УДК 343.6
DOI https://doi.org/10.24144/2788-6018.2022.01.50

ОКРЕМІ ПРОБЛЕМНІ АСПЕКТИ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ТА ПОКАРАННЯ ЗА ПРАВОПОРУШЕННЯ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), АВТОМАТИЗОВАНИХ СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Луцький Т.М.,
доктор філософії в галузі права,
старший викладач кафедри кримінального права і кримінології
Львівського державного університету внутрішніх справ
e-mail: taras.lu@ukr.net
ORCID ID: 0000-0002-1725-4029

Пасєка О.Ф.,
кандидат юридичних наук, доцент,
доцент кафедри кримінального права і кримінології
Львівського державного університету внутрішніх справ
e-mail: alxlviv@ukr.net
ORCID ID: 0000-0002-5797-3597

Луцький Т.М., Пасєка О.Ф. Окремі проблемні аспекти кримінальної відповідальності та покарання за правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку.

У статті висвітлено окремі проблемні аспекти відповідальності за вчинення кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку, а також методологію і результати аналізу призначення судами покарання за ці злочини.

Наведено співвідношення виду і розміру покарання, що призначались судами за статтями 361, 361-1, 361-2, 362, 363, 363-1 Кримінального кодексу України. Проаналізовано призначення судами кожного із передбачених цими статтями Кримінального кодексу України видів і розмірів покарань та виокремлено тенденції з їх призначення на прикладах конкретних судових вироків. Проаналізовано усі судові вироки за 2019 рік, що містяться в Єдиному державному реєстрі судових рішень, винесених щодо злочинів передбачених статтями 361, 361-1, 361-2, 362, 363, 363-1 КК України.

Крім того, авторами було досліджено стан застосування судами як основного так і додаткового покарання у вигляді позбавлення права обіймати певні посади або займатися певною діяльністю і запропоновано шляхи для його удосконалення. Авторами виокремлено проблеми, що виникають при призначенні судами того чи іншого виду основного покарання та запропоновано можливі шляхи їх вирішення. Також висвітлено питання щодо застосування судом статей 69 та 75 КК України при призначенні покарання за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку та доцільності застосування звільнення від відбування покарання з випробовуванням або призначення більш м'якого покарання, ніж передбачено законом.

Враховуючи на важливість глибокого вивчення і дослідження проблем призначення покарання за окремі кримінальні правопорушення, в межах цього дослідження здійснено відповідний аналіз стану призначення покарання за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку.

Ключові поняття: злочин, електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі, мережі електрозв'язку, покарання.

Lutskyi T., Pasyeka O. Certain problem aspects of criminal responsibility and punishment in cases of crimes in the field of the use of electronic computing machines (computers), automated systems, computer networks, and telecommunication networks.

The article deals with the methodology and results of the analysis of court sentencing for crimes in the

field of the use of electronic computing machines (computers), automated systems, computer networks, and telecommunication networks.

The correlation of the type and amount of punishment imposed by courts under Articles 361, 361^1, 361^2, 362, 363, 363^1 of the Criminal Code of Ukraine is presented. The infliction of the types and amount of punishments by courts under these articles of the Criminal Code of Ukraine is analyzed, and tendencies of their imposition on the examples of concrete court sentences are distinguished. All court sentences for 2019 contained in the Unified State Register of Judgments rendered in respect of crimes under Articles 361, 361^1, 361^2, 362, 363, and 363^1 of the Criminal Code of Ukraine are analyzed.

In addition, the authors examine the state of application of both primary and additional punishment by courts in the form of deprivation of the right to occupy certain positions or engage in certain activities and suggest ways to improve them. The authors single out the problems that arise when courts impose one or another type of primary punishment and suggest possible ways to solve them. The issue of the application of Articles 69 and 75 of the Criminal Code of Ukraine by the court in sentencing for crimes in the field of the use of electronic computing machines (computers), automated systems, computer networks, and telecommunication networks, and the expediency of exemption from serving a probation sentence or imposing more lenient punishment than provided by law, is elucidated.

Taking into account the importance of in-depth study and investigation of the problems of imposing punishment for certain criminal offenses, within the framework of this scientific work, an appropriate analysis of the state of sentencing for crimes in the field of the use of electronic computing machines (computers), automated systems, computer networks, and telecommunication networks is carried out.

