Розділ V. ПРОБЛЕМИ БОРОТЬБИ ЗІ ЗЛОЧИННІСТЮ ТА ПРАВООХОРОННА ДІЯЛЬНІСТЬ

DOI: 10.33766/2786-9156.105.254-266
УДК: 343:3/7:004(075:8)

Абламський С. Є., *кандидат юридичних наук, доцент, доцент кафедри кримінального процесу та організації досудового слідства факультету № 1 Харківського національного університету внутрішніх справ (м. Харків, Україна)*
e-mail: ablamu4@gmail.com
ORCID iD: https://orcid.org/0000-0003-4716-3985
Романюк В. В., *кандидат юридичних наук, доцент, декан факультету № 1 Харківського національного університету внутрішніх справ (м. Харків, Україна)*
e-mail: awitalimon@gmail.com
ORCID iD: https://orcid.org/0000-0001-6077-4591
Абламська В. В., *наукова співробітниця науково-дослідної лабораторії з проблем наукового забезпечення правоохоронної діяльності та якості підготовки кадрів Харківського національного університету внутрішніх справ (м. Харків, Україна)*
e-mail: ablamskaviktoria@gmail.com
ORCID iD: https://orcid.org/0000-0002-2415-7235

КІБЕРЗЛОЧИННІСТЬ ТА ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ: СУЧАСНІ ВИКЛИКИ ПРАВООХОРОННІЙ СИСТЕМІ

У статті досліджено питання протидії кіберзлочинності та можливості застосування цифрових технологій у діяльності правоохоронних органів. Наголошено, що стрімкий розвиток інформаційних, технічних технологій зумовив не лише появу цифрових правовідносин, але й «породив» нові форми протиправної діяльності, зокрема й нові види кіберзлочинів. Визначено, що кіберзлочинність являє собою суспільно-шкідливе явище, тобто всі види інтернет-злочинів, що здійснюються у сфері інформаційних технологій (у віртуальному просторі). Кіберзлочинність в умовах російської агресії набула нових форм, адже злочинці досить часто створюють фейкові сайти типу Кабінету Міністрів України, «Дії», «єДопомога» та ін., що наносить шкоди як приватним, так і державним інтересам. Окремо акцентовано увагу на використанні електронних зображень як доказів у кримінальному провадженні. Визначено особливості сучасного етапу досудового розслідування комп'ютерних злочинів у частині законодавчого врегулювання електронних доказів, їх відображення та застосування в діяльності правоохоронних органів. Доведено, що перспективи подальшого розвитку питання щодо застосування цифрових технологій повинні здійснюватися в пошуку найбільш оптимальних та ефективних шляхів законодавчого врегулювання питань, пов'язаних із визначенням сутності «електронних доказів», процедури їх збирання, дослідження в суді, особливостей їх технічного відтворення тощо. Зроблено висновок, що доцільним було б закріпити у всіх процесуальних кодексах положення про те, що

у випадку зберігання інформації з електронним зображенням на двох або більше електронних носіях, кожен такий носій прирівнюється до оригіналу електронного документу.

Ключові слова: кіберзлочинність, цифрові технології, кіберзахист, електронний доказ, цифрові відображення.

Постановка проблеми. Бурхливий розвиток інформаційних технологій активізував питання не лише людського цифрового прогресу, цифровізації діяльності органів державної влади та надання різноманітних послуг громадянам, але й став поштовхом до появи нових форм протиправної діяльності, у тому числі у сфері кіберзлочинності. Відповідно, у сучасних умовах розвитку інформаційних технологій існування та подальший розвиток кіберзлочинів становить досить серйозну проблему для правоохоронних органів. Означене негативно впливають як на життєдіяльність фізичних та юридичних осіб, так і на об'єкти критичної інфраструктури, органи державної влади. Окрім прямої шкоди, кіберзлочинність є величезною перешкодою для цифрової довіри, значною мірою підриваючи переваги кіберпростору. Так, відповідно до статистичних даних Офісу Генерального прокурора за 2022 рік, органами правопорядку зареєстровано 3 415 кримінальних правопорушень у сфері інформаційних технологій, у 2021 році – 3 187 кримінальних правопорушень та у 2020 році – 2 498, що свідчить про суттєве зростання вчинення кримінальних правопорушень у сфері інформаційних технологій [1]. Тим паче, необхідно брати до уваги той факт, що російська агресія проти України значно розширила масштаби злочинності в мережі Інтернет, де в більшості випадків кіберзлочинність має російське коріння. Зокрема, під час спільного прес-брифінгу Ради національної безпеки і оборони України, Національного банку України та АТ «Київстар», що відбувся 15 лютого 2023 року, С. Демедюк, зазначив, що «на сьогодні агресор використовує будь-які інструменти, щоб заподіяти якомога більше шкоди Україні, та застосовує різноманітні гібридні засоби, у тому числі й кібершахрайство. Найпопулярнішим методом кібершахраїв під час війни став фішинг – збір персональної інформації громадян, у тому числі необхідної для доступу до фінансових акаунтів та облікових записів. Злочинці створюють фейкові сайти, маскуючи їх, наприклад, під портал Кабінету Міністрів України, різних міжнародних організацій, платформи «єДопомога», «Дія» тощо» [2]. Тож проблема кіберзлочинності та протиправного використання цифрових технологій є вельми актуальною, а визначення нових методів протидії зазначеним негативним явищам є одним із ключових для правоохоронної системи України. На сьогодні в історії розбудови української державності правоохоронні органи стикнулися з новими викликами у сфері протидії кіберзлочинності та використанні цифрових технологій.

