Соціально-правові студії. 2021. Випуск 3 (13). С. 68-76
Social & Legal Studios. 2021. Issue 3 (13). P. 68-76

UDC (УДК) 004.056.53:351.746.2
JEL Classification: K 30

Шинкарук Олег Миколайович,
доктор технічних наук, професор, проректор
Львівського державного університету внутрішніх справ
(Львів, Україна)
e-mail: shincaruk@ukr.net
ORCID ID: 0000-0003-4499-8282

Сеник Володимир Васильович,
кандидат технічних наук, доцент,
завідувач кафедри
інформаційного та аналітичного забезпечення
діяльності правоохоронних органів
Львівського державного університету внутрішніх справ
(Львів, Україна)
e-mail: v.v.senyk@gmail.com
ORCID ID: 0000-0002-0428-6443

Зачек Олег Ігорович,
кандидат технічних наук, доцент,
доцент кафедри
інформаційного та аналітичного забезпечення
діяльності правоохоронних органів
Львівського державного університету внутрішніх справ
(Львів, Україна)
e-mail: zachekoi@gmail.com
ORCID ID: 0000-0002-4846-5718

Магеровська Тетяна Валеріївна,
кандидат фізико-математичних наук, доцент,
доцент кафедри
інформаційного та аналітичного забезпечення
діяльності правоохоронних органів
Львівського державного університету внутрішніх справ
(Львів, Україна)
e-mail: magerovskat@gmail.com
ORCID ID: 0000-0001-6763-4321

СТАН ТА ОСОБЛИВОСТІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ В УМОВАХ ПАНДЕМІЇ COVID-19

Анотація. Проаналізовано стан кібернетичної безпеки в Україні, який виник унаслідок розвитку пандемії COVID-19. Визначено головні причини зростання кіберзлочинів та їх основні види. За результатами аналізу статистичних даних, аналітичних матеріалів, міжнародного досвіду окреслено напрями нормативно-правового й організаційно-технічного характеру щодо вдосконалення заходів із протидії кіберзлочинності. Також розроблено окремі рекомендації щодо боротьби з цим суспільно небезпечним явищем.

Ключові поняття: протидія кіберзлочинності, пандемія COVID-19, кібербезпека, види кіберзлочинів, нормативно-правові та організаційно-технічні напрями протидії кіберзлочинності.

Shynkaruk Oleg,
Doctor of Tehnical Sciences,
Professor, Vice-rector,
Lviv State University of Internal Affairs
(Lviv, Ukraine)
e-mail: shincaruk@ukr.net
ORCID ID: 0000-0003-4499-8282

Senyk Volodymyr,
PhD (Technics), Associate Professor,
Head of the Department
of Information and Analytical Support
of Law Enforcement Agencies,
Lviv State University of Internal Affairs
(Lviv, Ukraine)
e-mail: v.v.senyk@gmail.com
ORCID ID: 0000-0002-0428-6443

Zachek Oleg,
PhD (Technics), Associate Professor,
Associate Professor
of the Department of Information
and Analytical Support
of Law Enforcement Agencies,
Lviv State University of Internal Affairs
(Lviv, Ukraine)
e-mail: zachekoi@gmail.com
ORCID ID: 0000-0002-4846-5718

Maherovska Tatiana,
PhD (Physical and Mathematical),
Associate Professor, Associate Professor
of the Department of Information
and Analytical Support
of Law Enforcement Agencies,
Lviv State University of Internal Affairs
(Lviv, Ukraine)
e-mail: magerovskat@gmail.com
ORCID ID: 0000-0001-6763-4321

STATUS AND FEATURES OF CYBER CRIME COUNTERACTION IN UKRAINE IN THE CONDITIONS OF THE COVID-19 PANDEMIC

Abstract. The paper analyzes the state of cyber security in Ukraine as a result of the COVID-19 pandemic. It is determined that the main reason for the aggravation of the situation in this area in 2020-2021 was the transition of an unprecedented number of citizens to remote working and an increase in the share of e-commerce. This situation has exacerbated existing and contributed to the emergence of new problems of legal, organizational, software and technical and other areas of cyber security in Ukraine. Based on the analysis of statistical data, analytical materials (obtained primarily from open sources of the Cyberpolice of Ukraine), international experience has shown that the COVID-19 pandemic most actively contributed to the development of such cybercrimes as: obtaining user credentials through malware distribution (usually phishing method); fraud schemes for the sale of personal protective equipment, medicines and other goods designed to prevent coronavirus (COVID-19) infection, as well as for the sale of other consumer goods; spreading misinformation and fakes in order to create panic and social instability in the state.

The conducted analysis allowed to outline the main priority areas in counteracting this socially dangerous phenomenon. Among them: the need to intensify the activities of law enforcement agencies in Ukraine in

cybercrime counteraction, to strengthen cooperation with law enforcement agencies of other countries; to create new and make amendments to existing regulatory legal acts to combat cyber threats, including on the basis of international experience and international standards; improvement of software and hardware of information and telecommunication systems; improving public awareness of the cyber security system in the country, etc.
Key concepts: counteraction to cybercrime, COVID-19 pandemic, cybersecurity, types of cybercrimes, normative-legal and organizational-technical directions of counteraction to cybercrime.

