(imposition of a penalty for non-appearance on summons to the investigator, prosecutor, investigating judge, court, for breach of personal obligation, recovery of bail to state revenue); 2) use of coercion (record, forced taking of biological samples, forced opening of storage facilities during a search); 3) organizational (procedural) liability (application of stricter precautionary measures or larger bail due to violation of previously applied precautionary measures, special pre-trial investigation and special court proceedings due to non-appearance on summons, inadmissibility of evidence obtained in violation of the procedure or were not opened to the prosecution in accordance with Article 290 of the CPC of Ukraine.

The article notes that the liability of the defense in evidence is a rather specific type of liability for several reasons. One of them is the right of the defense to participate in the evidence, not the obligation. Similarly, the defense decides whether or not to disclose certain materials, depending on its wishes.

It is emphasized that legal liability may arise in the presence of appropriate grounds: 1) the fact of the formation of a dangerous act (offense) – the factual basis; 2) the existence of a rule of law prohibiting such conduct and appropriate sanctions – the regulatory basis; 3) grounds for exemption from liability for liability: may contain references to laws that exclude the illegality of activities, and hence liability; 4) the existence of a law enforcement act: the decision of the competent authority, which imposes legal liability, shows the type and degree of state influence – the procedural basis.

Keywords: *responsibility, person subject to prosecution, criminal proceedings, procedural status, suspect, accused, defense.*

УДК 343.103+004
DOI: 10.31733/2078-3566-2021-6-619-626

Андрій ГРЕБЕНЮК©
кандидат технічних наук,
доцент

Тетяна БАДАЛОВА©
ад'юнкт

Юлія ТКАЧ©
ад'юнкт

(Дніпропетровський державний університет внутрішніх справ, м. Дніпро, Україна)

МІЖНАРОДНА СПІВПРАЦЯ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

У статті розкрито поняття кіберзлочину, кіберзлочинності та питання надання міжнародно-правової допомоги під час розслідування кримінальних проваджень цієї категорії. Також визначено досудового розслідування у кримінальних провадженнях, пов'язаних з кіберзлочинами проблематику застосування чинного законодавства України та міжнародних угод під час проведення.

Ключові слова: *Інтернет, кіберзлочин, кіберзлочинність, міжнародна правова допомога, розслідування.*

Постановка проблеми. По-перше, недосконаліть чинного законодавства України під час здійснення міжнародної правової допомоги під час проведення досудового розслідування кримінальних проваджень, пов'язаних з кіберзлочинами, по-друге, можливість перегляду та внесення змін до міжнародних угод у сфері кіберзлочинів.

© А. Гребенюк, 2021
ORCID iD: https://orcid.org/0000-0002-6529-683X
andreynmu@i.ua

© Т. Бадалова, 2021
badalova1702@ukr.net

© Ю. Ткач, 2021
k_kpk@dduvs.in.ua

Аналіз публікацій, в яких започатковано вирішення цієї проблеми. Вивченням питань займались Ю. Батуріна, П. Біленчук, В. Вєхова, В. Голубєва, М. Діхтяренко, Б. Толеубековата, А. Васильєва, О. Волеводза, В. Мещерякова, В. Голубєва, Т. Тропіна, Е. Авер'янова, Д. Азарова, В. Болгова С. Беляєв, О. Бойцов, Р. Валєєв, Ю. Васильєв, С. Вихрист, В. Волженкіна, Л. Галенська, Г. Єпур, С. Кучевська, Ю. Минкова, С. Нестеренко, І. Озерський, Ю. Пономаренко, Н. Сафаров, М. Свистуленко, Л. Філяніна.

Мета статті полягає в аналізі особливостей міжнародної співпраці з іноземними державами під час проведення досудового розслідування кримінальних проваджень, пов'язаних із кіберзлочинами.

Виклад основного матеріалу. Останнім часом в Україні дуже стрімко зростають кримінальні правопорушення у кіберпросторі. У звичайному спілкуванні поняття кіберзлочину стало звичним у правоохоронній системі та в громадян України. В Україні дуже швидкий темп розвитку всесвітньої павутини, що на сьогодні може конкурувати на всесвітньому рівні.

