

## ДЕЯКІ ПРОБЛЕМНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ДОПУСТИМОСТІ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

### SOME PROBLEMATIC ISSUES OF ENSURING THE ADMISSIBILITY OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS

Завидняк В.І., к.ю.н., доцент,  
доцент кафедри кримінального процесу та криміналістики  
Університет державної фіскальної служби України

Шильнікова А.О., здобувач другого (магістерського) рівня  
Навчально-науковий інститут права  
Університету державної фіскальної служби України

Стаття присвячена висвітленню проблемних питань забезпечення допустимості електронних доказів у кримінальному провадженні. Наголошено, що зібрані з дотриманням встановленого законодавством порядку, об'єктивні та достовірні докази – основа судового процесу. Фальсифікація, приховування, спотворення доказів, подання неправдивих відомостей можуть привести до винесення помилкового, а відтак незаконного процесуального рішення (вироку).

Виділено кілька видів критеріїв допустимості електронних доказів, а саме: загальні, які притаманні всім доказам; спеціальні, властиві тільки електронним доказам. Зазначено, що для того щоб служити доказом у кримінальній справі, фактичні дані (електронні докази) повинні бути отримані: 1) належним суб'єктом доказування, 2) належним способом збирання доказів і 3) з належного джерела доказів.

Звернено увагу, що у літературі виділяють ряд додаткових вимог до електронного документа як джерела судового доказу: по-перше, електронний документ повинен містити лише відомості про обставини, які підлягають встановленню по справі, тобто відомості про наявність або відсутність ознак суспільно небезпечного діяння в діях підозрюваного. По-друге, завжди повинна існувати можливість ідентифікації і автентифікації інформації, що міститься в електронному документі.

Для отримання інформації з електронних джерел запропоновано проводити «обшук за допомогою віддаленого доступу», де, на відміну від обшуку в класичному його розумінні, вилучення виявлених документів не відбувається, оскільки здійснюється копіювання вихідної інформації, яка залишається в обстежуваній системі.

Наголошено, що електронні докази в певних випадках є єдиними доказами винності або невинності особи у вчиненні злочину.

Зазначено, що до електронних доказів повинні пред'являтися більш суворі вимоги, оскільки для оцінки їх потрібні спеціальні пристрої, а так само і залучення осіб, які володіють знаннями у вузькій сфері науки. Крім того, електронні докази легко можуть бути піддані зміні або ж можуть бути знищеними. Отже, особливо важлива своєчасна і правильна фіксація електронних доказів.

З урахуванням розвитку інформаційних технологій і особливостей їх функціонування запропоновано введення в КПК України нового виду доказів, заснованих на електронній (цифровій) інформації, а також нової слідчої дії (віддаленого обшуку), що дозволить не тільки технологічно коректно, але і юридично обґрунтовано отримати таку інформацію.

**Ключові слова:** докази, допустимість доказів, джерело доказів, електронні докази, електронний документ, недопустимість доказів, критерії (умови) допустимості доказів, кримінальне провадження.

The article is devoted to the problematic issues of ensuring the admissibility of electronic evidence in criminal proceedings.

It is noted that objective and reliable evidence collected in compliance with the procedure established by law is the basis of the judicial process. Falsification, concealment, distortion of evidence, presentation of false information may lead to an erroneous and thus illegal procedural decision (sentence).

There are several types of criteria for the admissibility of electronic evidence, namely: General, which are inherent in all evidence, and secondly, special, which are inherent only in electronic evidence. It is specified that in order to serve as evidence in a criminal case, actual data (electronic evidence) must be obtained: 1) by the proper subject of proof, 2) by the proper method of collecting evidence, and 3) from the proper source of evidence.

Attention is drawn to the fact that the literature identifies a number of additional requirements for an electronic document as a source of judicial evidence: first, an electronic document must contain information about the circumstances to be established in the case, that is, information about the presence or absence of signs of a socially dangerous act in the actions of the suspect. Second, it should always be possible to identify and authenticate the information contained in an electronic document.

To obtain information from electronic sources, it is proposed to conduct a "remote access search", where, unlike a search in its classical sense, the seizure of discovered documents does not occur, since the original information is copied, which remains in the system under investigation.

It is noted that electronic evidence in certain cases is the only evidence of a person's guilt or innocence in committing a crime.

