DOI: https://doi.org/10.18371/fp.1(45).2022.113122

УДК 343.97

COVID-19 ЯК АКТИВАТОР ПАНДЕМІЇ КІБЕРЗЛОЧИННОСТІ

БРАЙЧЕНКО Сергій Миколайович
кандидат юридичних наук, доцент,
Черкаський навчально-науковий інститут
Університету банківської справи
ORCID ID: https://orcid.org/0000-0002-8476-6622

ПАНТЄЛЄЄВА Наталія Миколаївна
доктор економічних наук, професор,
Черкаський навчально-науковий інститут
Університету банківської справи
ORCID ID: https://orcid.org/0000-0001-6457-6912

ВДОВІЧЕНКО Руслана Володимирівна
студент
Черкаського навчально-наукового інституту
Університету банківської справи

Анотація. *В статті розглянуто понятійну сутність кіберзлочинності та її типологізацію, узагальнено сучасне правове регулювання боротьби з кіберзлочинністю. Надано кримінально-правову оцінка активізації кіберзлочинності під впливом COVID-19 в Україні. Проведено компаративний аналіз кримінологічної практики протидії пандемії кіберзлочинності в умовах COVID-19. Обгрунтовано рекомендації щодо криміналізації деяких видів злочинів і загроз в сфері цифрової трансформації, впровадження новітніх інструментів боротьби з кіберзлочинністю на основі сучасних цифрових технологій.*

Ключові слова: *кібербезпека, кіберзлочинність, цифровізація, криміналізація, COVID-19, кримінальні правопорушення у кіберпросторі, протидія кіберзлочинності.*

Анотация. *В статье рассмотрено сущность понятия киберпреступности и ее типологизация, обобщено современное правовое регулирование борьбы с киберпреступностью. Дано криминально-правовую оценку активизации киберпреступности под воздействием COVID-19 в Украине. Проведено компаративный анализ криминологической практики протидействия пандемии киберпреступности в условиях COVID-19. Обосновано рекомендации по криминализации некоторых видов преступлений и угроз в сфере цифровой трансформации, внедрения новых инструментов борьбы с киберпреступностью на основе современных цифровых технологий.*

Ключевые слова: *кибербезопасность, киберпреступность, цифровизация, криминализация, COVID-19, криминальные правонарушения в киберпространстве, противодействие киберпреступности*.

Постановка проблеми. На сучасному етапі свого розвитку людство стикається не тільки зі змінами, пов'язаними з глобалізацією і науково-технічним прогресом, але і з абсолютно новими викликами і загрозами, які несе в собі суспільство, що динамічно розвивається. Зараз світові економіки і суспільство зазнали безпрецедентного впливу пандемії COVID-19 і стали надзвичайно вразливими не тільки до трансформації економічних відносин, зміни бізнес-моделей, порушення психологічної рівноваги і соціальної захищеності внаслідок перенесення ділової активності в онлайн, але також до зростання активності злочинної діяльності в кіберпросторі, яка адаптивно розширила види і змінила свої методи, використовуючи на власну користь невизначеність, тривоги і страхи, а також ситуаційне зменшення в деяких країнах кількості або перепрофілювання фахівців правоохоронних органів боротьби з кіберзлочинністю. Таким чином, важливим стає проведення проактивних заходів протидії кіберзлочинності, які повинні бути законними, співставними і надійними, результативними як в частині розслідування і покарання, так і зміцнення кібер-довіри суспільства, підвищення свідомості і розширення можливостей захисту.

Аналіз останніх досліджень і публікацій. Теоретичні засади і проблемні питання криміналістичних особливостей кіберзлочинів, підходи їх виявлення і розслідування розглядають у своїх наукових працях зарубіжні та українські науковці, зокрема, М. Бабакова, О. Баранов, М. Баттон, Д. Біленчук, В. Бухарєв, Л. Веселова, В. Голубєв, М. Гуцалюк, С. Демедюк, І. Діордіца, О. Довгань, Д. Дубов, О. Заярний, М. Карчевський, М. Краненбарг, Н. Кшетрі, В. Маркова, С. Мельник, В. Прохоренко, І. Сезонова, Л. Скалозуб, О. Солодка, А. Ставер, В. Струков, О. Тихомиров, К. Фобер, Ю. Чанг, В. Шеломенцев, Ю. Якубівська та інші вчені. Проте необхідність реагування на виклики кризових явищ, до яких можна віднести кризу пандемії COVID-19 на тлі поширення глобального тренду цифровізації всіх галузей економіки, вказують на потребу проведення подальших досліджень щодо оцінки передумов, ефектів впливу та наслідків для вдосконалення нормативно-правової бази і розробки практичних рекомендацій попередження і протидії кіберзлочинам.