Key words: crimes, electronic computing machines (computers), automated systems, computer networks, telecommunication networks, punishment.

Вступ. Інформаційний розвиток суспільства та запровадження на державному рівні в Україні використання мережі інтернет та інших комп'ютерних систем в усіх сферах, поряд із позитивними здобутками, супроводжується і негативними явищами. Особливу занепокоєність зумовлює збільшення кількості кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (далі ЕОМ, С та КМ і МЕ), оскільки такі злочини не лише гальмують позитивні тенденції розвитку, а й завдають шкоду суспільству, державі, суб'єктам інформаційних відносин в усіх сферах господарювання та окремим громадянам.

Кримінальні правопорушення у сфері використання ЕОМ, С та КМ і МЕ (розділ XVI КК України) – це суспільно небезпечні, протиправні діяння (дія або бездіяльність), що посягають на суспільні відносини, які забезпечують контрольоване використання комп'ютерної інформації, а також забезпечують нормальну роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, вчинені суб'єктом кримінального правопорушення.

Проте, не зважаючи на небезпечність кримінальних правопорушень у сфері використання ЕОМ, С та КМ і МЕ, кількість кримінальних проваджень та судових вироків із зазначених правопорушень незначна. Це, обумовлено багатьма чинниками серед яких недосконаліть вітчизняного законодавства, висока латентність цих кримінальних правопорушень, недосконаліть засобів їх виявлення, розслідування, запобігання, недостатність спеціальних знань у працівників правоохоронних органів, які займаються виявленням та розслідуванням зазначеної категорії справ тощо.

Вказане свідчить про актуальність дослідження кримінально-правової характеристики правопорушень у сфері ЕОМ, С та КМ і МЕ.

Дослідженню питань кримінальної відповідальності за вчинення кримінальних правопорушень у сфері використання ЕОМ, С та КМ і МЕ присвячені праці українських вчених, зокрема: Д. С. Азарова, Ю. М. Батурина, М. В. Карчевського, С. А. Кузьміна, О. Е. Радутного та інших вчених.

Водночас, при всій значущості цих та інших наукових напрацювань, у судовій та слідчій практиці на сьогодні існує чимало проблем, зокрема, як щодо відмежування одного кримінального правопорушення від іншого та кваліфікації злочинів у сфері ЕОМ, С та КМ і МЕ так і щодо розбіжності в поглядах щодо призначення покарань за досліджуванні правопорушення.

Метою цієї наукової статті є аналіз окремих проблемних аспектів відповідальності та покарання за вчинення кримінальних правопорушень у сфері ЕОМ, С та КМ і МЕ та визначення шляхів подолання визначених проблем.

Виклад основних положень. На сучасному етапі розвитку суспільство стає все більше залежним від роботи комп'ютерних систем для автоматичної обробки інформації. Це стосується різних сфер діяльності людини. Усі найважливіші функції, так чи інакше, здійснюються з використанням комп'ютерів, автоматизованих систем (далі — АС) та комп'ютерних мереж і мереж електрозв'язку.

Завдяки удосконаленню комп'ютерних систем з'являються нові можливості для вчинення невідомих раніше правопорушень, а також традиційних кримінальних правопорушень новими засоба-

ми. Останнім часом в Україні наявна стійка тенденція до збільшення кількості правопорушень, учинених у сфері використання електронно-обчислювальних машин (комп'ютерів; далі — ЕОМ), АС та комп'ютерних мереж і мереж електрозв'язку (комп'ютерних кримінальних правопорушень).

1. Проблема імплементації у національне законодавство поняття «кримінальне правопорушення».

Перш ніж перейти до аналізу судової практики досліджуваних правопорушень, слід зазначити, що розділ 16 в якому вони розміщенні, із врахуванням змін внесених Закону України «Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій кримінальних правопорушень» від № 2617-VIII від 22.11.2018, який набрав чинності 01.07.2020 року отримав назву «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Однак, у цьому розділі не має жодного кримінального проступку, а усі діяння заборонені законом є злочинами відповідно до ст. 12 КК України. У цьому випадку законодавцем порушено принцип системності та логічності при побудові назви розділу, оскільки до прикладу розділ I Особливої частини КК в якому відсутні кримінальні проступки, а передбачено лише злочини має назву «Злочини проти основ національної безпеки України».