It is indicated that electronic evidence should be subject to stricter requirements, since special devices are needed to evaluate it, as well as the involvement of persons with knowledge in a narrow field of science. In addition, electronic evidence can easily be altered or destroyed. Therefore, timely and correct recording of electronic evidence is particularly important.

Taking into account the development of information technologies and the peculiarities of their functioning, it is proposed to introduce a new type of evidence based on electronic (digital) information, as well as a new investigative action (remote search), which will allow not only technologically correct, but also legally justified to obtain such information.

**Key words:** evidence, admissibility of evidence, source of evidence, electronic evidence, electronic document, inadmissibility of evidence, criteria (conditions) of admissibility of evidence, criminal proceedings.

Сьогодні активно розвивається наука і техніка, при цьому удосконалюються і способи передачі інформації. Новітні технології все частіше використовуються для вчинення злочинів, що своєю чергою викликає розробку нових способів їх розкриття і розслідування. Цей процес став причиною появи в практиці кримінального судочинства фактично нового виду доказів – електронних, хоча на цей час вказаний вид доказів не виділений в окрему

групу, однак питання допустимості електронних доказів сьогодні можна вважати одним із критеріїв справедливого судового розгляду, що зумовлює актуальність проведеного дослідження.

**Аналіз досліджень і публікацій.** Проблему допустимості доказів досліджували вчені у галузі кримінального процесу та криміналістики, а саме: О.В. Ряшко, Л.М. Лобойко, В.М. Іщенко, І.Л. Чупрікова та інші дослід-

ники. Питання електронних доказів привертало увагу Ю.Ю. Орлова, О.В. Сіренко, Д.М. Цехана.

**Метою статті** є дослідження проблемних питань забезпечення допустимості електронних доказів у кримінальному провадженні.

**Виклад основного матеріалу дослідження.** Чинний Кримінальний процесуальний кодекс України (далі – КПК) концептуально змінив порядок кримінального провадження, запровадив низку нових правових інститутів та механізмів їх реалізації. Зокрема, в Кодексі вперше закріплена глава «Докази і доказування» та передбачені параграфи, що містять поняття доказів, вимоги щодо належності та допустимості доказів, процесу доказування тощо. В ньому вперше визначено поняття допустимості доказів як одна із юридичних властивостей.

Згідно з КПК України ст. 86 «доказ визнається допустимим, якщо він отриманий у порядку, встановленому цим Кодексом» [1].

Докази можуть бути отримані в результаті слідчих (розшукових) і негласних слідчих (розшукових) дій, регламентованих КПК України. Більшість порушень правил, що регламентують проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, виключають можливість визнання отриманих доказів допустимими [2].

Зібрані з дотриманням встановленого законодавством порядку, об'єктивні та достовірні докази – основа судового процесу. Фальсифікація, приховування, спотворення доказів, подання неправдивих відомостей можуть привести до винесення помилкового, а відтак незаконного процесуального рішення (виroku).

Відповідно до ч. 2 ст. 84 процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів. Ст. 84 КПК України містить положення щодо документів, які можуть містити відомості, зафіксовані як у письмовому, так і в іншому вигляді.

Електронний вид доказів є різновидом доказів загалом і володіє при цьому певною специфікою, яка полягає передусім у носії електронних документів. Електронні документи містяться на особливих носіях: жорстких дисках, серверах, флеш-картах тощо.

Вважаємо, що умовами допустимості «класичного» документа як джерела доказів є такі: 1) має бути відомим автор документа (установа, організація, підприємство, посадова особа або громадянин); 2) зміст документа має відповідати компетенції і фактичній обізнаності автора. Це дозволяє перевірити доказ.

Вбачається, що такі умови допустимості слід висувати й до електронних відображень, що їх сформулювала людина. Наприклад, пост (повідомлення) на форумі або у блозі, відправлений під ніком (мережовим псевдонімом), який не можна перевірити, є анонімним і не може бути використаний у доказуванні. При цьому слід мати на увазі, що відомості про автора (укладача) електронного відображення далеко не завжди зафіксовані на цьому відображенні, особливо, коли воно містить заборонений контент або прямо призначене для вчинення злочину [3, с. 18].