Метою дослідження є узагальнення теоретико-правових засад і кримінологічних аспектів кіберзлочинності, розробка рекомендацій для вдосконалення кримінально-правового регулювання та підвищення ефективності системи заходів протидії для подолання викликів COVID-19.

Виклад основного матеріалу дослідження. Кримінологічний аналіз сучасної кіберзлочинності потребує, насамперед, термінологічної визначеності. Незважаючи на широке вживання правових категорій «кіберзлочинність» і «кіберзлочин», єдиного і чіткого тлумачення цих понять не вироблено (табл. 1).

Критичне вивчення різних точок зору дозволило сформулювати власні тлумачення цих понять, підкреслюючи їх суб'єктно-об'єктну особливість, предмет злочинних посягань і негативні наслідки:

На нашу думку, *кіберзлочинністю є сукупність незаконних протиправних дій, що скоюються особами або організованими угрупуваннями в кіберп-*

росторі за допомогою або через комп'ютерні системи та/або мережі, засоби мобільного зв'язку та інші засоби доступу, коли предметом злочинних посягань є інформація, інформаційні та технічні ресурси, інформаційна інфраструктура з метою їх захоплення і контролю, руйнування, порушення цілісності, спотворення або злочинного використання.

З позиції криміналістики *кіберзлочин, в свою чергу, це суспільно небезпечне діяння, що вчиняється в кіберпросторі, яке посягає на громадську безпеку, власність, права людини та інші відносини, що охороняються законом, а також необхідний елемент механізму підготовки, скоєння та приховування злочину, предмета чи засоби якого є комп'ютерна інформація, що може призвести до негативних наслідків технічного, економічного, соціального, морального, психологічного, екологічного характеру.*

Таблиця 1

Деякі наукові погляди на сутність поняття «кіберзлочинність» і «кіберзлочин»

Автор	**Тлумачення**
Кіберзлочинність – це …	
М. Дашян	порушення чужих прав та інтересів по відношенню до автоматизованих систем обробки даних [1, с.30]
В. Голубев	противоправна поведінка, спрямована на порушення суспільних відносин і персональної або корпоративної безпеки під час здійснення особами обміну даними за допомогою електронних засобів [2]
М. Кравцова	соціально-правовий феномен, що проявляється в забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку [3, с.4]
Кіберзлочин – це …	
Д. Карпова	акт соціальної девіації з метою нанесення економічного, політичного, морального, ідеологічного, культурного та інших видів збитків, індивіду, організації або державі за допомогою будь-якого технічного засобу з доступом до Інтернету. [4, с.47]
О. Сіренко	кримінальне правопорушення, що вчиняється за допомогою або через комп'ютерні системи, посягає на право захисту від несанкціонованого поширення і використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію і за яке передбачено кримінальну відповідальність [5, с.49]
В. Бєлєнький	винне, суспільно небезпечне, кримінально каране втручання в сферу безпеки обігу комп'ютерної інформації, роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, зроблені за допомогою комп'ютерів, комп'ютерних мереж і програм, а також за допомогою інших пристроїв із вбудованими процесорами і кон-

	тролерами, які можуть мати доступ до інформаційного простору [6, с.6]
А. Русецький Д. Куцолабський	протиправне винне діяння (дія або бездіяльність), яке передбачає втручання в дані персональних комп'ютерів, комп'ютерних програм і комп'ютерних мереж, або діяння, вчинене за допомогою комп'ютерів та інших сучасних технологій, за яке передбачається кримінальна відповідальність та яке може створити особисту небезпеку для громадян, загрозу національній безпеці держави та світовій безпеці [7, с.76]

Джерело: сформовано авторами на підставі опрацювання вказаних наукових праць

На фоні динаміки технологічного прогресу та використання його новацій спостерігаємо не тальки позитивні ефекти на благо суспільства, а також зростання злочинної діяльності різних деструктивних сил, простором якої стало кіберсередовище. Різноманітність злочинної діяльності, набуття нових форм і ознак можна прослідкувати через типологізацію кіберзлочинів. Так, Будапештська Конвенція, як основний документ у сфері боротьби з кіберзлочинністю, надає таку класифікацію кіберзлочинів [8]:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних та систем, зокрема:

- незаконний доступ, наприклад, шляхом злому, обману та іншими засобами;
- нелегальне перехоплення комп'ютерних даних;
- втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;
- втручання в систему, включаючи умисне створення серйозних перешкод для функціонування комп'ютерної системи, наприклад, шляхом розподілених атак на ключову інформаційну інфраструктуру;
- зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу для здійснення кіберзлочинів;

2) правопорушення, пов'язані з комп'ютерами, включаючи підробку та шахрайство, вчинені з використанням комп'ютерів;

3) правопорушення, пов'язані зі змістом інформації, зокрема, дитяча порнографія, расизм і ксенофобія;

4) правопорушення, пов'язані з порушенням авторських та суміжних прав, наприклад незаконне відтворення та використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних та книг.

Активатором кіберзлочинності стала пандемія COVID-19. Адже навіть медична сфера під час пандемії зазнала кібератак. Зокрема, в Європі протягом березня 2020 – січня 2022 загальна кількість інцидентів становила 21 у 10 країнах в середньому 0,3 інциденти на тиждень, з яких 19 були спрямовані проти надання медичних послуг пацієнтам, по 1 на фармацію та медичні розробки і виробництво [9].

Аналіз динаміки кіберзлочинів в Україні продовж 2018-2021 рр. (рис. 1) свідчить про стійку тенденцію до зростання правопорушень стосовно несанкціонованого втручання (ст. 361) і несанкціонованих дій з інформацією (ст. 362), які сукупно склали у 2021 році 94,24% проти 91,14% у 2018 році.

Варто відмітити, що в 2021 році в судах першої та другої інстанцій була максимальна кількість проваджень (1953) і таких, що було закрито – 333 провадження при загальному висхідному тренді (рис. 2).

Отже, бачимо, що пандемія COVID-19 зумовила зростання кіберзлочинності, що загострило проблему кримінально-правової оцінки кіберзлочинності і результативної протидії внаслідок слабкої законодавчої основи, складності збору доказів та самого процесу доведення, нестачі компетентних осіб ІТ-галузі в органах державної влади, відсутності узагальненої судової системи тощо.