DOI 10.32518/2617-4162-2021-3-68-76

Вступ

У 2017 році Верховна Рада України ухвалила Закон України «Про основні засади забезпечення кібербезпеки в Україні» [1], зробивши спробу врегулювати суспільні відносини у кіберпросторі держави. На підставі цього документа розроблено низку підзаконних нормативних актів, які мали б сприяти підвищенню кібербезпеки загалом. Однак, незважаючи на вжиті заходи, наша держава постійно стає жертвою кібератак. Потрібно констатувати, що впродовж останніх двох років кількість кібератак, інших кіберзлочинів суттєво зросла. Однією із основних причин активізації кіберзлочинності стала пандемія COVID-19, яка розпочалася в Україні у березні 2020 року. Її прихід став благом для кіберзлочинців, насамперед, через перехід безпрецедентної кількості людей на дистанційну форму роботи. Це створило сприятливі умови для фішерів, шахраїв і розробників шкідливих програм. Підтвердженням цього є те, що лише за перші два тижні локдауну до сервісної служби кіберполіції України надійшло понад 100 звернень громадян щодо шахрайських дій під час закупівлі засобів індивідуального захисту та значна кількість звернень стосовно поширення фейкової інформації [2]. Наведені факти підтверджують те, що питання протидії кіберзлочинності нині набуло особливої актуальності.

Поверхневий огляд ситуації, яка виникла у кіберпросторі України внаслідок пандемії COVID-19, дає змогу зробити висновок, що протидія кіберзлочинам на сучасному етапі розвитку інформаційного суспільства не можлива в ізольованій, окремо взятій галузі діяльності: політичній, правовій, економічній, технічній тощо. Нинішня ситуація потребує об'єднання зусиль фахівців різних галузей для створення комплексного підходу до протидії цьому суспільно небезпечному явищу. Для розроблення та запровадження нових правових, організаційних, технічних, програмних заходів у протидії кіберзлочинності є потреба здійснити аналіз ситуації, яка виникла у кіберпросторі України внаслідок пандемії COVID-19, окреслити головні її особливості та на їх основі визначити основні напрями для подальшого вдосконалення наявних та розроблення нових підходів до протидії цим злочинам.

Аналізуючи наукові публікації у галузі протидії кіберзлочинам, захисту інформації в інформаційно-телекомунікаційних системах, зазначимо, що проблемним питанням правового, організаційного, технічного, програмного напряму в цій сфері впродовж останніх років приділено значну увагу науковців різних галузей знань. З-поміж них доречно відзначити роботи В. Ліпкана, С. Гнатюка, В. Голубєва, В. Хахановського, В. Цимбалюка та інших, у яких досліджено чимало питань законодавчої регламентації правових і організаційних напрямів захисту інформаційних ресурсів, протидії кіберзлочинам; наукові здобутки В. Бурячка, В. Дудикевича, В. Максимовича, В. Хорошка, які зробили значний вклад як в організаційний, так і в технічний аспект протидії кіберзлочинності; Я. Соколовського, Ю. Грицюка, М. Марчука та інших фахівців у галузі створення програмних засобів забезпечення кібернетичної безпеки України.

Однак, на підставі загального аналізу наукових публікацій згаданих учених та інших фахівців, експертів можемо констатувати, що у них часто не бралась до уваги можливість різкого збільшення використання інтернет-простору суспільством, яке спричинила пандемія COVID-19 і, як наслідок, створення сприятливих умов для вчинення кіберзлочинів. Сучасний стан розвитку інформаційних систем і технологій, рівень розвитку кіберзлочинності загострили наявні та спричинили виникнення нових проблем нормативно-правової регламентації організаційно-правових заходів протидії кіберзлочинності, захисту інформаційних ресурсів, інформаційно-телекомунікаційних систем, інформаційного простору держави загалом. Стала очевидною проблема відсутності системних підходів до політики кібернетичної безпеки держави. Нинішній стан кібербезпеки в Україні демонструє відсутність ефективних заходів запобігання та протидії цьому явищу, а наявні є недостатніми. Виникли й інші проблеми, зокрема, значним недоліком чинного законодавства України у галузі кібернетичної безпеки є відсутність науково обґрунтованих понять і дефініцій, а інколи і їх цілковита відсутність. Тож, зважаючи на зазначене, констатуємо, що проблем у напрямі протидії

кіберзлочинності не лише не зменшується, а радше навпаки – старі залишаються до кінця не вирішеними, а нові потребують негайного реагування.

Зрозуміло, що в межах однієї публікації не можливо дослідити всі проблемні питання, які існували та загострилися (чи виникли) внаслідок пандемії COVID-19. Однак, для їх вирішення необхідно провести попередній ґрунтовний аналіз ситуації, яка виникла у сфері протидії кіберзлочинності, та визначити основні кроки, напрями для розроблення подальших заходів у цій сфері.

