ГРЕБЕНЬКОВА М. С.,
ад'юнкт кафедри криміналістики
та судової медицини
(Національна академія внутрішніх справ)

УДК 343.985.3
DOI https://doi.org/10.32842/2078-3736/2021.6.36

АКТУАЛЬНІ ПРОБЛЕМИ ЕЛЕКТРОННИХ ВІДОБРАЖЕНЬ У СОЦІАЛЬНИХ МЕРЕЖАХ ЯК ДЖЕРЕЛА ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Цифрові технології із кожним днем все ширше втілюються у повсякденне життя суспільства. Урядові установи, банки, торговельні організації, окремі громадяни дедалі більше залежать від надійного функціонування інформаційних інфраструктур, поєднаних глобальною мережею. Зі збільшенням кількості користувачів мережі Інтернет постійно виникають загрози протиправного використання інформаційних технологій. Водночас сучасне суспільство має бути впевнене в тому, що на кіберзлочинців чекає викриття і заслужене покарання.

У статті здійснено аналіз електронних відображень у соціальних мережах як джерел доказової бази у кримінальному провадженні, висвітлено їхню сутність і значення у сфері забезпечення кібербезпеки. Крім того, наголошено на проблематиці, пов'язаній із їхньою фіксацією такого виду доказів.

Зазначено, що наукова площина досліджень джерел доказів в електронному вигляді потребує постійного емпіричного оновлення і теоретичного осмислення у галузях криміналістики, кримінального процесу України та оперативно-розшукової діяльності. Обґрунтовано необхідність дотримання певних процедур вилучення і дослідження електронних (цифрових) доказів під час кримінальних проваджень та використання водночас спеціальних знань.

Основою наукового криміналістичного аналізу стало комплексне поєднання філософських (діалектичний), загальнонаукових (синтез, аналіз, індукція, дедукція, узагальнення) і спеціальних методів. Відповідно до мети дослідження використано спеціальні методи правових наук. Застосування комплексного системного підходу до вирішення завдань дослідження, а також таких наукових методів, як прогнозування, синтез, аналіз, порівняння та узагальнення, дали змогу отримати достовірні результати і висновки.

У роботі проаналізовано низку наукових джерел і матеріал статтей інформаційних видань, із яких можна зробити висновок, що використання «електронних зображень», зокрема зображень із соціальних мереж, як джерел доказів нині впроваджене у практичну діяльність багатьох закордонних країн. Однак визначено, що для впровадження «електронних відображень» у соціальних мережах потрібно вирішити питання, пов'язані із залученням спеціаліста у кримінальному провадженні, оскільки існує ризик підробки інформації із соціальних мереж та вилучення нетотожної копії оригіналу, що міститься на матеріальному носії, який може бути розташований поза межами України. Зроблено висновок щодо доповнення положень ст. 71 КПК України ч. 2-1, 2-2, в яких передбачено залучення спеціаліста і вимоги до останнього в разі нагальної потреби здійснення фіксації та вилучення «електронних відображень».

Ключові слова: електронні відображення, соціальна мережа, джерела доказів, кримінальне провадження.

Hrebenkova M. S. Actual problems of electronic mapping in social networks as sources of evidence in criminal proceedings

Digital technologies are becoming more and more embodied in the daily life of society. Government agencies, banks, trade organizations, and individual citizens are increasingly dependent on the reliable operation of information infrastructures connected to the global network. With the increase in the number of Internet users, there are constant threats of illegal use of information technology. At the same time, modern society must be convinced that cybercriminals will be exposed and deservedly punished.

The article analyzes electronic mapping in social networks as sources of evidence in criminal proceedings, highlights their essence and importance in the field of cybersecurity. In addition, the issues related to their fixation of this type of evidence are emphasized. It is noted that the scientific plane of research of sources of evidence in electronic form requires constant empirical updating and theoretical understanding in the fields of criminalistics, criminal procedure of Ukraine and operational and investigative activities. The necessity of observance of certain procedures of extraction and research of electronic (digital) evidence during criminal proceedings and use of special knowledge is substantiated.

The basis of scientific forensic analysis was a complex combination of philosophical (dialectical), general scientific (synthesis, analysis, induction, deduction, generalization) and special methods. In accordance with the purpose of the study, special methods of legal sciences were used. The application of a comprehensive systematic approach to solving research problems, as well as such scientific methods as forecasting, synthesis, analysis, comparison and generalization allowed to obtain reliable results and conclusions.