Аналіз останніх досліджень і публікацій. Питання протидії кіберзлочинності, дослідження цього явища як такого та застосування цифрових технологій у сфері запобігання кіберзлочинам неодноразово ставали предметом наукового пошуку й дискусій серед правників. Окремі проблемні питання досліджуваної тематики знайшла своє втілення в працях вітчизняних науковців. Так, наприклад, О. Пфо проаналізував основні поняття і класифікація кіберзлочинності [3];

І. Європіна приділила увагу видам протиправних діянь у сфері новітніх інформаційних технологій [6]; С. Мазуренко висвітлив правові проблеми забезпечення кібербезпеки та протидії кіберзлочинності [7]; І. Каланча розглядала питання щодо застосування копій електронної інформації як доказу в кримінальному провадженні [12]; М. Гуцалюк та П. Антонюк розглянули сутність електронної (цифрової) інформації та процесуальну можливість її використання як джерела доказів в кримінальному провадженні [14; 15]; Л. Перцова-Тодорова визначила поняття «електронних доказів» під час розслідування кіберзлочинів [18]; А. Ратнова вивчила кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні [19]; О. Можаєв, В. Пересічанський та В. Рог проаналізували проблемні аспекти протидії кіберзлочинам, на підставі чого визначив перспективи використання ГРІД-мереж у діяльності Національної поліції України у сфері протидії кіберзлочинності [21]. Звісно, наукові пошуку не обмежуються напрацюваннями згаданих авторів. Не викликає сумнівів, що й інші наукові надбання мають вагоме значення, проте в умовах інтенсивної інформаційної атаки зі сторони країни-агресора існує вельми нагальна потреба в перегляді низки положень щодо застосування цифрових технологій у сфері протидії кіберзлочинності.

Формулювання цілей. *Метою* статті є аналіз сучасного стану протидії кіберзлочинності та використання цифрових технологій у діяльності правоохоронних органів. Відповідно до окресленої мети, під час дослідження необхідно розв’язати такі завдання: проаналізувати категорію кіберзлочинність; визначити особливості застосування цифрових технологій під час протидії кіберзлочинам.

Виклад основного матеріалу. Ведучи мову про кіберзлочинність як суспільно-шкідливе явище, ми повинні мати на увазі всі види інтернет- злочинів, що здійснюються у сфері інформаційних технологій (у віртуальному просторі). Злочинність у віртуальному просторі є відносно новим явищем, але частина злочинів, скоєних у сфері інформаційних технологій, – це всім відомі вимагання, крадіжки, шахрайства тощо. Тобто, ті кримінальні правопорушення, що породили такі поняття, як віртуальний простір, кіберзлочинність, комп'ютерний злочин, кібертероризм тощо, але які необхідно відмежувати один від одного та суміжних понять. Зокрема, під кіберзлочинністю прийнято розуміти незаконні дії, що здійснюються людьми, які застосовують інформаційні технології для своїх злочинних цілей [3, с. 33; 4].

З теоретичної та практичної точки зору визначальним є розуміння кіберзлочинності, визначене на рівні Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII [5], де законодавець оперує такими поняттями, як кіберінцидент, кібератака, кіберзагроза, кіберзлочин або комп’ютерний злочин, які визначається законодавцем як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України; та кіберзлочинність як сукупність кіберзлочинів [5]. Як бачимо, законодавець кіберзлочинність розуміє як сукупність одного та більше кіберзлочинів. У цьому контексті

звернемо увагу на п. 14 доповіді комітету II десятого конгресу ООН 2000 р. з попередження злочинності і поводження з правопорушниками, де зазначено, що існує дві категорії інформаційних злочинів: по-перше, це кіберзлочини у вузькому розумінні («комп'ютерні» злочини) – будь-яке протиправне діяння, здійснюване шляхом електронних операцій, метою якого є подолання захисту комп'ютерних систем і оброблюваних ними даних; по-друге, кіберзлочини в широкому розумінні (злочини, пов'язані з використанням комп'ютерів) – будь-яке протиправне діяння, що вчинюється шляхом або в зв'язку з комп'ютерною системою або мережею, включаючи такі злочини, як незаконне зберігання, пропонування або розповсюдження інформації через комп'ютерні системи або мережі [6; 7, с. 576]. Своєю чергою, у Конвенції про кіберзлочинність від 23.11.2001 р. передбачено чотири групи злочинів, пов'язаних із використанням комп'ютерних технологій як інструменту їх учинення. До першої групи віднесено злочини проти конфіденційності, цілісності й доступності комп'ютерних даних і систем (протизаконний доступ, протизаконне перехоплення, вплив на дані, вплив на функціонування системи, а також протизаконне використання пристроїв і комп'ютерних програм). До другої – злочини, пов'язані з використанням комп'ютерних засобів (підроблення, шахрайство). До третьої групи віднесено злочини, пов'язані зі змістом даних. До четвертої – злочини, пов'язані з порушенням авторського права та суміжних прав [8].