Говорячи про критерії допустимості електронних доказів, можна виділити кілька їх видів. По-перше, загальні, які притаманні всім доказам. Наприклад, складання протоколу, збирання їх спеціально уповноваженою особою, зазначеною в законі, участь певних осіб (поняті тощо), і по-друге, спеціальні, властиві тільки електронним доказам. Так, комп'ютерна експертиза повинна проводитися компетентним фахівцем, огляд сайту повинен проводитися слідчим, дізнавачем, співробітником органу дізнання за участю фахівця і понятих, хід і результати слідчої дії повинні бути зафіксовані у відповідному протоколі тощо.

Тобто для того щоб служити доказом у кримінальній справі, фактичні дані (електронні докази) повинні бути отримані: 1) належним суб'єктом доказування, 2) належним способом збирання доказів і 3) з належного джерела доказів.

Також у літературі виділяють ряд додаткових вимог до електронного документа як джерела судового доказу: по-перше, електронний документ повинен містити лише відомості про обставини, які підлягають встановленню по справі, тобто відомості про наявність або відсутність ознак суспільно небезпечного діяння в діях підозрюваного. По-друге, завжди повинна існувати можливість ідентифікації і автентифікації інформації, що міститься в електронному документі. Технологія обміну електронними документами по телекомунікаційним засобам зв'язку або з використанням інших носіїв інформації дає цілий ряд переваг. Але при цьому виникає проблема ідентифікації автора документа, тобто можливість встановлення того, що він дійсно отриманий від особи, яка, наприклад, позначена в ньому як відправник. А також автентифікацією самого документа, під якою розуміється можливість перевірки цілісності і незмінності змісту електронного документа. По-третє, електронний документ тільки тоді стає джерелом судового доказу, коли він отриманий з дотриманням процесуальних правил оформлення, а тому, на наш погляд, найбільш вірним можна вважати таке визначення електронного документа – це матеріальний носій, на якому містяться відомості про обставини, що підлягають встановленню у кримінальній справі, записані на магнітний, оптичний, магнітооптичний накопичувач, карту флеш-пам'яті та інший подібний носій, отримані з дотриманням процесуального порядку їх збирання.

Збирання електронних доказів, як і інших видів доказів, здійснюється шляхом проведення слідчих та інших процесуальних дій. Тут особливо слід виділити обшук, виїмку і огляд.

Вважаємо, що попри те, що арсенал наявних процесуальних дій досить великий, він все ж, з одного боку, обмежений вичерпним списком, а з іншого – в розглянутих нами цілях фактично зводиться до єдиної слідчої дії – огляду.

Водночас говорити про безпосереднє сприйняття людиною електронної (цифрової) інформації не доводиться, оскільки для її огляду необхідна комп'ютерна техніка і програмне забезпечення, що дозволяє сформулювати якість уявлення про неї. Однак слідчий не завжди має справу безпосередньо з фізичним «електронним носієм інформації». Особливістю функціонування комп'ютерних мереж є та обставина, що отримати інформацію, що має значення для кримінальної справи, можливо і не маючи фізичного доступу до місця її зберігання (конкретного сервера) і навіть не знаючи її точного фізичного місця розташування. З урахуванням сказаного, на нашу думку, можна погодитися з оформленням отриманої цифрової інформації протоколом огляду, але тільки в тому разі, коли досліджуються загальнодоступні дані, розміщені у відкритих джерелах (інформація на сайтах, доступ до яких не вимагає знання паролів, тощо). Водночас інформація в комп'ютерних мережах зберігається і розміщується не тільки на сайтах у відкритому доступі. Найчастіше доступ до розділу Сайту можливий тільки «за паролем». Крім того, існує і так званий «закритий» («глибокий») Інтернет, який являє собою мережу, фактично не видиму для простих користувачів і пошукових машин, засновану на звичайній інфраструктурі Інтернету. Фактично весь його вміст розташовується на серверах, що знаходяться в зоні «глибокої павутини». Пошукові машини не можуть їх проіндексувати, а відтак і простий користувач просто так їх не побачить. Доступ до них здійснюється через ланцюжок зашифрованих з'єднань. При цьому вузлі, через які буде проходити інформація, розкидані по всьому світу, і відстежити, звідки був посланий запит, досить проблематично.