The author analyzes a number of scientific sources and material of articles of information publications, from which it can be concluded that the use of "electronic images", in particular images from social networks, as sources of evidence is now implemented in many foreign countries. However, it is determined that for the introduction of "electronic mapping" in social networks it is necessary to address issues related to the involvement of a specialist in criminal proceedings. Since there is a risk of forgery of information from social networks and the removal of an inaccurate copy of the original, which is contained on a tangible medium, which may be located outside of Ukraine. The conclusion concerning addition of provisions of Art. 71 of the CPC of Ukraine, parts 2-1, 2-2, which provide for the involvement of a specialist and requirements for the latter in case of urgent need to record and remove "electronic mapping".

Key words: *electronic mapping, social networks, sources of evidence, criminal proceedings*

Вступ.

Інформаційне суспільство, яке змінило індустріальне, швидко розвивається. Із появою науки і техніки люди почали все більше входити у віртуальне середовище. Водночас можна вважати, що факторами, які зумовлюють стрімке зростання злочинності та радикалізації суспільства, є не лише обіг незаконних засобів, зброї, але передусім підвищення рівня інформатизації суспільства, що здійснюється за допомогою ефективних засобів комунікації, зокрема мережі Інтернет. Нині кіберзлочинність є ключовою проблемою XXI століття, а володіння потрібною інформацією є значним ресурсом. Тому нагальним питанням є виокремлення «електронних відображень» як окремої категорії джерел доказів та розгляд доцільності використання у кримінальному судочинстві такої категорії «електронних відображень», як відомості із соціальних мереж.

Постановка завдання. Метою роботи є аналіз інформації із соціальних мереж як елементу «електронних відображень», джерела доказів у кримінальному провадженні.

Задля досягнення мети поставлено завдання охарактеризувати історичне, правове, соціальне і технологічне підґрунтя для вилучення електронних відображень як доказів. Основою наукового правового аналізу стало комплексне поєднання філософських (діалектичний), загальнонаукових (синтез, аналіз, індукція, дедукція, узагальнення) і спеціальних методів. Відповідно до мети дослідження використано спеціальні методи правових наук. Зокрема, застосування логіко-семантичного методу дозволило розкрити поняття та юридичні визначення сутності електронних відображень, а використання формально-юридичного (догматичного) методу сприяло формально-логічному тлумаченню законодавчих актів, дозволило виявити загальні тенденції законодавчого процесу та використані законодавцем юридичні принципи. Теоретичну основу статті становили наукові праці українських і зарубіжних науковців із криміналістики, оперативно-розшукової діяльності, кримінального процесу тощо; емпіричну – норми національного законодавства з питань «електронних відображень».

Результати дослідження

Джерела доказів нині відіграють вирішальну роль у кримінальному провадженні. Можна вважати, що джерела доказів є головним інструментом кримінального процесуального доказування. Як відомо, законодавець у нормах ст. 84 КПК України визначив, що доказами (ч. 1 ст. 84 КПК України), проте не надав визначення терміну процесуальних джерел доказів, а лише надав їхній перелік (ч. 2 ст. 84 КПК України) [1]. Така позиція законодавця не залишила байдужою наукову спільноту. Зі свого боку низка науковців-процесуалістів не залишають недослідженим і сам перелік процесуальних джерел доказів, говорячи про його недосконалість і неповноцінність. Зокрема, нині набуває актуальності доповнення до переліку процесуальних джерел так звані «електронні докази» або «електронні (цифрові) відображення». На нашу думку, саме друге визначення найбільш наближене до сутності досліджуваного явища як елементу процесуальних джерел. Оскільки, як було слушно зазначено у дослідженні Ю.Ю. Орловим та С.С. Чернявським, «*за критерієм відношення до кримінального провадження електронні відображення є подібними до речових доказів*» [2, с. 116], це дійсно може вказувати на «електронні зображення» як на окреме джерело доказів. Окрім того, що не менш важливо, поняття «електронне відображення» за властивостями не охоплюється повною мірою терміном «документ», оскільки воно не наділено всіма якостями документу і може змінюватись у часі та в електронному просторі.