Тому, було б правильно, щоб розділ 16 Особливої частини КК мав назву «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Враховуючи, що в дослідженні мова йтиметься лише про злочини, а не про кримінальні проступки, тому словосполучення «кримінальне правопорушення» під час аналізу положень розділу XVI Особливої частини КК України не використовуватиметься.

2. Аналіз судової практики із цієї категорії кримінальних правопорушень.

В ході дослідження було проаналізовано судову практику щодо злочинів у сфері ЕОМ, С та КМ і МЕ, а саме досліджено усі судові вироки винесені судами України протягом 2019 року. Встановлено, що таких вироків винесено 68 по 102 злочинах у сфері ЕОМ (враховуючи, те, що органами досудового розслідування злочини у сфері ЕОМ часто кваліфікуються за сукупністю із іншими злочинами, розміщеними в інших розділах КК України). Оскільки злочини проти власності, проти господарської діяльності не є предметом нашого дослідження, тому в даній статистиці відображатися не будуть.

У аналізованих злочинах таке покарання як позбавлення волі призначалося в 29 випадках, однак в 27 випадках із них особу було звільнено від відбування покарання з випробовуванням та застосовано ст. 75 КК України, обмеження волі призначалося у 2 випадках та у двох із них судом застосовано ст. 75 КК України, винесено 4 виправдувальних вироків, в одному випадку особу звільнено від кримінальної відповідальності та застосовано заходи виховного характеру, а в інших 32 випадках призначено покарання у вигляді штрафу.

В 35 вироках (51,47 %) покарання призначалося на підставі угоди про визнання винуватості або угоди про примирення винного з потерпілим, ще в 14 випадках застосовувалась спеціальна конфіскація (20,59 %), в 6 випадках застосовувалась стаття 69 КК України (8,82 %) та призначалося покарання більш м'яке ніж передбачено в санкції статті.

Реальне покарання у вигляді позбавлення волі призначалося всього у двох випадках [1, 2], або 2,94 % від кількості винесених вироків, засуджених за ці злочини. В обох випадках, коли особі призначалося реальне покарання у вигляді позбавлення волі особу було засуджено за сукупністю із іншими злочинами передбаченими іншими розділами Особливої частини КК України.

Штраф призначався у 32 вироках, або 47,06 % від кількості винесених вироків за ці злочини. Виправдувальні вироки винесено у 4 випадках, що становлять 5,88 % від загальної кількості вироків.

Також, в одному випадку особу звільнено від відбування покарання без визначення його виду та розміру та застосовано примусовий захід виховного характеру, а саме передано неповнолітнього під нагляд батька на один рік [3].

Стосовно кількості винесених вироків щодо злочинів у сфері ЕОМ, С, КМ та МЕ то серед 102 злочинів у справах про які наявні вироки у ЄДРСР за 2019 рік, 46 – за ст. 361 КК, що становить 45,10 % від загальної кількості злочинів, по яких були винесені вироки у 2019 році, 23 – за ст. 361^1 КК (22,55), 14 – за ст. 361^2 КК (13,73 %), 17 – за ст. 362 КК (16,67 %), 2 – за ст. 363^1 КК (1,95 %), а також жодного вироку не винесено за ст. 363 КК України.

В Україні найбільш поширеним злочином у сфері використання ЕОМ, С, КМ та МЕ є злочин, відповідальність за який передбачено ст. 361 КК України.

Розвиток мережі Інтернет призвів до того, що однією з основних проблем користувачів став надлишок інформації. Це стосується передусім так званого «спаму», тобто масового розповсюдження попередньо не обумовлених електронних листів. Через масовий характер спам-повідомлень останні утруднюють роботу інформаційних систем і ресурсів, створюючи для них зайве перевантаження, що може бути причиною їх виходу з ладу. «Спам» також може стати носієм шкідливих програм і комп'ютерних вірусів, поширених із метою отримання доступу до комп'ютерних систем, ви-

ведення їх із ладу або отримання конфіденційної інформації.