Метою статті є аналіз стану кіберзлочинності в Україні, який виник унаслідок пандемії COVID-19, та визначення основних першочергових напрямів протидії цьому суспільно небезпечному явищу з урахуванням особливостей українського кіберпростору.

1. Аналіз ситуації, що виникла у кіберпросторі внаслідок пандемії COVID-19

Пандемія COVID-19 пришвидшила і так стрімкий розвиток інформаційно-телекомунікаційних систем і технологій. Перехід на дистанційні форми діяльності, зокрема і на електронну комерцію, підвищили обсяг електронних розрахунків у декілька разів. Природно, що це призвело до активізації кіберзлочинності. Нинішній її стан потрібно розглядати як зростаючу загрозу безпеці не лише для України, а й для світової спільноти загалом. А це відтак спонукає до вироблення нових адекватних заходів протидії цьому явищу в кожному із напрямів суспільних відносин у інтернет-просторі.

Нині пандемія COVID-19 загострила п'ять основних напрямів у регулюванні суспільних відносин в інтернет-просторі:

– захист приватних і персональних даних;

– регулювання електронної комерції, фінансових угод;

– забезпечення безпеки електронних платежів;

– захист інтелектуальної власності;

– протидія протиправному змісту інформації.

Таке загострення насамперед стосується регулювання нормативно-правових аспектів.

Дискусії, які проводилися на майданчиках навчальних, наукових закладів, правоохоронних структур, на жаль, змушують погодитися з висновком ситуаційного звіту Європолу *(Pandemic profiteering: how criminals exploit the COVID-19 crisis* [3]*), що базується на даних власної експертизи та* інформації, наданій державами-членами ЄС і в якому аналізуються поточні події, пов'язані з 4-ма основними сферами злочинності (кіберзлочинність, шахрайство, контрольні та контрафактні товари, організована злочинність проти власності), про те, що кількість кібератак проти установ, організацій і приватних осіб є значною і, за прогнозами, зростатиме. Цей висновок стосується не лише держав-членів ЄС, а й України. Водночас виникає ситуація, яка спрямована на створення більшої кількості різноманітних атак. Однією з таких сприятливих ситуацій є те, що дедалі більше роботодавців застосовують роботу в дистанційному режимі на постійній основі й дозволяють підключення до інформаційних систем своїх установ та організацій. Підтвердженням цього слугує заява на міжнародній конференції «Безпечний онлайн 2020: Сучасні виклики» першого заступника голови Департаменту кіберполіції Національної поліції України Сергія Кропиви про те, що кількість звернень до Департаменту кіберполіції зросла в рази через перехід у 2020 році на роботу у форматі он-лайн великої кількості громадян та компаній, внаслідок чого зросла кількість онлайн-шахрайств [4].

І така ситуація є типовою не лише для України. В згаданому звіті Європолу констатується, що кіберзлочинність зросла більше, ніж будь-яка інша злочинна діяльність. Також, згідно з даними ФБР, кількість заяв про дії кіберзлочинців зросла в 4 рази з початку пандемії COVID-19 [5].

Іншою сприятливою ситуацією для інтернет-злочинів є те, що з початком пандемії значно зростають не лише обсяги он-лайн продажів, а й сервісів, які їх надають. І простежити за ними не завжди спроможні служби, які запобігають кіберзлочинності.

2. Статистичні дані та типові випадки, що характеризують особливості стану кіберзлочинності в Україні (на підставі матеріалів кіберполіції України)

Один із прикладів швидкого реагування кіберзлочинців на ситуацію, яка виникає унаслідок пандемії COVID-19 в Україні, викладено у повідомленні прес-служби Департаменту кіберполіції України, відповідно до якого зловмисники через мережу інтернет виманюють кошти під виглядом нібито надання державних компенсаційних виплат по 8 тисяч гривень. За два тижні грудня 2020 року до кіберполіції надійшло приблизно 100 звернень потерпілих від таких схем. Зазвичай правопорушники публікують відео, де Президент України Володимир Зеленський розповідає про виплати матеріальної допомоги підприємцям у розмірі 8 тисяч гривень. У описі до відео шахраї розміщують посилання на ресурс, де нібито можна подати заявку на отримання виплати, стверджуючи, що таку матеріальну допомогу може отримати кожен. На цьому ресурсі громадянам

пропонують ввести персональні дані та номер банківської картки для зарахування грошей. Але надалі шахраї просять сплатити послуги юриста за оформлення заяви, отримання електронного підпису, проходження ідентифікації тощо, використовуючи вбудований чат-бот. У результаті громадяни не лише переказують гроші за неіснуючі послуги, а й передають персональні дані аферистам [6].

Загалом упродовж 2020 року до кіберполіції України за формою зворотного зв'язку надійшло понад 41 тисяча звернень громадян, із них понад 80% – щодо шахрайств. У 2020 році кіберполіцією у взаємодії з іншими підрозділами та структурами заблоковано майже 30 тисяч шахрайських інтернет-посилань і майже 9 тисяч фінансових операцій зловмисників [7].