Ведучи мову про кіберзлочинність як суспільно-небезпечне діяння, зазначимо, що в розділі XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України визначено перелік видів кіберзлочинів. Зокрема, до останні віднесено: несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК); створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 КК); 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 (ст. 361-2 КК); несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК); порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК) [9].

У процесі протидії, документування та розслідування наведених кримінальних правопорушень одним із важливих питань є використання електронних зображень як доказів у кримінальному провадженні, про що неодноразово наголошували науковці та практики. Так, наприклад, Ю. Орлов та С. Чернявський зауважують, що «дослідження змісту електронного відображення та інформації в сервісних опціях операційної системи про нього надає можливість установити: подію кримінального правопорушення (наприклад, виявляючи сайт із забороненим контентом або з контентом, оприлюднення якого обмежено законом); особу правопорушника (зокрема, шляхом установлення його фізичної адреси за IP-адресою комп'ютера, вивчення даних його акаунта); спосіб, обставини вчинення злочину (наприклад, аналізуючи зміст електронного листування, результати моніторингу банківських рахунків тощо); характер і розмір шкоди, завданої злочином, яка може полягати в порушенні функціонування певних електронних відображень, неправомірному перерахуванні електронних грошових коштів, передплаті ненаданих послуг (товарів), підробленні документів, порушенні авторських прав тощо. Вивчення слідчим електронного відображення також дає змогу підтвердити факти, раніше встановлені іншими доказами, й отримати аргументи для спростування фактів, що належать до інших слідчих версій [10, с. 14]. Тим часом О. Метелев зауважує, що при збиранні цифрової інформації, яка має доказове значення для кримінального провадження, закономірно виникають такі проблемні питання: правова регламентація участі спеціаліста; оформлення процесуальних рішень; технічне забезпечення слідчих; достовірність отриманої цифрової інформації; правовий статус відомостей, отриманих із інформаційно-телекомунікаційних мереж, зокрема глобальної мережі Інтернет [11, с. 228].

Сьогодні під час розслідування кіберзлочинів у ході проведення слідчих (розшукових) дій перед слідчим стає питання щодо збору електронної інформації, яка в подальшому може бути використана як доказ. З цього приводу І. Г. Каланча зауважує, що під час слідчих (розшукових) дій фіксація доказів з електронних носіїв збирання інформації, що міститься на них, може здійснюватися двома способами: 1) вилученням носія або інформаційної системи, до якого він входить; 2) копіюванням інформації, що зберігається на відповідному електронному носії. Вилучення як класичний спосіб збирання доказів у формі матеріальних об'єктів, до яких належать електронні носії та інформаційні системи, попри всі очевидні переваги, має низку недоліків. Зокрема, це стосується випадків неможливості вилучення або неефективності дослідження електронних носіїв після вилучення в разі загрози зупинення критично важливих функцій бізнес-процесів або наявності шифрування тощо. Альтернативою є збирання інформації, що міститься в електронному носії, як доказу в кримінальному провадженні, шляхом виготовлення копії такої інформації [12, с. 336-337]. У цьому аспекті зауважимо, що, відповідно до положень КПК України, «у разі необхідності, слідчий чи прокурор виготовляє за допомогою технічних, програмно-технічних засобів, апаратно-програмних комплексів копії інформації, що міститься в інформацій-

них (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах. Копіювання такої інформації здійснюється із залученням спеціаліста. На вимогу володільця особа, яка здійснює тимчасове вилучення комп'ютерних систем або їх частин, залишає йому копії інформації з таких комп'ютерних систем або їх частин (за наявності технічної можливості здійснення копіювання) з використанням матеріальних носіїв володільця комп'ютерних систем або їх частин. Копії інформації з комп'ютерних систем або їх частин, які вилучаються, виготовляються з використанням технічних засобів, програмно-технічних засобів, апаратно-програмних комплексів володільця із залученням спеціаліста (пп. 2, 3 ч. 2 ст. 168); Дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа (ч. 4 ст. 99)» [13]. Відтак у КПК України з'явився альтернативний спосіб збирання інформації, що має електронну форму, – збирання доказів, що мають електронну форму шляхом копіювання інформації, для якого передбачено процесуальну форму, що можна представити як формулу: «копія інформації × (слідчий або прокурор + спеціаліст) = оригінал документа» [12, с. 337].