Говорити ж про огляд у процесуальному сенсі електронної (цифрової) інформації в тих випадках, коли вона зберігається в закритому для загального доступу вигляді, на нашу думку, не можна. Для отримання інформації в таких випадках пропонуємо проводити обшук або виїмку.

У традиційному розумінні обшук і виїмка, спрямовані на виявлення і вилучення цифрової інформації (документів), пов'язані з фізичним проникненням в приміщення, де знаходяться електронні носії, з подальшим вилученням або самих фізичних носіїв, або копіюванням (перенесенням) інформації на інші носії. Однак розвиток телекомунікаційних технологій в деяких ситуаціях призводить до марності проведення цих слідчих дій. Йдеться про використання в злочинних цілях віддалених ресурсів мережі, в тому числі «хмарних технологій», які отримали останнім часом велику популярність. У разі використання обвинуваченим «підозрюваним» хмарних сервісів вилучення органами розслідування його комп'ютера (іншого комунікаційного пристрою) дасть слідству тільки інформацію про звернення особи до тих чи інших ресурсів в мережі інтернет (їх IP-адреси), та й то лише через деякий час після проведеного огляду вмісту вилученого пристрою або його комп'ютерної експертизи. При цьому сама інформація, що зберігається на віддалених серверах і представляє доказове значення для кримінальної справи, так і не буде отримана слідством. Навіть більше, можливість доступу до зазначених сховищ обвинуваченого (підозрюваного) з будь-якого пристрою, що має вихід в Мережу (а не тільки з вилученого), дозволить йому знищити викривальну інформацію (докази). Таким чином, перед органами попереднього розслідування постає питання виявлення, доступу, вилучення інформації, що представляє доказове значення і, головне, правильне процесуальне оформлення цих дій.

Для отримання інформації з таких джерел пропонується проводити «обшук за допомогою віддаленого доступу». Але, на відміну від обшуку в класичному його розумінні, в цьому разі вилучення виявлених документів не відбувається, оскільки здійснюється копіювання вихідної інформації, яка залишається в обстежуваній системі. Технологія «віддаленого обшуку» передбачає використання спеціальних знань не тільки для виявлення і закріплення (копіювання) інформації, але і для отримання доступу до неї (обхід або злом паролів, використання спеціалізованих програмно-апаратних засобів і так далі). Слід зазначити, що обсяг використання спеціальних знань в рамках такої слідчої дії можна порівняти з виробництвом спеціалізованої комп'ютерної експертизи. Мабуть, на цій підставі деякими практиками пропонується в розглянутих випадках призначати комп'ютерну експертизу. На перший погляд така думка має право на існування, оскільки судова експертиза призначається за необхідності вирішення питань, що вимагають спеціальних знань в сфері науки, техніки, мистецтва або ремесла. Однак КПК України під час призначення експертизи вимагає від слідчого представити в розпорядження експерта відповідні матеріали, вказавши їх у постанові про призначення експертизи. Які матеріали повинен вказати слідчий в постанові при ситуації, що розглядається?

Проблемними є випадки, коли дані про умови та обставини проведення оперативно-розшукових заходів належать до відомостей, що становлять державну таємницю, перевірка достовірності доказів, сформованих на їх основі, в умовах гласного кримінального процесу стає принципово неможливою. Цим пояснюється те, що долучені до кримінальної справи матеріали оперативно-розшукової діяльності можуть не містити необхідної і достатньої інформації для формування на їх основі доказів, що задовольняють вимогам КПК.

Ситуація ускладнюється тим, що з розвитком науково-технічних засобів, особливо комп'ютерних технологій, істотно розширилися можливості монтажу, підробки й інших способів фальсифікації матеріалів аудіо- та відеозаписів. У той же час межі перевірки носіїв аудіо- та відеоматеріалів, доданих до рапорту (повідомлення) про зло-

чин, що подаються як результати оперативно-розшукової діяльності як джерела доказової інформації в рамках гласного змагального кримінального процесу, звужилися. Це пояснюється декількома причинами: по-перше, з розвитком науки і техніки багаторазово розширилися технологічні можливості виробництва комп'ютерного монтажу цифрових фонограм і відеофонограм без залишення видимих слідів маніпуляцій із записаною доказовою інформацією; по-друге, сучасні технології комп'ютерної графіки і мовного синтезу і витончені способи інтелектуального підроблення дозволяють штучно створювати нібито докази злочину за допомогою мультиплікації, інсценування, імітації тощо.