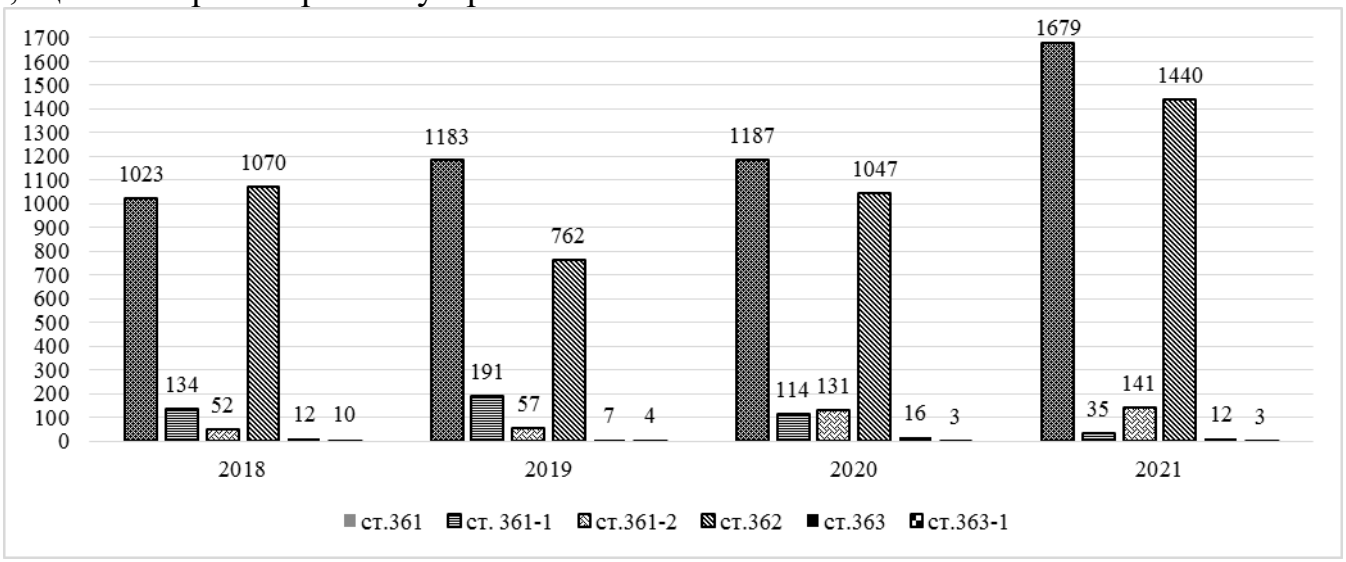

Рис. 1. Динаміка кримінальних правопорушень протягом 2018-2021 рр.
Джерело: побудовано автором на основі даних [10]

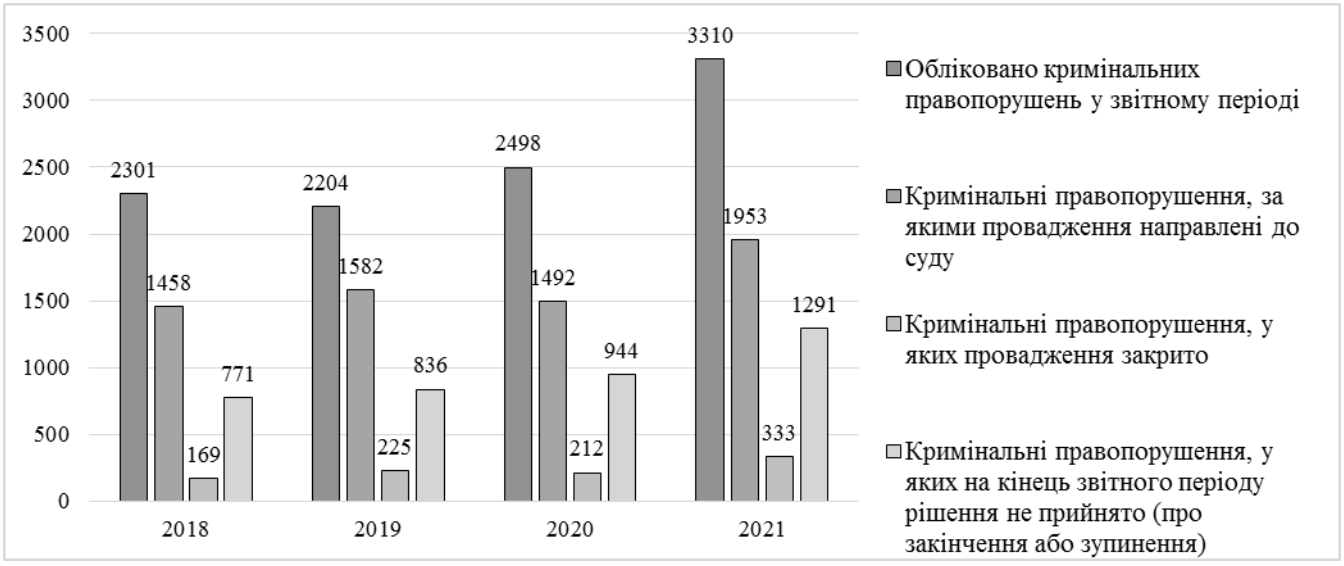

Рис. 2. Динаміка кримінальних правопорушень в розрізі досудового та судового розслідування
Джерело: побудовано автором на основі даних [10]

Вважаємо, що необхідно посилити комплекс заходів, спрямованих на ефективну протидію кіберзлочинності, шляхом:

- внесення змін до законодавства, що регламентує види санкцій за неправомірну поведінку в кіберпросторі, та удосконалення кримінологічних методик на підставі вивчення досвіду та моніторингу криміналістичної практики зарубіжних країн;
- вжиття заходів щодо посилення міжвідомчої співпраці між органами безпеки і різними ІТ-структурами для запобігання ризику виникнення та мінімізації наслідків кібератак на національному та міжнародному рівнях;
- підвищення рівня цифрової грамотності та обізнаності громадськості щодо необхідності належного використання ІТ-ресурсів, видів і проявів кіберзлочинів.

Пропонуємо розглянути можливість врахування в Кримінальному кодексі України [11] відповідальність за такі кримінальні правопорушення (табл. 2).