Щоденно в країні так званими «хакерами» вчиняється велика кількість кримінальних правопорушень, де порушуються права громадян. Одним із основних завдань держави в галузі кримінально-правової охорони прав людини є захист її життя і здоров'я. Згідно зі ст. 3 Конституції України людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави [6].

У Кримінальному кодексі України (далі – КК України) є низка статей, які можна віднести до так званих «кіберзлочинів», а саме: статті 361, 361-1, 361-2, 362, 363, 363-1 КК України. Станом на сьогодні в Кримінальному кодексі України є розділ «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», тоді як у чинному законодавстві відсуне поняття кіберзлочину. Але є злочини за статтями 190, 191, 301 КК України, які не віднесені до цього розділу тому, що можуть бути вчинені різними способами (шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки, створення фейкових інтернет-магазинів, збут і розповсюдження порнографічних предметів з використанням комп'ютерної техніки, привласнення коштів з рахунків тощо) кваліфікують їх як злочини загальнокримінальної спрямованості [1–2; 4; 6; 12].

Поняття «кіберзлочин» умовно поділило науковців на дві групи. Перша група відносить дії, в яких комп'ютер є об'єктом або засобом посягання, друга група визначає кіберзлочини як злочини, об'єктом посягання в яких є інформація, що обробляється в електронно-обчислювальній машині (комп'ютері) або в комп'ютерній системі, а засобом вчинення є електронно-обчислювальна машина (комп'ютер), тобто протизаконні дії у сфері автоматичної обробки інформації.

Загальне поняття «кіберзлочин» містить у собі злочини, що вчиняються з використанням електронно-обчислювальних машин (комп'ютерів) та комп'ютерних мереж. До основних видів цих злочинів належать: створення та поширення шкідливих програмних чи технічних засобів (вірусів), втручання у роботу комп'ютерів, автоматизованих систем та комп'ютерних мереж, крадіжку інформації, поширення протиправної інформації через систему Інтернет, фішинг, фармінг тощо [2; 3; 8; 12].

Скажімо, якщо в 2000 році «фактів, де комп'ютерна техніка була як об'єкт скоєння злочину, зокрема фактів несанкціонованого проникнення до локальних відомчих комп'ютерних мереж та банків, зареєстровано не було», то вже з 2001 року, відповідно до статистики МВС України (рис. 1) спостерігається стрімке зростання цього виду злочинності [16].

Аналізуючи особливості кримінальної відповідальності за злочини, передбачені ст. 361 Кримінального кодексу України, Ю. Бельський, П. Воробей, А. Савченко та О. Колб вказують, що завдяки глобальному проникненню комп'ютерних технологій у всі сфери суспільного життя створюються нові умови та способи для вчинення так званих комп'ютерних злочинів, що призводить до їх зростання [2]. Як свідчать статистичні дані Генеральної прокуратури України, в нашій державі спостерігається тенденція до збільшення кількості злочинів, вчинених у сфері використання ЕОМ

(комп'ютерів), систем та комп'ютерних мереж та мереж електрозв'язку (наприклад, у 2013 р. було зареєстровано 1 704 кримінальні правопорушення, у 2014 – 1 254, 2015 – 1 668, 2016 – 2 454, 2017 – 7 542, а станом на листопад 2018 р. – 6 591) [16].