За офіційними даними Департаменту кіберполіції Національної поліції України за 2020 рік, зростання кіберзлочинності з розвитком інтернет-простору особливо чітко відчулося під час пандемії COVID-19, коли в он-лайн масштабно перейшли робота, покупки, зустрічі. Впродовж 2020 року в Україні зареєстровано понад 5 000 кіберзлочинів. Оперативно затримано 106 фігурантів кримінальних проваджень [8].

Також кіберполіція України провела 10 міжнародних поліцейських операцій щодо викриття «хакерських» угруповань, які завдали збитків країнам Європейського Союзу, Великої Британії, США на суму понад 300 мільйонів доларів. Упродовж 2020 року затримано 326 осіб онлайн-шахраїв, які ошукали понад 26 тисяч громадян. Потерпілим забезпечено відшкодування майже 190 мільйонів гривень. Завдяки зусиллям правоохоронців у 2020 році врятовано 47 дітей та заарештовано 13 осіб, причетних до створення та розповсюдження порнографічного контенту за участі дітей. Припинено 62 факти порушення інтелектуальних прав [9].

Незважаючи на наведені успішні факти протидії кіберзлочинам, ситуація у цьому напрямі не поліпшується і у 2021 році. Ознайомлення громадськості зі згаданими фактами, розроблення рекомендацій кіберполіцією України для громадян як уберегтися від кібершахрайства не досягає кінцевої мети: зменшення кількості злочинів у вказаній сфері.

Показовим є один із останніх випадків, який викрила кіберполіція України на Миколаївщині. Там 18-річний онлайн-шахрай створював сторінки в одній із соціальних мереж, де продавав системи нагрівання тютюну та стіки до них, яких не мав у наявності. Від покупців шахрай отримував повну або часткову передплату за замовлення, а після того, як кошти надходили на рахунок, зловмисник блокував клієнтів та не виходив на зв'язок. У ході санкціонованого обшуку за місцем мешкання зловмисника, правоохоронці вилучили комп'ютерну техніку, мобільні телефони, на яких встановлена наявність облікових записів, що підтверджують факти злочинної діяльності, сім-карти різних операторів та банківські картки. Як з'ясували поліцейські, для своєї конспірації шахрай використовував декілька онлайн-магазинів, для створення яких спеціально реєстрував акаунти у популярній соціальній мережі, а надіслані кошти за товар скеровував на банківські картки, які були оформлені на підставних осіб. Задля того, щоб зацікавити покупців, хлопець пропонував товар за значно зниженими цінами, а тих клієнтів, які писали негативні відгуки щодо його бізнесу – видаляв і блокував. Так зловмисник у соціальній мережі ошукав понад 30 громадян із різних регіонів України. Сума спричинених ним збитків за попередніми підрахунками може сягати до 100 тисяч гривень. Зловмиснику слідчі повідомили про підозру у вчинені злочину, передбаченого ч. 2 ст. 190 КК України «Шахрайство». Санкція статті передбачає до трьох років позбавлення волі [10].

Там же у травні 2021 року співробітники відділу протидії кіберзлочинам у Миколаївській області ДКП НПУ та Первомайського районного відділу поліції припинили незаконну діяльність групи шахрайок. Зловмисниці створювали фейкові акаунти на сайтах комерційних оголошень та розміщували об'яви про продаж саджанців декоративних рослин і квітів за значно заниженими цінами. Клієнти з різних регіонів України як повну або часткову передоплату надсилали на рахунки зловмисниць, оформлені на підставних осіб, грошові кошти, після чого жінки одразу блокували їх та не виконували своїх зобов'язань. Правоохоронці встановили, що у такий спосіб зловмисниці ошукали близько 250 громадян на понад пів мільйона гривень.

У результаті слідчих дій поліцейські вилучили й направили на експертизу комп'ютерну техніку та мобільні телефони з обліковими записами, що підтверджують факти злочинної діяльності жінок, а також банківські карти та сім-картки різних мобільних операторів [11].

3. Вплив дезінформації на кіберпростір України

Значну загрозу становить поширення дезінформації та фейків через соціальні мережі насамперед країною-агресором Російською Федерацією з метою дестабілізації ситуації в Україні та світі. Згідно з дослідженнями компанії Facebook, Росія посіла перше місце як

виробник неправдивих новин з-поміж країн світу, а Україна посіла п'яте місце в цьому рейтингу. Також Україна визнана другою після США серед країн, які найбільше постраждали від зовнішніх фейків [12].

На думку Центру стратегічних комунікацій та інформаційної безпеки, п'яте місце України у рейтингу осередків дезінформації від Facebook означає, що інформаційне поле нашої держави є під значним впливом Росії із зовні та її агентів усередині України [13].

Одним із напрямів дезінформації є поширення фейків про шкідливість визнаних світових вакцин від COVID-19 з метою їх дискредитації та просування на світовий ринок російської вакцини Sputnik V. Зокрема за даними, які надає Укрінформ з посиланням на The Wall Street Journal, французька контррозвідка розслідує можливість компрометації з боку Російської Федерації вакцини від COVID американсько-німецького виробника Pfizer-BioNTech шляхом пропозиції французьким блогерам розмістити за оплату в розмірі до 2500 євро критичних матеріалів про цю вакцину в соціальних мережах [14].