Перевірити достовірність інформації, відображеної в матеріалах аудіо- та відеозапису, експертним шляхом можливо тільки за умови надання експерту вичерпних даних про технологічний ланцюжок виробництва речового доказу. Однак у разі застосування спеціальних технічних засобів негласного аудіо- та відеозапису ці відомості, включаючи інформацію про пристрої запису, зазвичай складають державну таємницю. При цьому до матеріалів кримінальної справи долучаються здебільшого вибірково переписані на один носій копії, отримані в різний час, причому зазвичай модифіковані. В кращому разі експерти по ним дають висновок про те, що ознак монтажу не виявлено (що саме по собі зовсім не гарантує достовірність записаної аудіо- та відеоінформації), а в гіршому – відмовляються від вирішення цього завдання, мотивуючи це нестачею наданих матеріалів.

Проблема полягає в тому, що виникає колізія захисту відомостей, що становлять державну таємницю, та забезпечення права на захист від фальсифікації результатів оперативно-розшукової діяльності, які лягають в основу формування доказів щодо кримінальної справи.

Для вирішення зазначеної колізії під час подання результатів оперативно-розшукової діяльності для використання в доведенні у кримінальній справі в умовах гласного судочинства представляється доцільним конкретизувати перелік криміналістично значущих даних, необхідних і достатніх для судово-експертної діагностики та автентичності матеріалів аудіо- та відеозапису, виконуваних під час проведення оперативно-розшукових заходів.

У світлі недавніх скандалів в Україні, пов'язаних із записами аудіорозмови членів уряду, варто згадати досвід ЄСПЛ, а саме недавню справу Букур і Тома проти Румунії [Bucur et Toma C. Roumanie] [4], де один із заявників, колишній співробітник румунської розвідки, був засуджений за розголошення секретної інформації про нібито незаконне прослуховування телефонних розмов. Під час судового розгляду він посилався на відсутність дозволів і обставин, які могли б становити загрозу для національної безпеки і обґрунтували б перехоплення телефонних переговорів, про які йшлося. Національна влада відмовилася надати певні надсекретні докази, щоб підтвердити справжність дозволів на перехоплення комунікацій. На думку суду, оприлюднена інформація набула особливої важливості в суспільстві, яке під час комуністичного режиму близько стикалося зі спостереженням, здійснюваним секретними службами. До того ж спокій громадянського суспільства було прямо порушено оприлюдненою інформацією, оскільки після цього кожен міг думати, що його телефонні розмови теж можуть прослуховувати. Крім того, ця інформація мала відношення і до зловживань демократичними основами держави, вчиненими високопосадовцями. Суд вважає, що, відмовляючись перевіряти чи була класифікація «Цілком таємно» виправдана і відмовляючись відповідати на питання чи перевищував інтерес збереження конфіденційності інформації суспільному інтересу бути в курсі передбачуваного незаконного перехоплення комунікацій, національні суди не намагалися вивчити питання у всіх його аспектах, тим

самим позбавляючи заявника права на справедливий судовий розгляд.

У справах Крюслен проти Франції [Kruslin c. France] [5] і Хювік проти Франції [Huvig c. France] [5] суд, враховуючи те, що прослуховування та інші форми перехоплення телефонних розмов представляють собою серйозне втручання в приватне життя і кореспонденцію, вважає, що вони повинні бути засновані на «законі», який в цій частині повинен бути особливо точним. Потрібні чіткі і детально розроблені правила проведення подібних оперативних заходів, тим більше, що використовувані технології постійно розвиваються і ускладнюються. Далі Суд описує, що саме повинно містити адекватне законодавство, зазначаючи, що французька система не надає достатніх гарантій проти можливості різного роду зловживань і в підсумку встановлює порушення статті 8. Наприклад, в жодному документі не визначені категорії осіб, телефони яких можуть бути прослухані за постановою суду, так само як не визначено характер правопорушень, з якого можливе прослуховування. Ніщо не зобов'язує суддю визначати тривалість цього заходу. Не встановлено порядок складання підсумкових протоколів, що фіксують прослухані розмови. Не зумовлені запобіжні заходи, які повинні прийматися для збереження записів в цілісності й правильному зберіганні на випадок можливої їх перевірки суддею або адвокатом. Не визначені обставини, за яких записи можуть або повинні бути розмагнічені, а також коли необхідно знищувати стрічки із записами (наприклад, при знятті обвинувачення або при виправданні судом) Вебер і Саравія проти Німеччини [Weber et Saravia c. Allemagne] [5]. Варто звернути увагу на те, що ця постанова вплинула на національну систему, оскільки згодом був прийнятий відповідний закон.