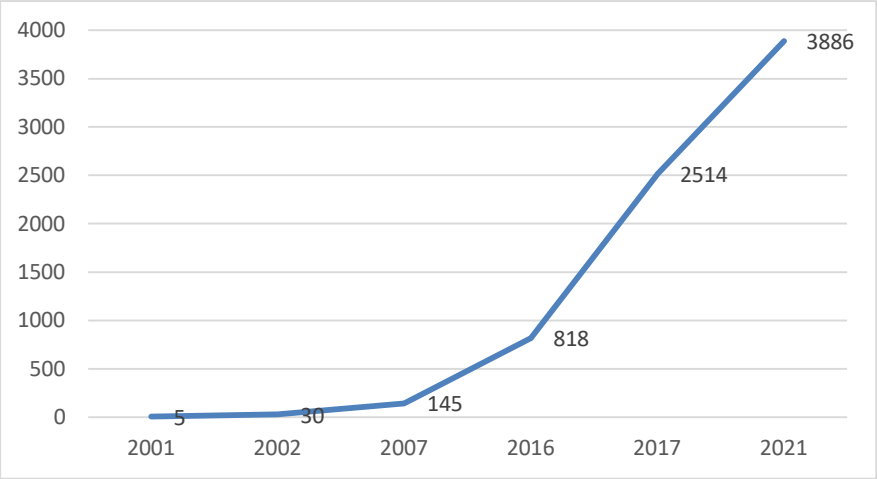

Рис. 1. Кількість кіберзлочинів відповідно до статистики МВС України

Станом на цей час згідно зі статистичними даними Генеральної прокуратури України лише за 11 місяців 2021 рік у провадженні слідчих підрозділів Національної поліції України перебувало 15 400 кримінальних проваджень, внесених до ЄРДР за фактами скоєння кримінальних правопорушень у сфері кіберзлочинів (13 379 – 2020 р.). За результатами досудового розслідування до суду у порядку ст. 291 КПК України направлено лише 6 264 кримінальні провадження (3352 – 2020 р.) [16].

Тож порівняно з 2020 р. у 2021 р. спостерігається збільшення на 2 021 кримінальне правопорушення цієї категорії. При цьому дуже мала кількість розкритих кримінальних правопорушень та у порядку ст. 291 КПК України направлених до суду – 6264 (3352 – 2020 рік) [16].

Зважаючи на те що рівень кіберзлочинів протягом 21 року дуже зростає, наша влада приділяє цьому питанню дедалі більше уваги. Зокрема, у жовтні 2015 р. було створено Кіберполіцію, яка функціонує як структурний підрозділ Національної поліції України й забезпечує захист прав і свобод людини та громадянина, інтересів суспільства й держави від кримінально протиправних посягань у кіберпросторі; здійснює заходи щодо запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі [3; 13].

Слідчі органи досудового розслідування у боротьбі з кіберзлочинністю співпрацюють з підрозділами кіберполіції та згідно з вимогами ст. 40 КПК України несуть відповідальність за законність та своєчасність здійснення процесуальних дій.

Важливу роль у боротьбі та розслідуванні кіберзлочинів мають значення міжнародні угоди, Конвенції Ради Європи, рішення Ради Европейского Союзу та ін.

Питання кібербезпеки перебуває на особливому контролі з боку міжнародної спільноти, про що свідчить ухвалення 23 листопада 2001 р. Конвенції про кіберзлочинність, яку Україна ратифікувала 07.09.2005.

У преамбулі цієї Конвенції вказано, що вона «є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва» [14].

Конвенція закріплює чимало різних положень, які декларують можливості отримати міжнародну допомогу країнам-учасницям у боротьбі з кіберзлочинністю,

серед яких треба виділити принцип надання міжнародно-правової допомоги, це, насамперед, пов'язано з отриманням необхідної інформації або документів, які суттєво впливають на процес доказу скоєного кримінального правопорушення.

Поняття міжнародна правова допомога містить у соб проведення компетентними органами однієї держави процесуальних дій, виконання яких необхідне для досудового розслідування, судового розгляду або для виконання вироку, ухваленого судом іншої держави або міжнародною судовою установою.

Згідно з вимогами ст. 542 КПК України міжнародна співпраця під час кримінального провадження полягає у вжитті необхідних заходів з метою надання міжнародної правової допомоги шляхом вручення документів, виконання окремих процесуальних дій, видачі осіб, які вчинили кримінальне правопорушення, тимчасової передачі осіб, перейняття кримінального переслідування, передачі засуджених осіб та виконання вироків. Міжнародним договором України можуть бути передбачені інші, ніж у цьому Кодексі, форми співпраці під час кримінального провадження.

Одними з основних проблем міжнародної співпраці під час розслідування кримінальних правопорушень у сфері кіберзлочинів є недосконаліть чинного законодавства України щодо здійснення міжнародно-правової допомоги. Це, насамперед, стосується отримання відповідних ухвал щодо тимчасових доступів до інформації та документів [7, 9, 10, 11].

Характеризуючи особу комп'ютерного злочинця, необхідно зазначити основне, а саме: в електронну злочинність втягнуто широке коло осіб — від висококваліфікованих фахівців до дилетантів. Правопорушники мають різний соціальний статус та різний рівень освіти (навчання та виховання).