Також на Всеукраїнському форумі «Україна 30. Коронавірус: виклики та відповіді», який відбувся 10 лютого 2021 року, в рамках панельної дискусії «Дезінформація і міфи про вакцинацію та COVID-19 – аналіз даних та масштаб інфодемії» повідомлено про факти формування російськими ЗМІ й українськими проросійськими медіа та блогерами негативної думки про вакцину компанії «Pfizer» шляхом перебільшення новин про летальні випадки після щеплення. А також поширення інформації про вакцину Sputnik V лише в позитивному спрямуванні [15].

4. Особливості та основні напрями вдосконалення протидії кіберзлочинам в Україні

Узагальнюючи наведені й інші приклади, статистичні дані, висновки та аналітичні доповіді експертів у цій галузі, результати аналізу стану кіберзлочинності як на міжнародному, так і на національному рівні, нами встановлено, що впродовж 2020–2021 років в Україні найпоширенішими способами вчинення злочинів у сфері кібернетичної безпеки були:

– створення та використання фейкових веб-сайтів для зараження засобів комп'ютерної техніки з метою отримання облікових даних користувачів за допомогою поширення шкідливих програм зазвичай методом фішингу;

– вимагання грошей шляхом поширення програм-вимагачів, що блокують роботу державних, наукових чи інших установ;

– атаки на об'єкти критичної інфраструктури;

– отримання доступу до мереж установ та організацій, співробітники яких працюють віддалено;

– схеми шахрайства із продажу масок, антисептиків, інших засобів індивідуального захисту, підроблених ліків для лікування чи запобігання короновірусній інфекції COVID-19;

– поширення дезінформації та фейків через фальшиві облікові записи для створення паніки та соціальної нестабільності.

Як бачимо, підвищення активності основної частини із перелічених способів учинення злочинів у сфері кібернетичної безпеки є наслідком виникнення пандемії, пов'язаної із короновірусною інфекцією COVID-19.

Аналізуючи отримані результати, а також результати інших наукових досліджень, насамперед у напрямі організаційно-правового забезпечення протидії кіберзлочинності, можемо констатувати, що:

1. Проблема протидії кіберзлочинності під час пандемії COVID-19 стає одним з пріоритетних напрямів у роботі правоохоронних структур в Україні та за її межами. Практика свідчить, що кіберзлочинність не має і не знає кордонів, тому лише спільна взаємодія правоохоронних структур різних держав здатна запобігти подальшому зростанню злочинів у цій сфері.

2. Проблеми нормативно-правової регламентації у сфері протидії кіберзлочинності, з якою стикаються правоохоронні органи України (насамперед Кіберполіція), не охоплюють увесь спектр сучасних загроз інформаційній, кібернетичній безпеці, а тому потребують як розроблення нових, так і істотного перегляду та доповнення чинних нормативно-правових актів. Для цього потрібно вивчити, визначити й узагальнити основні загрози у сфері кібернетичної безпеки держави та передбачити своєчасне розроблення нових нормативно-правових засобів для протидії цим загрозам, зокрема на основі міжнародного досвіду та міжнародних стандартів.

Частину досліджень у цьому напрямі проведено, в тому числі й авторами цієї публікації. Розроблено пропозиції та рекомендації, зокрема, які опубліковано у роботах [16–18].

3. Потребує суттєвого вдосконалення програмно-технічне забезпечення роботи інформаційних та телекомунікаційних систем, зокрема: вдосконалення операційних систем, які матимуть підвищену надійність і захищеність; розроблення апаратних засобів захисту даних, комунікаційних пристроїв, протоколів передавання даних тощо.

4. Як показує досвід, на один із передніх планів виходить питання поліпшення інформування суспільства про систему забезпечення

кібернетичної безпеки як на державному, так і на індивідуальному рівні, підвищення комп'ютерної грамотності населення.

5. І, зрештою, є необхідність створення на базі закладів вищої освіти зі специфічними умовами навчання системи підготовки висококваліфікованих фахівців у сфері протидії кіберзлочинності та у сфері проєктування, адміністрування інформаційно-телекомунікаційних систем.

Висновки

Узагальнюючи результати нашого дослідження, можемо зробити висновок, що настання пандемії COVID-19 є причиною активізації кіберзлочинності внаслідок переходу суспільства на дистанційну форму роботи та значної частки торгівлі у мережу інтернет. Така ситуація загострила наявні та сприяла виникненню нових проблем правового, організаційного, програмно-технічного й інших напрямів забезпечення кібернетичної безпеки в Україні.

Наведені у роботі приклади, аналіз статистичних даних, аналітичних матеріалів, міжнародного досвіду показали, що пандемія COVID-19 найактивніше сприяла розвитку таких видів кіберзлочинів, як: отримання облікових даних користувачів за допомогою поширення шкідливих програм, зазвичай методом фішингу; схем шахрайства зі продажу як засобів індивідуального захисту, медикаментів, інших товарів, що призначені для запобігання короновірусній інфекції COVID-19, так і з продажу інших товарів народного вжитку; поширення дезінформації та фейків із метою створення паніки та соціальної нестабільності.