Зокрема, вироком Приморського районного суду м. Маріуполь Донецької області від 04.04.2019 року [5], засуджено особу, за те, що вона, в період часу з 17.10.2016 по 05.03.2018 працювала у ТОВ «Дніпровська охоронна компанія «Професійний захист» на посаді інженера комп'ютерних систем.

Після звільнення із вказаного підприємства, бажаючи повернутись на колишню роботу та продемонструвати керівництву ТОВ необхідність його повернення на посаду, він, використовуючи вразливість обмеження налаштувань маршрутизаторів, вирішив заблокувати роботу підприємства шляхом здійснення DDoS-атаки, достовірно знаючи, що припинення дії атаки потребує перенаалаштування обладнання абонентів та підприємства, яке вимагатиме багато часу.

Реалізовуючи свій злочинний умисел, обвинувачений завантажив та скопіював на жорсткий диск свого ноутбуку з всесвітньої мережі Інтернет програмне забезпечення, необхідне для організації та проведення DDoS-атак під назвою «LOIC», що надавало йому можливість здійснювати DDoS-атаки на вибрані ним сервери, IP-адреси. Також він встановив на свій мобільний телефон додаток «DDOS», який може виконувати розподілену атаку виду «відмова в обслуговуванні» (ddos-атака) шляхом постійних передач на потрібні веб-сайти або IP-адреси та додаток «Ping», який також може надсилати постійні запити на потрібні IP-адреси.

30.04.2018 р., діючи умисно, за допомогою встановлених на його мобільному телефоні додатків здійснив масове розповсюдження повідомлень електрозв'язку, без попередньої згоди адресатів, в автоматизовані системи, маршрутизатори підприємства. Вказані умисні злочинні дії призвели до порушення та тимчасового припинення роботи обладнання ТОВ.

Зазначенні дії обвинувачений повторював систематично, що унеможливлювало моніторинг та не дозволяло керувати віддаленим обладнанням абонентів підприємства. Судом такі дії кваліфіковано за ч. 1 ст. 363[1] КК України, особу визнано винною та призначено покарання у вигляді двох років обмеження волі на підставі угоди про примирення.

Однією з характерних особливостей цього злочину є їхня латентність, яка спричинена небажанням користувачів мережі інформувати про них через недовіру до правоохоронних органів, а також небажанням публічно визнати слабкі місця у власних системах безпеки.

Згідно зі статистичною інформацією наявною в ЄДРСР у 2019 році суди не виносили вироків щодо злочину, передбаченого статтею 363 КК України.

Вивчення зазначеної категорії вироків засвідчило, що суди, призначаючи покарання, здебільшого дотримуються передбаченого законом принципу індивідуалізації покарання залежно від характеру і ступеня тяжкості вчиненого злочину. Однак при призначенні покарань ще мають місце недоліки, на які необхідно звернути увагу.

3. Проблеми кваліфікації та призначення покарання за злочини у сфері використання ЕОМ, С та КМ і МЕ

У деяких випадках сумнівними є рішення суду щодо призначення більш м'якого покарання, ніж передбачено законом, та звільнення осіб від відбування покарання з випробуванням. Згідно з вимогами ст. 69 КК суд може призначити більш м'яке покарання, ніж передбачено законом, лише за наявності декількох обставин (тобто не менше двох), що пом'якшують покарання та істотно знижують ступінь тяжкості вчиненого злочину, з урахуванням особи винного.

У деяких випадках суди при призначенні покарання не враховують, що від конфіскації майна як виду додаткового покарання необхідно відрізняти спеціальну конфіскацію, яка полягає у вилученні у засудженого програмних або технічних засобів, за допомогою яких було вчинено злочин. Оскільки законом не передбачено можливості звільнення від такої конфіскації, спеціальна конфіскація має застосовуватися судами незалежно від застосування статей 69, 75 КК.

Труднощі також виникають при кваліфікації дій винних осіб, коли несанкціоноване втручання в роботу ЕОМ, АС, КМ здійснювалося з корисливих мотивів із метою викрадення чи заволодіння чужим майном. Зазначені дії суди помилково кваліфікують лише за статтями КК, в яких передбачено відповідальність за вчинення «комп'ютерних» злочинів, однак не кваліфікують такі діяння за іншими статтями КК України.