Розглянемо особу комп'ютерного злочинця на прикладі кримінальних проваджень, відкритих слідчими підрозділами ГУНП в Дніпропетровській області, в яких дуже чітко простежується проблема незбігу законодавства України та законодавства іноземних держав.

Наприклад, згідно з матеріалами кримінального провадження: *«02.11.2017 р. до СУ ГУНП в Дніпропетровській області надійшло електронне звернення про вчинення кримінального правопорушення щодо громадянки Республіки Білорусь «К». У своїй заяві «К» вказала, що 17.08.2017 р., приблизно о 10:30 вона з метою обговорення умов продажу хутряних виробів, шляхом відправки особистих повідомлень через соціальну мережу «Однокласники» через листування з невстановленою слідством особою, що назвалась «Г», під час якої обговорила умови купівлі жіночого хутряного пальто.*

Під час листування невстановлена особа, увійшовши в довіру, вказала, що грошові кошти в сумі 185 доларів США необхідно перерахувати за допомогою системи «Western Union». У подальшому на надані невстановленою особою банківські реквізити «К» перерахувала вказану грошову суму. Проте обумовлений товар остання не отримала, внаслідок чого невстановлена особа заволоділа грошовими коштами «К» у вказаній сумі.

Далі невстановлена особа за допомогою анкетних даних «Г» і «К» аналогічним чином входила у довіру громадян Республіки Білорусь, отримуючи від них грошові перекази за допомогою платіжної системи «Western Union», не відправляючи сплачені товари, чим скоїла шахрайські дії і незаконно заволоділа грошовими коштами на загальну суму, еквівалентну 10000 доларів США. Встановлено, що відправниками грошових коштів на адресу «Г» і «К» громадяни Республіки Білорусь».

Зважаючи на те, що потерпілі особи були громадянами Республіки Білорусь та мешкали на території вказаної держави, виникла потреба в отримані міжнародно-правової допомоги. Згідно з вимогами чинного законодавства України було складено запит до компетентних органів Республіки Білорусь та долучено перелік необхідних документів разом із перекладом на мову, визначену відповідним міжнародним договором України. Підготовка та отримання відповідної ухвали та переклад зайняла дуже тривалий час. Під час виконання міжнародно-правої допомоги у компетентних органах вказаної держави виникли проблеми з використанням чинного законодавства республіки Білорусь, а саме з вимогами ч. 1 ст. 49 КПК Республіки Білорусь, в якій зазначено, що потерпілим може бути фізична особа, якій спричинено фізичну, майнову та моральну шкоду та щодо якої орган, що здійснює кримінальний процес, визнав її потерпілою та склав відповідну постанову.

Згідно з ч. 7 ст. 51 КПК України, якщо особа не подала заяву про вчинення щодо неї кримінального правопорушення або заяву про залучення її до провадження як

потерпілого, то слідчий, прокурор, суд має право визнати особу потерпілою лише за її письмовою згодою. За відсутності такої згоди особа в разі потреби може бути залучена до кримінального провадження як свідок.

Однак в розглянутому випадку потерпілих осіб встановлено працівниками підрозділу кіберполіції і з метою визнання вказаних осіб потерпілими направлено запит до компетентних органів Республіки Білорусь.

Компетентними органами Республіки Білорусь не виконано вимоги запиту та не визнано осіб потерпілими через незбіг законодавства України з законодавством Республіки Білорусь.

Адже згідно з вимогами ст. 8 Конвенції про правову допомогу та правові відносини у цивільних, сімейних та кримінальних справах від 22.01.1993 надання міжнародної правової допомоги здійснюється згідно з законодавством запитуваної держави за умови, якщо воно не суперечить законодавству виконуючої сторони [15].

Такий чинник надання міжнародної правової допомоги з боку компетентних органів Республіки Білорусь не надав бажаних результатів для проведення досудового розслідування вказаного кримінального провадження та визнання винними осіб, які скоїли вказаний злочин.

Також є проблематика щодо строку зберігання інформації та документів іншими державами [9-10].