Проведений аналіз дав змогу окреслити основні першочергові напрями у протидії цьому суспільно небезпечному явищу, з-поміж них: необхідність активізувати діяльність правоохоронних структур в Україні у протидії кібезлочинності, посилення взаємодії з правоохоронними структурами інших держав; створення нових і доповнення чинних нормативно-правових актів для протидії кіберзагрозам, зокрема на основі міжнародного досвіду та міжнародних стандартів; удосконалення програмно-технічного забезпечення роботи інформаційних та телекомунікаційних систем; поліпшення інформування суспільства про систему забезпечення кібернетичної безпеки тощо.

Лише комплексний підхід до вирішення питання забезпечення кібернетичної безпеки в державі сприятиме зниженню кількість злочинів у аналізованій сфері, а також дасть змогу підвищити ефективність заходів щодо їх розкриття.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 року № 2163-VIII. База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 30.05.2021).
2. Кіберполіція розповідає про типові випадки шахрайства під час коронавірусу. Офіційний сайт кіберполіції України. 25.03.2020. URL: https://cyberpolice.gov.ua/article/kiberpolicziya--rozpovidaye-pro-typovi-vypadky-shaxrajstva-pid-chas-koronavirusu-1820/ (дата звернення: 11.03.2021).
3. Pandemic profiteering: how criminals exploit the COVID-19 crisis. *Report of Europol* from 27 March 2020. URL: https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis (дата звернення: 07.03.2021).
4. В Україні зросла кількість кібершахрайств через перехід на роботу онлайн. *Укрінформ.* 19.01.2021. URL: https://www.ukrinform.ua/rubric-society/3173812-v-ukraini-zrosla-kilkist-kibersahrajstv-cerez-perehid-na-robotu-onlajn.html (дата звернення: 11.04.2021).
5. Геннадій Андрощук. COVID-19: вплив на електронну комерцію. *Юридична Газета*. 20.05.2020. URL: https://yur-gazeta.com/publications/practice/medichne-pravo-farmacevtika/covid19-vpliv-na-elektronnu-komerciyu.html (дата звернення: 07.04.2021).
6. Вісім тисяч кожному: в інтернеті шахраї «виплачують» карантинні. *Укрінформ*. 14.12.2020. URL: https://www.ukrinform.ua/rubric-society/3154421-visim-tisac-koznomu-v-interneti-sahrai-viplacuut-karantinni.html (дата звернення: 11.04.2021).
7. У 2020 році до кіберполіції надійшло понад 30 тисяч звернень щодо шахрайства в Інтернеті. *Офіційний сайт кіберполіції України.* 15.01.2021. URL: https://cyberpolice.gov.ua/news/u--roczi-do-kiberpolicziyi-nadijshlo-ponad--tysyach-zvernen-shhodo-shaxrajstva-v-interneti-8412/ (дата звернення: 11.04.2021).
8. У 2020-му Нацполіція викрила понад 5 000 кіберзлочинів. Офіційний сайт кіберполіції України. 29.01.2021. URL: https://cyberpolice.gov.ua/news/u--mu-naczpolicziya-vykryla-ponad---kiberzlochyniv-26/ (дата звернення: 11.04.2021).
9. У 2020 році кіберполіція провела 10 міжнародних поліцейських операцій із викриття «хакерських» угруповань – Олександр Гринчак. *Офіційний сайт кіберполіції України*. 05.02.2021. URL: https://cyberpolice.gov.ua/news/u--roczi-kiberpolicziya-provela--mizhnarodnyx-policzejskyx-operaczij-iz-vykryttya-xakerskyx-ugrupovan--oleksandr-grynchak-5855/ (дата звернення: 11.02.2021).