Суди при розгляді справ цієї категорії допускають помилки при кваліфікації дій винних осіб, які, маючи право доступу до комп'ютерної інформації, вчинювали щодо неї несанкціоновані дії.

Так, до прикладу, вироком Солом'янського районного суду м. Києва від 08.11.2019 року особу засуджено за вчинення злочинів передбачених ч. 1 ст. 182, ч. 2 ст. 361 КК України, який він вчинив за наступних обставин: обвинувачений з 10 листопада 2017 року працював на посаді ст. інспектора відділу розшуку та опрацювання матеріалів ДТП управління патрульної поліції у м. Києві Департаменту патрульної поліції. Відповідно до своїх посадових обов`язків має доступ до інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп`ютерах) та автоматизованих системах, створена та захищена відповідно до чинного законодавства та може використовуватися лише у службової діяльності у порядку передбаченому законом, у тому числі до відомостей, що містяться в інформаційно-телекомунікаційній

системі «Інформаційний портал Національної поліції України».

На початку 2019 року, особа досудове розслідування щодо якої здійснюється в іншому кримінальному провадженні, (далі Особа 1) з метою власного збагачення, вирішив вчинити протиправну дію, а саме зібрати та надати за грошову винагороду зацікавленим особам конфіденційну інформацію, що зберігається та оброблюється в електронних інформаційних системах, та є інформацією з обмеженим доступом. Для досягнення вказаної мети, Особа 1 вирішила вчинити ряд послідовних протиправних дій, спрямованих на незаконне збирання, зберігання та поширення конфіденційної інформації про осіб, зокрема, анкетних даних цих осіб (прізвище, ім`я, по-батькові, дата та місце народження тощо), реквізитів їх важливих особистих документів - паспортів громадянина України, відомостей щодо місця реєстрація та/або проживання цих осіб, номерів особистих засобів зв`язку, якими вони користуються, а також іншої інформації, яка могла б цікавити потенційних замовників збирання такої інформації. Розуміючи, що зазначені відомості є інформацією з обмеженим доступом, яка зберігається в ЕОМ та автоматизованих системах, створена та захищена відповідно до чинного законодавства та може використовуватися лише у службової діяльності та у порядку, передбаченому законом, Особа 1 вирішила підшукати та залучити до вчинення злочину осіб, які в силу виконання ними службових обов'язків мали б доступ до такої інформації та могли б зібрати та передати її за грошову винагороду.

Особа 1, маючи на меті подальше систематичне збирання, зберігання та поширення за грошову винагороду конфіденційної інформації про осіб, що міститься у вказаній базі даних, вирішила залучити обвинуваченого до своєї злочинної діяльності, відвівши йому роль особи, що здійснюватиме безпосереднє збирання конфіденційної інформації з ІТС «ІП НПУ», її зберігання та передачу Особі 1.

Згідно розробленого плану, обвинувачений мав отримувати грошові кошти в сумі 300 грн. за надання інформації, що міститься у ІТС «ІП НПУ», щодо однієї особи. На вказану пропозицію обвинувачений погодився.

Обвинувачений, діючи відповідно до раніше розподілених ролей, розуміючи, що не має відповідних законних підстав для збирання, зберігання та поширення конфіденційної інформації щодо інших осіб, використовуючи наданий йому доступ до ІТС «ІП НПУ» перебуваючи за місцем проходження служби з робочого комп`ютера зробив низку пошукових запитів, внаслідок чого зібрав з вказаної системи конфіденційну інформацію.

Зібрану інформацію обвинувачений, реалізуючи свій злочинний умисел, зберіг в своєму мобільному телефоні в текстовому вигляді, та в подальшому за допомогою мобільного додатку - месенджера «Telegram» передав Особі 1, тим самим поширивши її. Особа 1, в свою чергу, зберегла вказану інформацію на власному мобільному телефоні та з власного рахунку, перерахувала грошові кошти у сумі 300 грн. на банківський рахунок обвинуваченого, в рахунок сплати за надання останнім вищевказаної конфіденційної інформації.

Згодом, за допомогою мобільного додатку - месенджера «Telegram» отримала замовлення щодо отримання інформації з баз даних Національної поліції України та ОВС України щодо іншої особи, а на її банківський рахунок, надійшли грошові кошти в розмірі 9552 грн в рахунок сплати за отримання конфіденційної інформації, в тому числі, за отримання такої інформації з ІТС «ІП НПУ».