Саме через це, на нашу думку, можна ототожнювати такі терміни, як «електронні докази» та «електронні сліди» відносно поняття «електронні зображення». Подібність наданих термінів беззаперечно визначає те ж саме явище під різним кутом. Наприклад, А.В. Коваленко вважає «електронне відображення» синонімом «електронного сліду» [3, с. 240-241]. На думку Г.К. Авдєєвої та С.В. Стороженко, «електронні цифрові сліди» – це матеріальні невидимі неозброєним оком сліди, що можуть бути виявлені, зафіксовані та вивчені за допомогою цифрових електронних пристроїв, та які містять будь-яку криміналістично значущу інформацію (відомості, дані), зафіксовану в електронній цифровій формі на матеріальних носіях [4, с. 172]. В.Б. Вєхов, Б.П. Смагоринський та С.А. Ковальов розуміють поняття «електронний слід» як будь-яку криміналістично значущу інформацію, тобто відомості (повідомлення, дані), представлені у формі електричних сигналів незалежно від засобів їх зберігання, обробки та передачі. Механізм їх утворення заснований на електромагнітній взаємодії двох або більшої кількості об'єктів [5, с. 17].

І.О. Крицька інтерпретує поняття «цифрові джерела доказової інформації» як програми (програмне забезпечення), файли баз даних, аудіо-, відеозаписи тощо, джерелом і формою існування котрих виступають пристрої; постійні пристрої, що запам'ятовують; накопичувачі на жорстких магнітних дисках (вінчестери, дискети); мобільні машинні носії (оптичні носії, флеш-карти); NAS-системи тощо [6, с. 302], що черговий раз є аргументом на користь концепції «електронні відображення», вперше запропонованої Ю.Ю. Орловим і С.С. Чернявським. Останні наполягають на необхідності законодавчого врегулювання норм

КПК України, а саме у частині використання електронних відображень у кримінальному процесі. Зокрема, запропоновано доповнити КПК України положенням ст. 100-1 «Електронні відображення», відповідно до якої слідує таке: «*1) електронним відображенням є цілісна система відомостей та (або) комп'ютерних інструкцій в інформаційній мережі або на технічному носієві, яка може бути використана як доказ факту чи обставин, що встановлюються під час кримінального провадження*». Розглянувши наведене визначення, можна зрозуміти відмінність «електронних відображень» від документів та інших джерел доказів. На відміну від норми ч. 1 ст. 100-1 проєкту закону «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби із кіберзлочинністю та використання електронних доказів», де «електронні докази» – це «інформація в електронній (цифровій) формі із відомостями» [2, с. 117], ми розуміємо, що «електронні відображення» є частиною окремої цілісної системи, що працює за своїми внутрішніми правилами та відповідно до заданої структури (алгоритмів та інше), за допомогою якої учасниками кримінального провадження є змога отримувати, використовувати і досліджувати відомості, котрі мають значення для кримінального провадження замість абстрактної «інформації», що перебуває у «цифровій формі», якій законодавець досі не дав визначення та ознаки. Відповідно до ч. 2 ст. 100-1 пропозицій Ю.Ю. Орлова та С.С. Чернявського визначено перелік елементів, що підпадають під визначення «електронних доказів»: *«2) до електронних відображень (за умови наявності в них інформації, передбаченої частиною першою цієї статті) належать: портали, сайти у комп'ютерній мережі; електронні бази даних; файли і групи файлів; зміст електронної пошти, чатів; вихідні та виконувані модулі комп'ютерних програм; інші відомості та (або) комп'ютерні інструкції в інформаційній мережі або на технічному носієві*» [2, с. 117].

На нашу думку, соціальні мережі відносяться до категорій комп'ютерних порталів/сайтів. А.В. Турчин у своєму дослідженні класифікував соціальні мережі за такими ознаками: за географічним розташуванням: світового значення, окремо взята країна, територіальна одиниця, без регіональної належності; за спрямуванням: особисті, професійні, тематичні; соціальні мережі для спілкування («Вконтакте», «Facebook» та інші); соціальні мережі для обміну медіаконтентом (відео і фото) («Instagram», «YouTube»); соціальні мережі для колективного спілкування (обмін знаннями) («Quora», «Reddit»); соціальні мережі для авторського запису (блогінг) («Blogger», «Twitter»); сервіси соціальних закладок вподобань («Pinterest», «Flipboard»); соціальні мережі пошуку однодумців та людей зі схожими інтересами («Goodreads», «Friendster») [7, с. 206].