Зважаючи на особливості природи та сутність електронної (цифрової) інформації, фактичні дані, зафіксовані в такій формі, поряд із «традиційними» доказами повинні відповідати умовам належності та допустимості для встановлення наявності чи відсутності фактів та обставин, що мають значення для кримінального провадження. Це означає, що має бути чітка процесуальна визначеність як процесуального місця такої інформації, так і порядку її збирання, оцінки й перевірки [14, с. 120; 15, с. 39]. Тож у реаліях сьогодення виникає необхідність запровадження відповідної процесуальної регламентації електронних доказів. До того ж дослідники небезпідставно зазначаються, що необхідність забезпечення процесуальної спроможності електронних доказів у кримінальному провадженні продиктована схваленням Радою Європи 17 листопада 2021 року Другого додаткового протоколу до Конвенції про кіберзлочинність про посилене міжнародне співробітництво [16]. Оскільки Другий додатковий протокол скерований на забезпечення ефективності заходів кримінального правосуддя щодо кіберзлочинів та збору доказів в електронній формі в рамках міжнародного співробітництва, то й унормування понятійного апарату щодо таких доказів та відповідної процесуальної процедури використання їх в процесі доказування на державному рівні виступатиме запорукою узгодженості та злагодженості в міжнародному правовому просторі під час надання взаємної правової допомоги [14, с. 121].

Окремим аспектом, який заслуговує на увагу, є застосування цифрових технологій технічного спрямування, що полегшує органам правопорядку здій-

снювати заходи щодо протидії кіберзлочинності. Наприклад, досвід застосування цифрових технологій у сфері протидії злочинності в Колумбії свідчить, що в цій державі на законодавчому рівні врегульовано питання електронних доказів та визначено базові принципи щодо придатності фактичних даних, якими є нейтральність, цифрова технологія та еквівалентність. У Законі Колумбії № 527 від 1999 р., що регулює питання протидії кіберзлочинності, встановлена можливість надання електронних доказів у його формі «оригіналу», тобто в цифровому форматі, а також у друкованому або фізичному. Незалежно від формату подання, він матиме однакову силу як доказ у суді. Законодавець визначив, що достовірність доказу полягає в тому, що він є як такий, знаходить автентичне вираження на сайті або комп'ютері, який його генерує (тобто залишається неушкодженим) [17, с. 264, 265]. Проте, незважаючи на врегульований процес визначення електронних доказів допустимими, законодавство Колумбії не містить поняття «електронних доказів».

Варто згадати про законодавчий і правозастосовний досвід Сполучених Штатів Америки, де електронні докази як юридичне явище активно розвивається як окремий інститут доказового права. Електронними доказами в цій країні визнаються аудіо- та відеозаписи, фотографії, електронні документи, мобільний телефон, текстові повідомлення, персональний комп'ютер, електронний накопичувальний носій, дані інтернет-трафіку тощо [18, с. 244; 19].

Заслуговує на увагу позитивний досвід Індонезії щодо протидії кіберзлочинності з використанням цифрових технологій. Уряд цієї країні через швидкий розвиток технологічного прогресу та кіберзлочинності вжив багатьох заходів для того, щоб захистити громадян від інтернет-злочинів і кіберзлочинів, прийнявши відповідні нормативні та законодавчі акти. Кіберзакон в Індонезії був створений шляхом об'єднання трьох основних сфер: право інформатики, право ЗМІ та право телекомунікацій. Громадська (публічна) зона кіберправа охоплює кіберзлочинність, захист даних і конфіденційність споживачів, а приватна сфера кіберправа охоплює електронні контракти, інтелектуальну власність та будь-яку електронну комерцію як така. Ці закони мають багато цілей і встановлюють відповідальність за те, як люди використовують, спілкуються та взаємодіють через інтернет [20, с. 122-123]. Як бачимо, в Індонезії на законодавчому рівні врегульовано питання щодо протидії кіберзлочинності та захисту інформації, де застосовуються відповідні цифрові технології захисту.

Під час протидії кіберзлочинності важливе значення має застосування Grid-мереж. Технології Grid-мереж дали можливість виконувати програмні коди на одному або відразу декількох «чужих» комп'ютерах, стали всюди доступними сховища даних із структурованою (бази даних) і неструктурованою (файли) інформацією, джерела даних (датчики, інструменти спостереження) і програмно керовані пристрої [21, с. 69]. Ідейною основою технології Grid є об'єднання ресурсів шляхом створення комп'ютерної інфраструктури нового типу, що забезпечує глобальну інтеграцію інформаційних і обчислювальних ресурсів на основі мережевих технологій і спеціального програмного забезпечення проміжного рівня (між базовим і прикладним програмним забезпеченням), а також набору

стандартизованих служб для забезпечення надійного спільного доступу до географічно розподілених інформаційних і обчислювальних ресурсів: окремих комп'ютерів, кластерів, сховищ інформації і мереж [22, с. 123]. Дана модель кібербезпеки покликана захистити та передбачити можливість кібератак на такі важливі об'єкти, як об'єктів критичної інфраструктури, держаних сайтів, банківські системи тощо. У 2021 р. Національний координаційний центр кібербезпеки при РНБО спільно з проєктом USAID «Кібербезпека критично важливої інфраструктури України» провели заходи із кіберзахисту об'єктів критичної інфраструктури «Grid NetWars», де в основі було застосування Grid-мережі, тобто цілісного сервісу збору та обробки інформації. Опанування технікою Grid Net Wars дозволить здобути передовий досвід у сфері ідентифікації та протидії кібератакам на критичну інфраструктуру України та підвищить готовність українських фахівців до реагування на кіберінциденти будь-якої складності [23].