10. На Миколаївщині кіберполіція викрила молодика на інтернет-шахрайствах з продажем сучасних систем нагрівання тютюну. URL: https://cyberpolice.gov.ua/news/na-mykolayivshhyni-kiberpolicziya-vykryla-molodyka-na-internet-shaxrajstvax-z-prodazhem-suchasnyx-system-nagrivannya-tyutyunu-5095/ (дата звернення: 30.05.2021).
11. На Миколаївщині кіберполіція викрила двох жінок в Інтернет-шахрайстві неіснуючими товарами. URL: https://cyberpolice.gov.ua/news/na-mykolayivshhyni-kiberpolicziya-vykryla-sxemu-onlajn-shaxrajok-iz-prodazhem-cherez-internet-dekoratyvnyx-roslyn-6547/ (дата звернення: 30.05.2021).
12. Facebook назвав найбільших «виробників» фейків, Росія – на першому місці. *Укрінформ*. 27.05.2021. URL: https:// https://www.ukrinform.ua/rubric-world/3253944-facebook-nazvav-najbilsih-virobnikiv-fejkiv-rosia-na-persomu-misci.html (дата звернення: 30.05.2021).
13. «Зради немає»: фахівці пояснили, чому Україна опинилася в ТОП-5 рейтингу Facebook про фейки. *Укрінформ*. 27.05.2021. URL: https://www.ukrinform.ua/rubric-society/3253961-zradi-nemae-fahivci-poasnili-comu-ukraina-opinilasa-v-top5-rejtingu-facebook-pro-fejki.html (дата звернення: 30.05.2021).
14. Прохоренко Є. Поширення дезінформації та фейків про вакцинацію має на меті ослаблення України – експерти. *Аптека online.* 2021. 22 лют. № 7. URL: https://www.apteka.ua/article/584491 (дата звернення: 30.05.2021).
15. У Франції розслідують, чи платила Росія блогерам за наклеп на вакцину Pfizer – WSJ. *Укрінформ*. 26.05.2021. URL: https://www.ukrinform.ua/rubric-world/3253086-u-francii-rozsliduut-ci-platila-rosia-blogeram-za-naklep-na-vakcinu-pfizer-wst.html (дата звернення: 30.05.2021).
16. Зачек О. І., Дмитрик Ю. І. Застосування профайлінгу для протидії кіберзлочинності. *Соціально-правові студії* : науково-аналітичний журнал / гол. ред. О. Балинська. Львів : ЛьвДУВС, 2020. Вип. 4 (10). С. 94–100.
17. Zhyvko Z., Rudyi T., Senyk V., Kucharska L. Legal basis of ensuring cyber security of Ukraine. *Problems and ways of eliminating. Economics, Finance and Management Review*. 2020. Is. 2. P. 82–91.
18. Живко З. Б., Рудий Т. В., Сеник В. В., Родченко С. С. Проблеми нормативно-правової бази забезпечення кібербезпеки в Україні: стан і перспективи. *Соціально-правові студії* : науково-аналітичний журнал / гол. ред. О. Балинська. Львів : ЛьвДУВС, 2020. Вип. 3 (9). С. 18–25.

References

1. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 05 zhovtnia 2017 roku № 2163-VIII. Baza danykh «Zakonodavstvo Ukrainy» / VR Ukrainy [On the basic principles of cybersecurity of Ukraine: Law of Ukraine of October 5, 2017 № 2163-VIII. Database «Legislation of Ukraine» / Verkhovna Rada of Ukraine]. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukr.].
2. Kiberpolitsiia rozpovidaie pro typovi vypadky shakhraistva pid chas koronavirusu. Ofitsiinyi sait kiberpolitsii Ukrainy. 25.03.2020 [Cyberpolice reports typical cases of coronavirus fraud. Official site of the cyberpolice of Ukraine. 03/25/2020]. Retrieved from https://cyberpolice.gov.ua/article/kiberpolicziya--rozpovidaye-pro-typovi-vypadky-shaxrajstva-pid-chas-koronavirusu-1820 [in Ukr.].
3. Pandemic profiteering: how criminals exploit the COVID-19 crisis. Report of Europol from 27 March 2020. Retrieved from https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis.
4. V Ukraini zrosla kilkist kibershakhraistv cherez perekhid na robotu onlain. Ukrinform. 19.01.2021 [In Ukraine, the number of cyber frauds has increased due to the transition to work online. Ukrinform. 01/19/2021]. Retrieved from https://www.ukrinform.ua/rubric-society/3173812-v-ukraini-zrosla-kilkist-kibersahrajstv-cerez-perehid-na-robotu-onlajn.html [in Ukr.].
5. Hennadii Androshchuk. COVID-19: vplyv na elektronnu komertsiiu. Yurydychna Hazeta. 20.05.2020 [Gennady Androschuk. COVID-19: impact on e-commerce. Legal Gazette. 05/20/2020]. Retrieved from https://yur-gazeta.com/publications/practice/medichne-pravo-farmacevtika/covid19-vpliv-na-elektronnu-komerciyu.html [in Ukr.].
6. Visim tysiach kozhnomu: v interneti shakhrai «vyplachuiut» karantynni. Ukrinform. 14.12.2020 [Eight thousand each: on the Internet fraudsters «pay» quarantine. Ukrinform. 12/14/2020]. Retrieved from https://www.ukrinform.ua/rubric-society/3154421-visim-tisac-koznomu-v-interneti-sahrai-viplacuut-karantinni.html [in Ukr.].
7. U 2020 rotsi do kiberpolitsii nadiishlo ponad 30 tysiach zvernen shchodo shakhraistva v Interneti. Ofitsiinyi sait kiberpolitsii Ukrainy. 15.01.2021 [In 2020, the cyber police received more than 30,000 complaints about online fraud. Official site of the cyberpolice of Ukraine. 01/15/2021]. Retrieved from https://cyberpolice.gov.ua/news/u--roczi-do-kiberpolicziyi-nadijshlo-ponad--tysyach-zvernen-shhodo-shaxrajstva-v-interneti-8412/ [in Ukr.].