Під час розслідування кримінального провадження за фактом вчинення кримінального правопорушення, передбаченого ст. 301 КК України, встановлено, що: «*До правоохоронних органів звернулась з заявою «Т» про те, що 23.05.2017 р. невстановлена особа за допомогою соціальної мережі «Вконтакте» під псевдонімом «О», здійснила розповсюдження фотографій (фотоматеріалів) інтимного характеру, на яких зображено останню та елементи їх з чоловіком фото інтимного характеру «М» між користувачами соціальної мережі «Вконтакте», більшість яких є неповнолітніми особами, які є учнями Навчально-виховного комплексу.*

За даним фактом 29.05.2017 р. розпочато кримінальне провадження ознаками кримінального правопорушення, передбаченого ч. 2 ст. 301 КК України.

Під час проведення досудового розслідування по вказаному кримінальному провадженню встановлено, що з листопада 2016 року по липень 2017 року невідома особа за допомогою соціальної мережі «Вконтакте» зареєструвала низку неправдивих (фейкових) електронних сторінок, а саме: «Е» (періодично змінювала на «Т»), «Ш, «Ф» та «А», за допомогою яких здійснювалося розповсюдження фотографій (фотоматеріалів) інтимного характеру, на яких зображено потерпілу та елементи їх з чоловіком фото інтимного характеру «М» між користувачами соціальної мережі «Вконтакте» неповнолітнім учням НВК.

01.06.2017 року під час проведення слідчо-оперативних дій встановлені та зафіксовані фотоматеріали інтимного характеру, які розповсюджувалися неповнолітнім учням НВК, згідно з висновком судово-мистецтвознавчої експертизи № 32/15.1./228 від 10.08.2017 року досліджені фотоматеріали є порнографічними.

Згідно з інформацією, отриманою 01.09.2017 року від Інтерполу та Європолу ГУНП в Дніпропетровській області, компетентними органами Російської Федерації, встановлено та збережено (з 27.07.2017 року на 6 місяців) реєстраційні данні, лог файли адміністрування акаунтів та переписка користувачів, за вищевказаними раніше сторінками».

Під час проведення досудового розслідування вказаного кримінального провадження виникла потреба у проведенні процесуальних дій на території Російської Федерації, а саме: отримання інформації, яка є у володінні ТОВ «Вконтакте». Підготовка міжнародного запиту та отримання відповідних ухвал були тривалими, що негативно порушує розумні строки досудового розслідування та строк зберігання необхідної інформації, яка у володінні ТОВ «Вконтакте».

Сторони кримінального провадження в межах розслідування кримінальних проваджень відповідно до ст. 160 КПК України мають право звернутися до слідчого судді під час досудового розслідування чи суду під час судового провадження із клопотанням про тимчасовий доступ до речей і документів, за винятком зазначених у статті 161 цього Кодексу [5]. Слідчий має право звернутися із зазначеним клопотанням за погодженням з прокурором.

Згідно з вимогами КПК України є низка інформації і документів, які належать до охоронюваної законом таємниці, про що викладено в ч. 1 ст. 162 КПК України [5]:

1) інформація, що є у володінні засобу масової інформації або журналіста і надана їм за умови нерозголошення авторства або джерела інформації;

2) відомості, які можуть становити лікарську таємницю;

3) відомості, які можуть становити таємницю вчинення нотаріальних дій;

4) конфіденційна інформація, в тому числі така, що містить комерційну таємницю;

5) відомості, які можуть становити банківську таємницю;

6) особисте листування особи та інші записи особистого характеру;

7) інформація, яка є в операторів та провайдерів телекомунікацій про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо;

8) персональні дані особи, що є в її особистому володінні або в базі персональних даних, яка знаходиться у володільця персональних даних;

9) державна таємниця;

10) таємниця фінансового моніторингу.

Станом на 2017 рік відповідно до ч. 7 ст. 164 КПК України строк дії ухвали, який не може перевищувати одного місяця з дня постановлення ухвали.

Також згідно з положеннями ч. 2 ст. 16 Конвенції про кіберзлочинність 2005 року максимальний термін збереження комп'ютерних даних 90 днів тобто 3 місяці, що не унеможливлює втрати даних, які б суттєво вплинули на викриття дій правопорушника та оголошення йому про підозру.