Враховуючи викладене, слід зазначити, що процес протидії кіберзлочинності охоплює досить місткий об'єм питань, які необхідно врегулювати (електронні докази, програмне забезпечення систем аналізу, обробки та зберігання інформації, захист даних тощо).

Висновки. Кіберзлочинність являє найбільшу загрозу дестабілізаційного впливу на життєвоважливі процеси як суспільного життя, так і державної діяльності. Російська агресія проти України зумовила більш інтенсивний пошук нових форм та методів протидії цим негативним явищем, а також поставила на порядок денний питання щодо законодавчого врегулювання низки питань, пов'язаних із протидією кіберзлочинності.

Відтак перспективи подальшого дослідження мають полягати в пошуку найбільш оптимальних та ефективних шляхів законодавчого врегулювання питань, пов'язаних із визначенням сутності поняття «електронні докази», процедури їх збирання, дослідження в суді, особливостей їх технічного відтворення тощо. Також вбачається доцільним розроблення єдиного підходу до розуміння поняття «копія електронного доказу» та можливості його використання в суді як доказу. У цьому аспекті доцільним було б закріпити у всіх процесуальних кодексах положення про те, що у випадку зберігання інформації з електронним зображенням на двох або більше електронних носіях кожен із них прирівнюється до оригіналу електронного документу.

Використані джерела:

1. Продан Т. Кіберзлочинність: виклики часу. *Chernivtsi law school : сайт.* 2023. URL : https://law.chnu.edu.ua/kiberzlochyn nist-vyklyky-chasu/#:~:text=%D0%97%D0%BE%D0%BA%D1%80%D0%B5%D0%BC%D0%B0%2C%20%D0%B7%20%D0%BE%D0%B3%D0%BB%D1%8F%D0%B4%D1%83%20%D1%81%D1%82%D0%B0%D1%82%D0%B8%D1%81%D1%82%D0%B8%D1%87%D0%BD%D0%B8%D1%85%20%D0%B4%D0%B0%D0%BD%D0%B8%D1%85,%D0%B1%D1%96%D0%BB%D1%8C%D1%88%D0%B5%20%D0%BF%D0%BE%D1%80%D1%96%D0%B2%D0%BD%D1%8F%D0%BD%D0%BE%20%D0%B7%202020%20%D1%80%D0%BE%D0%BA%D0%BE%D0%BC.

2. Фейки, фішинг, крадіжка грошей із карт: у кібершахрайства в Україні російське коріння. *Фокус: електронне видання : сайт.* URL : https://focus.ua/uk/econo-

mics/550155-feyki-fishing-kraza-deneg-s-kart-u-kibermoshennichestva-v-ukra-ine-rossiyskie-korni.

3. Пфо О. М. Основні поняття і класифікація кіберзлочинності. *Актуальні задачі та досягнення у галузі кібербезпеки* : матеріали Всеук. наук.-практ. конф. (23-23 лист. 2016 р.). м. Кропивницький. С. 33-34. URL : https://core.ac.uk/ download/pdf/84825482.pdf.

4. Tropina T. Self- and Co-regulation in Fighting Cybercrime and Safeguarding Cybersecurity. In: Jähnke at al. (eds.), «Current Issues in ITU Security», Duncker & Humblot, Berlin, 2012.

5. Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 № 2163-VIII. *База даних. Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text. (дата звернення: 12.01.2024)

6. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. *Вісник академії адвокатури України*. 2010. № 3. С. 129.

7. Мазуренко С. В. Правові проблеми забезпечення кібербезпеки. URL : http://dspace.onua.edu.ua/bitstream/handle/11300/21618/%D0%9C%D0%B0%D0%B7%D1%83%D1%80%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%A1.%20%D0%92.%20%D0%9F%D1%80%D0%B0%D0%B2%D0%BE%D0%B2%D1%96%20%D0%BF%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC%D0%B8%20%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8.pdf?sequence=1&isAllowed=y.

8. Ткачук М. Поняття кіберзлочинності в українському та міжнародному законодавстві. *ЮРФЕМ.UA : електронне видання : сайт.* URL : https://jurfem.com.ua/ponyattya-kiberzlochynnosti-v-ukrainskomu-ta-mizhnarodnomu-zakonodav-stvi-tkachuk-mariana/.

9. Кримінальний кодекс України : закон України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text. (дата звернення: 12.01.2024)

10. Орлов Ю. Ю., Чернявський С. С. Використання електронних відображень як доказів у кримінальному провадженні. *Науковий вісник Національної академії внутрішніх справ*. 2017. № 3. С. 13-24.

11. Метелев О. П. Проблеми визначення допустимості і належності цифрових (електронних) доказів у кримінальному процесі. *Вісник кримінального судочинства*. 2019. № 3. С. 224-238.

12. Каланча І. Г. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал*. 2021. № 8. С. 336-339.

13. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI. URL : https://zakon.rada.gov.ua/laws/show/4651-17#Text. (дата звернення: 12.01.2024)

14. Гуцалюк М. В., Антонюк Є. П. Процесуальна спроможність використання електронної (цифрової) інформації як доказу в кримінальному провадженні. *Інформація і право*. 2022. № 2. С. 116-122.