Водночас кримінальне середовище теж перейшло на інший рівень спілкування. Операції із купівлі-продажу речей і речовин, що становлять загрозу для оточуючих чи заборонені у вільному обігу, або їхні аналоги здійснюються через так званий «чорний ринок» за допомогою так званої мережі «даркнет», тіньового Інтернету. Зокрема, за допомогою мережі так званого «даркнету» можна здійснити такі фінансові операції: найм кілера (домова про вбивство особи); купівля-продаж людських органів, наркотичних чи психотропних речовин, зброї, дитячої порнографії, контрафактних товарів, інформації про акаунти у соціальних мережах (або логіни та паролі до них), інформації із баз даних або доступ до них, персональної інформації про осіб, інформації із банківської таємниці, підроблених документів, послуг кібератак і терористичної діяльності [8].

Тож, на нашу думку, буде не менш важливим навести низку випадків притягнення до відповідальності осіб, які під час своєї протизаконної діяльності використовували соціальні мережі, «електронні відображення» котрих у подальшому можуть бути використані як докази.

За матеріалами сайту новин Ізраїлю від 09.03.2020, близько 14:00 годин на площі Рабіна поліцейськими було заарештовано двох чоловіків віком близько 30 років, які керували планерами, за допомогою котрих на площі було скоєно незаконне розповсюдження наркотичних засобів. Об'яву про здійснення зазначеного акту було викладено паном К. у групі месенджеру «Telegram», адміністратором якого був останній [9].

За матеріалами статті, опублікованої 26.08.2020 на інформаційному ресурсі «Секрет фирмы», судом Об'єднаних Арабських Еміратів (ОАЕ) було засуджено до 10 років позбавлення волі Артема Маслова за вчинення наруги над національною валютою ОАЕ «дирхам». Як відомо, останній був заарештований представниками влади ОАЕ у серпні 2020 року на півроку. Підставою і доказом у кримінальному провадженні слугувало оприлюднене Масловим відео у соціальній мережі «Інстаграм», у матеріалах якого останній тримав грошові знаки ОАЕ між двома пальцями ніг та їх рахував, водночас показуючи глядачам непристойні жести руками [10]. Як відомо, ст. 141 Федерального декрету-закону ОАЕ № 14 від 2018 року «Про Центральний банк та регулювання фінансових установ і діяльності» передбачає, що будь-яка особа, яка публічно навмисно спотворює, пошкоджує або рве державні грошові знаки ОАЕ, заслуговує покарання у вигляді штрафу у розмірі 1000 дирхамів або 10 подвійних сум знівечених, пошкоджених або первинних грошей залежно від того, яка сума більше. Також окремими законодавчими положеннями ОАЕ передбачено кримінальну відповідальність за наругу над державними символами ОАЕ (ст. 176 Федерального кримінального кодексу), за що передбачено покарання у вигляді позбавлення волі на термін від 10 до 25 років, а також штраф [11].

Із матеріалів, опублікованих інформаційним порталом «Compass.com» 24.01.2020 року, громадянина Російської Федерації Сергія Косенко працівниками регіонального відділення Балі Міністерства закону та прав людини було піддано адміністративному стягненню відповідно до положень п.п. 1, 2 ст. 75 Закону Балі № 6 від 2011 року «Про еміграцію». Доказом і підставою застосування щодо останнього депортації відзначилися відеоматеріали соціальної мережі «Інстаграм», у котрих порушник виконував небезпечний трюк, занурившись у море під час їзди на мотоциклі. Як стало відомо, зазначена діяльність вважалася порушенням циркуляру Робочої групи з питань боротьби з Covid-19 № 02 від 2021 року щодо міжнародних протоколів охорони здоров'я під час пандемії коронавірусу 2019 (Covid-19) [12].

Таким чином, за наданими вище відомостями можна стверджувати, що «електронні відображення» у соціальних мережах вже нині відіграють доказове значення у притягненні до відповідальності.

Через це не менш значущими, на нашу думку, слід відзначити проблеми із підроблення інформаційних даних соціальних мереж та інформаційну тотожність вилучених копій оригіналам, розміщеним у соціальних мережах, що зберігаються на носіях, на які установлення та/або подальше накладення арешту у кримінальному провадженні не представляється можливим.