У розглянутому випадку надання міжнародної правової допомоги з боку компетентних органів Російської Федерації надало позитивний результат та особу правопорушника викрито. Позитивний результат від компетентних органів Російської Федерації отримано тільки за умови попереднього внутрішнього службового листування між працівниками кіберполіції та відповідними органами Російської Федерації, в інших випадках до моменту відправлення міжнародних запитів та проведення процесуальних дій на території іноземних держав необхідну інформацію можливо втратити.

Висновки. В епоху стрімкого й активного розвитку інформаційних технологій вони стають невід'ємною частиною нашого повсякденного життя, робочих процесів і діяльності державних органів та бізнесу, а тому особливу увагу треба приділяти власній кібербезпеці. Вочевидь, наша країна перебуває на початковому етапі впровадження інституцій та механізмів у сфері кібербезпеки, проте певну законодавчу базу вже створено – необхідно лише її дотримуватися та розвивати.

Варто сподіватись, що чинна державна влада не зупиниться на досягнутому, буде запозичувати досвід інших країн Європи та брати участь у міжнародній співпраці з питань кібербезпеки. Також вважаємо за доцільне звернути увагу на недосконалість чинного законодавства України щодо здійснення міжнародної співпраці під час проведення досудового розслідування кримінальних проваджень цієї категорії та відповідних міжнародних угод.

Список використаних джерел

1. Удалова Л. Д., Макаров М. А., Азаров Ю. І. та ін. Кримінальний процес України у питаннях і відповідях : навч. посібник. 5-е вид., перероб. і доп. Київ : Центр учбової літератури, 2020. 432 с.

2. Бельський Ю. А., Воробей П. А., Савченко А. В., Колб О. Г. Кримінальна відповідальність за несанкціоноване втручання в роботу ЕОМ : монограф. Київ : Юрінком Інтер, 2019. 264 с.

3. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навч. посібник. Дніпро : ДДУВС, 2020. 144 с.

4. Кримінальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

5. Кримінальний процесуальний кодекс України. URL : https://zakon.rada.gov.ua/laws/show/4651-17/ed20211004#n1598.

6. Конституція України. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96%D0%B2%D1%80#Text.

7. Бабакін В. М. Особливості міжнародного співробітництва при розслідуванні кіберзлочинів. *Форум права*. 2011. № 4. С. 27–30.

8. Тихоненко О. М., Тихоненко В. С. Нормативно-правові основи боротьби з кіберзлочинністю в Україні. *Вісник Луганського національного університету імені Тараса Шевченка. Педагогічні науки*. 2012. № 20. С. 171–179.

9. Войціховський А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. *Право і Безпека*. 2011. № 4. С. 107–112.

10. Орлов О. В. Міжнародна співпраця у сфері боротьби з кіберзлочинністю. *Теорія та*

практика державного управління. 2013. Вип. 4. С. 17–23.

11. Демедюк С. В. Міжнародний досвід протидії кіберзлочинності. *Вісник Харківського національного університету внутрішніх справ*. 2014. № 4. С. 65–75.

12. Кундеус В. Поняття та види кіберзлочинів. Держава і злочинність. Нові виклики в епоху постмодерну. Харків, 2020. URL : http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/7723/Poniattia_Kundeus_2020.pdf?sequence=1&isAllowed=y.

13. Сіренко О. В. Кібербезпека в Україні: правові та організаційні питання. URL : http://dspace.oduvs.edu.ua/bitstream/123456789/486/1/ilovepdf_com-48-49%5B15D.pdf.

14. Конвенція про кіберзлочинність, яку Україною ратифіковано 07.09.2005. URL : https://zakon.rada.gov.ua/laws/show/994_575#Text.

15. Конвенція про правову допомогу та правові відносини у цивільних, сімейних та кримінальних справах від 22.01.1993. URL : https://zakon.rada.gov.ua/laws/show/997_009#Text.

16. Електронні статистичні дані сайту Офісу Генеральної прокуратури України. URL : https://old.gp.gov.ua/ua/stst2011.html?dir_id=114140&libid=100820&c=edit&_c=fo#.