15. Гуцалюк М. В., Антонюк П. Є. Щодо сутності електронної (цифрової) інформації як джерела доказів в кримінальному провадженні. *Криміналістичний вісник*. 2020. № 1(32). С. 37- 49.

16. Enhanced cooperation and disclosure of electronic evidence. URL : https://www.coe.int/en/web/cybercrime/opening-for-signature-of-the-second-additional-protocol-to-the-cybercrime-convention.

17. Yepes Gomez, M. M., Perez Benitorevollo, J. A., Peinado Peinado, M. Application of Electronic Evidence in the Colombian Regulatory System. *Novum Jus.* 2022. Vol. 16, No. 1. Pp. 253-277. DOI: https://doi.org/10.14718/NovumJus.2022.16.1.11

18. Перцова-Тодорова Л. «Електронний доказ» під час обшуку. *Підприємництво, господарство і право*. 2020. № 6. С. 243-247.

19. Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : дис. … докт. філософ. : 081 Право. Львів. 2021. 248 с.

20. Hasbullah A. Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers. *International Journal of Cyber Criminology*. 2022. Vol. 16. Issue 2. Pp. 119-130. DOI : https://doi.org/10.5281/ zenodo.4766569

21. Можаєв О., Пересічанський В., Рог В. Аналіз використанні ГРІД-мереж для потреб Національної поліції України : зб. матеріалів Міжнарод. наук.-практ. конф. «Протидія кіберзлочинності та торгівлі людьми» (м. Харків, 18 травня 2021 р.) / МВС України, Харків. нац. ун-т внутр. справ ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків : ХНУВС, 2021. С. 69-70.

22. Мазур В. І., Іванкевич О. В. Grid-технології як ресурс сучасного етапу інформатизації суспільства. *Проблеми інформатизації та управління*. 2010. № 2(30). С. 123-130.

23. Україна перше проводить міжнародні навчання з кіберзахисту. *Процес: сайт.* URL : https://processer.media/ua/ukraini-vpershe-provede-mizhna-rodni-navchannya-z-kiberzahistu-grid-netwars.

References:

1. Prodan, T. (2023) Kiberzlochynnist: vyklyky chasu. *Chernivtsi law school : sait.* N. p. URL : https://law.chnu.edu.ua/kiberzlochynnist-vyklyky-chasu/#:~:text=%D0%97%D0%BE%D0%BA%D1%80%D0%B5%D0%BC%D0%B0%2C%20%D0%B7%20%D0%BE%D0%B3%D0%BB%D1%8F%D0%B4%D1%83%20%D1%81%D1%82%D0%B0%D1%82%D0%B8%D1%81%D1%82%D0%B8%D1%87%D0%BD%D0%B8%D1%85%20%D0%B4%D0%B0%D0%BD%D0%B8%D1%85,%D0%B1%D1%96%D0%BB%D1%8C%D1%88%D0%B5%20%D0%BF%D0%BE%D1%80%D1%96%D0%B2%D0%BD%D1%8F%D0%BD%D0%BE%20%D0%B7%202020%20%D1%80%D0%BE%D0%BA%D0%BE%D0%BC. [in Ukrainian].

2. Feiky, fishynh, kradizhka hroshei iz kart: u kibershakhraistva v Ukraini rosiiske korinnia. (N. d.) *Fokus: elektronne vydannia : sait.* N. p. URL : https:// focus.ua/uk/economics/550155-feyki-fishing-kraza-deneg-s-kart-u-kibermoshennichestva-v-ukra-ine-rossiyskie-korni. [in Ukrainian].

3. Pfo, O. M. (2016) Osnovni poniattia i klasyfikatsiia kiberzlochynnosti. *Aktualni zadachi ta dosiahnennia u haluzi kiberbezpeky : materialy Vseuk. nauk.-prakt. konf. (23-23 lyst. 2016 r.). m. Kropyvnytskyi - Actual tasks and achievements in the field of cyber security: materials of Vseuk. science and practice conf. (November 23-23, 2016). Kropyvnytskyi, 33-34.* URL : https://core.ac.uk/download/pdf/84825482. pdf. [in Ukrainian].

4. Tropina, T. (2012) Self- and Co-regulation in Fighting Cybercrime and Safeguarding Cybersecurity. In: Jähnke at al. (eds.), «Current Issues in ITU Security», Duncker & Humblot, Berlin. [in English].

5. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : zakon Ukrainy vid 05.10.2017 № 2163-VIII. (2017) *Baza danykh. Vidomosti Verkhovnoi Rady Ukrainy - Database. Information of the Verkhovna Rada of Ukraine.* N. p. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text. [in Ukrainian].

6. Yevropina, I. V. (2010) Vydy protypravnykh diian u sferi novitnikh informatsiinykh tekhnolohii. *Visnyk akademii advokatury Ukrainy - Bulletin of the Bar Academy of Ukraine, 3, 129.* [in Ukrainian].