Кіберзлочинність є феноменом, сформованим у процесі науково-технічного та технологічного прогресу [12].

Активне впровадження інформаційних та телекомунікаційних технологій в усі сфери життєдіяльності загострило проблеми охорони персональних даних, комерційної, корпоративної та банківської таємниці [13].

Таблиця 2

Рекомендації щодо криміналізації деяких видів злочинів і загроз

Гіпотеза	Диспозиція	Санкція
Розповсюдження в мережі «Інтернет» неправдивої інформації про пандемію COVID-19	розповсюдження в мережі «інтернет» неправдивої інформації про пандемію covid-19	карається штрафом від 600 до 1000 неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до одного року
	ті самі дії, вчинені групою осіб за попередньою змовою, а також із заподіянням значної шкоди громадянину	карається штрафом від 5 тисяч до 10 тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років
Шахрайство з використанням електронних засобів платежу	шахрайство з використанням електронних засобів платежу	караються штрафом від 2 до 4 тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк
	ті самі дії, вчинені групою осіб за попередньою змовою, а також із заподіянням значної шкоди громадянину	караються позбавленням волі на строк до трьох років
	дії, передбачені частинами першою або другою цієї статті, вчинені особою з використанням свого службового становища	караються позбавленням волі на строк від трьох до п’яти років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк п’ять років
Кібертероризм	протиправне заволодіння комп'ютерною інформацією, що охороняється законом, її використання або загроза використ-	карається позбавленням волі на строк від одного до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльні-

	тання, що створює небезпеку настання тяжких наслідків, вчинене з метою залякування населення або (і) впливу на орган влади	стю на строк до трьох років
	ті самі дії, що спричинили смерть людини або інші тяжкі наслідки	карається позбавленням волі терміном від п'яти до восьми років

Джерело: власна розробка

Проте цифрові технології, на нашу думку, можуть стати результативним інструментом боротьби з кіберзлочинністю.

- Штучний інтелект (ШІ) – основний інструмент боротьби з сучасними кіберзагрозами, завдяки алгоритмам машинного навчання та обробці великих масивів даних. Використання ШІ дозволяє покращити кібербезпеку за трьома основними категоріями: 1) виявлення кіберзагроз на основі аналізу нових або нестандартних моделей поведінки, виявлення подій з високим ступенем ризиків і зловмисників, покращення пошуку вразливостей за рахунок побудови профілів програмних застосунків і мережевих засобів, оптимізація налаштувань конфігурації інфраструктури, вивчення моделі мережевого трафіку і пропозиції удосконалення політики захисту; 2) відповідь на загрозу, що включає створення та автоматичний запуск необхідних засобів захисту, зокрема зупинення дії програм-вимагачів; 3) вивільнення людських ресурсів за рахунок систем самонавчання на основі ШІ.

- Blockchain. При застосуванні технології блокчейн [14] немає єдиної точки атаки на базу даних, а отримати доступ до даних, які зашифровані за допомогою ключа, неможливо без знання цього ключа. Ключі зберігаються не централізовано, а в кожного користувача-власника. При атаці на такий центр-сервер неможливо викрасти всі дані, що знаходяться на ньому. Кримінальній сфері буде завдано відчутного удару, оскільки зберігається історія операцій, фінансові потоки будуть видні в ланцюжку блоків і замаскувати їх буде практично неможливо, що зведе нанівець нелегальні транзакції, ускладнить фінансування терористичних та екстремістських організацій.

- XDR здійснює міжрівневе виявлення загроз та реагування на них за рахунок об'єднання інформації про безпеку та управління подіями [15]. XDR збирає та зіставляє дані на різних рівнях безпеки, включаючи кінцеві точки, електронну пошту, сервери, хмарні інфраструктури та спільну мережу. Такий аналіз даних дозволяє швидше виявляти загрози та скорочувати час розслідування та реагування.

- Secure Access Service Edge (прикордонні сервіси безпечного доступу) або SASE виділяються відносно новою моделлю захисту, що передбачає комбінацію мережевих сервісів та сервісів безпеки [12]. Інструменти SASE можуть ідентифікувати конфіденційні дані або шкідливе програмне забезпечення, розшифровувати контент і безперервно відстежувати сеанси щодо ризиків та рівнів довіри, тим самим забезпечуючи контроль злочинності в кіберпросторі.