Надійшла до редакції 15.12.2021

References

1. Udalova, L. D., Makarov, M. A., Azarov, Yu. I. ta in. (2020) Kryminal'nyy protses Ukrayiny u pytannyakh i vidpovidyakh [riminal process of Ukraine in questions and answers] : navch. posibnyk. 5-e vyd., pererob. i dop. Kyiv : Tsentr uchbovoyi literatury, 432 p. [in Ukr.].

2. Bel's'kyy, Yu. A., Vorobey, P. A., Savchenko, A. V., Kolb, O. H. (2019) Kryminal'na vidpovidal'nist' za nesanktsionovane vtruchannya v robotu EOM [Criminal liability for unauthorized interference in the work of computers] : monohraf. Kyiv : Yurinkom Inter, 264 p. [in Ukr.].

3. Hrebenyuk, A. M., Rybal'chenko, L. V. (2020) Osnovy upravlinnya informatsiynoyu bezpekoyu [Fundamentals of information security management] : navch. posibnyk. Dnipro : DDUVS, 144 p. [in Ukr.].

4. Kryminal'nyy kodeks Ukrayiny [Criminal Code of Ukraine]. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text. [in Ukr.].

5. Kryminal'nyy protsesual'nyy kodeks Ukrayiny [Criminal Procedure Code of Ukraine]. URL : https://zakon.rada.gov.ua/ laws/show/4651-17/ed20211004#n1598. [in Ukr.].

6. Konstytutsiya Ukrayiny [The Constitution of Ukraine]. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96% D0%B2%D1%80#Text. [in Ukr.].

7. Babakin, V. M. (2011) Osoblyvosti mizhnarodnoho spivrobitnytstva pry rozsliduvanni kiberzlochyniv [Features of international cooperation in the investigation of cybercrime]. *Forum prava*. № 4, pp. 27–30. [in Ukr.].

8. Tykhonenko, O. M., Tykhonenko, V. S. (2012) Normatyvno-pravovi osnovy borot'by z kiberzlochynnistyu v Ukrayini [Regulatory framework for combating cybercrime in Ukraine]. *Visnyk Luhans'koho natsional'noho universytetu imeni Tarasa Shevchenka. Pedahohichni nauky*. № 20, pp. 171–179. [in Ukr.].

9. Voytsikhovs'kyy, A. V. (2011) Mizhnarodne spivrobitnytstvo v borot'bi z kiberzlochynnistyu [International cooperation in the fight against cybercrime]. *Pravo i Bezpeka*. № 4, pp. 107–112. [in Ukr.].

10. Orlov, O. V. (2013) Mizhnarodna spivpratsya u sferi borot'by z kiberzlochynnistyu [International cooperation in the fight against cybercrime]. *Teoriya ta praktyka derzhavnoho upravlinnya*. Vyp. 4, pp. 17–23. [in Ukr.].

11. Demedyuk, S. V. (2014) Mizhnarodnyy dosvid protydiyi kiberzlochynnosti [International experience in combating cybercrime]. *Visnyk Kharkivs'koho natsional'noho universytetu vnutrishnikh sprav*. № 4, pp. 65–75. [in Ukr.].

12. Kundeus, V. (2020) Ponyattya ta vydy kiberzlochyniv. Derzhava i zlochynnist'. Novi vyklyky v epokhu postmodernu [The concept and types of cybercrime. State and crime. New challenges in the postmodern era]. Kharkiv. URL : http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/7723/Poniattia_Kundeus_2020.pdf?sequence=1&isAllowed=y. [in Ukr.].

13. Sirenko, O. V. Kiberbezpeka v Ukrayini: pravovi ta orhanizatsiyni pytannya [Cybersecurity in Ukraine: legal and organizational issues]. URL : http://dspace.oduvs.edu.ua/bitstream/123456789/486/1/ilovepdf_com-48-49%5B15D.pdf. [in Ukr.].

14. Konventsiya pro kiberzlochynnist' [Convention on Cybercrime], yaku Ukrayinoyu ratyfikovano 07.09.2005. URL : https://zakon.rada.gov.ua/laws/show/994_575#Text. [in Ukr.].

15. Konventsiya pro pravovu dopomohu ta pravovi vidnosyny u tsyvil'nykh, simeynykh ta kryminal'nykh spravakh vid 22.01.1993 [Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Cases of January 22 1993]. URL : https://zakon.rada.gov.ua/laws/show/997_009#Text. [in Ukr.].