7. Mazurenko, S. V. (N. d.) Pravovi problemy zabezpechennia kiberbezpeky. N. p. URL : http://dspace.onua.edu.ua/bitstream/handle/11300/21618/%D0%9C%D0%B0%D0%B7%D1%83%D1%80%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%A1.%20%D0%92.%20%D0%9F%D1%80 %D0%B0%D0%B2%D0%B E%D0%B2%D1 %96 %20 %D0 %B F%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC%D0%B8%20%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8.pdf?sequence=1&isAllowed=y. [in Ukrainian].

8. Tkachuk, M. (N. d.) Poniattia kiberzlochynnosti v ukrainskomu ta mizhnarodnomu zakonodavstvi. *YuRFEM.UA : elektronne vydannia : sait.* N. p. URL : https://jurfem.com.ua/ponyattya-kiberzlochynnosti-v-ukrainskomu-ta-mizhnarodnomu-zakonoda-vstvi-tkachuk-mariana/. [in Ukrainian].

9. Kryminalnyi kodeks Ukrainy : zakon Ukrainy vid 05.04.2001 r. № 2341-III. (2001) N. p. URL: https://zakon.rada.gov.ua/laws/ show/2341-14#Text. [in Ukrainian].

10. Orlov, Yu. Yu., Cherniavskyi, S. S. (2017) Vykorystannia elektronnykh vidobrazhen yak dokaziv u kryminalnomu provadzhenni. *Naukovyi visnyk Natsionalnoi akademii vnutrishnikh sprav - Scientific Bulletin of the National Academy of Internal Affairs, 3, 13-24.* [in Ukrainian].

11. Metelev, O. P. (2019) Problemy vyznachennia dopustymosti i nalezhnosti tsyfrovykh (elektronnykh) dokaziv u kryminalnomu protsesi. *Visnyk kryminalnoho sudochynstva - Herald of criminal justice, 3, 224-238.* [in Ukrainian].

12. Kalancha, I. H. (2021) Kopiia elektronnoi informatsii yak dokaz u kryminalnomu provadzhenni: protsesualnyi ta tekhnichnyi aspekty. *Yurydychnyi naukovyi elektronnyi zhurnal - Legal scientific electronic journal, 8, 336-339.* [in Ukrainian].

13. Kryminalnyi protsesualnyi kodeks Ukrainy : Zakon Ukrainy vid 13.04.2012 r. № 4651-VI. (2012) N. p. URL : https://zakon.rada.gov.ua/laws/show/4651-17#Text. [in Ukrainian].

14. Hutsaliuk, M. V., Antoniuk, Ye. P. (2022) Protsesualna spromozhnist vykorystannia elektronnoi (tsyfrovoi) informatsii yak dokazu v kryminalnomu prova dzhenni. *Informatsiia i pravo - Information and law, 2, 116-122.* [in Ukrainian].

15. Hutsaliuk, M. V., Antoniuk, P. Ye. (2020) Shchodo sutnosti elektronnoi (tsyfrovoi) informatsii yak dzherela dokaziv v kryminalnomu provadzhenni. *Kryminalistychnyi visnyk - Forensic Heral , 1(32), 37-49.* [in Ukrainian].

16. Enhanced cooperation and disclosure of electronic evidence. (N. d.) (N. p.) URL: https://www.coe.int/en/web/cybercrime/opening-for-signature-of-the-second-additional-protocol-to-the-cybercrime-convention. [in English].

17. Yepes Gomez, M. M., Perez Benitorevollo, J. A., Peinado Peinado, M. (2022) Application of Electronic Evidence in the Colombian Regulatory System. *Novum Jus.* Vol. 16, No. 1. Pp. 253-277. DOI : https://doi.org/10.14718/NovumJus. 2022.16.1.11. [in English].

18. Pertsova-Todorova, L. (2020) «Elektronnyi dokaz» pid chas obshuku. *Pidpryiemnytstvo, hospodarstvo i pravo - Entrepreneurship, economy and law, 6, 243-247.* [in Ukrainian].

19. Ratnova, A. V. (2021) Kryminalni protsesualni ta kryminalistychni osnovy vykorystannia elektronnykh dokumentiv u dokazuvanni. *Doctor`s thesis:* 081 Pravo. Lviv. [in Ukrainian].

20. Hasbullah A. (2022) Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers. *International Journal of Cyber Criminology*. Vol. 16. Issue 2. Pp. 119-130. DOI : https://doi.org/10.5281/zenodo. 4766569. [in English].

21. Mozhaiev, O., Peresichanskyi, V., Roh, V. (2021) Protydiia kiberzlochynnosti ta torhivli liudmy. *Analiz vykorystanni HRID-merezh dlia potreb Natsionalnoi politsii Ukrainy : zb. materialiv mizhnarod. nauk.-prakt. konf. (m. Kharkiv, 18 travnia 2021 r.) - Analysis of the use of GRID networks for the needs of the National Police of Ukraine: coll. materials international. science and practice conf. (Kharkov, May 18, 2021), 69-70.* / MVS Ukrainy, Kharkiv. nats. un-t vnutr. sprav ; HS «Hlobalnyi tsentr vzaiemodii v kiberprostori». Kharkiv : KhNUVS. [in Ukrainian].