Зокрема, проблеми із підробки «електронних відображень» соціальних мереж дослідив у своїй праці доктор М. Кнасмюллер. У роботі останнього можна побачити напрацювання із виявлених дефектів у діяльності деяких популярних соціальних мереж та інших засобів комунікації, які залишають слідову картину в «електронних відображеннях». Наприклад, «*маніпуляція SMS цілком можлива, найпростіший варіант – просто зробити вигляд, що певний відправник передав повідомлення. Якщо час надсилання не має значення, то відповідні Інтернет-платформи, такі як http://www.fakemysms.com, дозволяють надсилання, завдяки чому можна записати номер відправника. На дисплеї мобільного телефону виглядає так, ніби SMS дійсно надіслано із цього номера. Подальша обробка отриманого SMS також можлива шляхом маніпулювання SIM-карткою*» [13, с. 203] (підробка SMS повідомлень); «*навіть якщо одержувач не змінив електронну пошту, її можна підробити, оскільки адресу відправника електронної пошти можна просто вказати. Для цього також існують такі сервіси, як http://www.fakemyemail.com, які можна використовувати аналогічно вже згадуваному http://www.fakemysms.com*» [13, с. 204] (підробка повідомлень електронної пошти); «*з іншого боку, резервне копіювання може бути зроблено лише за допомогою файлів, наприклад, за допомогою функції «завантажити копію своїх даних Facebook або скриншотів». Насправді обома можна маніпулювати за бажанням. Тому, безумовно, розумно, якщо таке збереження доказів проводити незалежною третьою стороною*» (підробка повідомлень соцмережі Facebook) [13, с. 205]. «*Як і SMS, центрального сховища немає, але надіслані та*

отримані повідомлення зберігаються на смартфоні у своєрідному локальному сейфі (файл mgstore.db). Цей файл, по суті, служить базою даних, яка насправді повинна бути прихована від користувача. Однак ключі шифрування доступні в Інтернеті» [13, с. 8]. «*Виходячи із цього, також доступні різні програми, які декодують уміст цієї бази даних навіть безкоштовно*» [13, с. 206] (підробка повідомлень месенджеру WhatsApp).

Відповідно до КПК України та методичних рекомендацій існує процедура зняття інформації із електронних інформаційних систем (метод рекомендації). Однак є питання про залучення як доказу не оригіналу документу, а копії. Вилучити з Інтернету можна перероблену копію (стиснуту у розмірі) фотографії чи відеозапису, що не можна вважати, відповідно до норм КПК, оригіналом електронного документу. Сам оригінал знаходиться у так званому «хмарному середовищі», а його носій може бути розташованим на території не лише України, але інших частин світу. Через це виникає ще не менш важлива проблема, яка полягає у визначенні вимог до спеціалістів, зобов'язаних брати участь у слідчих (розшукових) діях і негласних слідчих (розшукових) діях, пов'язаних зі зняттям інформації із інформаційних і транспортних телекомунікаційних мереж. Такими вимогами є: наявність програмних навичок відповідного кваліфікаційно-освітнього рівня; мати при собі та користуватися програмним забезпеченням і технічними засобами, які за своїми функціями повинні здійснювати вилучення та фіксацію «електронних відображень» та у разі нагальної необхідності їх консультативне дослідження. Окрім того, на нашу думку, слід законодавчо закріпити вимоги до технічних характеристик та особливостей пристроїв, із якими особа має право бути допущеною до здійснення свої процесуальної діяльності у кримінальному провадженні.

У статті 71 (Спеціаліст) КПК не передбачено вилучення інформації в електронному вигляді, але у главі 21 КПК у ст. 264 законодавець нормою ч. 2 ст. 264 чітко пояснив, що «*не потребує дозволу слідчого судді здобуття відомостей із електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний із подоланням системи логічного захисту*» [1]. Тобто можна зрозуміти, що законодавець у такому випадку передбачив залучення спеціаліста до відповідних слідчих (розшукових) дій на розсуд слідчого, дізнавача. На нашу думку, це недопустимо, оскільки існує вірогідність втрати слідів у разі, якщо слідчий не володіє навичками із використання тих чи інших програм та/або фіксації «електронних відображень» із соціальних мереж.