8. U 2020-mu Natspolitsiia vykryla ponad 5 000 kiberzlochyniv. Ofitsiinyi sait kiberpolitsii Ukrainy. 29.01.2021. [In 2020, the National Police uncovered more than 5,000 cybercrimes. Official site of the cyberpolice of Ukraine. 01/29/2021]. Retrieved from https://cyberpolice.gov.ua/news/u--mu-naczpolicziya-vykryla-ponad--kiberzlochyniv-26/ [in Ukr.].
9. U 2020 rotsi kiberpolitsiia provela 10 mizhnarodnykh politseiskykh operatsii iz vykryttia «khakerskykh» uhrupovan – Oleksandr Hrynchak. Ofitsiinyi sait kiberpolitsii Ukrainy. 05.02.2021. Retrieved from https://cyberpolice.gov.ua/news/u--roczi-kiberpolicziya-provela--mizhnarodnyx-policzejskyx-operaczij-iz-vykryttya-xakerskyx-ugrupovan--oleksandr-grynchak-5855/ [in Ukr.].
10. Na Mykolaivshchyni kiberpolitsiia vykryla molodyka na internet-shakhraistvakh z prodazhem suchasnykh system nahrivannia tiutiunu [In the Nikolaev area the cyberpolice exposed a new moon on the Internet frauds with sale of modern systems of heating of tobacco]. Retrieved from https://cyberpolice.gov.ua/news/na-mykolayivshhyni-kiberpolicziya-vykryla-molodyka-na-internet-shaxrajstvax-z-prodazhem-suchasnyx-system-nagrivannya-tyutyunu-5095/ [in Ukr.].
11. Na Mykolaivshchyni kiberpolitsiia vykryla dvokh zhinok v Internet-shakhraistvi neisnuiuchymy tovaramy [In Nikolayevshchina the cyberpolice exposed two women in Internet fraud by non-existent goods]. Retrieved from https://cyberpolice.gov.ua/news/na-mykolayivshhyni-kiberpolicziya-vykryla-sxemu-onlajn-shaxrajok-iz-prodazhem-cherez-internet-dekoratyvnyx-roslyn-6547/ [in Ukr.].
12. Facebook nazvav naibilshykh «vyrobnykiv» feikiv, Rosiia – na pershomu mistsi. Ukrinform. 27.05.2021 [Facebook named the biggest «producers» of fakes, Russia – in the first place. Ukrinform. 05/27/2021]. Retrieved from https:// https://www.ukrinform.ua/rubric-world/3253944-facebook-nazvav-najbilsih-virobnikiv-fejkiv-rosia-na-persomu-misci.html [in Ukr.].
13. «Zrady nemaie»: fakhivtsi poiasnyly, chomu Ukraina opynylasia v TOP-5 reitynhu Facebook pro feiky. Ukrinform. 27.05.2021 [«There is no betrayal»: experts explained why Ukraine was in the TOP-5 rating of Facebook about fakes. Ukrinform. 05/27/2021]. Retrieved from https://www.ukrinform.ua/rubric-society/3253961-zradi-nemae-fahivci-poasnili-comu-ukraina-opinilasa-v-top5-rejtingu-facebook-pro-fejki.html [in Ukr.].
14. Prokhorenko, Ye. (2021). Poshyrennia dezinformatsii ta feikiv pro vaktsynatsiiu maie na meti oslablennia Ukrainy – eksperty. *Apteka online*. *Pharmacy online.* [Dissemination of misinformation and fakes about vaccination aims to weaken Ukraine – experts]. Retrieved from https://www.apteka.ua/article/584491 [in Ukr.].
15. U Frantsii rozsliduiut, chy platyla Rosiia bloheram za naklep na vaktsynu Pfizer – WSJ. Ukrinform. 26.05.2021 [France is investigating whether Russia paid bloggers for slandering the Pfizer-WSJ vaccine. Ukrinform. 05/26/2021]. Retrieved from: https://www.ukrinform.ua/rubric-world/3253086-u-francii-rozsliduut-ci-platila-rosia-blogeram-za-naklep-na-vakcinu-pfizer-wst.html [in Ukr.].
16. Zachek, O. I. & Dmytryk, Yu. I. (2020). Zastosuvannia profailinhu dlia protydii kiberzlochynnosti. *Sotsialno-pravovi studii : naukovo-analitychnyi zhurnal.* LvDUVS, [Application of profiling to combat cybercrime]. *(Socio-legal studies: scientific-analytical journal)*. Lviv : Lviv Department of Internal Affairs, 4 *(10),* 94–100 [in Ukr.].
17. Zhyvko, Z., Rudyi, T., Senyk, V. & Kucharska, L. (2020). Legal basis of ensuring cyber security of Ukraine. Problems and ways of eliminating. Economics, Finance and Management Review, 2, 82–91.
18. Zhyvko, Z. B., Rudyi, T. V., Senyk, V. V. & Rodchenko, S. S. (2020). Problemy normatyvno-pravovoi bazy zabezpechennia kiberbezpeky v Ukraini: stan i perspektyvy [Problems of normative-legal base of cybersecurity provision in Ukraine: state and prospects]. *Sotsialno-pravovi studii : naukovo-analitychnyi zhurnal (Socio-legal studies: scientific-analytical journal)*. Lviv : Lviv Department of Internal Affairs, 3 *(9),* 18–25 [in Ukr.].

Стаття: надійшла до редакції 10.06.2021
прийнята до друку 12.08.2021
The article: is received 10.06.2021
is accepted 12.08.2021