В той же день, Особа 1 відповідно до раніше досягнутих домовленостей, з власного рахунку, перерахувала грошові кошти у сумі 300 грн. на банківський рахунок обвинуваченого в рахунок сплати за надання останнім вищевказаної конфіденційної інформації, тим самим забезпечивши відповідно до розробленого злочинного плану надходження та розподіл грошових коштів, отриманих від замовника вчинення злочину.

Вказані злочинні дії обвинувачений здійснював систематично протягом певного періоду часу, за що отримував грошові кошти в сумі 300 гривень за інформацію відносно однієї особи.

Правоохоронними органами, дії обвинуваченого кваліфіковані за сукупністю кримінальних правопорушень, передбачених: ч. 1 ст. 182 КК України, а саме – у незаконному збиранні, зберіганні та поширенні конфіденційної інформації про особу; та ч. 2 ст. 361 КК України, а саме – у несанкціонованому втручанні в роботу автоматизованої системи, що призвело до витоку інформації, вчиненому за попередньою змовою групою осіб.

В свою чергу, категорично не погоджуємося із зазначеною кваліфікацією, вважаємо за необхідне такі діяння кваліфікувати не за ч.2 ст. 361 КК України, а за ч.2 ст. 362 КК України. Оскільки, обвинувачений є спеціальним суб'єктом злочину передбаченого статтею 362 КК України, тобто особою, яка має право доступу до інформації, що є предметом цього злочину (інформація, що не призначена для вільного доступу і відкритого користування, тобто комп'ютерна інформація з обмеженим доступом), у зв'язку із виконанням нею службових обов'язків і зловживаючи цим правом, використовує надані їй можливості для вчинення заборонених дії. За несанкціоноване перехоплення або копіювання інформації, яка оброблюється в ЕОМ, АС, КМ або зберігається на носіях такої інформації, вчинене особою, яка має право доступу до такої інформації, якщо ці дії призвели до її витоку, настає відповідальність, передбачена ч. 2 ст. 362 КК, але аж ніяк не ч.2 ст. 361 КК.

Оскільки обвинувачений неодноразово отримував неправомірну вигоду у вигляді грошових коштів за копіювання інформації з обмеженим доступом та її подальший збут, то в цьому випадку зазначені дії потребують додаткової кваліфікації ще й за ст. 368 КК (Прийняття пропозиції, обіцянки або одержання неправомірної вигоди службовою особою).

Крім цього, дії Особи 1, яка замовляла у працівника поліції інформацію з обмеженим доступом повинні бути кваліфіковані за статтею 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації).

Висновки. Обґрунтовано факт необхідності внесення змін у назву розділу 16 Особливої частини КК на «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», оскільки, в даному розділі наявні лише злочини, і відсутні кримінальні проступки, тому словосполучення «кримінальні правопорушення» у назві розділу XVI Особливої частини КК України використовувати не доцільно.

На підставі аналізу судової практики встановлено, що найпоширенішим злочином у сфері ЕОМ є злочин передбачений ст. 361 КК України, а також підтверджено випадки неправильної кваліфікації злочинів у сфері ЕОМ правоохоронними органами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Вирок Луцького міськрайонного суду Волинської області від 28.05.2019 року. URL: https://reyestr.court.gov.ua/Review/82009185 (дата звернення 09.12.2021).
2. Вирок Соснівського районного суду Черкаської області від 04.07.2019 року. URL: https://reyestr.court.gov.ua/Review/82881414 (дата звернення 09.12.2021).
3. Вирок Мукачівського міськрайонного суду Закарпатської області від 13.05.2019 року. URL: https://reyestr.court.gov.ua/Review/81700235 (дата звернення 09.12.2021).
4. Вирок Дзержинського районного суду м. Харкова від 18.03.2019 року. URL: https://reyestr.court.gov.ua/Review/80514083 (дата звернення 10.12.2021).
5. Вирок Приморського районного суду м. Маріуполь Донецької області від 04.04.2019 року. URL: https://reyestr.court.gov.ua/Review/80937191 (дата звернення 10.12.2021).