Висновки

Отже, все ще існують прогалини у праві під час збирання доказів, зокрема під час вилучення доказів в електронному вигляді. У законодавстві відсутні поняття «електронне відображення», «електронні сліди», існує лише «електронний документ», який повністю не може охарактеризувати поняття і природу електронних відображень. Використання джерела доказів «електронних відображень», зокрема відомостей із соціальних мереж, нині є поширеною практикою. Недосконалість останніх притаманна в тій частині, що відомості із соціальних мереж можна підробити, змінити, замінити, відкоригувати, оскільки останнім також притаманні мінливі процеси матеріального світу, але здійснення подібних маніпулювань вимагає додаткових знань та навичок від зацікавлених осіб. Через це виникає необхідність із залучення спеціаліста, особливо у тих випадках, коли здійснення слідчих (розшукових) дій потребує негайних рішень та існує ризик знищення слідів злочину. Тому нагальною постає необхідність законодавчого закріплення до норм КПК України положень щодо впровадження джерел доказів «електронних відображень». Водночас слід визначити положення щодо вимог до спеціаліста, який залучається під час здійснення вилучення та/або копіювання «електронних зображень», зокрема доповнити ст. 71 КПК України «Спеціаліст» положенням ч. 2-1: «*спеціаліст залучається у разі відсутності практичних навичок у слідчого, дізнавача із здобуття відомостей із електронних інформаційних систем або її частини для виявлення та фіксації «електронних відображень» за допомогою використання програмного забезпечення, соціальних мереж і технічних приладів-носіїв інформації*»; ч. 2-2: «*спеціаліст, який залучається слідчим, дізнавачем під час здобуття відомостей із електронних інформаційних систем або її частин, має володіти програмними навичками відповідного*

кваліфікаційно-освітнього рівня; мати при собі та користуватися програмним забезпеченням і технічними засобами, які за своїми функціями повинні здійснювати вилучення і фіксацію «електронних відображень» та у разі нагальної необхідності – їхнє консультативне дослідження».

Список використаних джерел:

1. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651-VI. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 01.10.2021).

2. 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. URL: http://elar.naiau.kiev.ua/jspui/handle/123456789/2392 (дата звернення: 01.10.2021).

3. Коваленко А.В. Електронні докази в кримінальному провадженні: сучасний стан та перспективи використання. *Вісник ЛДУВС ім. Е.О. Дідоренка.* 2018. Вип. 4 (84). С. 237–245.

4. Авдєєва Г. К., Стороженко С. В. Електронні сліди: поняття та види. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* 2017. Вип. № 1 (77) С. 168–175. URL : http://dspace.nulau.edu.ua/bitstream/123456789/13283/1/Avdeeva_168-175.pdf (дата звернення: 01.10.2021).

5. Вехов Б. В., Смагоринский Б. П., Ковалев С. А. Электронные следы в системе криминалистики. *Судебная экспертиза.: научно-практический журнал.* 2016. Вып. 2 (46). С. 10–19.

6. Крицька І. О. Речові докази та цифрова інформація: поняття та співвідношення. *Часопис Київського університету права.* 2016. Вип. № 1. С. 301–304. URL: http://dspace.nlu.edu.ua/bitstream/123456789/12330/1/Krucka_301_305.pdf (дата звернення: 01.10.2021).

7. Турчин А.В. Класифікація соціальних мереж. Матеріали Всеукраїнської науково-практичної конференції. С. 206. URL : https://core.ac.uk/download/pdf/84825408.pdf (дата звернення: 01.10.2021).

8. Що таке Даркнет і чи варто його боятися. URL: https://www.radiosvoboda.org/a/29166176.html (дата звернення: 01.10.2021).

9. Дождь канабиса סיבאנק לש משג :תויקש תע מסה תחנ ותלב לת ביבא URL: https://www.mako.co.il/news-israel/2020_q3/Article-de6ba3b74e35471026.htm (дата звернення: 01.10.2021).

10. Российского блогера-афериста посадили на 10 лет за надругательство над валютой URL: https://secretmag.ru/criminal/rossiiskogo-blogera-aferista-posadili-na-10-let-za-nadrugatelstvo-nad-valyutoi-26-08-2021.htm (дата звернення: 01.10.2021).

11. Дирхам الإمارات دولة الوطنية العملة. URL: https://u.ae/ar-ae/information-and-services/finance-and-investment/the-uae-national-currency (дата звернення: 01.10.2021).

12. Sergei Kosenko, Turis Rusia yang Ceburkan Diri ke Laut bersama Motor Dideportasi dari Indonesia. URL: https://regional.kompas.com/read/2021/01/24/13540831/sergei-kosenko-turis-rusia-yang-ceburkan-diri-ke-laut-bersama-motor? page=all (дата звернення: 01.10.2021).

13. Dr. Knasmüller M. Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informations- und Kommunikationstechnologie; Abteilungsleiter Entwicklung, BMD Systemhaus GmbH, Steyr. URL: https://widab.gerichts-sv.at/website2016/wp-content/uploads/2016/08/Sach-2015-203-206-Knasmueller.pdf (дата звернення: 01.10.2021).