22. Mazur, V. I., Ivankevych, O. V. (2010) Grid-tekhnolohii yak resurs suchasnoho etapu informatyzatsii suspilstva. Problemy informatyzatsii ta upravlinnia - *Problems of informatization and management*, *2(30), 123-130.* [in Ukrainian].

23. Ukraina pershe provodyt mizhnarodni navchannia z kiberzakhystu. *Protses: sait.* (N. d.) (N. p.) URL : https://processer .media/ua/ukraini-vpershe-provede-mizhnaro-dni-nav-channya-z-kiberzahistu-grid-netwars. [in Ukrainian].

Стаття надійшла до редколегії 16.01.2024

Ablamskyi S., *PhD in Law, Associate Professor, Head of the Department of Scientific Activity Organization and Intellectual Property Protection, Kharkiv National University of Internal Affairs (Kharkiv, Ukraine)*
Romaniuk V., *PhD in Law, Associate Professor, Dean of the Faculty No 1 Kharkiv National University of Internal Affairs (Kharkiv, Ukraine)*
Ablamska V., *Scientific and Research Laboratory for the Support of Law Enforcement and the Quality of Personnel Training (Kharkiv, Ukraine)*

CYBERCRIME AND THE USE OF DIGITAL TECHNOLOGIES: MODERN CHALLENGES TO THE LAW ENFORCEMENT SYSTEM

The article examines the issue of combating cybercrime and the possibility of using digital technologies in the activities of law enforcement agencies. It is emphasized that the rapid development of information and technical technologies led not only to the emergence of digital legal relations, but also "gave birth" to new forms of illegal activity, including new types of cybercrimes. It was determined that cybercrime is a socially harmful phenomenon, that is, it means all types of Internet crimes committed in the field of information technologies (in virtual space). Cybercrime in the conditions of Russian aggression has acquired new forms, because criminals quite often create fake websites such as the Cabinet of Ministers of Ukraine, "Diya", "yeDopomoga", etc., which harm both private and state interests. Particular emphasis is placed on such an important aspect as the use of electronic images as evidence in criminal proceedings. The peculiarities of the modern stage of the pre-trial investigation of computer crimes in terms of the legislative regulation of electronic evidence, their display and application in the activities of law enforcement agencies have been determined. It has

been proven that the prospects for the further development of the issue of the use of digital technologies should be carried out in the search for the most optimal and effective ways of legislative settlement of issues related to the definition of the essence of "electronic evidence", the procedure for their collection, research in court, the peculiarities of their technical reproduction, etc. It was concluded that it would be expedient to enshrine in all procedural codes the provision that in the case of storing information with an electronic image on two or more electronic media, each such media is equated to the original electronic document.

Keywords: cybercrime, digital technologies, cyber protection, electronic evidence, digital displays.

DOI: 10.33766/2786-9156.105.266-279
УДК: 343.14

Грига М. А., *кандидатка юридичних наук, старша дослідниця, старша наукова співробітниця наукової лабораторії з проблем протидії злочинності ННІ № 1 Національної академії внутрішніх справ (м. Київ, Україна)*
e-mail: mariya_gryga@ukr.net
ORCID ID: https://orcid.org/0000-0003-4561-712X
Бурнос О.О., *аспірантка науково-дослідної лабораторії з проблем криміналістичного забезпечення та судової експертології ННІ № 2 Національної академії внутрішніх справ (м. Київ, Україна)*
e-mail: Helen_Burnos@i.ua
ORCID ID: https://orcid.org/0009-0003-9640-5511

ДОКУМЕНТУВАННЯ ЖОРСТОКОГО ПОВОДЖЕННЯ З ВІЙСЬКОВОПОЛОНЕНИМИ ТА ЦИВІЛЬНИМ НАСЕЛЕННЯМ: УСКЛАДНЕННЯ ТА ВИКЛИКИ

Стаття присвячена актуальним проблемам, які виникають під час документування жорстокого поводження з військовополоненими та цивільним населенням. Акцентовано, що формування якісної доказової бази в таких провадженнях є вкрай важливим етапом притягнення до кримінальної відповідальності російських військових, які вчинили досліджуваний воєнний злочин на території України. Констатовано, що збір та фіксація доказової інформації в таких провадженнях є вкрай ускладненими через цілу низку факторів, найбільш значущими з яких є такі: загроза безпеці учасників слідчих (розшукових) дій унаслідок мінування території, руйнувань, обстрілів тощо; суттєвий розрив у часі між вчиненням досліджуваних злочинів і можливістю дослідити їх слідову картину, а також втрата значної частини слідів унаслідок ведення активних бойових дій; відсутність основних учасників події (свідків, потерпілих та ін.) внаслідок їх смерті, поранення, переїзду, полону тощо; недостатній досвід розслідування воєнних злочинів, а також брак знань у галузі міжнародного гуманітарного права у вітчизняних правоохоронців; недосконалі алгоритми (методика) документування таких злочинів; залучення до процесу документування значної кількості осіб (представників сил безпеки, експертних підрозділів, міжнародних та волонтер-