Отже, вважаємо, що електронні докази в певних випадках є єдиними доказами винності або невинності особи у вчиненні злочину.

Таким чином, до електронних доказів повинні пред'являтися більш суворі вимоги, оскільки для оцінки їх потрібні спеціальні пристрої, а так само і залучення осіб, які володіють знаннями у вузькій сфері науки. Крім того, електронні докази легко можуть бути піддані змінам або ж можуть бути знищеними. Отже, особливо важлива своєчасна і правильна фіксація електронних доказів.

Міжнародне співтовариство вже робить певні кроки в цьому напрямку. Так, питання віддаленого обшуку в комп'ютерних мережах отримало спробу врегулювання в Конвенції про злочинність у сфері комп'ютерної інформації ETS № 185: «Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб у разі, коли її компетентні органи здійснюють обшук або подібний доступ до конкретної комп'ютерної системи або її частини ... і мають підстави вважати, що дані, які розшуковуються, зберігаються у іншій комп'ютерній системі чи її частині, яка знаходиться на її території, і до таких даних можна здійснити законний доступ з першої системи чи вони є доступними першій системі, такі компетентні органи мали право терміново поширити обшук або подібний доступ на іншу систему» (ч. 2 ст. 19) [6]. Тим більше, що Україна приєдналася до цієї Конвенції.

Отже, з урахуванням розвитку інформаційних технологій і особливостей їх функціонування пропонуємо введення в КПК України нового виду доказів, заснованих на електронній (цифровій) інформації, а також нової слідчої дії (віддаленого обшуку), що дозволить не тільки технологічно коректно, але і юридично обґрунтовано отримати таку інформацію.

#### ЛІТЕРАТУРА

1. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 №4651-VI. Дата оновлення: 16.01.2020. URL: <https://zakon.rada.gov.ua/laws/show/4651-17> (дата звернення: 16.08.2020).
2. Ряшко О.В. Деякі проблемні питання щодо значення та умов допустимості отримання доказів у кримінальному процесі. *Науковий вісник Львівського державного університету внутрішніх справ. серія юридична*. 2013. Вип С. 428-436. URL: [http://nbuv.gov.ua/UJRN/Nviduvs\\_2013\\_4\\_48](http://nbuv.gov.ua/UJRN/Nviduvs_2013_4_48) (дата звернення: 14.07.2020).
3. Орлов Ю.Ю. Використання електронних відображень як доказів у кримінальному провадженні. *Науковий вісник Національної академії внутрішніх справ*. 2017. №3. С. 13–25. URL: [http://nbuv.gov.ua/UJRN/Nvknuvs\\_2017\\_3\\_3](http://nbuv.gov.ua/UJRN/Nvknuvs_2017_3_3) (дата звернення: 19.08.2020).
4. Постанова Європейського суду з прав людини від 8 січня 2013 р. справа «Букур і Тома проти Румунії» [Bucur and Toma v. Romania] (скарга N 40238/02) (III секція) URL: <https://base.garant.ru/70427960/> (дата звернення: 18.07.2020).
5. Фулей Т.І. Застосування практики Європейського суду з прав людини при здійсненні правосуддя: Науково-методичний посібник для суддів. 2-ге вид. випр., допов. Київ, 2015. 208 с. URL: <https://www.osce.org/uk/ukraine/232716?download=true> (дата звернення: 20.08.2020).
6. Конвенція о преступности в сфере компьютерной информации ETS №185 (Будапешт, 23 ноября 2001 г.). СПС «Гарант». URL: [https://zakon.rada.gov.ua/laws/show/994\\_575](https://zakon.rada.gov.ua/laws/show/994_575) (дата звернення: 12.09.2020).