Отже, потенціал сучасних цифрових технологій може успішно бути використаний для протидії загрозам інформаційного суспільства [16], попередження та боротьби з кіберзлочинами для прискорення процесів цифровізації і набуття стратегічної конкурентоспроможності країни.

Висновки. Під впливом COVID-19 спостерігаємо активізацію кіберзлочинності, про що свідчить зростаюча динаміка кримінальних правопорушень. Використання суб'єктно-об'єктного і цільового й підходів, що також дозволило сформулювати авторське тлумачення понять «кіберзлочинність» і «кіберзлочин», розвинути криміналістичні характеристики кіберзлочинів за рахунок, поряд іншими, введення таких, як інноваційність, нестандартність здійснення, стратифікація, високий рівень загрози і руйнівного впливу, складність розкриття. Виявлені проблеми і слабкі сторони кримінально-правової оцінки і результативної протидії кіберзлочинності дозволили сформувати практичні рекомендації щодо криміналізації деяких видів злочинів на основі уточнення ознак окремих їх складів у сфері комп'ютерної інформації та кола їх суб'єктів, а також запропонувати заходи для підвищення ефективності протидії кіберзлочинності.

Вважаємо, що потрібно і надалі проводити постійний моніторинг і здійснювати дослідження на виявлення об'єктивних закономірностей, детермінантів і характеристик окремих видів кіберзлочинів, прогнозування поведінкових профілів кіберзлочинців для забезпечення кібербезпеки в період постковідного відновлення.

Список використаних джерел

1. Дашян М.С. Право информационных магистралей. М.: Норма, 2007.
2. Голубев В.А. «Кибертерроризм» - миф или реальность? Центр исследования компьютернных преступлений URL: http://www.crime-research.org (дата звернення: 10.01.2022)
3. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: автореф. дис. ... канд. юрид. наук: 12.00.08. Харків, 2016. 16 с.
4. Карпова Д.М. Кіберзлочинність: глобальна проблема та її вирішення. *Влада*. 2014. № 8. С. 46-50.
5. Сіренко О.В. Поняття кіберзлочинів та особливості методики їх розслідування. URL: http://dspace.oduvs.edu.ua/bitstream/123456789/486/1/ilovepdf_com-48-49%5B1%5D.pdf (дата звернення: 10.01.2022)
6. Бєлєнький В. П. Відповідальність за кіберзлочини за кримінальним правом США, Великобританії та України (порівняльно-правове дослідження) : автореф. дис. ... канд. юрид. наук : 12.00.08. Київ, 2016. 19 с.
7. Русецький А. А., Куцолабський Д. А. Теоретико-правовий аналіз понять «кіберзлочин» і «кіберзлочинність». *Право і Безпека*. 2017. №1. С 74-78.
8. Конвенція про кіберзлочинність Ради Європи від 23.11.2001 р. (Конвенцію ратифіковано із застереженнями і заявами Законом N 2824-IV

(2824-15) від 07.09.2005, ВВР, 2006, N 5-6, ст.71) URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 10.01.2022)

9. Номоконов В. А. Актуальні проблеми боротьби з кіберзлочинністю // Інформаційні технології і безпека: зб. науч. тр. міжнар. конф. Київ: Національна академія наук України, 2003. Вип. 3. С. 104-108.

10. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. Звітність Офісу Генерального прокурора URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2 (дата звернення: 10.01.2022)

11. Кримінальний кодекс України (Відомості Верховної Ради України (ВВР), 2001,№ 25-26, ст.131. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 10.01.2022)

12. Кіберзлочинність не спить – як не потрапити у тенета аферистів URL: https://news.finance.ua/ua/news/-/395023/kiberzlochynnist-ne-spyt-yak-ne-potrapyty-v-siti-aferystiv (дата звернення: 10.01.2022)

13. Інформаційне протистояння як фактор загрози національній безпеці України. Основні тенденції проявів організованої злочинності в сучасних умовах (зб. наук.- аналіт. матеріалів). К.: МНДЦ. 2014. Вип. 1. С. 161-165.

14. Синьоокий О.В. Основи інформаційного права та законодавства у галузі високих технологій та ІТ – інновацій. Х.: Право, 2011. 592с.

15. Харчук В. Запровадження правового регулювання відносин у глобальній мережі Інтернет. *Юридичний журнал*. 2010. № 12. С. 80-82.

16. Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector URL: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf (дата звернення: 10.01.2022)