INTERPOL and Homeland Security Investigations issue public warning. URL: https://www.interpol.int/News-and-Events/News/2021/Online-vaccine-scams-INTERPOL-and-Homeland-Security-Investigations-issue-public-warning (дата звернення: 17.11.2021).