16. Elektronni statystychni dani saytu Ofisu Heneral'noyi prokuratury Ukrayiny [Electronic statistical data of the website of the Office of the Prosecutor General of Ukraine]. URL : https://old.gp.gov.ua/ua/stst2011.html?dir_id=114140&libid=100820&c=edit&_c=fo#. [in Ukr.].

ABSTRACT

Andriy Hrebeniuk, Tetyana Badalova, Yuliya Tkach. International cooperation in cyber crimes investigations. Recently, criminal offenses in the field of cybercrime have been growing very rapidly in Ukraine. In ordinary communication, the concept of cybercrime has become commonplace in the law enforcement system and the citizens of Ukraine. Every day in the country, so-called «hackers» commit a large number of criminal offenses where the rights of citizens are violated.

The article reveals the concept of cybercrime, cybercrime and the issue of providing international legal assistance in the investigation of criminal proceedings in this category. Interaction of pre-trial investigation bodies in the fight against cybercrime with Cyberpolice, which functions as a structural unit of the National Police of Ukraine and protects human and civil rights and freedoms, interests of society and the state from criminal encroachment in cyberspace; takes measures to prevent, detect, stop and detect cybercrime, raise public awareness of security in cyberspace. The materials of the pre-trial investigation of the criminal proceedings which required procedural actions on the territory of other states where the problem of discrepancy between the legislation of Ukraine and the legislation of foreign states is very clearly traced are considered.

International agreements, Council of Europe Conventions, decisions of the Council of the European Union and others play an important role in the fight against and investigation of cybercrime.

The issues of implementation of institutions and mechanisms in the field of cybersecurity are highlighted. The issues of application of the current legislation of Ukraine and international agreements in conducting pre-trial investigations in criminal proceedings related to cybercrime have also been identified.

Keywords: *internet, cybercrime, cyber criminatyli, international legal assistance, investigation.*

УДК 351.74(477)
DOI: 10.31733/2078-3566-2021-6-626-632

Андрій ЖБАНЧИК©
кандидат юридичних наук
(Дніпропетровський державний університет внутрішніх справ, м. Дніпро, Україна)

ЗАСТОСУВАННЯ ЗБРОЇ ДЛЯ ЗУПИНКИ ТРАНСПОРТНОГО ЗАСОБУ

Статтю присвячено проблематиці застосування та використання зброї та спеціальних засобів для примусової зупинки транспортного засобу, якщо водій своїми діями створює загрозу життю чи здоров'ю людей та/або поліцейського. У статті наголошено, що цей вид поліцейського примусу є досить травматичним для водія, пасажирів та сторонніх осіб на місці події, а поліцейському загрожує настанням кримінальної відповідальності за навмисне вбивство або перевищення службових повноважень.

Здійснено аналіз нормативно-правових повноважень із застосування поліцейськими вогнепальної зброї, який дав змогу висвітлити їх недосконалість та запропонувати зміни до Закону України «Про Національну поліцію». Зазначено, що термінологічний апарат у цьому законі логічно неузгоджений, що утворює правові колізії. Акцентовано на потребі ефективної вогневої підготовки з використанням інноваційних технологій, зокрема інтерактивних тирів та автомобілів-тренажерів, які імітують стрільбу в русі, та симуляцій обстановки, в якій може виникнути потреба зупинки транспортного засобу із застосуванням зброї.

Ключові слова: *застосування та використання вогнепальної зброї, транспортний засіб, поліцейський, підстави застосування зброї.*

Постановка проблеми. Відповідно до п. 3 ч. 1 ст. 42 Закону України «Про Національну поліцію» (далі – ЗУНП), поліція під час виконання повноважень, визначених цим Законом, уповноважена застосовувати примусові поліцейські заходи, зокрема вогнепальну зброю [1]. П. 7 ч. 4 ст. 46 ЗУНП уповноважує поліцейського у виняткових випадках застосовувати вогнепальну зброю для зупинки транспортного засобу шляхом його пошкодження, якщо водій своїми діями створює загрозу життю чи здоров'ю людей та/або поліцейського.

k_tsp@dduvs.in.ua
ORCID iD: https://orcid.org/0000-0001-8149-2323